(cc) BY


***Калинина Луиза Владимировна***
бакалавр экон. наук, магистрант
ФГБОУ ВО «Кубанский государственный университет»
г. Краснодар, Краснодарский край

# ПРОБЛЕМЫ ВНЕДРЕНИЯ ИННОВАЦИЙ В БАНКОВСКУЮ СРЕДУ И ОСНОВНЫЕ НАПРАВЛЕНИЯ ИХ РЕШЕНИЯ

***Аннотация****: статья посвящена проблемам, с которыми сталкиваются банки в процессе внедрения инноваций в банковскую среду. Автором также рассматриваются основные направления решения данных проблем.*

***Ключевые слова****: банковские инновации, цифровизация экономики, кибербезопасность.*

Несмотря на то, что цифровая трансформация экономики, включая кредитно-денежную и финансовую систему, дает свои преимущества, неизбежно несет за собой ряд рисков. С развитием цифровых технологий возникают риски, связанные с ростом киберугроз, требующих оперативного и своевременного мониторинга, обнаружения, оценки и разработки соответствующих мер по их предотвращению либо минимизации их возможных последствий. В качестве мирового тренда отмечается увеличение финансовых потерь от кибератак, нарушение целостности и непрерывности функционирования в том числе финансового рынка (17% всего объема кибератак приходится на финансовый сектор). К ключевым рискам от киберугроз можно отнести финансовые потери клиентов, организаций, нарушение операционной надежности.

Обеспечение информационной безопасности на финансовом рынке требует формирования механизма правового регулирования, включающего в том числе полномочия Банка России по организации такого обеспечения и установлению регуляторных требований к участникам финансового рынка. В соответствии с Доктриной информационной безопасности, которая утверждена Указом президента от 05.12.2016 №646 Банк России определен в качестве органа, составляю-


Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

щего организационную основу системы обеспечения информационной безопасности Российской Федерации, а организации кредитно-финансовой сферы – в качестве участников системы. К регулятивному ведению Банка России относятся переводы денежных средств, ведение базы данных о несанкционированных переводах, информационный обмен с Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка (далее – ФинЦЕРТ). Угроза кибератак действительно актуальна на сегодняшний день. В период с 2015 по 2018 год Центральным Банком в среднем было зафиксированно 1,21 млн ед. несанкционированных операций с использованием платежных карт. В 2018 году наблюдается прирост по сравнению с 2017 в 0,42 млн ед. (рис.1). Данный факт говорит о том, что с возрастанием роли информационной оснащенности финансовых операций возникает и опасность в виде несанкционированных проникновений в финансовую среду электронного оборота.

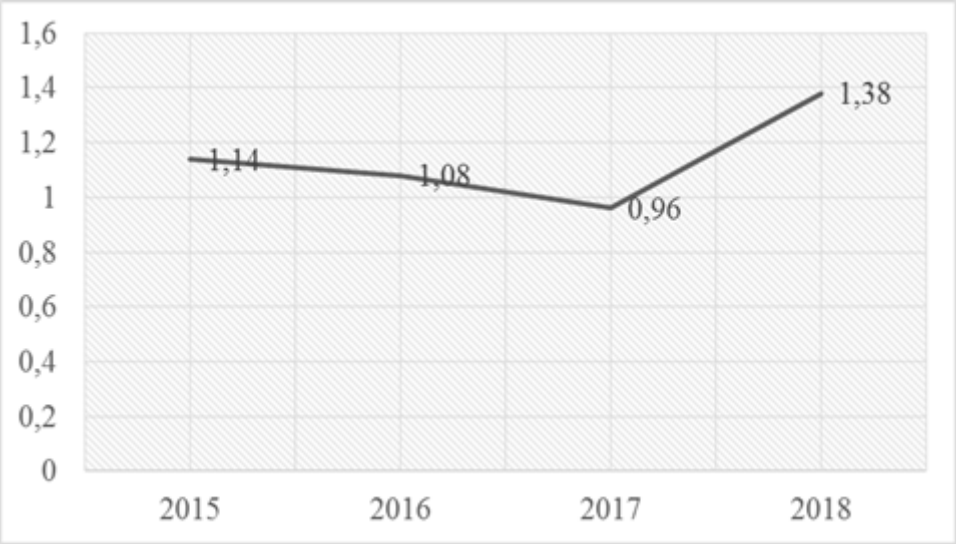


Рис. 1. Объем несанкционированных операций
с использованием платежных карт (млн ед.)

Каждый год Центральный Банк Российской Федерации публикует отчет о кибербезопасности. Исходя из отчета о кибербезопасности, можно подчеркнуть, что за прошедший 2019 год ФинЦЕРТ отправил в соответствующие структуры информацию о 4936 телефонных номерах, задействованных в мошеннических СМС-рассылках, звонках, заражениях вредоносным программным обеспечением


Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

и т. д., для блокировки данных номеров. С сентября прошлого года ФинЦЕРТ инициировал разделегирование 9778 фишинговых доменов (около 2/3 таких доменов было зарегистрировано за рубежом). При этом минимальное время разделегирования сократилось с 24 до 3 часов. Снятие доменов с делегирования осуществляется в режиме 24/7/365. В 2019 году по инициативе Банка России участники финансового рынка стали отслеживать и фиксировать признаки операций, совершенных без согласия клиента. На основании этих признаков принимаются меры, препятствующие несанкционированному списанию средств. В отчете также сообщается, что за последние полгода (1 января – 30 июня 2019 года) обнаружено 12 903 предложения о покупке или продаже различных баз данных. При этом лишь 12% относились к базам данных кредитно-финансовых организаций. В настоящий момент участниками информационного обмена с ФинЦЕРТ являются 826 организаций, в том числе все банки, работающие на территории России. С октября 2018 года от них получено более 300 тыс. сообщений об инцидентах.

Обеспечение безопасности обработки данных с использованием цифровых технологий является первоочередной задачей, решение которой требует незамедлительного реагирования. Среди мер, нацеленных на сокращение риска кибератак можно выделить: обеспечение целостности и подлинности информации на каждом технологическом участке ее обработки; протоколирование действий на технологических участках, использование средств электронной подписи (криптографии), реализация принципа «двойного контроля» при обработке защищаемой информации, многофакторная аутентификация клиентов, реализация механизмов получения дополнительного подтверждения клиентами финансовых операций.

Наряду с проблемой обеспечения кибербезопасности возникает проблема сложности внедрения банковских инноваций в общественную повседневную жизнь. Безусловно, цифровизация банковских процессов способна коренным образом изменить систему банковских операций, упрощая ее и сокращая временные издержки. Между тем, инновации банковского сектора все еще остаются



Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

труднодоступными для населения прежде всего в части их сложности. По статистики на первое полугодие 2020 года 55% населения нашей страны смогли перейти на дистанционное взаимодействие с банками посредством интернет-банкинга и мобильного банка, 34% из которых полностью перешли на удаленные операции. Видимой проблемой остается и внедрение банковских инноваций среди отдельных групп населения. По статистике люди в возрастной категории до 40 лет более активно пользуются онлайн услугами банка, их доля в общей массе пользователей составляет 73% и только 21% пользователей относится к категории 41–55 лет. Остальные 6% – люди пенсионного возраста (рис.2).

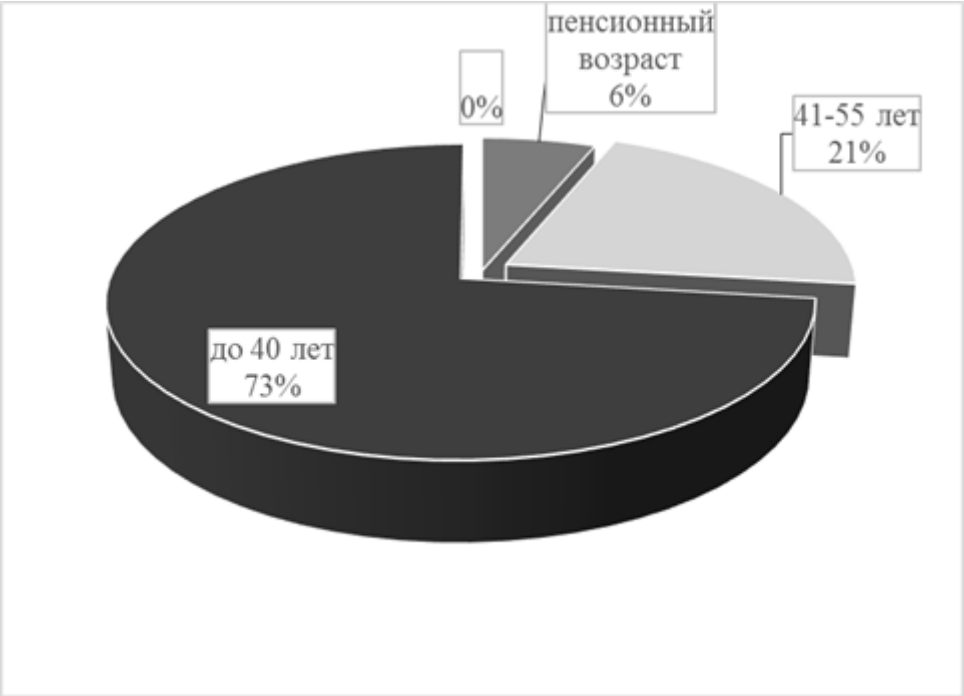


Рис. 2. Доля населения, использующая интернет-услуги банка (по возрастному признаку)

Приведенная статистика указывает на необходимость разработки централизованной системы клиентского обучения и адаптации населения к онлайн сервисам. Альтернативой выхода из сложившейся обстановки может быть упрощение интернет-банкинга и его интерфейса.

Внедрение инноваций в розничную сферу банковской деятельности имеет как явные преимущества в виде упрощения клиентских операций, так и несомненные недостатки, которые выражаются в повышенных рисках, возникающих


Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

в условиях развивающейся киберпреступности, а также в невозможности полноценного и всеобъемлющего внедрения данных инноваций в общественную среду в силу их сложности для восприятия и пользования. Существующие проблемы требуют незамедлительного решения. На наш взгляд, основным направлениям реализации политики безопасности банковских инноваций может стать программа рискоустойчивости банков, а система по упрощению мобильного интерфейса способна навсегда решить вопрос об их повсеместном пользовании.

***Список литературы***

1. Указ Президента РФ от 5 декабря 2016 г. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС Гарант.

2. Третьякова С.Н. Количественная характеристика денег: взаимосвязь денежных и кредитных агрегатов / С.Н. Третьякова, М.М. Третьяков // Вестник Тихоокеанского государственного университета – 2014. – №3 (34). – С. 147–156.

3. Третьякова С.Н. Некоторые вопросы повышения эффективности внутреннего аудита в коммерческом банке // Власть и управление на Востоке России – 2010. – №3 (52). – С. 37–41.

4. Статистические данные Центрального Банка России [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/ (дата обращения: 20.05.2020).

5. Данные о пользователях онлайн-сервисов банка [Электронный ресурс]. – Режим доступа: https://www.banki.ru/ (дата обращения: 01.06.2020).



Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)