УДК 336.717

Шубина Анна Юрьевна,
студент,
кафедра финансов, денежного обращения и кредита,
Институт экономики и управления,
ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»
г. Екатеринбург, Российская Федерация

Долгих Юлия Александровна,
кандидат экономических наук, доцент,
кафедра финансов, денежного обращения и кредита,
Институт экономики и управления,
ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»
г. Екатеринбург, Российская Федерация

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В БАНКОВСКОМ СЕКТОРЕ: РИСКИ И ВОЗМОЖНОСТИ

Аннотация:
В статье рассматриваются риски и возможности эскалации информационных технологий в банковском секторе. Проанализирована динамика объемов несанкционированных операций в России, динамика количества субъектов с признаками нелегальной деятельности за период 2016-2020 гг. Сформулированы ключевые задачи по борьбе с незаконными методами хищения и отмывания денежных средств.

Ключевые слова:
финансовые технологии, информационные технологии, банковский сектор, киберриски.

В последние годы наблюдается тенденция все большего повышения требований экономических субъектов, как физических, так и юридических лиц, к скорости, доступности и комфорту получения доступа к различным сервисам по предоставлению финансовых услуг. Это способствует активному внедрению современных информационных технологий, дает новые возможности как потребителям финансовых услуг, так и тем, кто их предоставляет. Происходит глобальный процесс цифровизации экономики, внедрения финансовых технологий, однако этим пользуются нелегальные участники рынка, что приводит к росту интернет-проектов в сфере незаконного оборота денежных средств. Вследствие этого генерируются так называемые киберриски. К данной категории относятся:

- риски незаконного изъятия средств со счетов клиентов в финансовых организациях;
- риски хищения средств самих финансовых организаций;
- риски снижения надежности услуг, предоставляемых финансовыми организациями;
- риски кибератак, направленных на программное обеспечение финансовых организаций и их клиентов.

Финансовая инфраструктура довольно быстро меняется под влиянием стремительного развития цифровых технологий и отражает те изменения, которые претерпевает наша жизнь. Кредитные и дебетовые карты, электронные кошельки, интернет-переводы, бесконтактные платежи – этими и другими продуктами и сервисами пользуются сотни миллионов клиентов, для которых это стало уже не новинками, а обыденностью. Поэтому вполне логично, что

развитие финансовых инноваций неизбежно влияет и на активизацию мошеннических операций [1].

В рамках «Основных направлений развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов» в числе первоочередных задач закреплено совершенствование нормативно-правового регулирования сфер деятельности, связанных с использованием современных электронных технологий [2]. Ее реализация позволит минимизировать киберриски, гармонизировав это с обеспечением доступности финансовых услуг, эффективной защитой прав потребителей и устойчивым ростом экономики.

На рисунке 1 представлена динамика объемов несанкционированных операций в России за период 2016-2020 гг.

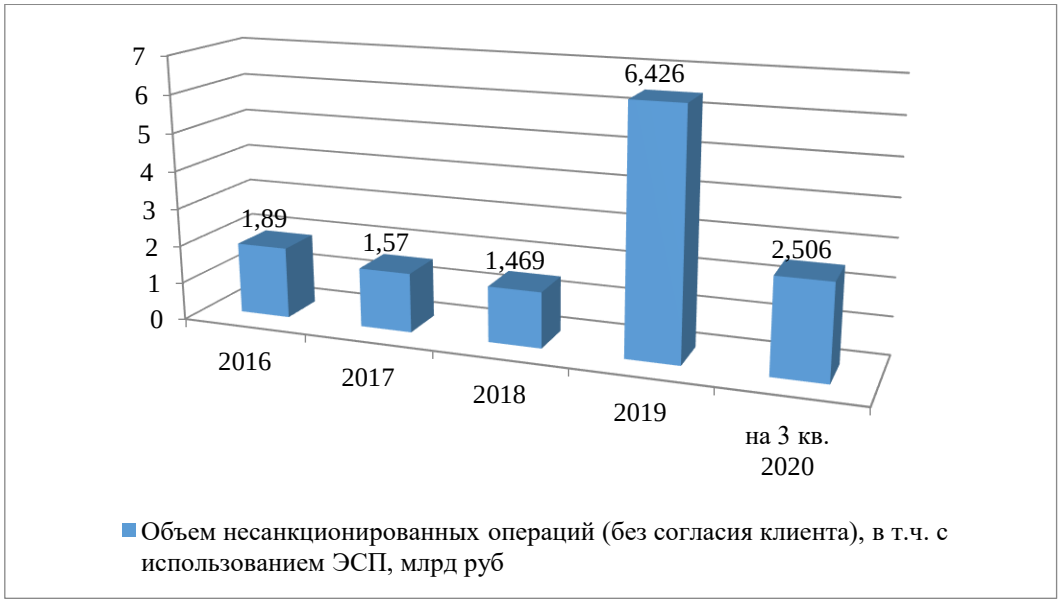

Рисунок 1 – Динамика объемов несанкционированных операций в России за 2016-2020 гг., млрд руб.[46]

Как видно из диаграммы, за период 2019-2020 гг. произошел резкий рост объема незаконных финансовых операций. Это обусловлено такими тенденциями как массовый переход на дистанционное банковское обслуживание, распространение фишинга, совершенствование методов внедрения специализированных вредоносных программ. Значительный рост в 2019 году, в частности, объясняется внедрением такой разновидности мошенничества как «социальная инженерия», за 2019 год было совершено порядка 572 тысячи хакерских атак.

Основная тенденция 2020 года – рост востребованности дистанционных услуг, как следствие массовый переход нелегальных услуг в онлайн [3]. Ограничения, связанные с пандемией, способствовали распространению мошенничества, в том числе нелегальных финансовых интернет-проектов.

Далее на рисунке 2 представлена динамика количества субъектов с признаками нелегальной деятельности за период 2016-2020 гг. В 2020 году Банком России было выявлено около 1,5 тысячи субъектов, которые осуществляют нелегальную деятельность или имеют признаки нелегальной деятельности, в том числе признаки финансовых пирамид. Более половины нелегальных участников финансового рынка осуществляли незаконное кредитование, так называемые нелегальные или черные кредиторы (53%). Выделяются и две не менее крупные группы в среде противозаконной деятельности – это нелегальные форекс-дилеры (занимают 25,5% в общем объеме незаконных формирований) и финансовые пирамиды (14,3%). В 2020 году прослеживается тенденция к снижению выявленных черных кредиторов, связывается это,

[46] Составлено авторами на основании источника [3]

в первую очередь, с пандемией коронавирусной инфекции. Нелегальные кредиторы, как правило, предпочитают действовать в офлайн-среде, производя оборот средств без документов, на руки, либо по документам, оформленным с нарушением законодательных норм.

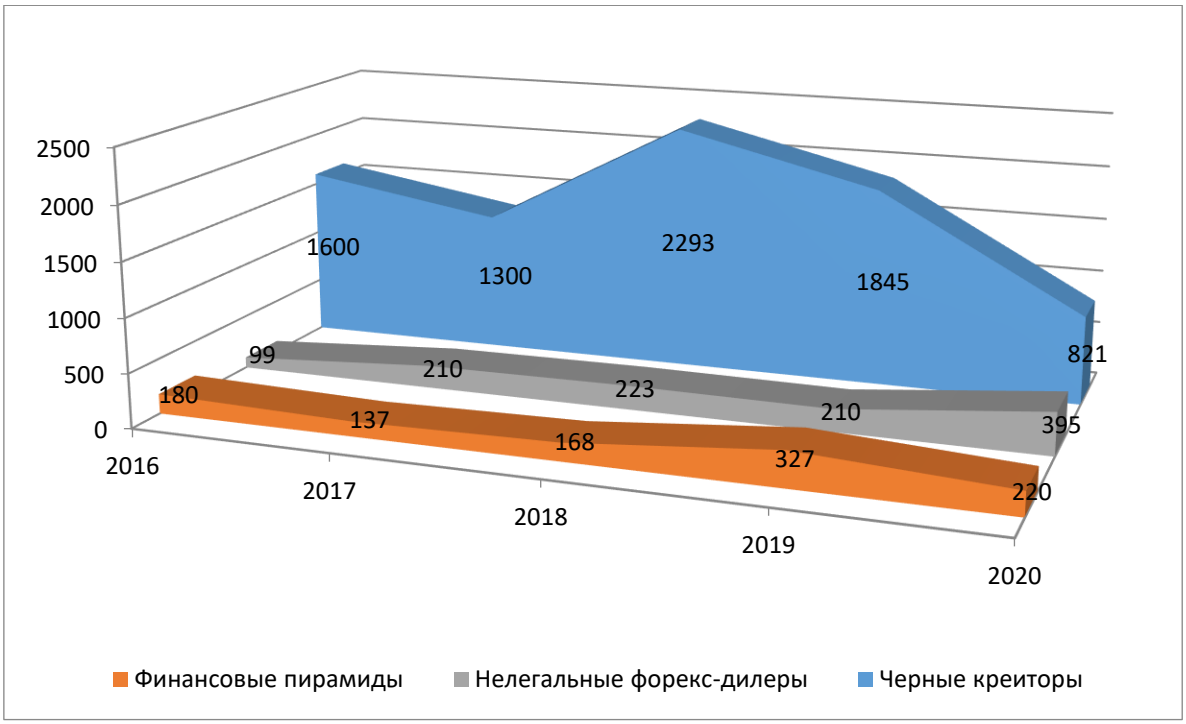

Рисунок 2 – Динамика количества субъектов с признаками нелегальной деятельности за 2016-2020 гг., ед.[47]

В условиях пандемии COVID-19 отмечается рост мобильного мошенничества, совершаемого против граждан. В режиме самоизоляции люди больше времени проводят за мобильными телефонами (за покупками, за финансовыми услугами, в социальных сетях и т.д.). Новая коронавирусная инфекция не только изменила образ жизни населения, но и перенаправила работу злоумышленников. Одной из популярных уловок во время пандемии было использование таких тем как компенсация, государственные пособия и государственная поддержка. Киберпреступники вымогали у граждан личные данные и денежные средства под предлогом оказания или содействия в получении мер государственной поддержки. Также активно появлялись сайты организаций без соответствующей лицензии, предлагающие гражданам «простые деньги» на финансовом рынке. Наиболее часто встречающимися направлениями фишинговых сайтов в этот период являлись интернет-магазины (48%) и социальные службы (43%). Злоумышленники быстро сориентировались, как в своей деятельности использовать введенный режим ограничений и меры поддержки, оказываемой государством гражданам.

Можно выделить следующие основные каналы вывода денежных средств:

1. Вывод через операторов электронных денежных средств системы;

2. Вывод на операторов сотовой связи. Таким образом, мошенники либо переводят средства на кредит мобильного телефона, а затем выводят средства оператору ЭДС, либо предоставляют жертве номер виртуальной карты, которая привязана к учетной записи мобильного телефона злоумышленника;

3. Переводы с карты на карту. Используя сервисы денежных переводов, мошенники, ранее получившие информацию о карте жертвы, переводят средства на заранее подготовленные карты;

[47] Составлено авторами на основании источника [3]

4. Вывод на обменники (криптообменники). Один из самых популярных способов вывода украденных активов – это вывод на обменники, в том числе на криптообменники. Так называемые обменники – это сервисы, позволяющие покупать или продавать валюты (криптовалюты), в которых сервис выступает в качестве покупателя или продавца. Проследить цепочку привлечения средств практически невозможно, так как переводы осуществляются с разных счетов, открытых в разных организациях финансово-кредитного сектора.

Таким образом, развитие цифровой среды неразрывно связано с использованием прорывных и перспективных цифровых технологий при одновременном совершенствовании новых видов и методов осуществления незаконных операций. Ключевыми задачами по борьбе с незаконными методами хищения и отмывания денежных средств являются:

– выявление и оперативное прекращение работы сайтов с предоставлением незаконных финансовых услуг;

– сокращение срока «жизни» нелегальных организаций и вывод их с рынка;

– сопровождение развития цифровых финансовых услуг в контексте повышения удобства и усиления защиты прав потребителей финансовых услуг;

– обеспечение киберустойчивости (в первую очередь, сюда следует отнести готовность субъектов финансово-кредитной сферы гарантировать финансовую стабильность и операционную надежность, контроль показателей риска реализации информационных угроз; контроль уровня банковских и финансовых операций, совершенных без согласия клиентов; мониторинг, оперативное реагирование и предотвращение компьютерных атак на финансово-кредитные организации);

– обеспечение необходимого уровня информационной безопасности;

– противодействие распространению информации в финансово-кредитной сфере о деятельности нелегальных участников в этой сфере и об их услугах.

Особое внимание к инновациям объясняется несколькими причинами. Во-первых, это широкое распространение новых финансовых технологий среди населения, которые перестали занимать узкую нишу и стали поистине массовыми. Во-вторых, интересы самого государства: во многих странах вытеснение наличных денег и уход от теневой экономики стали первоочередными задачами, и регуляторы понимают, что их невозможно решить без новых информационных технологий. Реализация обозначенных авторами мер будет способствовать развитию информационных технологий в финансово-кредитном секторе, нивелируя при этом объективно возникающие киберриски.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Шуст П.М. Влияние финансовых технологий на практику борьбы с отмыванием денег и финансированием терроризма / П.М. Шуст, В.Л. Достов // Финансовые исследования. – 2018. – № 4 (61). – С. 40-46.
2. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов [Электронный ресурс]. – Режим доступа: https://cbr.ru/Content/Document/File/83253/onrib_2021.pdf
3. Противодействие нелегальной деятельности на финансовом рынке. Аналитические материалы Банка России [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/inside/analitics/

Shubina Anna Yurievna,
Student,
Department of Finance, money circulation and credit,
Institute of Economics and Management,
Federal State Autonomous Educational Institution of Higher Education “Ural Federal University named after the first President of Russia B.N. Yeltsin"
Yekaterinburg, Russian Federation

Dolgikh Yulia Alexandrovna,
Assistant professor,
Department of Finance, money circulation and credit,
Institute of Economics and Management,
Federal State Autonomous Educational Institution of Higher Education “Ural Federal University named after the first President of Russia B.N. Yeltsin"
Yekaterinburg, Russian Federation

INFORMATION TECHNOLOGIES IN THE BANKING SECTOR: RISKS AND OPPORTUNITIES

Abstract:
The article discusses the risks and opportunities of information technology escalation in the banking sector. The dynamics of the volume of unauthorized operations in Russia, the dynamics of the number of entities with signs of illegal activity for the period 2016-2020 are analyzed. The key tasks for combating illegal methods of embezzlement and money laundering are formulated.

Keywords:
financial technologies, information technologies, banking sector, cyber risks.