ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ИНСТИТУТ ЭКОНОМИКИ И УПРАВЛЕНИЯ

КАФЕДРА ФИНАНСОВ, ИНВЕСТИЦИЙ И ИННОВАЦИЙ

НАПРАВЛЕНИЯ РАЗВИТИЯ БАНКОВСКИХ ЭЛЕКТРОННЫХ УСЛУГ И СПОСОБЫ ОБЕСПЕЧЕНИЯ ИХ БЕЗОПАСНОСТИ

Магистерская диссертация
обучающегося по направлению подготовки 38.04.08 Финансы и кредит
магистерская программа Банки и банковская деятельность
заочной формы обучения, группы 09001684
Битюковой Анастасии Федоровны

Научный руководитель
к.э.н, доцент кафедры
финансов, инвестиций и
инноваций
Быканова Н.И.

Рецензент
заместитель директора
Белгородского
регионального филиала
АО «Россельхозбанк» по
розничному бизнесу
Мартынюк Н.В.

БЕЛГОРОД 2019

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования обусловлена важным социально-экономическим значением электронных услуг для банковской системы и общества в целом, а также необходимостью обеспечения информационной безопасности банков в сфере электронного обслуживания.

В настоящее время развитие банковского сервиса на потребительском рынке сопровождается внедрением инновационных банковских и информационных технологий, а также связано с выбором финансовых инструментов, повышающих востребованность электронных банковских услуг. Достижение поступательного увеличения клиентопотока при минимальных значениях операционных издержек на обслуживание каждой операции требует создания привлекательной для населения и простой в использовании модели электронного банкинга.

При дальнейшем развитии отдельных систем электронного банковского обслуживания возможны проблемы их эксплуатации, связанные с неспособностью системы корректно работать в условиях резкого роста клиентской базы. Проблемой развития электронных банковских услуг в России является недостаточно безопасное обеспечение состояния системы дистанционного банковского обслуживания. Поскольку защита от мошеннических операций относится к числу основных социальных ценностей электронного банковского обслуживания, то ее недостаток или отсутствие не могут быть компенсированы никакими другими ценностями и благами. Если будет отсутствовать должная защита информационных платформ банков, то это будет грозить списанием денежных средств со счетов клиентов. Таким образом, это подорвет репутацию банка и объектов национальной платежной инфраструктуры. В связи с этим необходимо отметить, что от постоянного контроля и мониторинга над деятельностью банка на наличие возможных угроз воздействия извне на информационную

систему зависит эффективность его работы и количество как фактических, так потенциальных клиентов, а также на эффективность банковского сектора в целом.

Степень научной разработанности проблемы обуславливается тем, что за последнее время отечественными авторами было написано множество работ, посвященных видам и технологиям создания новых банковских продуктов в сфере электронных услуг. Следует отметить следующих авторов, внесших весомый вклад в развитие теоретической базы современного банковского обслуживания: Г.Н. Белоглазову, Д.В. Трофимова, К.Э. Пустовалову, О. И. Лаврушина и других.

Целью магистерской диссертации является разработка направлений развития банковских электронных услуг и способов обеспечения их безопасности на основе анализа современной практики функционирования рынка электронных банковских услуг в России.

Для достижения данной цели определены следующие **задачи**:

– изучить и систематизировать теоретические основы электронного банковского обслуживания в коммерческом банке;

– охарактеризовать современное состояние рынка банковских электронных услуг в России;

– определить основные угрозы безопасности при осуществлении операций посредством системы дистанционного банковского обслуживания;

– выявить и обосновать перспективы развития электронных банковских услуг в коммерческих банках;

– разработать мероприятия по обеспечению безопасности банковских электронных услуг в условиях цифровизации экономики.

Объектом магистерской диссертации является рынок банковских электронных услуг.

Предметом исследования является система организации и реализации банковских электронных услуг в отечественных коммерческих банках.

Теоретической основой работы послужили учебники, учебные пособия, учебно-методические материалы, а также теории и концепции, сформированные в трудах отечественных экономистов в области рассматриваемой темы, в числе которых работы: Т.М. Гадисовой, Н.Г. Сосниной, Н.Н. Мартыненко, Е. А. Черкашиной, С. В. Ануреева и других.

Информационной базой работы послужили законодательные и нормативные акты, регулирующие банковскую деятельность в Российской Федерации, статистические данные, опубликованные Банком России, данные информационных и рейтинговых агентств, статьи в периодических изданиях по исследуемой тематике.

Методологическая база работы включает следующие методы исследования: наблюдение и сбор фактов – целенаправленное и преднамеренное восприятие процессов и явлений без явного вмешательства в их движение, которое подчинено задачам научного исследования; анализ – метод научного познания, который предполагает не только установление отношений между частями, но и их фиксацию; индукцию – метод научного мышления от частного к общему; дедукцию – метод научного мышления от общего к частному; графический метод - возможность наглядно изобразить конкретные экономические зависимости; сравнение – метод, который определяет различие или сходство процессов и явлений.

Научная новизна работы заключается в отражении направлений развития электронных банковских услуг и разработке практических рекомендаций по обеспечению их безопасности.

Научная новизна подтверждается следующими результатами:

1) определена сущность и роль электронных банковских услуг в коммерческом банке;

2) выявлены проблемы развития дистанционного банковского обслуживания в России;

3) проведен анализ безопасности электронных банковских услуг в отечественном банковском секторе;

4) сформулированы и обоснованы основные перспективы развития электронных банковских услуг в инновационном развитии отечественного банковского сектора.

Практическая значимость работы состоит в том, что основные теоретические положения и выводы доведены до уровня конкретных предложений, которые могут использоваться для развития электронного банковского обслуживания клиентов в коммерческом банке.

Апробация результатов работы. Результаты исследования докладывались на VII Международной научно-практической конференции «Наука и инновации в XXI веке: актуальные вопросы, открытия и достижения» (Пенза, 2017).

Публикации. Основные положения и результаты исследования изложены в трех печатных работах общим объемом 1.2 п. л. в журналах «Современная экономика: проблемы и решения», «Экономика и предпринимательство» (2 – РИНЦ, 2- ВАК).

Структура магистерской диссертации определена поставленной целью и последовательностью решения сформулированных задач. Диссертация состоит из введения, в котором обоснована актуальность выбранной темы, сформулированы цели и задачи исследования; трех логически взаимосвязанных глав, раскрывающих обусловленные аспекты исследуемой темы; заключения, где представлены обобщающие выводы по проведенному исследованию; списка литературы, приложений. Работа изложена на 101 странице, содержит 5 таблиц, 18 рисунков и 3 приложения, при подготовке работы была использована информация из 65 источников.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ СТАНОВЛЕНИЯ ЭЛЕКТРОННЫХ БАНКОВСКИХ УСЛУГ

1.1.Сущность и роль электронных банковских услуг в коммерческом банке

В настоящее время в российском банковском законодательстве, также как и в научной литературе по банковскому бизнесу нет четкой трактовки понятия «электронная банковская услуга». Несмотря на то, что с каждым годом происходит увеличение рынка банковских услуг: появляются новые виды услуг, внедряются новые технологии, готовятся поправки в законодательство. Главная причина этому состоит в том, что действия, которые можно назвать услугами, многочисленны и разнообразны, также как и объекты, на которые направлены эти действия. [37, с. 26]

Итак, по мнению Черненко В. А. электронные банковские услуги – услуги, оказываемые банковскими организациями с использованием электронных средств.

Н. Н. Мартыненко, О. М. Макарова, О. С. Рудакова и Н. В. Сергеева под банковскими электронными услугами понимают новый технологический способ производства банковских продуктов, удовлетворяющий потребности клиентов с помощью современных информационных технологий.

О. Н. Дьякова «электронные услуги» определяет как совокупность упорядоченных банковских операций, осуществляемых с помощью информационных телекоммуникационных технологий.

Р. Р. Гайзатуллин и З. Ф. Гараев в своих научных работах под электронными услугами понимают – услуги, предоставляемые с использованием компьютерных информационных систем и других технологических средств и предполагающие обмен документами посредством телефонной, электронной и иной связи, не требующей физического участия лиц, которые используют средства электронных услуг.

И. А. Резник дает свое определение термину «электронные услуги» - это использование технологии на основе передового опыта индустриально развитых стран в сфере широкого применения на практике заменителей наличных денег и платежных инструментов и средств, создания технологий и технических устройств для их автоматической обработки.

На основании вышеизложенных определений можно заключить, что электронные банковские услуги – это удаленные услуги, оказываемые банковскими организациями клиентам с помощью современных информационных технологий. [28, с. 54]

Возникновение и распространение информационных технологий влияет на развитие коммерческих банков, позволяет им дифференцированно работать с клиентами в зависимости от их предпочтений, сделать доступной банковскую услугу в любое время суток, уменьшить затраты, повысить качество обслуживания и тем самым усилить конкуренцию в банковской сфере. Все эти обстоятельства и отличают традиционную банковскую услугу, оказываемую непосредственно в отделении Банка от электронной банковской услуги. Основные отличия традиционного и дистанционного (удаленного) обслуживания можно увидеть в таблице 1.1.

Таким образом, отличием электронных банковских услуг от традиционных является технология удовлетворения потребностей клиента. Наряду с обладанием традиционными признаками банковских услуг им присущи определенные особенности. Это общедоступность, обезличенность, экстерриториальность, интерактивность обслуживания и множественность каналов доступа. [39, с. 69]

Таблица 1.1

Основные различия между традиционной и новой моделями банковского обслуживания

Отличительные признаки	Традиционная модель	Новая модель
1	2	3
Временные рамки осуществления обслуживания	Ограниченные.	Неограниченные. Возможность круглосуточного доступа.
Скорость обслуживания	Зависит от квалификации и опыта сотрудника банка.	Скорость обслуживания мгновенная.
Подход к обслуживанию	Гибкий, однако, ограничивается небольшой разновидностью каналов обслуживания.	Гибкий и осуществляется через любой удобный для клиента канал.
Стоимость обслуживания	Высокая, учитывая расходы банка на содержание персонала и отделений.	Низкая, зачастую услуги предоставляются бесплатно.
Масштабы обслуживания	Ограниченные разветвленностью филиальной сети и кадровым обеспечением.	Неограниченные, могут выходить за рамки географического расположения банковского учреждения.
Статус операциониста в процессе обслуживания	Функции операциониста выполняет сотрудник банка.	Функции операциониста выполняет клиент банка.
Порядок ознакомления с новыми услугами и акциями	Требует времени и затрат на рекламу.	Осуществляется оперативно, через SMS- и e-mail рассылку.
Расходная компонента функционирования системы обслуживания	Ключевыми являются статьи на содержание персонала и отделений.	Ключевыми являются статьи на приобретение и содержание серверов и на программный комплекс.

В настоящее время электронные банковские услуги отождествляют с банковскими инновациями - доведенными до клиентов и принятыми ими новые или кардинально измененные банковские продукты, новые банковские услуги и услуги более нового качественного уровня, предоставленные на основе использования современных инфокоммуникационных технологий, внедренные в банковский процесс организационные и информационные технологии, позволяющие банку напрямую или опосредованно получать экономический или социальный эффект. [20, с. 7]

Генезис банковских инноваций свидетельствует о том, что инновации обеспечивают банкам конкурентные преимущества и способствуют динамичному развитию через получение маркетингового эффекта, сокращения издержек, повышения прозрачности деятельности и качества обслуживания клиентов, расширение ассортимента продуктов.

Классификацию инновационных банковских продуктов по различным критериям можно будет увидеть в приложении 1. Из вышеназванного приложения в рамках предмета исследования необходимо выделить процессные (технологические) и продуктовые банковские инновации, поскольку данная классификация и лежит в основе понятия «банковская инновация» [20, с. 8].

Под технологической инновацией понимается использование в банковской деятельности современного технологического оборудования и информационных технологий в целях повышения эффективности и конкурентоспособности оказываемых услуг [44, с. 58].

В свою очередь продуктовая инновация подразумевают внедрение новых банковских продуктов, которые могут быть связаны как с новыми, так и с традиционными операциями, совершенствование существующих услуг, а также значительные улучшения в обеспечении услугами.

С экономической точки зрения систему банковских электронных услуг подразделяют на три уровня: [34, с. 52]

- розничные банковские электронные услуги;
- оптовые банковские электронные услуги;
- автоматические расчетные палаты.

К розничным электронным услугам относят:

- проведение безналичных расчетов с использованием платежных карт в точках продаж товаров и услуг;
- использование банкоматов и других форм самообслуживания клиентов;
- выполнение электронных расчетов; . [21, с. 34]

– обслуживание клиентов на дому и в офисе;

– услуги, связанные с обработкой и хранением денежных документов.

К оптовой банковской деятельности относятся те банковские операции, которые осуществляются между торговыми банками и другими финансовыми организациями. К ним относятся переводы денежных средств между банками, управление денежными потоками и их контроль. [29, с. 17]

Под автоматическими расчетными палатами подразумевают специальные организации, создаваемые коммерческими банками для помощи в проведении сделок между клиентами и использованием электронных средств. Они выполняют те же функции, что и обычная расчетная палата, но здесь безналичные взаимные расчеты между финансовыми учреждениями определенного региона осуществляются в автоматизированном режиме и вся информация о платежах поступает в форме, подготовленной для ввода в ЭВМ.

В данной работе будут рассмотрены только розничные банковские услуги как многообразие банковских услуг, оказываемых частным лицам. Как было сказано ранее к розничным банковским услугам относятся безналичные операции, осуществляемые с использованием платежных карт в точках продаж товаров и услуг.

Под банковской пластиковой картой подразумевают платежный инструмент, посредством которого ее держатели могут осуществлять безналичные расчеты за товары, работы и услуги, получать наличные денежные средства. [31, с. 580]

Банковская карта является средством доступа к денежным средствам, находящимся на счете держателя. Для систематизации основных понятий в области банковских карт целесообразно привести их классификацию (таб.1.2).

Таблица 1.2

Классификация банковских пластиковых карт

Классификационный признак	Виды пластиковых карт
1	2
По принадлежности к учреждению-эмитенту:	– банковские карты, эмитентом которых является банк, либо финансовые компании; – частные карты – выпускаются нефинансовыми учреждениями.
По характеру использования:	– индивидуальная карта, которая выдается отдельным клиентам банка; – корпоративная карта выдается организации, которая на основе этой карты может выдать индивидуальные карты избранным лицам.
По видам проводимых расчетов:	– кредитные карты, которые связаны с открытием кредитной линии в банке, что дает возможность клиенту пользоваться кредитом при покупке товаров и при получении кассовых ссуд; – дебетовые карты – предназначены для оплаты товаров и услуг путем прямого списание средств с банковского счета плательщика; – карты с разрешенным овердрафтом представляют собой платежные карты, позволяющие осуществлять платежи как за счет средств держателя карты размещённых на банковском счёте, так и за счёт кредита, предоставляемого банком в случае недостатка средств на счёте.
По категории клиентуры:	– стандартная; – «золотая» - для лиц с высокой кредитоспособностью, предусматривает множество льгот для пользователей.
По способу записи информации на карту:	– графическая запись – нанесение на карту имени и фамилии держателя и сведений о ее эмитенте; – эмбоссирование – нанесение данных в виде рельефных знаков; – штрих-кодирование; – кодирование на магнитной полосе; – запись в интегральную микросхему;
По методу считывания информации с банковской карты:	– контактные; – бесконтактные; – со сдвоенным интерфейсом.

Итак, осуществление безналичных операций в точках продаж товаров и услуг называется торговым эквайрингом – это отношения между банком – эквайером и торговой точкой – магазином, в основе которого лежит договор эквайринга. Предметом такого договора являются услуги банка по приему платежей за товары с помощью банковских карт. Банк (эквайер) накладывает на себя обязательство по обслуживанию и установке POS-терминала по оформлению операций по картам. [33, с. 406]

POS-терминал – это компактное электронное устройство, предназначенное для проведения операций по платежным картам с магнитной полосой и микропроцессором.

POS-терминал может использоваться в торгово-сервисных предприятиях и выполнять следующие операции:

– оплата покупки;

– возврат товара;

– преавторизация (для использования в отелях/ресторанах);

– завершение преавторизации (для использования в отелях/ресторанах).

Кроме данных сторон договора в этих отношениях есть и иные участники: физические лица, платежная система и банк. [33, с. 4077]

В общем, схема взаимодействия состоит из следующих этапов: банк-эквайер получает от банка-эмитента допуск на проведение операции. В свою очередь процессинговый центр обрабатывает информацию и отправляет ее в банк, после чего эмитент высылает процессингу разрешение на транзакцию, присваивает код авторизации. [33, с. 408]

Таким образом, плюсами эквайринговых отношений для государства являются: экономия государственных средств на печатание банкнот банка России; возможность контроля над денежным оборотом в стране; уменьшение количества незаконных сделок; возможность ведения статистической отчетности, планирования, прогнозирования, и т.д.

В качестве электронных расчетов выступают электронные денежные средства - это безналичные денежные средства в рублях или иностранной валюте, учитываемые кредитными организациями без открытия банковского счета и переводимые с использованием электронных средств платежа (ЭСП).

ЭСП предназначены для осуществления перевода ЭДС, доступ к которым может осуществляться с использованием компьютеров, мобильных устройств, в том числе посредством устанавливаемого на этих устройствах специального программного обеспечения, а также банковские предоплаченные карты. [2]

В зависимости от необходимости идентификации клиента выделяют персонифицированные (для юридических лиц и ИП) и

неперсонифицированные (для физических лиц) ЭСП. Различия между данными видами ЭСП проявляются в предельно допустимой сумме переводов и в возможностях распоряжения остатком электронных денег.

Оказывать услуги по переводу ЭДС вправе только кредитные организации (банки и небанковские кредитные организации), уведомившие Банк России в установленном порядке о начале осуществления соответствующей деятельности. В число небанковских кредитных организаций входят: РНКО «Деньги.Мэйл.Ру» (ООО), ООО РНКО «Единая касса», НКО «ЕРП» (ООО), ООО НКО «МОБИ.Деньги», ООО НКО «ПэйПал РУ», ООО НКО «Яндекс.Деньги» и другие. [2]

Помимо осуществления безналичных расчетов с использованием банковских карт в точках продаж товаров и услуг, а также использования электронных средств платежа наибольшей популярностью среди населения пользуются дистанционные банковские услуги (мобильный банкинг, интернет банкинг, АТМ-банкинг и др.). Более подробно данные виды дистанционного банковского обслуживания будут рассмотрены ниже.

С растущей популярностью рынка электронных банковских услуг (безналичных платежей, использования разновидностей ДБО, электронных кошельков и т.д.) все острее ощущается необходимость в правовом регулировании его. [27, с.104]

В связи с этим условно действующие в отношении электронного банковского обслуживания правовые акты и акты неправового характера можно разделить на несколько групп.

В первую группу входят федеральные законы, регламентирующие правовое положение кредитных организаций и особенности осуществления банковской деятельности с применением средств электронного банкинга:

Федеральный закон «О Центральном банке Российской Федерации (Банке России)» от 10.07.2002 № 86-ФЗ; Федеральный закон «О банках и банковской деятельности» от 02.12.1990 № 395-1. [1]

Во вторую – федеральные законы и подзаконные акты, устанавливающие правовой режим информации и порядок ее защиты различными субъектами хозяйственной деятельности, в том числе кредитными организациями. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ; Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ; Федеральный закон «О техническом регулировании» от 27.12.2002 N 184-ФЗ; Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». [7]

И наконец, в третью группу следует выделить нормативные акты и рекомендательные документы Банка России. Особую роль при этом выполняют стандарты и рекомендации Банка России по информационной безопасности. В их числе: Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств. (утв. Банком России 09.06.2012 N 382-П); Письмо Банка России от 23.10.2009 N 128-Т «О Рекомендациях по информационному содержанию и организации Web-сайтов кредитных организаций в сети Интернет»; Письмо Банка России от 07.12.2007 N 197-Т «О рисках при дистанционном банковском обслуживании»; Письмо Банка России от 31.03.2008 N 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем Интернет-банкинга»; Письмо Банка России от 26.10.2010 N 141-Т «О Рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания». [12]

Таким образом, внедрение систем электронного банкинга кредитными организациями в процесс банковского обслуживания и его комбинирования с традиционными формами банковского обслуживания создает положительные условия для расширения рынка сбыта услуг и закрепление конкурентных позиций банка на рынке банковских услуг.

1.2 Дистанционное банковское обслуживание как разновидноть электронного обслуживания

В современном обществе все более ярко выраженными становятся процессы глобализации и информатизации. Они оказывают существенное влияние на трансформацию и развитие банковских систем. Так, ускоренное развитие информационных продуктов и технологий в банковском секторе явилось причиной возникновения одного из перспективных и наиболее развивающихся направлений – дистанционного банковского обслуживания.

Усиление преимуществ дистанционного банковского обслуживания, при одновременной работе по устранению и минимизации имеющихся недостатков, обеспечивают непрерывное совершенствование системы дистанционного банковского обслуживания, удовлетворение потребности корпоративных и частных клиентов в банковских услугах.

Технологии дистанционного банковского обслуживания можно классифицировать с точки зрения субъекта, которому предоставляется данный вид услуг: [23, с.44]

– электронный банкинг для физических лиц;

– электронный банкинг для юридических лиц.

В разрезе принципа работы системы можно классифицировать:

– онлайновая система дистанционного банковского обслуживания;

– оффлайновая система дистанционного банковского обслуживания. [35, с.158]

Стоит отметить, что доминирующее положение на рынке дистанционного банковского обслуживания занимают онлайновые системы дистанционного банковского обслуживания.

Система дистанционного банковского обслуживания также можно классифицировать по источнику возникновения: [36, с.467]

– собственная разработка банка;

– приобретенная разработка.

Выделяют следующие основные виды дистанционного банковского обслуживания (рис. 1.1).

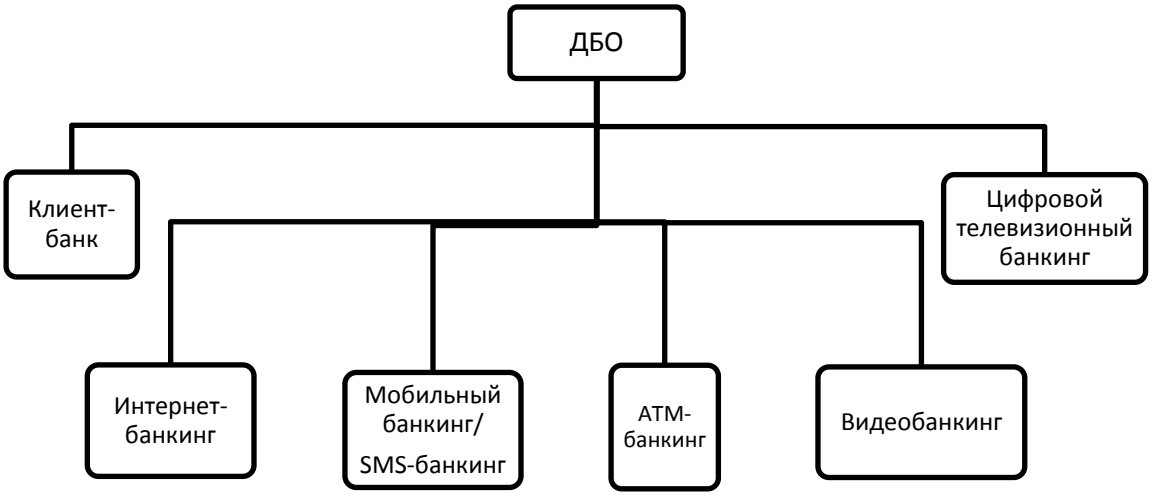

Рис. 1.1. Классификация системы дистанционного банковского обслуживания

При классическом клиент-банке – пользователь получает доступ к системе при помощи специализированной программы (программного обеспечения), установленной на компьютере. С помощью нее на компьютере хранятся все данные клиента: платежные поручения, выписки из лицевых счетов, документы зачисления и списания и т.д. Работу системы «клиент-банк» обеспечивают следующие программные комплексы:

– клиентская часть – комплекс, расположенный у клиента: обеспечивает ввод в систему расчетных документов, их корректировку, печать и проверку. Программное обеспечение клиентской части системы

«клиент-банк» может быть расположен в одном отдельном компьютере или работать в локальной сети клиента; [27, с.104]

– банковская часть – комплекс, расположенный в банке и является неотъемлемой составляющей системы автоматизации банка. Должна обеспечивать непрерывную защиту электронных расчетных документов клиента во время обработки их в САБ (система автоматизации банка).

Программное обеспечение систем дистанционного банковского обслуживания должно соответствовать требованиям нормативно-правовых актов ЦБ к технологии и защите электронных банковских расчетов. [40, с.260]

Юридическим основанием для работы клиента с помощью систем дистанционного обслуживания и обработки банком дистанционных распоряжений клиента является договор о расчетно-кассовом обслуживании.

При использовании системы «клиент-банк» банк ежедневно распечатывает реестр электронных расчетных документов, отправленных клиентом. Электронные расчетные документы, отправленные клиентом, ежедневно архивируют и хранят в банке в течение установленного срока. После получения от банка выписки со счета клиента составляется реестр электронных расчетных документов, отправленных в банк каналами связи.

Дистанционное распоряжение считается переданным клиентом и принятым банком к исполнению, если клиент:

– для доступа к системе ввел правильное значение средства идентификации;

– ввел код операции и все параметры, которые запрашивает система;

– подтвердил это распоряжение.

Банк, обслуживающий плательщика, списывая на основании дистанционного распоряжения средства со счета плательщика, оформляет расчетный документ, в котором отмечает информацию о платеже и документах, на основании которых осуществляется перечисление средств.

Если клиент не подтвердил распоряжение на совершение сделки, то банк операцию не выполняет, о чем информирует клиента. Передача дистанционного распоряжения и регистрация его банком осуществляется по согласованному каналу доступа в автоматическом режиме.

Возможностями данной системы являются:

– осуществление безналичных платежей с рабочего места в офисе, оборудованного персональным компьютером с установленным необходимым программным обеспечением (передавать в Банк платежные документы);

– контроль за оборотом имеющихся денежных средств на текущем счете (sms –информирование);

– запрос выписок по счетам, документов по зачислению и списанию средств;

– ведение справочников (контрагентов, банков, счетов клиента, владельцев ЭЦП, статуса налогоплательщиков, кодов ОКАТО, оснований платежа, налогового перида и типа налогового платежа);

– сохранность документов архива;

– двусторонний обмен .

В общем виде преимуществами системы «Клиент-банк» являются:

– автоматизированная подготовка документов, предполагающая наличие шаблонов для введения электронных документов согласно типовым стандартам, которые действуют в РФ и максимально приближены к бумажным. Как и бумажные, электронные платежные документы, отправленные в банк, подписывают должностные лица предприятия, но вместо рукописной подписи используют электронную цифровую подпись;

– высокая скорость осуществления операций при использовании системы «клиент-банк»;

– мобильность, позволяющая контактировать с банком без ограничений во времени, поскольку технические возможности большинства

программных комплексов дают возможность круглосуточно отправлять документыв банк и просматривать полученные оттуда данные;

– безопасность, при которой средства защиты информации в системе «клиент-банк» при корректном их использовании гарантируют надежную защиту от несанкционированного доступа и модификации информации.

Однако, наряду с очевидными преимуществами система «клиент-банк» имеет и определенные недостатки. Основным недостатком является то, что перевод средств с использованием данной системы требует постоянного присутствия руководящих лиц – директора и главного бухгалтера, которые наделены правом первой и второй подписи. Кроме этого могут возникнуть ошибки при переносе информации из системы «клиент-банк» в автоматизированную банковскую систему (АБС), если эти системы создавались разными разработчиками. Поэтому уместным было бы определить, насколько совместнимыми является программный комплекс «клиент-банк» и АБС, используемой в банке. Также высокая цена разработки и внедрения системы «клиент-банк» делает ее неэффективной для небольших банков, а необходимость загрузки и оплаты специального программного обеспечения ограничивает круг потенциальных клиентов.

Особенностью сети Интернет-банк является взаимодействие с банком посредством сети Интернет через браузер. В данном случае вся информация о действиях пользователя хранится на серверах банка. При этом установка дистрибутива системы на компьютер пользователя не требуется. Следует различать интернет-банк для физических и для юридических лиц. Услуги, предоставляемые в рамках интернет-банкинга схематически представлены на рисунке 1.2.

При заключении договора по подключению к системе ДБО, клиенту могут быть необходимы дополнительные продукты такие как: сертификат ключа проверки электронной подписи, зарплатный проект, интернет-бухгалтерия, дополнительные сервисы безопасности.

Для предотвращения подделки или несанкционированного использования электронной подписи используют особый код (ключ электронной подписи).

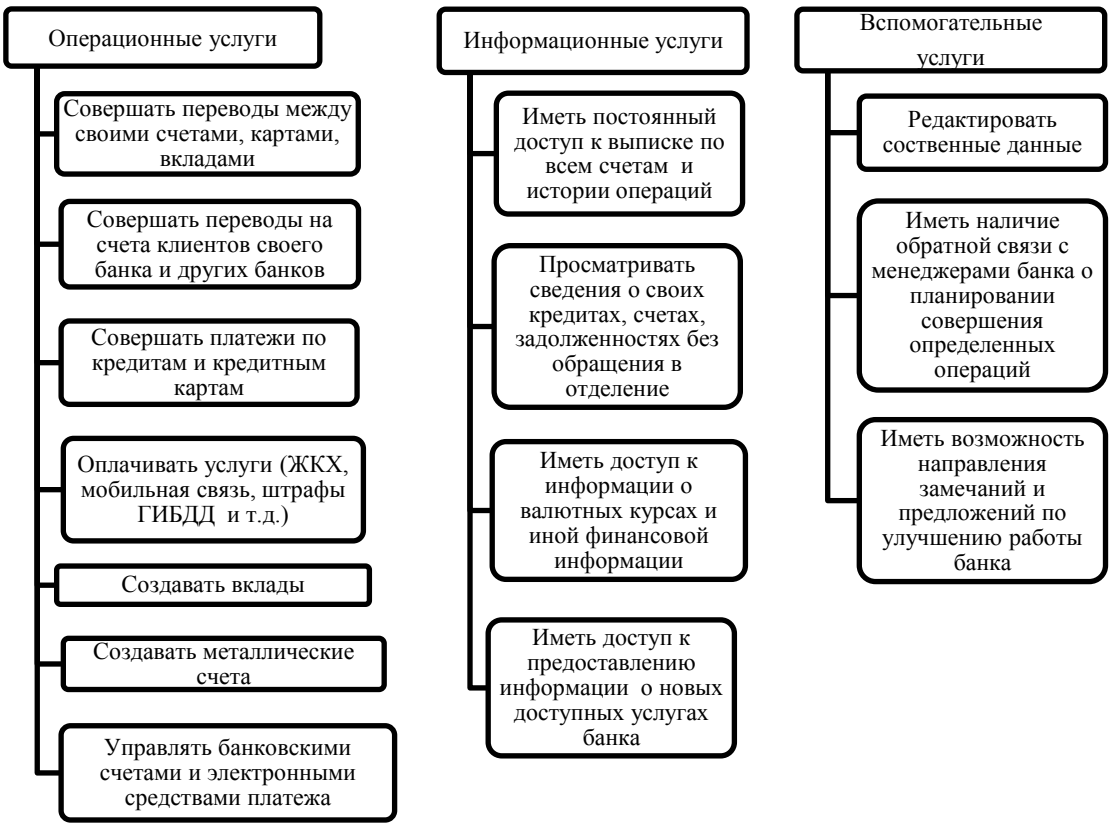

Рис.1.2. Услуги, предоставляемые в рамках интернет-банкинга

Электронная цифровая подпись – это реквизит электронного документа, предназначенный для защиты данного документа от подделки; получен в результате криптографического преобразования информации с использованием ключа ЭЦП и позволяет идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Участие в зарплатном проекте позволяет вести справочник сотрудников, формировать и отправлять в Банк реестры на открытие зарплатных счетов, формировать и отправлять в банк платежные поручения

на зачисление заработной платы, автоматически формировать платежные поручения на комиссию за обслуживание и др.

Сервисы интернет-бухгалтерии, интегрированные с интернет-банком для юридических лиц предназначены для ведения бухгалтерского, налогового и кадрового учета, формирования и сдачи отчетности через интернет, отображение выписок из интернет-банка в сервисе интернет-бухгалтерии, отправка платежных поручений из бухгалтерии в банк, автоматического распределения денежных средств по статьям доходов и расходов, расчета суммы налогов и взносов, а также для автоматического отслеживания оплаты счетов.

На данный момент наблюдается тенденция подключения интернет-банка для юридических лиц в рамках договора о комплексном банковском обслуживании, что обусловлено стремлением банков перевести большее количество клиентов на системы дистанционного банковского обслуживания. Основными преимуществами данной системы для юридических лиц являются снижение риска неэффективного использования средств на различных уровнях управления, повышение степени контролируемости и прозрачности бизнеса, снижение затрат на банковское обслуживание.

Мобильный банк предполагает доступ пользователя к услугам посредством устройств мобильной связи (телефона, планшета). Наиболее часто для совершения операций и обеспечения связи с банком требуется интернет-канал (3-G, GPRS, 4-G LTE, Wi-Fi), реже для обеспечения функционирования используются SMS-сообщения. [22, с.382]

Как правило, такие системы имеют ограниченный набор функций, по сравнению с системами интернет-банкинга. Так, в настоящее время посредством мобильного банкинга, можно осуществлять как информационные операции (запросить баланс, выписку об операциях по счетам, сумму обязательного платежа или задолженность по кредитной карте

и т.д.), так и производить различные платежи и осуществлять денежные переводы с помощью мобильного телефона (рис.1.3).

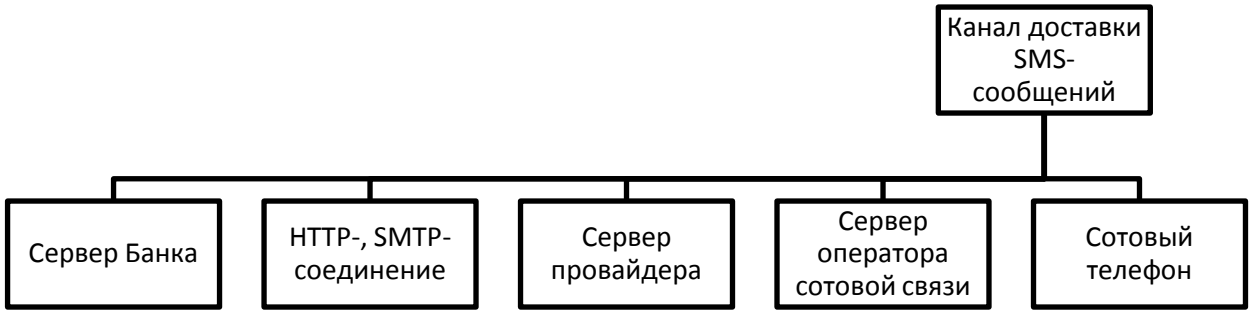

Рис.1. 3. Схема соединения сервера банка с сервером провайдера в целях осуществления мобильного банкинга

Также одним из вариантов обслуживания - вне офиса банка является использование для совершения разного рода банковских операций устройств самообслуживания (банкоматов и платежных терминалов).

Банкомат – автоматическое устройство для осуществления расчетов, обеспечивающее возможность выдачи и (или) приема наличных денежных средств, в том числе с использованием электронных средств платежа, и по передаче распоряжений кредитной организации об осуществлении перевода денежных средств. [2]

Платежный терминал – это устройство для осуществления наличных денежных расчетов в автоматическом режиме.

Основными операциями, доступными пользователям банкоматов являются:

– получение доступа к собственным счетам (пополнение баланса или снятие с него дененых средств);

– оплата текущих счетов: мобильная связь, ЖКХ и домашний телефон, Интернет и ТВ, налоги, штрафы, пошлины, бюджетные платежи, погашение кредитов и прочее;

– переводы: между своими счетами, клиенту вашего Банка (на карту или счет), на карту в другой Банк (по номеру телефона или карты) и на счет в другой Банк;

– запрос баланса счета — предоставление информации о движении денежных средств и остатке на счету в указанный период;

– печать документов, подтверждающих проведение операций со счетами (по запросу);

– конвертация валют;

– активация различных услуг.

Платежные терминалы обладают тем же набором функций, что и банкоматы, однако, отсутствует возможность снятия денежных средств со счета. В некоторых организациях торговли и услуг вкупе с вышеуказанными устройствами самообслуживания существует возможность оплаты покупки (товара, услуги) при помощи импринтера - механического устройства, предназначенного для оформления слипа (переноса оттиска рельефных реквизитов банковской карты на документ, составленный на бумажном носителе) при совершении операции с платежной картой.

В свою очередь функции импринтера ограничены только осуществлением платежных операций. Участниками, которых являются работник торговой точки (кассир), покупатель, авторизационный центр, а также банк-эквайер и банк-эмитент.

Видеобанкинг – это еще одно направление удаленного банковского обслуживания. Считается одним из самых перспективных. Видеобанкинг представляет собой оказание дистанционных услуг по видеосвязи через камеры мобильных телефонов либо специальные банковские терминалы, снабженные телемониторами. Данный вид обслуживания имеет актуальность в связи с развитием цифрового банкинга, по сути своего рода прямого физического контакта клиента с банком.

Цифровой телевизионный банкинг - вид дистанционных услуг, оказываемых через экран телевизора. В России из всех вышеперечисленных

каналов удаленной связи банка с клиентами на сегодняшний день видеобанкинг и цифровой телевизионный банкинг пока не получили распространение.

Между тем разделять банковское обслуживание по каналам не совсем правильно. Мультиканальность банковской деятельности постепенно уходит в прошлое, а на ее место приходит омниканальность, интеграция всех каналов сбыта. Самая большая разница между этими двумя понятиями состоит в фокусе внимания. Если в первой случае – это наличие разных каналов продаж, то во втором случае акцент делается на удобство потребителя банковских услуг при осуществлении операций.

По сути, разновидности дистанционного банковского обслуживания (мобильный банк, интернет-банк, Call-центр, банкоматы и платежные терминалы) также не являются каналами обслуживания. Они тесно вплетены в оцифрованную для удобства проживания в XXI веке жизнь. [52, с. 437]

Исходя из этого, для многих кредитных организаций главной на сегодняшний день является задача создания такой системы дистанционного обслуживания, при которой клиент смог бы действовать, исключительно отталкиваясь от своих желаний. Это важно, ведь основной целью банковского обслуживания является удовлетворение потребностей каждого клиента. И банк, который производит лучшее впечатление при обслуживании, выделяется среди остальных. [47, с. 359]

Таким образом, с появлением дистанционного облуживания у банка появляется возможность предложить своим клиентам целую систему взаимодействия в режиме реального времени. Удобство данной системы заключается в праве выбора наиболее актуальной для потребителя банковской услуги: то ли это будет обслуживание клиента посредством использования банкомата, а то ли посредством интернет-банкинга. [30, с. 150]

1.3 Современные проблемы развития дистанционного банковского обслуживания в России

Очевидно, что столь массовая и «ускоренная» автоматизация обусловила возникновение целого комплекса проблем в совершенно различных сферах: организационных, финансовых, технических и иных.

В общем, проблемы, которые мешают развивать банковские услуги в глобальной сети Интернет, можно разделить на несколько крупных блоков:

Психологические проблемы связаны со сложностью работы с обществом в целом. Все еще существует недоверие значительной части населения к проведению операций через Интернет. Очень часто людям психологически проще прийти в офис банка и отстоять в очереди, чем провести платежи со своего компьютера. Как правило, данный род проблем характерен для социально незащищенных слоев населения (пенсионеров, лиц с особыми потребностями, жителей удаленных от федерального центра регионов и небольших городов). Вышеуказанные лица в силу отсутствия определенных навыков в использовании телефонов, планшетов и компьютеров не в состоянии удаленно осуществлять банковские операции. К тому же преимущественно у многих из них при наличии компьютера или телефона, нет доступа в Интернет. [14, с. 38]

В свою очередь к другому роду проблем относятся кадровые проблемы, поскольку качество и оперативность решения любых задач напрямую зависит от квалификации специалистов, которые за нее берутся. Для разработки и поддержки систем Интернет-банкинга сегодня очень сильно нужны программисты, системные администраторы, Веб-дизайнеры, Веб-программисты, эксперты по компьютерной и коммуникационной защите, экономисты, маркетологи, юристы. Все они обязаны хорошо представлять мир Интернета, что сейчас далеко не всегда возможно. В связи с этим возникают кадровые сложности, обусловленные, во-первых, необходимостью поиска значительного числа высококвалифицированных

специалистов в области IT и, с другой стороны, ростом безработицы из-за внедрения нового программного обеспечения. [48, с. 360]

Есть так же технологические проблемы, они же ограничивают область, в которой можно применить электронные каналы, которые используются в деятельности банка. В отличие от отделений банка, где количество проводимых операций ограничено числом сотрудников, в Интернет-банкинге число операций в принципе может быть практически неограниченным. Но это потребует от банков такого уровня развития внутренних бизнес-процессов и состояния информационных систем, которые смогут позволить единовременно выполнять операций намного больше, чем это можно будет сделать в отделениях. [51, с. 425]

В связи с техническими сбоями у клиента могут не проходить операции или отсутствовать возможность использования удаленного доступа управления счетами. Такие проблемы негативно сказываются на имидже банка. Кроме технических сбоев в сервисе банков возможны сбои и у посредников, услугами которых пользуется клиент при использовании услуг банка. Такими посредниками могут быть интернет-провайдер или поставщик сотовой связи. От качества предоставляемых ими услуг зависит качество получаемой клиентом услуги. Например, неполучение клиентом из банка СМС-сообщения для подтверждения входа в интернет-банкинг или проведения операции вызывает определенные трудности; медленное соединение, которое не позволяет загрузить страницу или увеличивает время проведения операции, создает негативное впечатление о предоставляемой услуге. [54, с. 39]

Существует проблема сложности интерфейса, созданного для обслуживания интернет-банкинга. Следует отметить, что, как правило, банковские организации покупают готовое программное обеспечение и не заостряют своего внимания на таких мелочах, как простота и понятность проведения банковского платежа, а клиенты сталкиваются с такой проблемой, как сложность совершения простейших банковских платежей.

Также к числу проблем, замедляющих развитие Интернет-банкинга, является отсутствие четко сформулированного и систематизированного законодательства как по вопросам защиты и безопасности, так и в области электронной коммерции вообще. [49, с. 75]

Наиболее важной проблемой развития дистанционного банковского обслуживания в России является недостаточный уровень информационной безопасности: слабая организация защиты платежей и сохранности финансовых средств клиентов на счетах. Данная проблема является общей как для пользователей интернет и мобильных услуг, так и для кредитных организаций, выступающих посредниками при осуществлении платежных операций. В настоящее время наиболее популярным способом воздействия на организации и физических лиц мошенниками является массовая рассылка sms-сообщений или электронных сообщений клиенту банка от лица кредитной организации. По-прежнему актуален такой способ мошенничества как создание фишинговых сайтов, имитирующих интерфейс соответствующей системы интернет-банкинга, и подделывающих электронную цифровую подпись клиента с помощью различных средств.

Согласно мнению экспертов в области информационной безопасности проблема, связанная с кражами персональных данных злоумышленниками еще долго будет давать о себе знать. Безусловно, наличие данной проблемы толкает банки к поиску путей ее ликвидации посредством использования новейших методов и разработок в области безопасности интернет-платежей, а Банк России – к оперативному реагированию через издание соответствующих указаний и информационных писем. [53, с. 30]

Недостаточная информированность клиентов банка о новых технологиях и способах защиты от мошеннических действий также в настоящее время является большой проблемой. Этот недостаток, прежде всего, связан с отношением самой кредитной организации к интернет-банкингу как к сопутствующей услуге. Филиальная модель ведения бизнеса приводит к тому, что в силу недостаточной информированности клиент либо

просто не пользуется услугой, либо попадает в руки мошенников, приобретая негативный опыт и отказываясь в дальнейшем от использования услуги.

Сегодня по-прежнему актуальна проблема ограниченных технических возможностей электронных услуг. Дело в том, что неравномерное развитие телекоммуникационных систем в стране оборачивается тем, что в регионах у пользователя отсутствуют дешевые каналы передачи данных, которые могут обеспечить нормальную работоспособность технологии интернет-банкинга. В итоге клиенты вынуждены пользоваться мобильными каналами связи для входа в личные кабинеты, в результате чего теряются скорость операций и часть функционала системы. [22, с. 383]

В свою очередь финансовые проблемы связаны с большими затратами на приобретение системы, создание и внедрение.

Для построения цифрового пространства современной финансовой организации необходим отдельный класс фронтальных решений, обеспечивающий единый процесс обслуживания клиентов в любом канале: банкомате, call-центре, интернет-банке, мобильном банке, сети банковских отделений. [49, с. 73]

Соответственно, возникает проблема приобретения нового программного обеспечения, технических решений, обучения персонала и т.д.

К основным проблемам, присущим системам дистанционного банковского обслуживания следует отнести:

– высокие затраты на разработку, внедрение и обслуживание системы «Клиент-Банк»; необходимость поддержания в актуальном состоянии баз данных на стороне клиента; необходимость обучения персонала на стороне клиента; риски несанкционированного доступа и вмешательства извне при передаче информации посредством интетернет-банкинга; зависимость от сети интернет-провайдера; поломка компьютера; необходимость использования услуг процессингового центра и наличие абонентской платы интернет провайдера.

– зависимость от сети мобильной связи системы мобильного банкинга; недостаточно высокий уровень безопасности доступа и передачи информации; риск, поломки, кражи или потери мобильного устройства; ограниченный круг услуг банка клиенту; наличие комиссии.

– затраты на создание информационно-справочной системы (ИСС) банка, автоматической голосовой системы управления и сети Call-центров системы телефонного банкинга; невысокий уровень безопасности доступа и передачи информации; ограниченный круг услуг банка клиенту; наличие абонентской платы. [15, с. 10]

– привязка к существующей банковской сети стационарных платежных устройств системы АТМ-банкинга; риск мошенничества и технологических сбоев в работе оборудования и средств связи; затраты банка на развитие сети платежных устройств и ее обслуживание; недостаточный уровень финансовой грамотности населения.

На основании вышеизложенного необходимо сказать, что специфика электронных банковских услуг требует от потребителей экономической культуры, вызывает необходимость разъяснения содержания услуги клиенту, усиливает значение фактора доверия клиентов к банковскому сектору экономики. [18, с. 340]

Так, с переходом на цифровую экономику население все активней начинает пользоваться удаленными каналами обслуживания такими как: мобильный банкинг, интернет-банкинг, клиент-банк, АТМ-банкинг.

Но вместе с этим нельзя не сказать о возможных проблемах, развития дистанционного банковского обслуживания: психологических, кадровых, технологических, юридических и иных проблем. Поскольку было бы глупо не учитывать данный ряд проблем при предоставлении со стороны кредитных организаций и использовании удаленных каналов обслуживания со стороны потребителей банковских услуг. Зная о них проще найти способы их минимизации или полного устранения.

ГЛАВА 2. СОВРЕМЕННАЯ ПРАКТИКА ФУНКЦИОНИРОВАНИЯ РЫНКА ЭЛЕКТРОННЫХ БАНКОВСКИХ УСЛУГ В РОССИИ

2.1 Анализ безопасности электронных банковских услуг в отечественном банковском секторе

В последние годы активное развитие сферы информационно-коммуникационных технологий и внедрение новых цифровых технологий в банковский бизнес привело не только к распространению технологий электронного банкинга (интернет-банкинга, мобильного банкинга и др.), но и к стремительному росту киберпреступлений в кредитно-финансовой сфере.

Объем несанкционированных операций с использованием платежных карт, эмитированных (выданных) на территории РФ в 2017 году составил 0,96 млрд. руб., что ниже аналогичного показателя 2016 года (на 0,11 млрд. рублей или на 10,6 %) и 2015 года (на 0,19 млрд. рублей или на 16,2 %).

Указанная тенденция может быть обусловлена проводимой операторами по переводу денежных средств работой, направленной на активное развитие систем выявления и противодействия несанкционированным операциям - система антифрод, которая анализирует активность пользователей и блокирует подозрительные транзакции и операции, основываясь на проанализированных данных активности. Эффективное использование подобных систем повышает качество верификации лица, осуществляющего перевод денежных средств вследствие чего снижается эффективность действий злоумышленников (средняя сумма одной несанкционированной операции за анализируемый период уменьшилась с 4,34 тыс. руб. (2015 г.) до 3,03 тыс. руб. (2017 г.) [56]

Динамику количества и объема несанкционированных операций с использованием платежных карт за 2015-2017 гг. представим на рис.2.1.

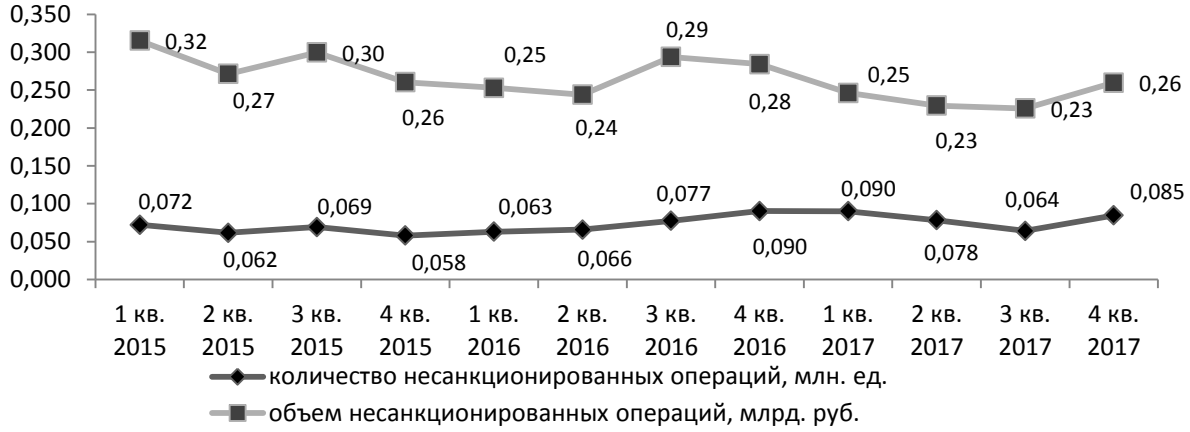

Рис. 2.1. Динамика количества и объема несанкционированных операций с использованием платежных карт за 2015-2017 гг.

Вместе с тем, количество таких операций в течение рассматриваемого периода напротив имело тенденцию к росту и к концу 2017 году достигло 0,31 млн. ед. (увеличение по сравнению с 2015 годом составило – 0,056 млн. ед., а по сравнению с 2016 годом – 0,020 млн. ед.). Доля несанкционированных операций в общем объеме операций, совершенных с использованием платежных карт с 4 квартала 2015 года по 4 квартал 2017 году снизилась с 0,0021% до 0,0015 %. Значение данного показателя в 2017 году - 0,0016 % не превышает установленный Банком России целевой показатель доли объема несанкционированных операций в общем объеме операций, совершенных с использованием платежных карт - 0,0050 %.

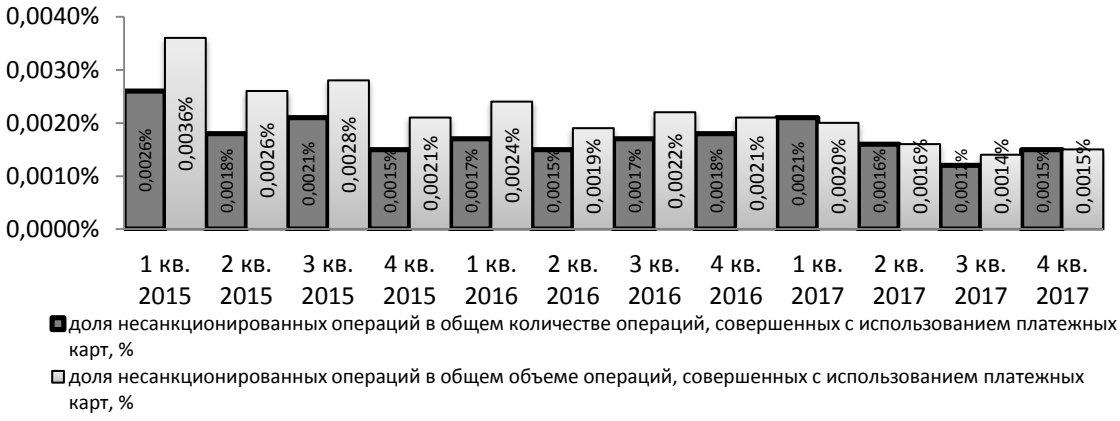

Рис.2.2. Доля количества и объема несанкционированных операций в общем числе операций, совершенных с использованием платежных карт за 2015-2017 гг., %

В свою очередь доля несанкционированных операций в общем количестве несанкционированных операций в 4 квартале 2017 года по отношению к 4 кварталу 2015 года осталась неизменной - 0,0015 % (рис. 2.2)

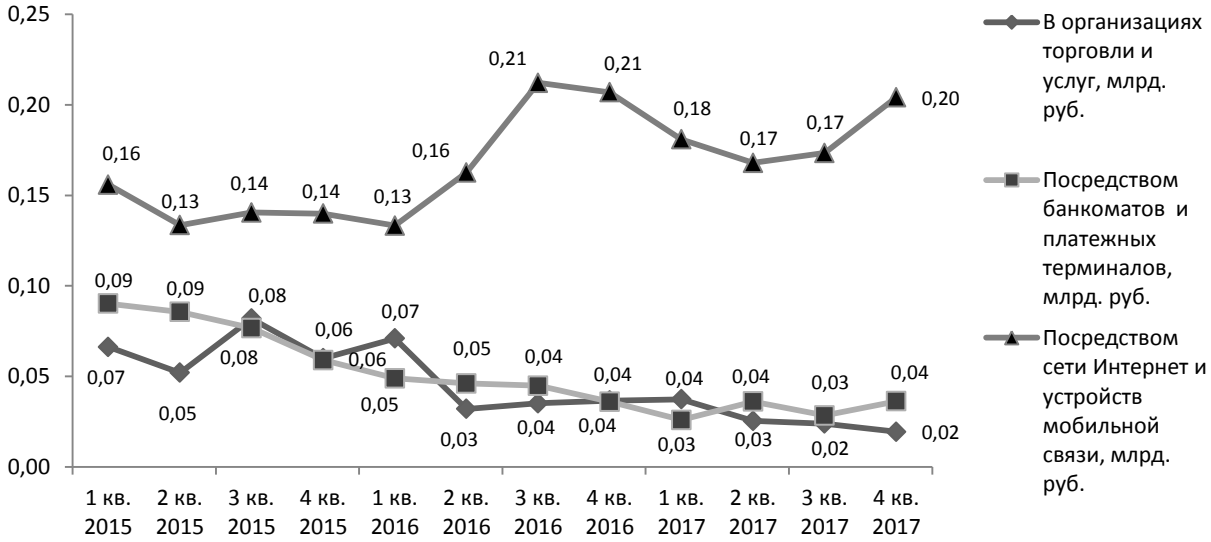

Рис. 2.3. Динамика несанкционированных операций с использованием платежных карт в разрезе условий их проведения за 2015-2017 гг., млрд. руб.

Из рис. 2.3 видно, что объемы несанкционированных операций, осуществляемых в организациях торговли и банкоматах, снижаются, в то время как объем несанкционированных операций без предъявления карты (CNP-транзакции) растет. CNP-транзакция – это транзакция типа «Card Not Present» – операция, осуществленная в сети Интернет с использованием реквизитов платежной карты. [57]

Подобный характер тренда может быть обусловлен смещением вектора интересов пользователей и провайдеров услуг в сторону сети Интернет в рамках повышения доступности платежных услуг, вследствие чего вектор интересов злоумышленников смещается от банкоматов и организаций торговли в сторону CNP-транзакций. [57]

На данный момент формой отчетности 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

предусмотрены следующие возможные причины несанкционированных операций:

– использование электронных средств платежа без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности;

– нарушение клиентом порядка использования электронных средств платежа;

– побуждение владельца электронных средств платежа к совершению операции путем обмана или злоупотребления доверием;

– воздействие вредоносного кода; [58]

– другие причины.

В качестве наиболее часто встречаемой причины возникновения большинства несанкционированных операций (более 90 %) в рассматриваемом периоде отчитывающимися операторами указывается использование электронных средств платежа без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности аутентификационной информации.

Необходимо отметить, что полученные сведения отчитывающихся операторов основываются на данных, представленных клиентами банков в заявлении. В связи с этим отчитывающимся операторам в силу неполноты информации о причинах совершения несанкционированных операций приходится проводить дополнительные проверки права пользования платежной картой, в результате которых вышеуказанная причина в большинстве случаев может быть сведена к воздействию вредоносного кода или побуждению владельца электронного средства платежа к совершению операции путем обмана или злоупотребления доверием.[56]

На долю несанкционированных операций, совершенных за пределами РФ, в течение анализируемого периода приходилось более 40 % (52,2 % в 2015 году, 40,4 % в 2016 году и 40,8 % в 2017 году) от количества и более 43

% от объема всех несанкционированных операций (57,6 % в 2015 году, 44,3% в 2016 году и 43,8 % в 2017 году) (рис.2.4).

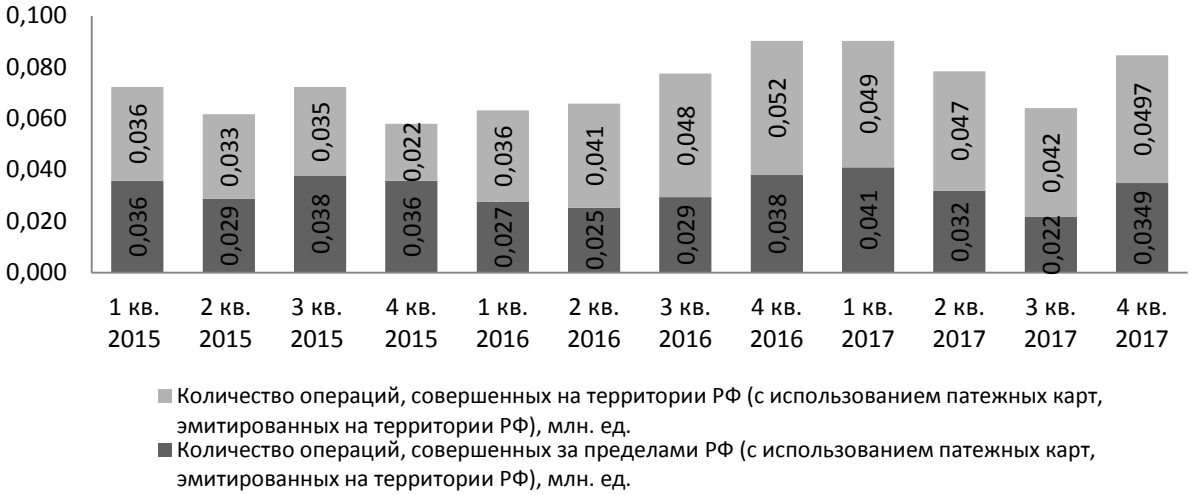

Рис. 2.4. Количество несанкционированных операций с использованием платежных карт, эмитированных на территории РФ за 2015-2017 гг., млн. ед.

Нахождение злоумышленника вне Российской Федерации существенно затрудняет его привлечение к ответственности правоохранительными органами. Показатели свидетельствуют о том, что при использовании антифрод-систем трансграничным операциям должно уделяться пристальное внимание (рис.2.5).

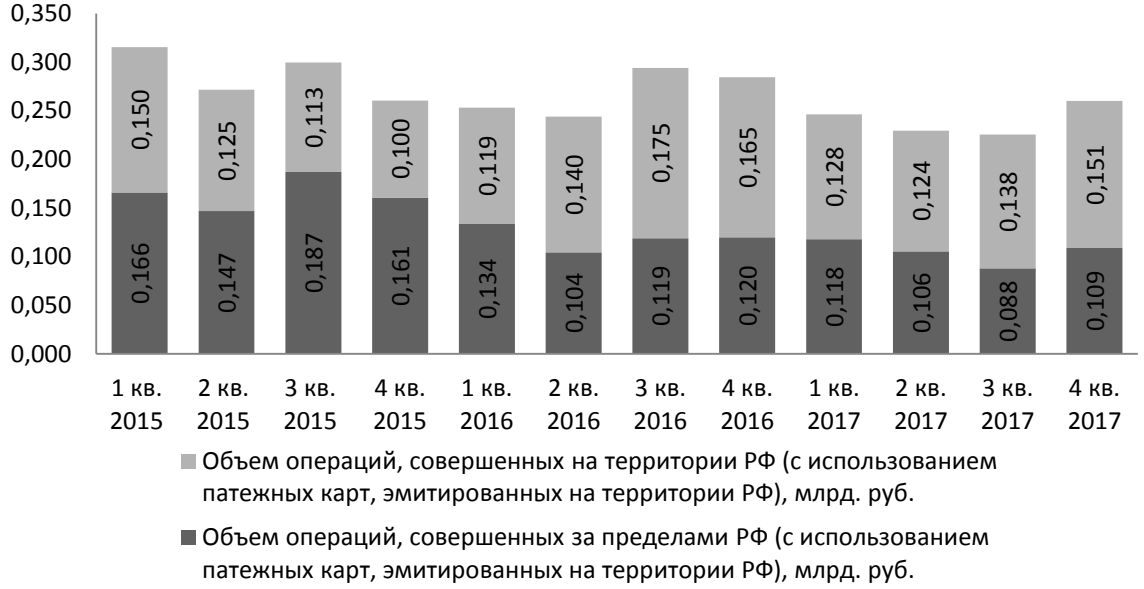

Рис. 2.5. Объем несанкционированных операций с использованием платежных карт, эмитированных на территории РФ за 2015-2017 гг.

Также необходимо сказать о местах осуществления несанкционированных операций с использованием банковских карт в РФ (в разрезе федеральных округов за 2017 год). Так, наибольшее количество и объем операций совершено в центральном федеральном округе (ЦФО) – 0,11 млн. ед. на сумму 0,38 млрд. руб. (60,93 % от общего количества и 70,63 % от общего объема несанкционированных операций в РФ), в т. ч. в городе Москве – 0,86 млн. ед. на сумму 0,33 млрд. руб. (45,71 % от количества и 60,20 % от объема), далее за ЦФО по убыванию следуют: Приволжской федеральный округ – 0,019 млн. ед. на сумму 0,04 млрд. руб. (10,02 % от количества и 7,4 % от объема), Северо-Западный федеральный округ – 0,016 млн. ед. на сумму 0,04 млрд. руб. (8,42 % от количества и 7,25 % от объема), в т. ч. в городе Санкт-Петербург – 0,05 млн. ед. на сумму 0,019 млрд. руб. (2,91 % от количества и 3,6 % от объема), на оставшиеся федеральные округа (Сибирский федеральный округ, Уральский федеральный округ, Южный федеральный округ, Дальневосточный федеральный округ и Северо – Кавказский федеральный округ) приходится 20,63 % от количества и 14,72 % от объема всех несанкционированных операций, совершенных с использованием банковских карт в РФ. [56]

Таким образом, наибольшее количество и объем несанкционированных операций, осуществлялось в Центральном федеральном округе, преимущественно в городе Москве.

Под несанкционированными операциями со счетов юридических лиц понимаются события, связанные с покушением на хищение денежных средств со счета юридического лица с использованием систем ДБО.

За анализируемый период в отношении юридических лиц было совершено 2622 несанкционированных операций на общую сумму 7257,6 млн. руб. Причем, наибольший объем и количество несанкционированных операций в системах ДБО отмечается в 2015 году – 1064 несанкционированных атак на сумму 3793,6 млн. рублей. Это было связано с рядом крупных инцидентов, зафиксированных во 2 и 3 кварталах 2015 года,

которые привели к несанкционированному переводу денежных средств со счетов юридических лиц. В 2016 г. и в первой половине 2017 г. отмечено большое количество атак на юридических лиц, использующих бухгалтерские системы. Преимущественно заражение происходило при посещении скомпрометированных бухгалтерских и финансовых сайтов в сети Интернет. Основная характерная особенность этих атак – это автоматическая подмена платежных поручений на этапе их передачи из бухгалтерской системы в систему дистанционного банковского обслуживания. Суммарный ущерб от реализации вышеназванных атак превысил 200 млн. руб. Целью используемого в таких атаках вредоносного программного обеспечения, как правило, является файл экспорта-импорта, генерируемый бухгалтерской системой для передачи платежных поручений в систему ДБО, содержащий реквизиты получателя, сумму и иную необходимую для осуществления переводов информацию. (рис. 2.6).

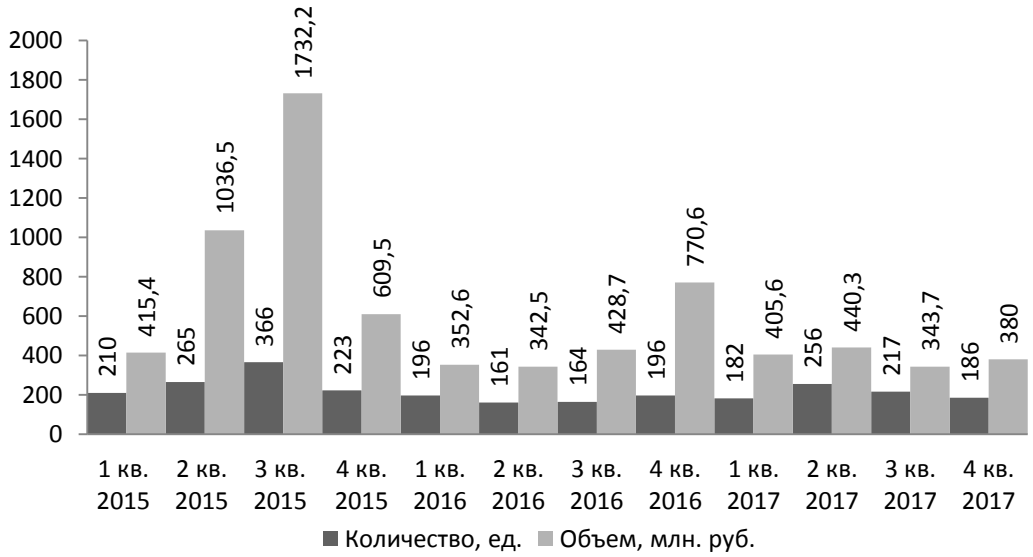

Рис. 2.6. Количество и объем несанкционированных операций со счетов юридических лиц, совершенных с использованием систем ДБО за 2015-2017 гг.

В свою очередь, вышеуказанные данные не дают полного представления об объеме хищений денежных средств со счетов юридических лиц, в связи с наличием приостановленных операций (приостановленные

операции - операции, по которым перевод денежных средств не достиг окончательности, либо окончательность перевода денежных средств наступила, но денежные средства заблокированы на счете получателя в соответствии с законодательством Российской Федерации до получения обоснования перевода денежных средств). Соотношение объема остановленных и неостановленных несанкционированных операций наглядно можно будет увидеть из рисунка 2.7.

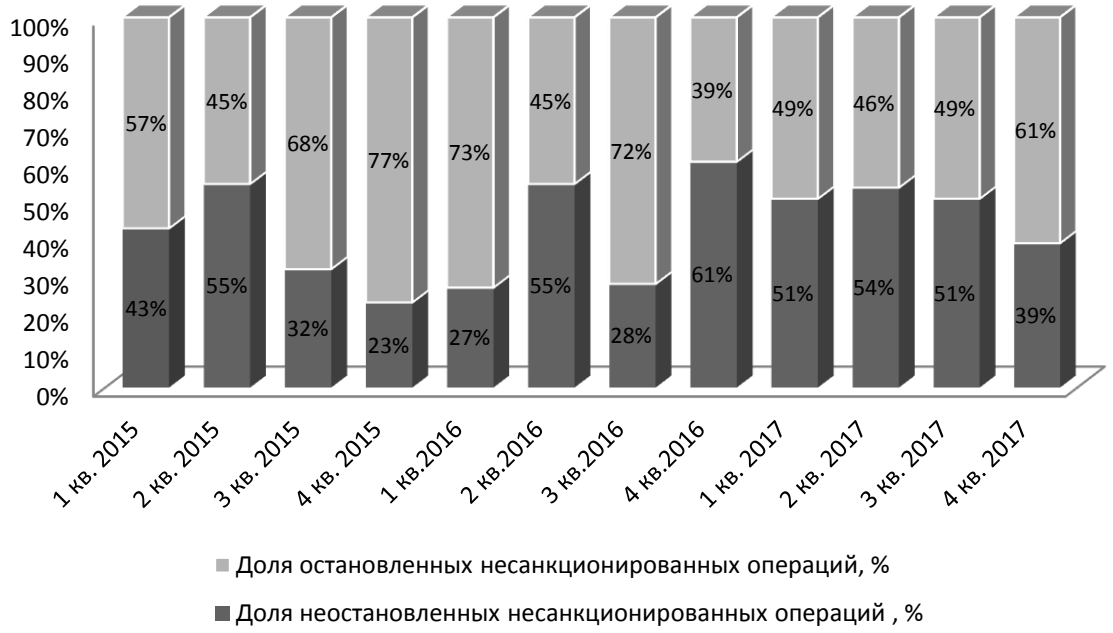

Рис. 2.7. Соотношение объема остановленных и неостановленных несанкционированных операций со счетов юридических лиц, совершенных с использованием систем ДБО за 2015-2017 гг., %

Из представленных выше рисунков можно заключить, что в 1 квартале 2015 года из 415,4 млн. рублей – 178,6 млн. руб. (43 %) было похищено киберпреступниками, таким образом, во 2 квартале -570,1 млн. рублей, в 3 и в 4 кварталах 554,3 млн. рублей и 140,2 млн. рублей из этого следует, что больше 61 % несанкционированных операций со счетов юридических лиц были остановлены в полном объеме, в том числе по обращениям клиентов, до наступления окончательности перевода денежных средств. Проведя

аналогичный анализ за два последующих года можно заметить увеличение доли неостановленных операций с 46,1 % в 2016 году до 48,9 % в 2017 году.

Основное количество несанкционированных операций приходится на сегмент от 10 тыс. рублей и до 10 млн. рублей, и достигает пика в сегменте от 100 тыс. рублей до 1 млн. рублей. В рассматриваемом периоде удельный вес количества таких операций находился в диапазоне от 42,0 % в 2015 году и до 50,9 % в 2017 году (рис.2.8).

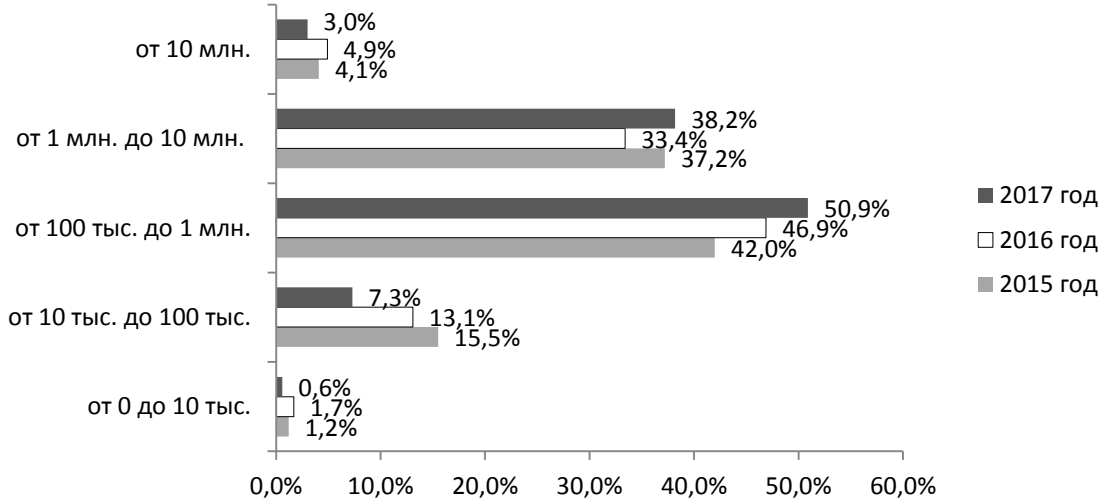

Рис.2.8. Распределение количества несанкционированных операций со счетов юридических лиц по суммам за 2015-2017 гг., %

Подобное распределение указывает на то, что интерес злоумышленников сфокусирован на юридических лицах, имеющих на своих банковских счетах суммы объемом не превышающие нескольких миллионов рублей, и не имеющих возможности на должном уровне выполнять мероприятия по защите информации при использовании дистанционных платежных сервисов. [57]

Согласно обзору Банка России причинами осуществления несанкционированных операций со счетов юридических лиц в 2017 году являются, в частности, нарушение порядка использования электронного средства платежа (9 %), использование электронного средства платежа без согласия клиента (34%), воздействие вредоносного кода (54%) и другие.

Распределение по причинам совершения несанкционированных операций со счетов юридических лиц за 2017 г. наглядно можно увидеть из рис.2.9.

Рис.2.9. Распределение по причинам совершения несанкционированных операций со счетов юридических лиц за 2017 г., %

Касательно места осуществления несанкционированных операций со счетов юридических лиц (место ведения счета) посредством дистанционного банковского обслуживания в 2017 году по количеству и объему в разрезе федеральных округов лидирует ЦФО – 61,65 % от общего количества несанкционированных операций и 77,28 % от общего объема, далее следует Приволжский федеральный округ – 10,13 % от количества и 5,15 % от объема, Сибирский федеральный округ - 6,08 % от количества и 4,38 % от объема, из этого следует, что на остальные федеральные округа приходится всего лишь малая часть (22,14 % от количества и 13,19 % от объема). Исходя из этого можно заключить, что большая часть несанкционированных операций (в количественном и суммовом выражении), как посредством использования платежных карт, так и осуществленных со счетов юридических лиц посредством дистанционного банковского обслуживания была осуществлена в Центральном федеральном округе. [57]

Также одним из распространенных среди злоумышленников типов атак является рассылка электронных сообщений, содержащих вредоносное

программное обеспечение (ВПО). Процентное соотношение типов вложений фишинговых писем в 2017 году приведено на рисунке 2.10.

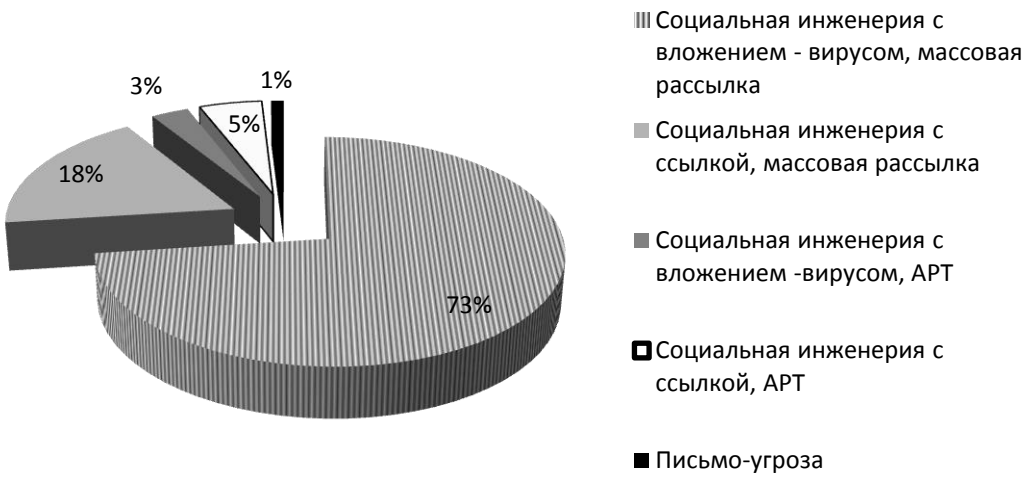

Рис.2.10. Типы вложений фишинговых писем за 2017 г., %

Из представленного выше рисунка можно заметить, что кибермошенники в большей степени осуществляют массовую рассылку сообщений (с вложением-вирусом или ссылкой) поскольку в таком случае присутствует высокая вероятность прочтения организацией сообщения и (или) прочтения и перехода по указанной в нем ссылке, что может побудить пользователя к раскрытию конфиденциальной информации для доступа к тому или иному сайту (например, логина и пароля). Помимо массовой рассылки злоумышленниками практикуются и целевые кибератаки (Advanced Persistent Threat (APT) – «Развитая устойчивая угроза»), представляющие серьезную угрозу информационно-технологической инфраструктуре организации из-за сложности обнаружения и тяжести последствий. [58]

Наибольшая доля рассылок писем с вредоносным программным обеспечением приходится на финансовые организации. Статистику по типам вредоносного программного обеспечения за 2017 год можно будет увидеть из рисунка 2.11.

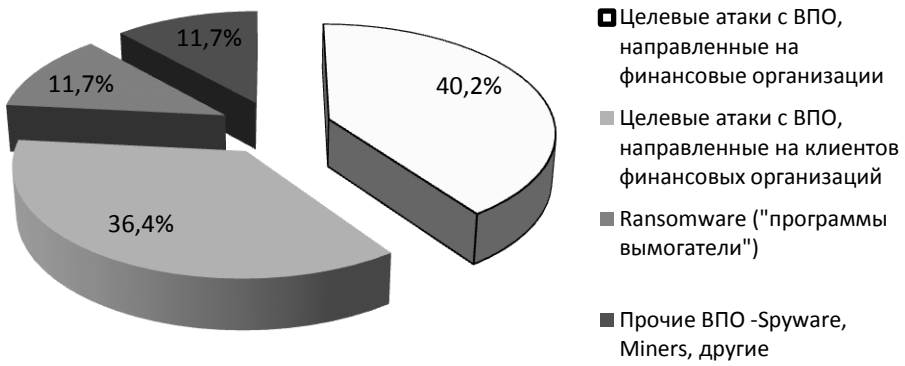

Рис.2.11. Типы вредоносного программного обеспечения за 2017 г., %

Из рисунка можно заметить, что на целевые атаки с вредоносным программным обеспечением направленные: на финансовые организации в 2017 году приходилось 40,2 %, а на клиентов финансовых организаций – 36,4 %. На программы вымогатели и прочие вредоносные программные обеспечения приходилось по 11,7 %. [58]

В течение 2015 года в Банк России было сообщено о хищениях денежных средств из банкоматов на сумму более 29 млн. руб. В 2016 году количество таких инцидентов составило 30 единиц. Восемь отчитывающихся операторов представили информацию об атаках на платежные терминалы, в результате которых операторы понесли ущерб на сумму более 5 млн. рублей.

В 2017 году десять отчитывающихся операторов направили в Банк России информацию о 21 инциденте, связанном с покушением на хищение денежных средств посредством воздействия на банкоматы, ущерб от которых составил 40 млн. рублей. Четыре отчитывающихся оператора сообщили о 120 фактах покушения на хищение денежных средств из платежных терминалов. Ущерб от данного типа атак составил 2 млн. рублей.

Таким образом, Банком России на протяжении всего анализируемого периода зафиксированы различные способы воздействия на банкоматы и платежные терминалы:

1. Прямое подключение к банкомату технических устройств, осуществляющих управляющее воздействие на банкомат.

2. Удаленное управление банкоматом, платежным терминалом, в том числе вследствие заражения вредоносным кодом.

3. Физическое воздействие на банкомат, платежный терминал (взрыв, взлом и т.д.). [56]

Данная статистика еще раз подтверждает слабую степень защиты банкоматов и платежных терминалов от воздействия мошеннических группировок.

Также необходимо отметить, что Банк России отмечает смещение вектора атак с дистанционных платежных сервисов на информационную инфраструктуру операторов по переводу денежных средств и услуг платежной инфраструктуры. Так, результатом воздействия злоумышленников на операционную инфраструктуру кредитных организаций и платежных систем в 2015 году стали финансовые потери на сумму более 900 млн. рублей. В 2016 году 9 операторов по переводу денежных средств представили данные о несанкционированных операциях по переводу с корреспондентских счетов, открытых в расчетных центрах платежной системы ЦБ РФ денежных средств на сумму 2,18 млрд. руб. При этом окончательность перевода денежных средств наступила на сумму 1,5 млрд. рублей. Причиной осуществления указанных несанкционированных операций является воздействие вредоносного кода на объекты информационной инфраструктуры операторов по переводу денежных средств. В III – IV кварталах 2016 года 10 отчитывающихся операторов сообщили о случаях перевода кассиром денежных средств, принадлежавших работодателю, на банковские счета злоумышленников в результате побуждения работника к совершению операции путем обмана или злоупотребления доверием [57].

В 2017 году отчитывающиеся операторы направили в Банк России информацию о восьми атаках на свои процессинговые центры. В результате

доступа к автоматизированным системам процессинговых центров, изменения доступного остатка средств и установленных лимитов злоумышленники совершили покушения на хищение денежных средств на сумму 950 млн. рублей. Помимо этого, в Банк России направлена информация об одной успешной атаке на рабочее место оператора системы SWIFT. Объем несанкционированных операций в результате данной атаки составил 339,5 млн. рублей. Указанные инциденты свидетельствуют о недостаточной защищенности внутренней локальной сети кредитных организаций. В 2017 г. данные о несанкционированных операциях с корреспондентских счетов, открытых в расчетных центрах платежной системы Банка России, были представлены только двумя операторами по переводу денежных средств на общую сумму 54 млн. рублей. Причиной осуществления указанных несанкционированных операций является воздействие вредоносного кода на объекты информационной инфраструктуры операторов по переводу денежных средств. [57]

Таким образом, объемы несанкционированных операций, осуществляемых посредством ЭСП на протяжении всего анализируемого периода имели тенденцию к снижению, что свидетельствуют о переориентации злоумышленников с дистанционных платежных сервисов на информационную инфраструктуру операторов по переводу денежных средств и операторов услуг платежной инфраструктуры.

2.2. Характеристика угроз безопасности при осуществлении клиентами банков электронных банковских услуг

В настоящее время вопросы обеспечения информационной безопасности в кредитных организациях являются приоритетным направлением регулятивной и надзорной деятельности центральных банков. Такое внимание финансовых регуляторов вызвано, прежде всего, стремительным внедрением современных ИТ-технологий, что так же

привлекает интерес и внимание криминалитета. При всем при этом, с применением ИТ-технологий на данный момент осуществляется значительная доля операций, имеющих финансовые последствия, в первую очередь платежных транзакций. Проникновение информационных технологий в банковский бизнес привело к повышению удобства и скорости выполнения транзакций, снижению операционных затрат кредитных организаций, а с другой стороны потребовало внедрения процессов выявления и предотвращения несанкционированных транзакций. [38, с. 180]

Под угрозой понимают потенциально возможные воздействия на систему, которые прямо или косвенно могут нанести урон пользователю. Преднамеренные угрозы могут реализовывать как внутренние для системы участники процесса обработки данных, так и люди внешние по отношению к системе, так называемые хакеры. [38, с. 182]

Не существует общепринятой классификации угроз безопасности. Один из вариантов классификации может быть выполнен по следующим признакам:

По цели реализации:

– нарушение конфиденциальности;

– нарушение целостности данных;

– нарушение работоспособности системы.

По принципу воздействия на систему:

– с использованием доступа субъекта к объектам системы (файлу данных, каналу связи);

– с использованием скрытых каналов.

По характеру воздействия на систему:

– активное воздействие - всегда связано с выполнением каких-либо действий;

– пассивное – осуществляется путем наблюдения пользователем побочных эффектов и их последующим анализом.

По причине появления используемой ошибки защиты:

– неадекватность защиты системы;

– ошибки административного управления;

– ошибки в алгоритмах программ.

По способу воздействия на систему:

– в интерактивном режиме; [45, с. 25]

– в пакетном режиме.

По используемым средствам атаки:

– стандартное программное обеспечение;

– специально разработанные программы.

Рассмотрим наиболее популярные угрозы безопасности: атаки на клиентов кредитных организаций, атаки на операционную инфраструктуру и атаки на устройства самообслуживания.

К атакам на клиентов кредитных организаций относят следующие: Рассылка электронных сообщений, содержащих вредоносное программное обеспечение. Сообщения электронной почты, отправляются преимущественно с сайтов лжегосударственных органов власти; крупных телекоммуникационных операторов; кредитно-финансовых организаций, не имеющих лицензии Банка России на оказание предлагаемых финансовых услуг; лжебанков и страховых организаций; организаций–партнеров и с других мошеннических сайтов. В качестве содержания данных сообщений выступают: требования, поступившие от органов исполнительной власти; рассылки изменений в нормативных актах; взыскание/погашение задолженности/штрафа, оплата услуг; поиск документов для проверки. Вложения (может быть представлено в виде гиперссылки, при переходе по которой скачиваются перечисляемые вложения): исполняемый файл, замаскированный под документ; архив, содержащий в себе исполнительный файл; специально сформированный файл и файл, содержащий макровирусы.

Заражение при посещении специализированного сайта (например, сайта по бухгалтерскому учету), домен которого содержит ВПО. В общем виде подобного рода атака выглядит следующим образом:

– после заражения ВПО клиент формирует в бухгалтерской программе платежные поручения и отправляет их на экспорт для системы дистанционного банковского обслуживания. Бухгалтерская система формирует текстовый файл экспорта-импорта;[60]

– вредоносная программа отслеживает появление этого файла и производит подмену реквизитов получателя на заранее подготовленные злоумышленником. При этом название получателя остается неизменным, меняется БИК кредитной организации, номер счета, ИНН получателя. Сумма переводов, как правило, не меняется;

– клиент производит вход в систему ДБО и загружает подготовленные (и уже измененные) платежные поручения. В результате чего происходит списание денежных средств по платежным поручениям в счет преступной группировки.[60]

Разновидностями вредоносного программного обеспечения являются:

– trojan.downloader представляет собой вредоносное ПО, предназначенное для скрытой загрузки и установки на компьютер различного вредоносного ПО и троянских программ. Подобного рода ПО содержит в себе заранее прописанные имена и расположение файлов, скачиваемых загрузчиком с управляющего сервера;[59]

– trojan.encoder представляет собой вредоносное ПО, шифрующее файлы на жестком диске компьютера и требующее деньги за их расшифровку. В результате действия указанного вредоносного ПО зашифрованными могут оказаться, среди прочего, файлы *.doc, *.docx, *.pdf, *.jpg, *.rar. Отличительной особенностью некоторых рассылок является изменение вредоносного вложения с каждой итерацией рассылки;

– trojan.dropper представляет собой вредоносное ПО, предназначенное для скрытной установки на компьютер пользователя ПО,

содержащегося в теле троянской программы. В некоторых случаях пользователю приходят ложные сообщения об ошибке в ПО, при открытии файла, ошибке в архиве и т.д. Обычно вредоносное ПО сохраняется троянской программой в каталоги Windows, в том числе в системные или временные каталоги;[59]

– trojan.psw – класс вредоносных программ, предназначенных для кражи пользовательских авторизационных данных (логин и пароль, в некоторых случаях – сертификаты пользователей).

В связи с широким распространением мобильного банкинга в РФ активизировались Android-трояны. Как правило, для получения доступа к счетам владельцев телефонов под управлением ОС Android, преступники используют ВПО, работающее с системами СМС-банкинга или создающее поддельные окна приложений онлайн-банкинга.

Целью данного вредоносного программного обеспечения является сбор персональных данных о владельце смартфона или планшета и списание денежных средств со счетов в банке. Объем списанных со счетов физических лиц денежных средств посредством работы троянов за 2015-2017 гг. можно будет увидеть из таблице 2.1.

Согласно данным международной компании по предотвращению и расследованию киберпреступлений и мошенничеств – Group-IB за 2015-2017 гг. количество группировок, осуществляющих хищения денежных средств посредством троянов у физических лиц с телефонов операционной системы Android находилось в пределах от 11 ед. в 2015 году и до 8 ед. в 2017 году.

Таблица 2.1

Показатели хищения денежных средств у физических лиц Andoird-троянами за 2015-2017 гг.

Показатели	Годы			Отклонение, +/-	
	2015 г.	2016 г.	2017 г.	2016/ 2015	2017/ 2016
Количество групп, ед.	11	10	8	-1	-2
Успешных атак в день, ед.	350	300	110	-50	-190
Средняя сумма одного хищения, руб.	4000	11000	7000	7000	-4000
Средняя сумма хищений в день, млн. руб.	1,4	3,3	0,8	1,9	-2,5
Годовой объем хищений, млн. руб.	348, 6	821, 7	191, 7	473,1	-630

При этом наибольшее количество успешных атак в день наблюдалось в 2015 году – 350 ед., в последующие годы значение данного показателя уменьшилось до 110 ед. Средние показатели сумм хищений (одного/всех в день) характеризовались неоднозначной динамикой. Так, отклонения значений данных показателей в 2016 году были положительные, а в 2017 году отрицательными. Годовой объем хищений 2016 года к 2015 году вырос на 473,1 млн. руб., а уже 2017 года к 2016 году упал на 630 млн. руб.

– backdoor представляет собой вредоносное ПО, назначением которого является скрытое от пользователя удаленное управление злоумышленником компьютером жертвы. Часто подобного типа программы используются для создания ботнетов; [61]

– exploit – вредоносная программа, содержимое которой (некоторые данные, исполняемый код) позволяет использовать имеющиеся уязвимости в программном обеспечении, установленном на компьютере;

– фишинг – мошеннические письма с отсутствующими вредоносными вложениями, но содержащие различные ссылки, по которым предлагается перейти пользователю.

Годовой объем хищений у юридических лиц от фишинга можно будет увидеть из таблицы 2.2.

После полной автоматизации фишинговых атак на клиентов банков и платежных систем ущерб от их активности в России стал очень заметным. Согласно данным Group-IB за 2016-2017 гг. количество группировок осуществляющих такие рассылки в 2017 году выросло на 11 единиц и составило 26 единиц.

Таблица 2.2

Показатели хищения денежных средств у юридических лиц посредством фишинга за 2016-2017 гг.

Показатели	Годы		Отклонение, +/-
	2016 г.	2017 г.	2017/2016
Количество групп, ед.	15	26	11
Успешных атак в день, руб.	950	108	-842
Средняя сумма одного хищения, руб.	1000	1000	0,0
Средняя сумма хищений в день, млн. руб.	0,9	0,1	-0,8
Годовой объем хищений, млн. руб.	236,6	251,0	14,4

При неизменной средней суммы одного хищения в 1000 рублей, годовой объем хищений 2017 года составил 251,0 млн. руб. (отклонение по сравнению с предыдущим годом – 14,4 млн. руб.).

Мошеннические call-центры также являются угрозами безопасности, в силу наличия слабозащищённых финансово безграмотных слоев населения, которые из-за своей доверчивости добровольно сообщают злоумышленникам по телефону всю конфиденциальную информацию для списания денежных средств со счета. [61]

Также угрозами безопасности со стороны злоумышленников являются: осуществление несанкционированных операций с использованием банковских карт (в банкоматах, в организациях торговли и услуг и при осуществлении интернет-транзакций).

Для экономически активной части населения, пользующейся Интернетом, злоумышленники находят другие актуальные способы вхождения в контакт. В первую очередь – это спам-рассылки писем, содержание которых рассчитано на разные категории получателей. [61]

Это сообщения о скидках, предложения о знакомстве и другие заманчивые предложения, содержащие вредоносные файлы или ссылки на фишинговые сайты. Получив такое письмо, человек открывает файл или переходит по ссылке, в результате чего происходит заражение устройства и компрометация платежных данных его владельца.

В последнее время набирает обороты взлом аккаунтов в соцсетях с целью рассылки по списку контактов их владельцев просьб о материальной помощи от их имени. Вместе с тем по мере снижения доходов от подобного рода хищений преступники будут изыскивать новые возможности извлечения дохода, даже если для этого потребуется тщательный поиск и анализ компрометирующей информации, перехват переписки, шантаж, угрозы, вымогательство, продвинутые схемы мошенничества.

Атаки на операционную инфраструктуру представлены Reversal-атаками. Особенность данных атак заключается в обработки сообщений об отмене авторизации переводов денежных средств процессинговым центром. В большинстве случаев процессинговые центры не проверяют подлинность подобного запроса, в связи с отсутствием контроля ряда полей указанной операции. [58]

Атаки на устройства самообслуживания представлены логическими атаками (устройство не повреждается или не вскрывается, не устанавливаются дополнительные аппаратные компоненты с подключением к шинам устройства, все операции выполняются через удаленный доступ с использованием программных средств) и физическими атаками (повреждение или вскрытие устройства, установка дополнительных аппаратных компонентов, подключение внешних устройств, в том числе для возможности удаленного управления).

Основной тренд логических атак во второй половине 2016 года и первой половине 2017 года - использование программного обеспечения Cobalt Strike – средство для получения удаленного доступа к банкоматам и передача на них программного обеспечения, непосредственно взаимодействующего с XFS-фреймворком банкомата для выдачи денежных средств. После выдачи денежных средств, как правило, запускаются программы для уничтожения информации. [61]

Основные категории «физических» атак остались традиционными.

Под скиммингом понимают установку специальных технических средств, причем не обязательно в картоприемник, для хищения данных, записанных на магнитную ленту платежной карты. PIN-код, как правило, похищается с помощью отдельного технического устройства – видеокамеры или фальшивой накладки на PIN-пад.

Под шиммингом понимают установку в картоприемник специальных технических средств, предназначенных для хищения данных с EMV-чипа карты. Таким образом, похищается следующая информация: история платежей, информация содержащаяся на Track 2 карты, срок действия.

Под Black Box понимают установку либо подключение технического устройства, взаимодействующего с компонентами банкомата и отдающего последнему команду для выдачи денежных средств.[61]

Другой физической атакой является подмена процессинга. В этом случае банкомат отключается от процессинга кредитной организации и подключается к устройству, имитирующему его. Передовые устройства могут эмулировать нормальное состояние банкомата для мониторинга программного обеспечения. Так, суть атаки заключается в передаче банкомату подложных команд о выдаче денежных средств без нарушения общей логики работы банкомата и модификации его компонентов, как аппаратных, так и программных. [60]

Таким образом, наиболее часто встречаемыми угрозами безопасности клиентов кредитных организаций являются: рассылка электронных

сообщений с вредоносным программным обеспечением, воздействие мошенников методами «социальной инженерии» посредством звонков с call-центров и sms-рассылок, взлом аккаунтов в социальных сетях (шантаж, угрозы, вымогательство), осуществление несанкционированных операций с использованием платежных карт (в банкоматах, в организациях торговли и услуг и при осуществлении интернет-транзакций). В свою очередь в качестве угроз безопасности на устройства самообслуживания замечены логические и физические атаки на банкоматы и POS-терминалы.

2.3. Особенности функционирования рынка электронных банковских услуг в России

В настоящее время отечественные банки предлагают своим клиентам различные электронные услуги. Для большинства банков развитие электронных услуг стало не просто актуальным нововведением, а стратегическим направлением деятельности. Растут активы банков, объем привлеченных вкладов, капитализация банковской системы. Развитие технических средств и технологий, интернета и мобильной связи открывает все большие перспективы для развития электронного банковского обслуживания. [16, с. 400]

Сегодня при помощи смартфона, планшета или компьютера с доступом в Интернет можно осуществлять платежи по кредитам, оплачивать коммунальные услуги, налоги, штрафы; перечислять деньги со своего счета на другой; пополнять депозиты; производить блокировку/разблокировку банковской карточки; оформлять заявку на получение кредита, ипотеки; получать уведомление о приходных/расходных операциях и многое другое. Осуществление данных электронных платежей – это специализированный комплекс программных продуктов, который обеспечивает оперативные транзакции между контрагентами, либо денежные переводы от потребителей на счета поставщиков услуг и товаров.[50, с.56]

Для осуществления этих операций необходимо Интернет-соединение, наличие программы и электронного счета или кошелька. Таким образом, под электронными банковскими услугами подразумевают выпуск пластиковых карт, обеспечение банкоматами, терминалами и электронными устройствами для расчетов в торговых точках, обеспечение дистанционного банковского самообслуживания и сервис с электронными деньгами и кошельками.

В целом за 2013 - 2017 гг. российскими кредитными организациями было эмитировано 1215,5 млн. ед. платежных карт. Из них – 1062,8 млн. ед. и 152,7 млн. ед. расчетных и кредитных карт соответственно. Таким образом, наибольшую долю среди общего количества эмитированных кредитными организациями карт занимали расчетные карты, удельный вес которых колебался от 86,6 % в 2013 году и до 88,2 % в 2017 году. Объем выпуска банковских пластиковых карт за 2013-2017 гг. наглядно можно будет увидеть в таблице 2.3.

Таблица 2.3

Динамика эмитированных платежных карт отечественными коммерческими банками за 2013-2017 гг., млн. ед.

Показатели	Годы					Темп роста, %				
	2013г	2014г	2015г	2016г	2017г	2014/ 2013	2015/ 2014	2016/ 2015	2017/ 2016	2017/ 2013
Расчетные карты	188,3	195,9	214,4	224,6	239,6	104,0	109,4	104,8	106,7	127,2
Кредитные карты	29,2	31,8	29,5	30,1	32,1	108,9	92,8	102,0	106,6	109,9
Всего:	217,5	227,7	243,9	254,7	271,7	104,7	107,1	104,4	106,7	124,9

Из представленной выше таблицы 2.3 видно, что за рассматриваемый период количество расчетных карт значительно выросло. Так, значение данного показателя увеличилось на 51,3 млн. ед. или на 27,2 %. В свою очередь величина кредитных карт в течение анализируемого периода характеризовалась неоднозначной динамикой. Так, по итогу 2015 года объем выпуска кредитных карт резко снизился (уменьшение по сравнение с 2014

годом составило 2,3 млн. ед. или 7,2 %) и достиг 29,5 млн. ед. Однако, начиная с 2016 года кредитными организациями было эмитировано на 2,0 % больше по сравнению с 2015 годом, и на 6,6 % в 2017 году по сравнению с 2016 годом. Увеличение спроса на данный банковский продукт в 2016-2017 гг. было вызвано нормализацией уровня реальной заработной платы в стране на фоне снижения уровня цен, что свидетельствует об улучшении экономической ситуации в стране и оздоровлении рынка кредитных карт.

Одним из признаков, наиболее полно отражающим развитие ЭСП, в т. ч. банковских карт является критерий «доступность платежных услуг». Под данным критерием понимается возможность совершения платежей с использованием ЭСП в любое время на всей территории страны. [65]

Для осуществления любой операции, с использованием электронных средств платежа, требуются: электронное средство платежа, и/или объект платежной инфраструктуры. Таким образом, одним из показателей критерия «доступность платежных услуг» являются коэффициент доступности платежных карт. Коэффициент доступности платежных карт отражает обеспеченность населения платежными картами и рассчитывается как отношение общего количества эмитированных карт к численности населения. На основании проведенного анализа доступности платежных карт можно сказать, что в РФ на каждого человека в среднем приходится более одной банковской карты. Так, коэффициент достаточности платежных карт на протяжении всего рассматриваемого периода имел положительную динамику, отклонение данного коэффициента в 2017 году по отношению к 2013 году составило 0,33 единицы, что свидетельствует о востребованности данного ЭСП.

В отношении количества безналичных транзакций по платежным картам в России на протяжении анализируемого периода отчетливо наблюдается положительная динамика. В данном случае к безналичным операциям отнесены – операции по оплате товаров (работ, услуг), совершенные в организациях торговли и услуг, а также посредством сети

Интернет и банкоматов, таможенные платежи и прочие операции не связанные с оплатой товаров и услуг. Так, по итогам 2013 года из общего числа карточных транзакций (7 744,7 млн. ед.) 55,8 % (4 322,9 млн. ед.) составили операции по оплате товаров и услуг. В свою очередь в 2014 году их доля выросла и составила 63 % (6 366,4 млн. транзакций из 10 112,6 млн. ед.). И начиная уже со следующего года, их доля в общем количестве карточных операций начала составлять уже более двух третей, о чем свидетельствуют данные ЦБ РФ (в 2015 году - 68,9 % (9037 млн. транзакций из 13117,9 млн. ед.), в 2016 году - 72,8 % (13012,6 млн. транзакций из 17871,6 млн. ед.), а в 2017 году - 17939 млн. транзакций (74,7 % из 24005,7 млн. ед.)). Доли операций по снятию наличных денег в общем количестве транзакций по платежным картам за рассматриваемый период находились в пределах от 40,8 % в 2013 году и до 13,9 % в 2017 году, остальные доли приходились на прочие операции юридических и физических лиц. В прочие операции по данным Банка России включались безналичные операции, не связанные с оплатой товаров и услуг (например, переводы с карты на карты, переводы на благотворительные цели и т.д.). [65]

Наглядно соотношение количества операций, совершенных по картам физических и юридических лиц за 2013-2017 гг. можно будет увидеть на рис.2.12.

Увеличивается и объем безналичных транзакций по картам российских банков. Здесь также налицо устойчивый тренд медленного и плавного увеличения данного показателя при очень существенном росте общих объемов транзакций по картам.

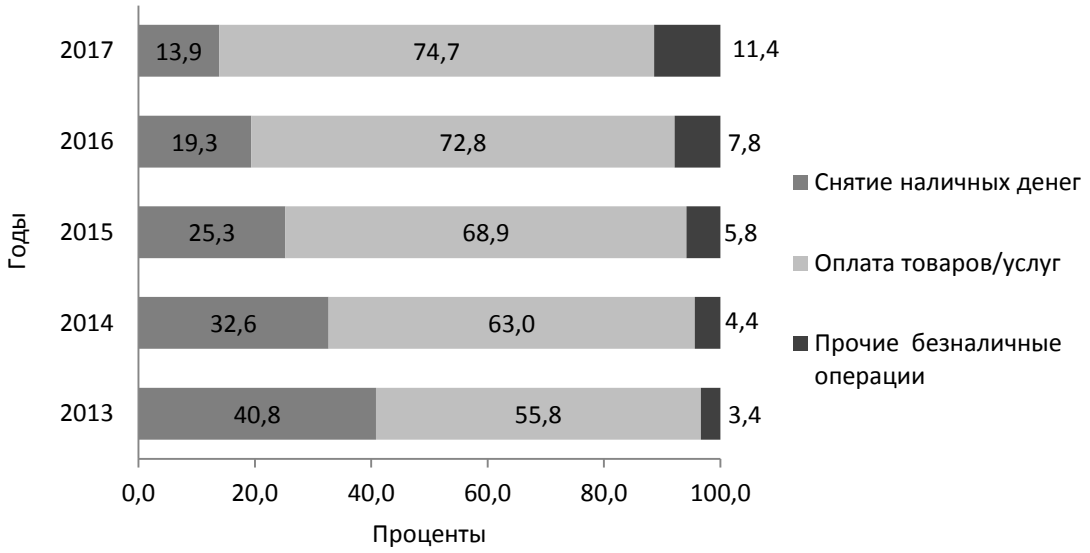

Рис.2.12. Соотношение количества банковских операций по платежным картам физических и юридических лиц за 2013-2017 гг., %

По данным ЦБ РФ, в 2013 году доля безналичных операций по оплате товаров и услуг в общем объеме карточных транзакций на рынке РФ составила 18,9 % (5597,8 млрд. руб. из общего объема 29613 млрд. руб.). При этом в 2014 году значение данного показателя увеличилось на 2,5 п.п. и составило 21,4 % (7738,9 млрд. руб. из общего объема 36130,7 млрд. руб.), в 2015 году – 23,2 % (9640,9 млрд. руб. из общего объема 41507,5 млрд. руб.), в 2016 году – 26 % (13122 млрд. руб. из общего объема 50434,9 млрд. руб.) и в 2017 году -26,9 % (17034,6 млрд. руб. из общего объема 63361,5 млрд. руб.).

На фоне роста количества платежных карт наблюдается увеличение электронных терминалов (в пунктах выдачи наличных, в организациях торговли и услуг) позволяющих оплачивать товары (работы) услуги с использованием карт без участия, уполномоченного работника кредитной организации или организации торговли (услуг) – по состоянию на 01.01.2018 года количество этих устройств увеличилось на 415, 3 тыс. единиц (прирост за 2017 год – 21,2 %) и достигло величины 2 372,6 тыс. единиц. За период с 2013 по 2017 годы количество электронных терминалов увеличилось в 2,1 раза. Напротив, количество банкоматов, за рассматриваемый период

сократилось на 31,1 тыс. единиц, достигнув величины 206,3 тыс. устройств (рис.2.13).

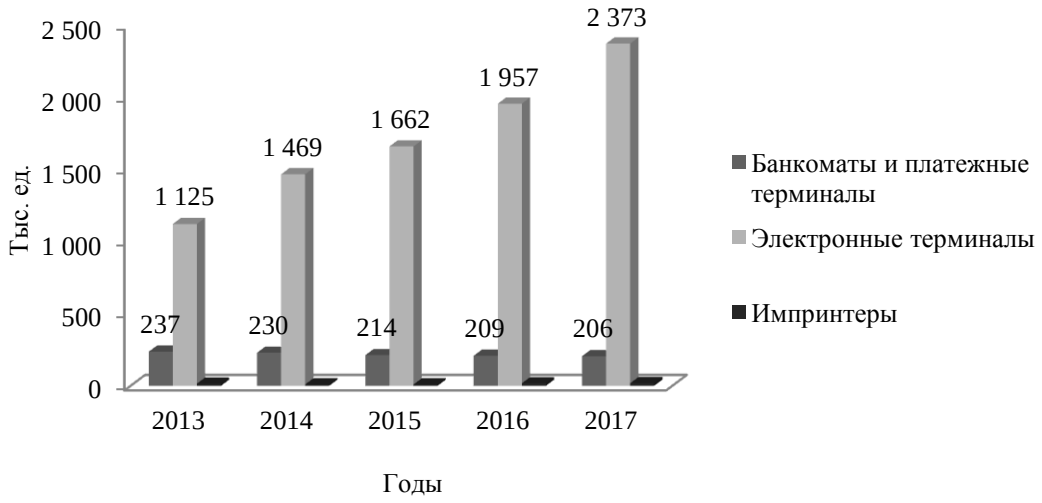

Рис.2.13. Динамика количества банкоматов, электронных терминалов и импринтеров за 2013-2017 гг.

Также необходимо отметить, что количество импринтеров, используемых преимущественно в качестве резервных устройств за рассматриваемый период изменилось незначительно в силу устаревания технологии осуществления платежных операций. Так, в 2013 году их количество составило 15 тыс. ед., а по итогам 2017 года достигло величины в 18 тыс. единиц. [65]

Подтверждением доступности удаленных каналов самообслуживания (банкоматов и электронных терминалов) может послужить расчет следующих коэффициентов:

Коэффициент доступности банкоматов рассчитывается как отношение общего количества банкоматов к численности населения.

Для сопоставимости данных, при расчете коэффициента доступности рассчитывается количество банкоматов на 1000 человек в стране.

Коэффициент доступности POS – терминалов рассчитывается как отношение общего количества POS – терминалов к численности населения.

Для сопоставимости данных, при расчете коэффициента доступности рассчитывается количество POS – терминалов на 1000 человек в стране.

Изменения обеспеченности населения банкоматами и электронными терминалами представлены на рисунке 2.15.

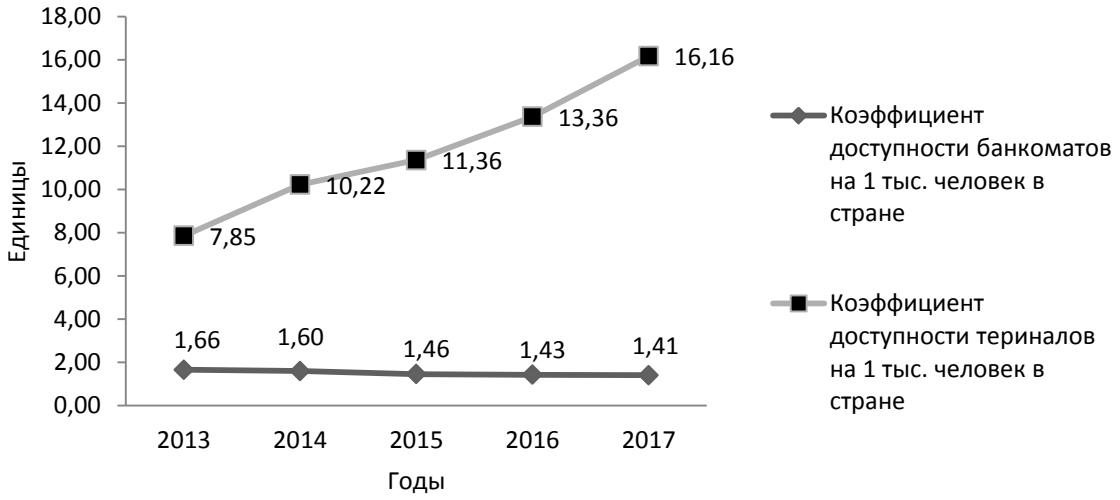

Рис.2.15. Изменения коэффициентов доступности банкоматов и электронных терминалов коммерческих банков в России за 2013-2017 гг., ед.

Из представленных выше сведений можно заключить, что непрерывное увеличение коэффициента доступности сети электронных терминалов для оплаты и сокращение коэффициента доступности банкоматов за 2013-2017 гг., может способствовать расширению безналичного платежного оборота в стране в силу удобства оплаты посредством данного устройства самообслуживания.

За период с 2013 - 2017 гг. количество открытых в банках расчетных счетов возросло в 1,2 раза. При этом наибольший удельный вес в структуре открытых счетов на протяжении всего анализируемого периода занимали счета открытые физическим лицам. [65]

Их доля в общем объеме, открытых счетов на протяжении уже многих лет находится в пределах от 98 % до 99 %. Так, в 2017 году в отечественных коммерческих банках было открыто более 883 млн. счетов, из них более 8 млн. счетов юридических лиц и около 875 млн. счетов физических лиц. [65]

Из статистических данных ЦБ РФ можно предположить, что прирост количества открытых расчетных счетов как физическим, так и юридическим лицам в период развития электронного общества влечет за собой увеличение объема предоставления банковских услуг посредством систем ДБО. Подтверждением этому является увеличение объема счетов, открытых юридическим и физическим лицам, с дистанционным доступом на 93,6 % или на 104,7 млн. ед. в анализируемом периоде. При этом доля счетов с дистанционным доступом, открытым корпоративным клиентам за 2013-2017 гг. не поднималась выше показателя в 2,8 % от общего количества счетов с дистанционным доступом.

Так, в 2013 году 82 % платежных поручений юридических лиц и 54 % платежных поручений физических лиц были совершены в электронной форме, то есть с использованием дистанционных каналов обслуживания (через сеть Интернет, посредством сообщений с использованием абонентских устройств мобильной связи), однако уже к концу 2017 года можно заметить увеличение доли таких платежей до 94 % у юридических лиц и до 69 % у физических лиц из общего числа платежных поручений (приложение 1). Также необходимо отметить, что в рассматриваемом периоде наблюдается прирост платежей по платежным поручениям, переданных через сеть Интернет вышеуказанными лицами в количественном и в суммовом выражениях. [65]

Так, в количественном выражении юридическими и физическими лицами через сеть Интернет в 2017 году было направлено – 1254,9 млн. ед. платежных поручений (прирост по сравнению с 2013 годом составил 67,9 %), в том числе прирост количества платежей, поступивших от юридических и физических лиц, составил 71 % и 40,4 % соответственно (приложения 2,3).

С развитием системы мобильного банкинга растет и количество потребителей данного вида услуг (рис. 2.16).

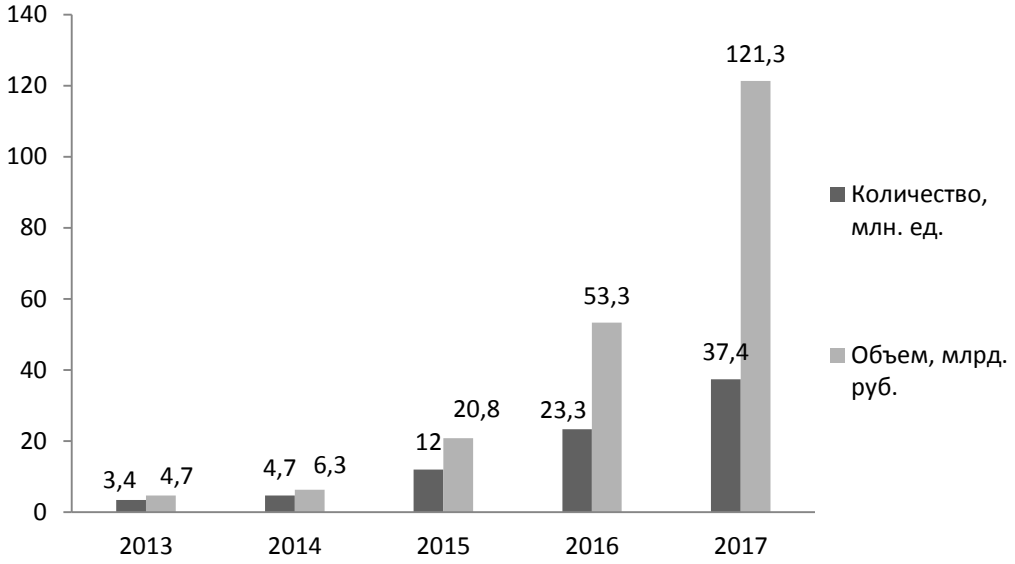

Рис.2.16. Распоряжения по платежам физических лиц, поданные в кредитные организации посредством сообщений с использованием абонентских устройств мобильной связи за 2013-2017гг.

На протяжении всего анализируемого периода посредством сообщений с использованием абонентских устройств мобильной связи физическими лицами было совершено 80,8 млн. ед. операций на общую сумму 206,4 млрд. рублей. Причем, за последние пять лет объем, и количество таких операций имели только положительную динамику. Распоряжения на основной объем средств по-прежнему поступают от физических лиц в бумажном виде. Это свидетельствует о пока ещё недостаточной степени доверия потребителя к использованию мобильного банкинга. Но, несмотря на это удельный вес таких платежей постоянно уменьшается. По данным ЦБ РФ, в 2013 году доля платежных поручений, поступивших от физических в бумажном виде в общем объеме платежей составила 78,7 %, в то время как в последующие годы составляла – 72,4 % в 2014 году, 70,2 % в 2015 году, 67,0 % в 2016 году и 66,9 % в 2017 году. [65]

Помимо прочего нельзя не сказать о суммовом приросте платежных поручений, поступивших через сеть Интернет от юридических и физических лиц. Так, у юридических и физических лиц в 2017 году по платежным поручениям, переданным через сеть Интернет со счета было списано

413497,7 млрд. руб. (прирост объема платежей 44,9 % по сравнению с 2013 годом), что свидетельствует о положительной динамики данного показателя, и, следовательно, о популярности данной формы расчета.

Говоря об электронных платежах, стоит сказать о банках, посредством которых и осуществляются такие платежи. Сведения об эффективности мобильного и интернет-банкинга получены в результате ряда проведенных исследований консалтинговым агентством Markswebb. Согласно данному исследованию лучшими мобильными банками для смартфонов IPhone и Android в 2017 году стали приложения Тинькофф банка, Бинбанка, Альфа-банка, Почта-банка и Сбербанка. Возможность провести оплату без физического наличия карты – с помощью мобильного телефона или умных часов – имеют клиенты всех вышеперечисленных банков. Такие банки, как АО «Альфа-банк», АО «Русский Стандарт», ПАО «Банк ВТБ» запустили приложения, которые позиционируются как персональный финансовый помощник. Приложение анализирует все расходы клиента по картам, ведет их статистику и дает советы. Главным преимуществом таких банковских приложений является то, что в отличие от сторонних программ, в них не надо вносить данные вручную, все доходы и расходы структурируются автоматически. Наиболее эффективными интернет-банками для физических лиц с точки зрения удобства интерфейсов и функциональности были признаны интернет-банки Бинбанка, Тинькофф банка, Промсвязьбанка, Альфа-Банка и ВТБ. Теперь к личному кабинету можно подключать карты разных банков – такую возможность дает клиентам АО «Тинькофф», АО «Русский Стандарт» (в рамках приложения «Банк в кармане») и ПАО «Сбербанк» (в рамках приложения «Кошелек»). Такой виртуальный кошелек становится аналогом обычного, в котором у многих людей хранятся карты сразу нескольких банков – зарплатная, кредитная, карта с кэшбэк, карта с накоплением миль авиакомпаний и так далее. Подключение карт разных банков к одному личному кабинету – это очень ценная возможность, поскольку значительно упрощает контроль за всеми финансами. В свою

очередь наиболее эффективными интернет-банками для юридических лиц стали: Точка, Модульбанк и Тинькофф банк, преимуществами, которых является возможность ведения бухгалтерии и выставления счетов контрагентам. [63]

В результате проведенного анализа безопасности электронного банкинга в Российской Федерации было выявлено изменение объема несанкционированных операций, как с использованием платежных карт, так и со счетов юридических лиц, осуществляемых посредством ДБО. Так, значения данных показателей на протяжении всего анализируемого периода имели тенденцию к снижению, что может свидетельствовать о слаженной работе ФинЦЕРТ с участниками информационного обмена.

В качестве угроз безопасности, воздействующих на объемы несанкционированных операций ФинЦЕРТ были обнаружены: рассылка электронных сообщений с вредоносным программным обеспечением, осуществление несанкционированных операций с использованием платежных карт (в банкоматах, в организациях торговли и услуг и при осуществлении интернет-транзакций), а также физические атаки на устройства самообслуживания.

Результатом проведенного исследования современной практики функционирования рынка электронных банковских услуг в России стало выявление роста количества расчетных банковских карт и вместе с ними доли безналичных операций по оплате товаров и услуг. В свою очередь, увеличение количества электронных терминалов при уменьшении количества банкоматов и платежных терминалов свидетельствует о продолжении формирования в российском банковском бизнесе тенденции замены операционистов – кассиров электронными терминалами. В свою очередь увеличение количества открытых счетов с дистанционным доступом и операций по ним обусловлено улучшением качества предоставляемых сервисов дистанционного банковского обслуживания, а также повышающимся спросом на их использование со стороны населения.

ГЛАВА 3. ПЕРСПЕКТИВЫ РАЗВИТИЯ ЭЛЕКТРОННЫХ БАНКОВСКИХ УСЛУГ В ИННОВАЦИОННОМ РАЗВИТИИ ОТЕЧЕСТВЕННОГО БАНКОВСКОГО СЕКТОРА

3.1.Стратегия развития национальной платежной системы в условиях санкций

В условиях глобализации каждое государство должно формировать эффективную суверенную экономическую политику. При этом особую значимость для РФ приобретают санкции в обеспечении роста конкурентоспособности нашей национальной экономики. Очень важно не создать предпосылок для оттока капитала, а, напротив, нарастить инвестиционный потенциал страны. Учитывая тот факт, что стратегия развития должна быть упреждающей направленности, требуется внимательное изучение последствий принимаемых решений. В сложившихся условиях вопросы экономической безопасности приобретают дополнительную актуальность. Государство должно определить степень свободы рынка, но при этом роль самого государства нельзя недооценивать. Национальная безопасность в сложившейся ситуации основана в первую очередь, на той роли, которую играет государство в экономике страны. И банковские платежи, и реестр владельцев карт позволяют судить о многих процессах, происходящих в государстве. При этом доступ к этой информации носит стратегический характер. Тем более стратегической является информация о представителях бюджетной сферы, среди которых: военные, представители спецслужб и правоохранительных органов. Только то, что эти люди находятся в реестрах зарубежных платёжных систем уже влечёт за собой определенные риски. Банковские трансакции позволяют судить о передвижениях, предпочтениях и уровне благосостояния таких работников. Кроме того, данные о размерах начисляемых сумм содержат информацию об экономических процессах в бюджетной сфере, тем более что

размеры таких выплат прямо указывают на место работника в государственной иерархии.

С каждым годом рынок платежных систем стремительно развивается, и каждому государству важно не упускать контроль над финансовыми ресурсами страны и ее граждан и, в особенности, не позволять международным платежным системам злоупотреблять правом и нарушать принятые на себя обязательства. Ни один сегмент в отрасли банковских услуг не затрагивает массы населения в таком большом количестве, как банковские карты и розничные платежные услуги. Развитие в России национальной системы платежных карт имеет государственное значение.

На современном платежном рынке России прослеживаются следующие тенденции: фрагментация рынка по размеру активов; рост количества средних и малых предприятий; переход обслуживания клиентов на удаленные каналы; использование межбанковских систем расчетов и электронных систем; разделение на базовую услугу и дополнительные сервисы; появление нового типа регулирования на финансовом рынке.

Наличие этих тенденций указывает на явную переориентацию экономики России, на безналичную экономику. Система розничных платежей становится все более актуальной и приобретает новые грани с развитием новых платежных эквайринговых услуг. Как утверждает Арутюнян А. В. «состояние современной системы розничных платежей характеризуется тенденцией постепенного сокращения доли наличных и ростом доли безналичных платежей». Безналичные расчеты это часть экономики, обеспечивающая перечисление валюты конкретно со счета предприятия, которое платит на счет предприятия, получающего средства. В этих расчетах банк выступает финансовым посредником. Услуги, которые он предоставляет своим клиентам организациям, предпринимателям и физическим лицам являются важным аспектом современной экономической системы. Порядок безналичных расчетов регламентирован законодательством. Осуществление расчетных операций через банк снижает

потребность в наличных деньгах, это способствует концентрации в банке свободных денежных средств для кредитования, обеспечивает их сохранность и более эффективное использование, а это в свою очередь оптимизирует и ускоряет денежный оборот государства в целом.

Участники безналичных расчетов могут открывать счета во всех банках Российской Федерации и осуществлять деятельность в порядке, установленном нормативно- правовыми актами ЦБ РФ и другими актами российского законодательства. Положение Банка России «О правилах осуществления перевода денежных средств», предусматривает создание счетов для учета средств в расчетах по конкретным операциям. Данным нормативно-правовым актом закреплены следующие формы безналичных расчетов: расчеты платежными поручениями, расчеты по аккредитиву, расчеты инкассовыми поручениями, расчеты чеками, расчеты в форме перевода денежных средств по требованию получателя средств, расчеты в форме перевода электронных денежных средств.

Счета по таким операциям как расчетные чеки и аккредитивы предприятия открывают в том банке, который их обслуживает, на основании заявления на аккредитив, или заявления на перечисление средств и т.п. Безналичный оборот является структурным элементом денежного оборота. Основным условием организации эффективного безналичного оборота розничных платежей является их законодательное регулирование. Основным правовым актом в сфере электронных и безналичных платежей как было сказано ранее является Федеральный закон «О национальной платежной системе», вступивший в силу 27 июня 2011 г. Именно этим нормативно-правовым актом урегулированы правила функционирования электронных платежей, в том числе операции с пластиковыми картами и электронными кошельками.

Национальная система платежных карт России была создана 23 июля 2014 г., и функционирует в рамках правового поля, урегулированного

Федеральным законом № 161-ФЗ «О национальной платежной системе», Стратегией развития Национальной платежной системы.

Основным средством осуществления безналичных операций на сегодняшний день являются: платежные карты и мобильный банкинг. К наиболее крупным платежным системам относят: «Visa», «MasterCard», «Diners Club International», «American Express», «JCB». Эти гиганты на рынке платежных систем утверждают общие правила международных платежных систем, изучают и контролируют деятельность международного рынка. Самыми распространёнными платёжными система во всем мире являются «Visa» и «MasterCard». Две американские компании прочно занимают лидирующие позиции, причем платежные инструменты обеих компаний обладают практически одинаковым функционалом. Кроме того, «Visa», как и «MasterCard» являются американскими брендами. Однако сервис «MasterCard» сосредоточился в основном на европейском рынке, причем в качестве основной валюты он использует евро. Тогда как «Visa» сохраняет верность американскому доллару и американскому рынку.

Цифровизация финансового и банковского сектора России в последние несколько лет, эффективно влияют на форсирование развития слаженной деятельности Национальной платежной системы (НПС). В 2017 году частота использования платежных карт в точках продаж выросла на 38% по сравнению с 2016 годом. То есть россияне начали использовать карты по их прямому назначению проведению безналичных расчетов непосредственно в точках продаж товаров и услуг, вместо ранее популярной услуги снятия наличных средств. В соответствии с докладом директора департамента Национальной платежной системы Банка России к концу 2018 года в России ожидается рост объема безналичных розничных платежей свыше 45% .Это объясняется устойчивым ростом объема безналичных платежей, связанным с появлением новых игроков в карточном сегменте валютно - банковского рынка, и как следствие усложнением структуры рынка. Среди других важных

причин роста безналичных платежей названы популярность дистанционных каналов (интернет, мобильные приложения).

Однако наиболее важным фактором является популярность банковских карт среди населения и постоянная модернизация и оптимизация карточных услуг (выгодные тарифы, кэшбэк и другие).

Ведущим участником национальной платежной системы России является платежная система «Мир», разработанная в целях обеспечения надежности, безопасности, удобства и доступности национальных платежных инструментов - платежных карт «Мир». Создание, выпуск и организация приема национальных платежных карт в России было продиктовано необходимостью обеспечения финансового суверенитета РФ, вызванного уязвимостью российской банковской системы, проявившейся в результате санкционного режима США в отношении России. Так, в марте 2014 года основные международные платежные системы Visa и MasterCard, присоединившись к режиму международных антироссийских санкций, заблокировали работу карт Банка «Россия» и СМП-банка и подконтрольных им банковских учреждений на территории России и Крыма. В связи с этим возникла крайняя необходимость в краткие сроки разработать и запустить альтернативную национальную платежную систему, которая бы отвечала всем требованиям международной финансовой безопасности и вернула бы россиянам комфорт использования эквайринговых и карточных банковских услуг. Сегодня основная задача Банка России наращивание операций по картам «Мир» и увеличение количества выпущенных в оборот платежных карт. Развитию системы платежных карт «Мир» сопутствует и соответствующее законодательное регулирование. Так, в апреле 2017 года Государственная Дума приняла Федеральный закон № 88-ФЗ «О внесении изменений в статью 16.1 Закона Российской Федерации «О защите прав потребителей» и Федеральный закон «О национальной платежной системе» от 01.05.2017, в соответствии с которым установлены четкие сроки перехода банков на выплаты клиентам-физическим лицам на карты «Мир».

С 1 июля 2018 г. все выплаты из государственного бюджета должны осуществляться только на банковские счета, привязанные к платежным картам национальной платежной системы «Мир». Динамичное развитие этой платежной системы, дополненное совершенствованием платежных сервисов на базе современных технологий поспособствовало повышению уровня доступности платежных услуг и росту безналичных розничных операций. При этом эффективность платежной системы «Мир» в России была доказана в наиболее кратчайшие сроки. В связи с чем, в рамках общей интеграции России в ЕАЭС, Национальная система платежных карт намерена до конца 2019 года обеспечить прием карт «Мир» на территории Евразийского экономического союза. То есть основная стратегия развития НПС – выход на международный уровень обслуживания клиентов. В России развитию отрасли безналичных платежей сопутствует и активное развитие отрасли электронных денег. Так, в 2009 г. была учреждена Ассоциация «Электронные деньги», которая объединила основных участников российского рынка электронных платежей: «Яндекс.Деньги»,QIWI, WebMoney, iFree, Национальную ассоциацию участников электронной торговли и Национальное партнерство участников микрофинансового рынка. Основная цель Ассоциации развитие рынка электронных денег в качестве общедоступной финансовой услуги. Помимо технологической основы и эффективного законодательного регулирования системы безналичных розничных платежей, существует еще целый ряд преимуществ для пользователей/клиентов, которые собственно формируют спрос на развитие и наращивание оборота безналичных операций. Основные преимущества безналичных розничных расчетов:

1) прогрессирующее развитие системы дистанционного банковского обслуживания в России и мире;

2) систематический рост ассортимента товаров и услуг, которые доступны для покупки через Интернет;

3) увеличение количества и популяризация банковских программ и услуг в области безналичных расчетов (специальные акции, дополнительные услуги);

4) популяризация сервиса кобрендинговых карт с дополнительными скидками и бонусами.

Развитие безналичных платежей является одним из приоритетов развития национальной стратегии финансового сектора, поскольку бесконтрольный оборот наличных денег в национальной экономике является благоприятной средой для теневой экономики и стимулом для развития коррупции в государственных и муниципальных органах. Также наличные средства обычно используются в других криминальных целях – финансирование терроризма, контрабанды, стимулирование развития нелегальной миграции и трудоустройства, поэтому очевиден и такой «плюс» безналичных расчетов–как четкая контролируемость фискальными службами финансового состояния отправителя и получателя платежа.

Основными драйверами развития рынка безналичных платежей в России являются:

1) появление на рынке платежных технологий новых игроков, а именно национальной платежной системы «Мир», заменившей мировые аналоги Visa и MasterCard;

2) развитие национальной законодательной базы;

3) модернизация программ лояльности банков (бонусные программы, услуги cash-back);

4) развитие онлайн-торговли;

5) развитие технологичности и цифровизация банковского сектора;

6) повсеместное использование смартфонов и других девайсов, поддерживающих новые платежные технологии.

Развитие системы безналичных платежей стимулирует и научно-технический прогресс, а именно создание нового оборудования и разработка нового программного обеспечения. Такие технологии не только отвечают

новым запросам пользователей, но и должны отвечать систематически развивающейся законодательной базе. Развитие технологий в области эквайринга продиктовано не только запросом потребителей, но владельцев торговых предприятий, которые являются основным пользователем услуг эквайринга. Поскольку спрос таких клиентов на различные виды услуг растет, то и разработчики, и поставщики решений эквайринга должны постоянно развиваться, чтобы удовлетворить потребности рынка новыми высокотехнологичными сервисами. Развитию рынка эквайринговых услуг также сопутствует прогрессирующее сотрудничество банков и поставщиками платежных услуг в нескольких приоритетных направлениях – аутсорсинг эквайринговых услуг, техническое и программное обеспечение эквайринговых услуг банков, продажа эквайринговых услуг банков.

Таким образом, национальная платежная система является важным элементом в финансовой системе, обеспечивающим экономическую безопасность страны, а также экономический суверенитет в условиях глобализации и интеграции России в мировую экономику. Развитие национальной платежной системе позволит укрепить экономику страны и усилить позиции России на международной арене.

3.2. Направления повышения безопасности электронных банковских услуг

Противодействие угрозам безопасности электронных банковских услуг должно рассматриваться в контексте объекта, на который направлена эта угроза. То есть для определения направлений повышения безопасности электронных банковских услуг необходимо описание предметного воздействия на юридическое или физическое лицо, субъект национальной платежной системы, банкомат или терминал.

Так, для обеспечения безопасности внутренней информационной инфраструктуры организаций от воздействия вредоносного программного обеспечения, рассылаемого электронным способом на корпоративную почту организаций или их сотрудников необходимо выполнять следующие мероприятия:

1. проводить обучение среди работников организаций по вопросам обеспечения информационной безопасности, осуществлять контроль знаний работников (выборочные проверки службой информационной безопасности алгоритма действий сотрудника при получении фишингового электронного письма), а также проводить иные мероприятия, направленные на повышение грамотности работников в области информационной безопасности.

2. установить запрет на использование учетных записей с расширенными правами доступа, если это не входит в круг должностных обязанностей работника; установить запрет для работника на управление средствами антивирусной защиты; контролировать и проверять средствами антивирусной защиты внешние носители информации, а также своевременно обновлять антивирусные базы и сигнатур хостовых систем обнаружения вторжений.

3. осуществлять проверки SPF записи (текстовой записи в системе доменных имен, в которой указано с каких почтовых серверов может быть отправлена почта для домена), использовать почтовые средства антивирусной защиты и спам-листы. Наиболее эффективным способом борьбы со спамом можно считать наличие в организации специализированных решений по проверке почты и оперативное добавление адресатов в списки нежелательных отправителей на почтовом шлюзе.

При подозрении на вложение, содержащее вредоносное ПО, целесообразно изъятие указанного вложения из электронного письма и перемещение его в «карантин». При этом, доставляя электронное письмо до конечного пользователя, необходимо информировать его об изъятии подозрительного вложения. В случае необходимости восстановления

(разблокировки) вложения дать рекомендацию обратиться в подразделение, отвечающее за обеспечение информационной безопасности в организации.

Помимо данного способа заражения системы информационной инфраструктуры организаций (посредством электронных рассылок) существует также и другая возможность заражения - при посещении скомпрометированных бухгалтерских и финансовых сайтов в сети Интернет.

Мероприятиями по противодействию подобным атакам со стороны кредитной организации являются:

– настройка правил антифрода, учитывающего типовые платежи клиента;

– предупреждение клиента в случаях, если совершаемые платежи вызывают срабатывание правил антифрода;

– оповещение всех клиентов о данном способе хищений, с указанием мер противодействия со стороны клиента.

Мероприятиями по противодействию со стороны клиента являются:

– использовать антивирусное программное обеспечение; поддерживать его базы в актуальном состоянии, не реже одного раза в неделю проводить полное сканирование системы;

– выполнять все рекомендации по работе с вложениями, пришедшими из подозрительных источников, не открывать вложения – исполняемые файлы и не включать макросы в документах Microsoft Office, если нет уверенности в надежности отправителя;

– постоянная визуальная проверка в системе ДБО всех реквизитов платежных поручений, подготовленных в бухгалтерской системе. Отказ в подтверждении вызывающих сомнение платежей до выяснения всех обстоятельств;

– изменение наименования файлов выгрузки платежных поручений штатными средствами бухгалтерской системы.

Так, способами минимизации потерь от воздействия мошеннических call- центров на счета физических лиц являются: со стороны Банка России и сотовых операторов - совместный контроль и блокировка номеров сотых телефонов в случае выявления проведения мошеннических операций. Представим сценарии, по которым может работать злоумышленник. На сотовый номер жертвы отправляется текстовое сообщение:

1 сценарий – «Совершена покупка на сумму 5000 рублей в интернет-магазине, если вы не проводили операцию, то перезвоните в службу безопасности».

2 сценарий - «Карта заблокирована, если вы не проводили операцию – позвоните по номеру 8-800».

В данном случае, целью злоумышленника является создание стрессовой ситуации, согласно которой клиент, не совершавший подобную банковскую операцию, будет осуществлять дозвон по указанному в сообщении номеру.

Таким образом, чтобы повысить безопасность электронных банковских услуг физическому лицу в описанной ситуации необходимо не сообщать персональные данные или информацию о банковской карте (после сообщения или звонка с call-центра), а позвонить в кредитную организацию и донести о данном факте мошенничества.

Порядок действий в отношении спам-рассылок описан в общих рекомендациях памятки ЦБ РФ «О мерах безопасного использования банковских карт». Так, не рекомендуется отвечать на письма подозрительного содержания от имени кредитной организации, в которых предлагается предоставить персональные данные. Не следует переходить по «ссылкам», указанным в письмах (включая ссылки на сайт кредитной организации), т.к. они могут вести на сайты-двойники.

В связи с вышеуказанным мерами безопасного использования банковских карт являются:

1. неразглашение конфиденциальной информации третьим лицам (не сообщайте ПИН-код, реквизиты банковской карты, CVC/CVV2 код);

2. использование банковской карты только ее владельцем (запрещается передача банковской карты в пользование третьим лицам);

3. установка суточного лимита на сумму операций по банковской карте и одновременно подключение электронной услуги оповещения о проведенных операциях с целью предотвращения неправомерных действий по снятию денежных средств;

4. осуществление взаимодействия с кредитной организацией только по реквизитам связи, указанным в документах, полученных непосредственно в кредитной организации;

5. незамедлительная блокировка банковской карты в случае ее утраты.

Банкомат, как и другие объекты, находится под пристальным вниманием мошенников, желающих получить «легкую наживу». В соответствии с этим при осуществлении операций в банкомате необходимо выполнять следующие рекомендации:

1. осуществлять операции с использованием банкоматов, установленных в безопасных местах (в отделениях банков, в государственных учреждениях, в крупных торговых комплексах и т. п.);

2. не использовать устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат;

3. набирать ПИН-код таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН–код прикрывать клавиатуру рукой;

4. не использовать банкомат в случае некорректной его работы;

5. после выдачи наличности осуществить ее пересчет, забрать банковскую карту и чек и только после этого отходить от банкомата;

6. сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету;

7. не прислушиваться к советам третьих лиц, а также не принимать их помощь при проведении операций с банковской картой в банкоматах;

8. если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту), которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.

При осуществлении безналичной оплаты товаров и услуг также может возникнуть риск незаконного списания денежных средств со счета. Однако при выполнении определенных рекомендаций, вероятность совершения данных операций минимизируется или сведется на нет.

1. не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия;

2. требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте;

3. при использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН-код. Перед набором ПИН-кода следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке;

4. в случае если при попытке оплаты банковской картой имела место “неуспешная” операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

Рекомендации при совершении операций с банковской картой через сеть Интернет:

1. не используйте ПИН-код при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу;

2. не сообщайте персональные данные или информацию о банковской (ом) карте (счете) через сеть Интернет, например ПИН-код, пароли доступа к ресурсам банка, срок действия банковской карты, кредитные лимиты, историю операций, персональные данные;

3. с целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет использовать отдельную банковскую карту (так называемую виртуальную карту) с предельным лимитом, предназначенную только для указанной цели и не позволяющую проводить с ее использованием операции в организациях торговли и услуг;

4. следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг;

5. обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий;

6. рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о банковской(ом) карте (счете). В случае если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки);

7. установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых программных продуктов (операционной системы и

прикладных программ), это может защитить от проникновения вредоносного программного обеспечения.

Помимо вышеназванных рекомендаций по повышению безопасности электронных банковских услуг при использовании банковской карты необходимо сделать акцент на проведение разного рода мероприятий, посвященных тематики: «Киберграмотность и киберкультура населения». Реализация данной программы может осуществляться: в территориальных учреждениях Банка России (проведение открытых дверей, тематикой которых будет являться финансовая культура), в кредитных организациях (путем доведения до клиентов банка информации, касающейся киберпреступности, раздача тематических листовок), в учебных заведениях высшего и среднего звена (проведение просветительских семинаров о безопасности платежных услуг и кибербезопасности в целом) и т.п.

Общими мерами по противодействию reversal-атакам являются следующие:

– контроль доступа и предоставления прав доступа к системам, с использованием которых осуществляется передача платежных сообщений;

– контроль соблюдения порядка формирования, удостоверения, передачи операционному центру платежной системы электронных сообщений;

– контроль доступа работников к проведению операций reversal;

– сверка реквизитов операций отмены и исходной операции, в частности, следующих полей электронных сообщений: идентификатор эквайера, идентификатор транзакции, Retrieval Reference Number (RRN), AIR – код авторизации;

– контроль нетипичных операций reversal, а также аномальных изменений расходного лимита;

– мониторинг нештатного функционирования объектов инфраструктуры;

– своевременная установка обновлений ПО процессинговых центров.

В связи с ростом физических атак злоумышленников на устройства самообслуживания (скимминг, шимминг, BlackBox) лицам, осуществляющим банковские операции стоит проявлять бдительность.

Перед использованием банкомата необходимо осмотреть его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН-кода и в месте, предназначенном для приема карт.

В случае если клавиатура или место для приема карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержаться от использования банковской карты в данном банкомате и сообщить о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.

Таким образом, направлениями повышения безопасности электронных банковских услуг являются проведение целого комплекса мероприятий, в отношении той или иной угрозы безопасности. Исходя из этого выполнение какого-то определенного условия из предложенного алгоритма действий не будет способствовать предотвращению ряда осуществляемых злоумышленниками атак.

3.3 Пути внедрения и использования электронных технологий в банковском бизнесе

Благодаря технологическому прогрессу, развитию инфокоммуникационных технологий и интернету возникло понятие «цифровая экономика». Считается, что «цифровая экономика» является не чем иным, как экономической деятельностью, основанной на цифровых технологиях. При этом речь идет не столько о разработке или продажи программного обеспечения, а сколько об электронных товарах и услугах,

производимых электронным бизнесом и электронной коммерцией. В этом случае все что можно купить и продать не отходя от компьютера, получить и использовать через компьютер (планшет, смартфон) – все это электронные продукты, составляющие цифровую (электронную) экономику. На основании этого, необходимо отметить присутствие цифровизации во всех сферах экономики и в т. ч. в банковском бизнесе.

Так, с развитием мобильного банкинга получили свое распространение технологии NFC – это способ беспроводной связи, осуществляемой на высокой частоте и позволяющей обмениваться данными между устройствами, находящимися на небольшом расстоянии. С ее помощью достаточно приложить устройство со смарт-чипом к устройству-считывателю для проведения операции. Для осуществления бесконтактной оплаты без участия телефона необходимо иметь для оплаты банковскую карту с технологией: PayWave от «Visa» или PayPass от «MasterCard».

Новая технология упрощает и делает более удобными для потребителей разнообразные платежи, обмен цифровым контентом и соединение всевозможных электронных гаджетов. Платёж на сумму менее 1000 рублей можно провести без введения пин-кода, просто поднесся карту к устройству считывателю. Специалисты считают, что NFC обладает большим потенциалом, особенно если эта технология связи будет реализована в устройствах мобильной связи. NFC-технология способна заменить разнообразные бесконтактные технологии в таких областях, как контроль доступа в различные помещения, мобильные платежи, в области обеспечения программ скидок, сбора и обмена информацией, здравоохранения и потребительской электроники. Основными преимуществами данной технологии являются быстрота проведения операций на маленькие суммы (до 1000 рублей) и уменьшение износа при механическом воздействии банковской карты. В свою очередь к недостаткам данной технологии относят: немногочисленность устройств, поддерживающих данную технологию и действия мошенников.

Разновидностью бесконтактного взаимодействия является применение подкожного NFC-микрочипа. Данный чип представляет собой радиочастотные метки (RFID), которые можно считать с помощью специального оборудования. Такие системы разделяют на три вида в зависимости от расстояния, на котором они способны считывать данные:

1. ближние – до 20 см.
2. средние – от 20 см. до 5 м.
3. дальние – от 5 м. до 300 м.

Имплантируют устройство с технологией NFC преимущественно между большим и указательным пальцем. Достоинства применения NFC-чипов заключаются в их универсальности и широте сферы применения, нежели у традиционных систем контроля доступа по магнитным пропускам, отпечаткам пальцев или ладоней. Так, данные устройства заменяют кредитные карты, визитки, ключи, пропуска на работу и др. Но, несмотря на это официальное применение данных технологий в России еще не возможно в силу отсутствия на это сертификации.

С целью обеспечения высокого уровня безопасности транзакций по картам в сети Интернет была разработана система 3-D Secure (Verified by Visa/MasterCard SecureCode). Для согласования всех осуществляющих платежей в данной системе участвуют три домена: банк-эмитент, платежная система, банк-эквайер. Алгоритм действий при совершении оплаты товаров (услуг) в интернет-магазине, участвующем в программе 3-D Secure выглядит следующим образом: после выбора покупки необходимо нажать кнопку оплатить или оформить платеж, после чего произойдет переадресация на платежную страницу банка-эквайера, обслуживающего интернет-магазин. Для осуществления оплаты покупателю будет предложено ввести реквизиты карты, а также при необходимости - данные кода проверки подлинности карты (CVV2/CVC2 код). После этого платежный сервер произведет проверку карты, и в автоматическом режиме переадресует на специализированную (платежную) страницу сайта, где будет предложено

ввести секретный код. Результатами ввода секретного кода могут быть: при введении неверного кода, система попросит ввести его повторно (всего есть 3 попытки ввода, после чего в случае неправильного ввода секретного кода операция оплаты будет отклонена); если секретный код введен правильно, то в зависимости от ряда конкретных условий (корректности ввода реквизитов карты, достаточности средств на карте/счете, статусе карты и ряда ограничений, которые может накладывать банк-эквайер, обслуживающий интернет-магазин) операция оплаты может быть завершена успешно либо отклонена.

Другой разновидностью безналичных платежей является оплата по QR-коду (двухмерному штрих-коду). Задача этих кодов обусловлена хранением большого объема информации на небольшой площади поверхности. QR – код состоит из черных квадратов, расположенных в квадратной сетке на белом фоне, которые могут быть распознаны с помощью специальных устройств и программного обеспечения для обработки изображений. Данные, которые необходимо закодировать, разбиваются на блоки в зависимости от режима кодирования: числовой, буквенно-цифровой, двоичный и кандзи (на основе китайских иероглифов). К разбитым по блокам данным добавляется заголовок, указывающий режим кодирования и количество блоков. В российском банковском секторе только несколько крупных банков (ВТБ, Тинькофф Банк и Сбербанк) внедрили возможность проведения платежей и переводов с использованием QR-кодов в свои мобильные приложения, что может свидетельствовать о дальнейшем внедрении и усовершенствовании данного способа оплаты в других приложениях мобильных банков.

Биометрия расширяет спектр услуг, доступных клиенту банка онлайн. В широком смысле под биометрией понимают измерение уникальных физических и (или) поведенческих характеристик личности. В более узком – технологии и системы автоматической идентификации человека и (или) подтверждения его личности, основанные на анализе биометрических параметров (отпечатков пальцев, форм кистей, рисунков вен рук, радужной

оболочки глаза, форм лица, голоса и др.) Уже с середины 2018 года более чем в 400 точках банковского обслуживания в 140 городах России открыт сбор биометрических данных. Для регистрации в Единой системе идентификации и аутентификации (ЕСИА) и Единой биометрической системе клиенту будет необходимо посетить офис банка с паспортом и СНИЛС для занесения своих биометрических данных в единую систему, для дальнейшего осуществления удаленных банковских услуг не посещая при этом их офисы. Преимуществами данных технологий являются: простота внедрения, автоматизация обслуживания, быстрая окупаемость и новые возможности для клиентов. Так, с помощью отпечатка пальца можно безналичным способом оплатить покупки, что делает ненужным физическое наличие пластиковой карты при использовании банкоматами, облегчает доступ к терминалам самообслуживания, депозитным ячейкам и т.д.

ПАО «Сбербанк» разработал проект, нацеленный на семьи с детьми «Ладошки», который уже действует в школах на территории России. Новая биометрическая технология позволяет школьникам оплачивать обеды в школьных столовых с помощью ладони или пальца – сканер считывает информацию и сумма списывается со счета. Таким образом, родители могут отслеживать, что покупает их ребенок и не беспокоиться о том, что наличные деньги он потеряет или забудет дома.

На современном этапе популярность набирает применение искусственного интеллекта, элементы которого в ближайшем будущем станут обязательными для каждого банка. Примером применения данного вида финансовых технологий является проект ПАО «Сбербанк» под названием «Iron Lady». Данная система предназначена для обзвона физических лиц с задолженностью по кредитам. Преимущества искусственного интеллекта заключаются в том, что он может работать 24 часа в сутки, не склонен к психологическим расстройствам и обладает безграничным объемом знаний, при применении которых может быстро

найти ответ на любой вопрос. Это хороший инструмент для управления издержками банка.

С развитием финансовых технологий в банковский бизнес потихоньку начинает внедряться технология Blockchain. Данная технология заключается в выстраивании непрерывных, последовательных цепочек в виде блоков, каждый из которых хранит определенную информацию. Это некий цифровой журнал экономических транзакций, который запрограммирован для записи не только финансовых операций, но и всего, что имеет какую-то ценность. Как и многие другие технологии, вышеупомянутая технология имеет определенные преимущества и недостатки. Так, преимуществами Blockchain технологии являются: организация международных переводов без комиссий; возможность переноса главных операционных систем на платформу коллективной работы с данными; сокращение времени и средств на проверку информации о клиенте и его идентификацию; гарантированность правильности заполнения банковской отчетности; осуществление документооборота без посредников; возможность заключения сделок по оплате услуг через аккредитив с применением смарт-контрактов и увеличение безопасности осуществляемых операций. В свою очередь к недостаткам данной технологии относят: уменьшение клиентского потока банков в связи с применением нового механизма финансирования ICO (первичного размещения криптовалюты); невозможность обеспечения большого количества транзакций и возникновение сложностей при мотивировании клиентов иметь свою запись в Blockchain-цепи.

Таким образом, по вышеуказанным преимуществам и недостаткам применения технологии Blockchain, достаточно сложно говорить о дальнейшей ее судьбе в банковской системе. Так, при скором масштабировании и развитии ее встанет вопрос: «а будут ли существовать банки в том виде, в котором они существуют сейчас?». Поэтому пробовать и внедрять новшества в банковскую сферу нужно уже в ближайшее время, чтобы в дальнейшем остаться на рынке и быть конкурентоспособными.

Таким образом, на основании вышеизложенного можно заключить, что введение санкций в отношении Российской Федерации Соединенными Штатами Америки положительно сказались на развитии системы розничных безналичных платежей и в том числе на становление и развитие Национальной платежной системы, частью которой является Национальная система платежных карт – «Мир».

Как было сказано ранее, с развитием системы безналичного обслуживания растет и количество несанкционированных операций, осуществляемых с использованием банковских карт, а также со счетов юридических лиц посредством системы дистанционного банковского обслуживания. Задача поднадзорных органов в данном случае состоит в проведении различного рода мероприятий по повышению безопасности электронных банковских услуг в т. ч. осуществление просветительских семинаров, касающихся повышению финансовой грамотности населения.

С развитием цифровой экономики в банковский бизнес внедряется большое количество современных технологий с целью удобства осуществления банковских операций со стороны потребителей банковских услуг и контролю со стороны вышестоящих органов. Так, в банковский бизнес продолжает внедряться система бесконтактной оплаты (NFC), оплаты посредством QR-кода, искусственный интеллект, биометрия, осуществление безопасных платежей посредством 3-D Secure и Blockchain технологии.

ЗАКЛЮЧЕНИЕ

Таким образом, проанализировав банковские электронные услуги и способы обеспечения их безопасности были сделаны следующие выводы и предложения.

Одним из механизмов привлечения современного клиента, пользующегося инновационными продуктами и заинтересованного в оптимизации издержек времени является электронное банковское обслуживание. Актуальность использования данного вида обслуживания в стратегическом направлении развития банка обусловлена повышением эффективности его работы и конкурентными преимуществами перед банками, которые еще не применяют такой вид услуг.

С появлением дистанционного облуживания у банка появляется возможность предложить своим клиентам целую систему взаимодействия в режиме реального времени. Удобство данной системы заключается в праве выбора наиболее актуальной для потребителя банковской услуги: то ли это будет обслуживание клиента посредством использования банкомата, а то ли посредством интернет-банкинга.

В России электронное банковское обслуживание появилось сравнительно недавно и активно развивается только около 10 лет, что непосредственно связано с возросшей цифровой мобильностью. Сегодняшний российский банковский сектор можно назвать развивающимся. Российская Федерация в настоящее время уступает развитым и некоторым развивающимся странам по количеству операций, совершенным с помощью банковских карт, а также по уровню использования интернет-банкинга и мобильного банкинга.

Результатом проведенного анализа стало выявление роста количества расчетных банковских карт и вместе с ними доли безналичных операций по оплате товаров и услуг. В свою очередь, увеличение количества электронных терминалов при уменьшении количества банкоматов и

платежных терминалов свидетельствует о продолжении формирования в российском банковском бизнесе тенденции замены операционистов – кассиров электронными терминалами. В свою очередь увеличение количества открытых счетов с дистанционным доступом и операций по ним обусловлено улучшением качества предоставляемых сервисов дистанционного банковского обслуживания, а также повышающимся спросом на их использование со стороны населения.

В свою очередь анализ безопасности электронного банкинга в Российской Федерации выявил изменение объема несанкционированных операций, как с использованием платежных карт, так и со счетов юридических лиц, осуществляемых посредством ДБО. Так, значения данных показателей на протяжении всего анализируемого периода имели тенденцию к снижению, что может свидетельствовать о слаженной работе ФинЦЕРТ с участниками информационного обмена.

В качестве угроз безопасности, воздействующих на объемы несанкционированных операций ФинЦЕРТ были обнаружены: рассылка электронных сообщений с вредоносным программным обеспечением, осуществление несанкционированных операций с использованием платежных карт (в банкоматах, в организациях торговли и услуг и при осуществлении интернет-транзакций), а также физические атаки на устройства самообслуживания.

К основным мерам по повышению безопасности использования банковских карт следует отнести неразглашение конфиденциальной информации третьим лицам (не сообщайте ПИН-код, реквизиты банковской карты, CVC/CVV2 код);использование банковской карты только ее владельцем (запрещается передача банковской карты в пользование третьим лицам);установка суточного лимита на сумму операций по банковской карте и одновременно подключение электронной услуги оповещения о проведенных операциях с целью предотвращения неправомерных действий по снятию денежных средств; осуществление взаимодействия с кредитной

организацией только по реквизитам связи, указанным в документах, полученных непосредственно в кредитной организации; незамедлительная блокировка банковской карты в случае ее утраты.

Таким образом, на основании вышеизложенного можно заключить, что введение санкций в отношении Российской Федерации Соединенными Штатами Америки положительно сказались на развитии системы розничных безналичных платежей и в том числе на становление и развитие Национальной платежной системы, частью которой является Национальная система платежных карт – «Мир».

Как было сказано ранее, с развитием системы безналичного обслуживания растет и количество несанкционированных операций, осуществляемых с использованием банковских карт, а также со счетов юридических лиц посредством системы дистанционного банковского обслуживания. Задача поднадзорных органов в данном случае состоит в проведении различного рода мероприятий по повышению безопасности электронных банковских услуг в т. ч. осуществление просветительских семинаров, касающихся повышению финансовой грамотности населения.

С развитием цифровой экономики в банковский бизнес внедряется большое количество современных технологий с целью удобства осуществления банковских операций со стороны потребителей банковских услуг и контролю со стороны вышестоящих органов. Так, в банковский бизнес продолжает внедряться система бесконтактной оплаты (NFC), оплаты посредством QR-кода, искусственный интеллект, биометрия, осуществление безопасных платежей посредством 3-D Secure и Blockchain технологии.

СПИСОК ЛИТЕРАТУРЫ

1. О банках и банковской деятельности [Электронный ресурс]: федеральный закон от 2 декабря 1990 г. № 395 – 1 (ред. от 27.12.2018). – Режим доступа: http://base.garant.ru/5883160/

2. О национальной платежной системе [Электронный ресурс]: федеральный закон от 27 июня 2011 г. № 161-ФЗ (ред. 28.11.2018). – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_115625/

3. О персональных данных [Электронный ресурс]: федеральный закон от 27 июля 2006 г. № 152 – ФЗ (ред. от 31.12.2017). – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

4. О техническом регулировании [Электронный ресурс]: федеральный закон от 27 декабря 2002 г. № 184-ФЗ (ред. от 29.07.2017).– Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/

5. О Центральном банке Российской Федерации (Банке России) [Электронный ресурс]: федеральный закон от 10 июля 2002 г. № 86 – ФЗ (ред. от 27.12.2018). – Режим доступа: http://www.consultant.ru /document/cons_doc_LAW_37570/

6. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федеральный закон от 27 июля 2006 г. № 149 – ФЗ (ред. от 18.12.2018). – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

7. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: постановление Правительства РФ от 1 ноября 2012 г. 1119. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_13735/

8. О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств [Электронный

ресурс]: положение утв. Банком России от 9 июня 2012 г. № 382-П (ред. от 07.05.2018).– Режим доступа: http://www.garant.ru/products/ipo/prime/doc/71875536/

9. О памятке О мерах безопасности использования банковских карт [Электронный ресурс]: письмо Банка России от 2 ноября 2009 г. № 120-Т. – Режим доступа: http://base.garant.ru/589868/

10. О рекомендациях по информационному содержанию и организации Web-сайтов кредитных организаций в сети Интернет [Электронный ресурс]: письмо Банка России от 23 октября 2009 г. № 128-Т. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_93100/

11. О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем Интернет-банкинга [Электронный ресурс]: письмо Банка России от 31 марта 2008 г. № 36-Т – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_100931/

12. О рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания [Электронный ресурс]: письмо Банка России от 26 октября 2010 г. № 141-Т.– Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_106206/

13. О рисках при дистанционном банковском обслуживании [Электронный ресурс]: письмо Банка России от 7 декабря 2007 г. № 197-Т – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_73368/

14. Агибалов, А. В. Состояние современных банковских технологий, преимущество их применения [Текст] / А. В. Агибалов, А.А. Алексейченко// Финансовый вестник. – 2018. – № 2(41). – С. 37-41.

15. Андреева, О. В. Современное состояние розничного банковского обслуживания в России [Текст] / О. В. Андреева, Р. И. Камалетдинова // Заметки ученого. – 2015. – № 3. – С. 8-13.

16. Белоглазова, Г. Н. Банковское дело: Розничный бизнес [Текст]: учеб. пособие / под ред. Г. Н. Белоглазовой, Л. П. Кроливецкой. – М.: Кнорус, 2016. - 414 с.

17. Битюкова, А.Ф. Национальная система платежных карт как фактор формирования национального платежного пространства [Текст]:/ А.Ф. Битюкова, А.А. Гулько // Экономика и предпринимательство. – 2015. – № 5 -1(58-1). – С. 1065 -1067.

18. Боровкова, В. А. Банки и банковское дело [Текст]: учебник для бакалавров / В.А. Боровкова. – 3-е изд. перераб. и доп. – М.: Юрайт, 2016. – 623 с.

19. Быканова, Н. И. К вопросу о повышении информационной безопасности системы дистанционного банковского облуживании [Текст] / Н. И. Быканова, А.Ф. Битюкова // Наука и инновации в XXI веке: актуальные вопросы, открытия и достижения: сборник статей VII Междунар. науч.-практ. конф. – Пенза: "Наука и Просвещение" (ИП Гуляев Г.Ю.), 2017. – С. 209-212.

20. Вадимова, С.А. Инновации в банковской сфере на примере развития удаленных каналов обслуживания клиентов банка [Текст] / С.А. Вадимова, Е.А. Витчукова // Актуальные проблемы гуманитарных и общественных наук: материалы международной науч.- практ. конф. – П: Пензенский государственный аграрный университет, 2016 – С. 6-10.

21. Ванько, Т. Д. Проблемы и перспективы развития рынка розничных банковских услуг в России [Текст] /Т. Д. Ванько // Теория и практика современного образования: Актуальные проблемы и перспективы развития: материалы всероссийской науч.-практ. конф. – Рославль: Принт – Экспресс, 2014 –С. 32-40.

22. Воронина Е.В. Мобильный банкинг в РФ [Текст] / Е.В. Воронина, Н.В. Береза // Электронный научный журнал. – 2016. – №2. – С. 381 - 385.

23. Гаврилин, А.В. Дистанционное банковское обслуживание в современном банковском бизнесе [Текст] / А.В. Гаврилин, В.В. Васильев//

Актуальные мировые тренды развития социально-гуманитарного знания: сборник научных трудов по материалам международной науч.- практ. конф. в 3 частях – Белгород: ООО «Агентство перспективных научных исследований», 2017 - С. 42-62.

24. Гулько, А. А. К вопросу об обеспечении информационной безопасности коммерческих банков [Текст] / А. А. Гулько, С. Б. Гладкова, А.Ф. Битюкова, В. Ю. Мартынюк// Экономика и предпринимательство. – 2016. – № 3-1(68). – С. 588–592.

25. Гулько, А. А. Национальная система платежных карт как фактор формирования национального платежного пространства [Текст] / А. А. Гулько, А.Ф. Битюкова// Экономика и предпринимательство. – 2015. – № 5-1(58). – С. 1065–1067.

26. Зимин, С. И. Обеспечение подлинности электронных документов [Текст] / С. И. Зимин, С. А. Иванов, В. В. Вилесов// REDS:телекоммуникационные устройства и системы. – 2016. – № 4. – С. 555–559.

27. Кабакова, Е. В. Дистанционное банковское обслуживание: проблемы и перспективы развития [Текст] / Е. В. Кабакова // Формирование общекультурных и профессиональных компетенций финансиста: сборник научных трудов студентов, аспирантов и преподавателей Финансового университета при Правительстве Российской Федерации / под науч. ред. А.Н. Лебедева, Н.В. Анненковой, Е.В. Камневой, Ю.Е. Мужичковой. – М.: Спутник +, 2014. – С. 103–107.

28. Калденова, Г. С. Тенденции развития электронных банковских услуг [Текст] / Г. С. Калденова, А. У. Конакбаева//Актуальные научные исследования в современном мире. – 2018. – № 1–4(33). – С. 53–56.

29. Козырь, Н. С. Технологии в сфере дистанционного банковского обслуживания: анализ и перспективы развития [Текст] / Н. С. Козырь, А. В. Гетманова// Финансовая аналитика: проблемы и решения. – 2016. – № 25(307). – С. 14–29.

30. Костерина, Т. М. Банковское дело [Текст]: учебник для СПО / Т. М. Костерина. – 3-е изд. перераб. и доп. – М.: Юрайт, 2016. –332 с.

31. Лаврушин, О.И. Банковское дело [Текст]: учебник / О. И. Лаврушин, Н. И. Валенцева [и др.]. – 11-е изд., стереотип. – М.: Кнорус, 2014. – 800 с.

32. Лапина, Ю. В. Совершенствование организации банковского обслуживания с использованием пластиковых карт и услуг на их основе [Текст] / Ю. В. Лапина, И. А. Чеховская // Актуальные вопросы развития современного общества: сборник статей 4-й Междунар. науч. - практ. конференции.- Курск: ЗАО «Университетская книга», 2014. – С. 14–17.

33. Мартынов, В. В. Торговый и интернет-эквайринг по банковским картам в современной России [Текст] / В. В. Мартынов // Технолого - экономическое образование: достижения, инновации, перспективы: сборник XVI междунар. науч.- практ. конференции Тула: Тульский государственный педагогический университет им. Л.Н. Толстого, 2015. – С. 405–408.

34. Мирошниченко, М. А. Внедрение информационно-коммуникационных технологий и новых форм в системе банковского обслуживания клиентов [Текст] / М. А. Мирошниченко, А. Ю. Короткевич // Актуальные проблемы права, экономики и управления. – 2015. – № 11. – С. 52–53.

35. Палий, М. В. Дистанционное банковское обслуживание клиентов: преимущества, недостатки и тенденции развития [Текст] / М. В. Палий // Лучшая студенческая статья 2017. – 2017. – С. 156–163.

36. Попова, В. В. Дистанционное банковское обслуживание в России [Текст] / В. В. Попова// Инновационные технологии в машиностроении, образовании и экономике. – 2018. –№ 1–2(7). – С. 465–468.

37. Прибыткова, Е. Н. Современные формы банковского обслуживания и перспективы развития электронных банковских услуг [Текст] / Е. Н. Прибыткова, Е. Ю. Маслова// Вестник академии знаний. – 2017. – № 1(20). – С. 25–28.

38. Пузанов, В. Е. Проблемы обеспечения информационной безопасности систем дистанционного банковского обслуживания кредитно-финансовых организаций с разветвленной сетью филиалов [Текст] / В. Е. Пузанов// Современные материалы, техника и технологии. – 2016. – № 1(4). – С. 178–184.

39. Пшеничников, В. В. Традиционное банковское обслуживание и электронный банкинг: особенности и отличия [Текст] / В. В. Пшеничников, Е. Е. Ковтунова// Финансовый вестник. – 2018. – № 1(40). –С. 68–77.

40. Разуваева, Е. Б. Современный рынок электронных банковских услуг [Текст] / Е. Б. Разуваева, И. А. Габитова// Вестник современных исследований. – 2018. – № 6.2(21). – С. 260–262.

41. Садуллаев, Х. Х. У Звездный час блокчейна еще не наступил [Текст] / Х. Х. У. Садуллаев// Аллея науки. – 2018. – № 1(17). – С. 878–880.

42. Скиннер, К. Цифровой банк [Текст]: монография / К. Скиннер. – М.: Манн, Иванов и Фербер, 2014. – 399 с.

43. Скрыпник, И. С. Особенности развития интернет - банкинга в россии [Текст] / И. С. Скрыпник// Символ науки. – 2018. – № 6. – С. 65–67.

44. Соснина, Н. Г. Факторы успешного развития электронных банковских услуг [Текст] / Н. Г. Соснина, А. А. Полякова // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации. – 2016. – № 9. – С. 57–61.

45. Трохова, Я. А. Актуальные проблемы обеспечения экономической безопасности коммерческого банка [Текст] / Я. А. Трохова// Вектор экономики. – 2018. – № 8(26). – С. 25

46. Фролов, Д. Б. Кибербезопасность в условиях применения систем электронного банкинга [Текст] / Д. Б. Фролов, П. В. Ревенков// Деньги и кредит. – 2016. – № 6. – С. 9–12.

47. Цханадзе, Н. В. Развитие системы дистанционного банковского обслуживания: деньги уходят в онлайн [Текст] / Н. В. Цханадзе// Вестник экономической безопасности. –2018. – № 2. – С. 357–364.

48. Цханадзе, Н. В. Эффективность использования дистанционных технологий в предоставлении банковских услуг [Текст] / Н. В. Цханадзе// Экономика: вчера, сегодня, завтра. – 2018. – № 3А. – С. 358–367.

49. Чеботарь, Ю. М. Формирование и развитие современной финансовой инфраструктуры [Текст] / Ю. М. Чеботарь// Финансовая жизнь. – 2017. –№ 3. – С. 72–77.

50. Черкашин, Е.А. Развитие российского рынка платежных карт / Е.А. Черкашин, В.В. Чучалина // Социально–экономические и гуманитарные науки. – 2015. – том 2, №7. – С. 55–57.

51. Черкашнев, Р. Ю. Экономическая сущность дистанционного банковского обслуживания [Текст] / Р. Ю. Черкашнев, Р. А. Разем // Современные проблемы и перспективы развития банковского сектора: сборник трудов междунар. науч.- практ. конференции.- Тамбов: Тамбовский государственный университет имени Г.Р. Державина, 2016. – С. 420–431.

52. Шабунин, Н. В. Электронный банкинг и система многоканального обслуживания клиентов [Текст] / Н. В. Шабунин, А. И. Григоров, Н. А. Инютин // Финансы, экономика и управление: проблемы, тенденции и перспективы развития в условиях нестабильности: материалы ежегодной межвузовской рег. науч.- практ. конференции студентов, магистрантов и аспирантов.- Воронеж: Общество с ограниченной ответственностью «Издательство Ритм», 2017. – С. 436–439.

53. Юсупова, О. А. Безопасность транзакций при использовании интернет-банкинга [Текст] / О. А. Юсупова// Финансовая аналитика: проблемы и решения. – 2016. – № 35(317). – С. 26–40.

54. Юсупова, О. А. Развитие и место дистанционного банковского обслуживания в банковской конкурентной среде [Текст] / О. А. Юсупова// Финансовая аналитика: проблемы и решения. – 2016. – № 33(315). – С. 37–51.

55. Обзор о несанкционированных переводах денежных средств за 2015 год [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/Collection/Collection/File/262/survey_2015.pdf

56. Обзор о несанкционированных переводах денежных средств за 2016 год [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/StaticHtml/File/14435/survey_transfers_16.pdf

57. Обзор о несанкционированных переводах денежных средств за 2017 год [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/statichtml/file/14435/survey_transfers_17.pdf

58. Основные типы атак в кредитно-финансовой сфере в 2017 году [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/StaticHtml/File/14435/gubzi_17.pdf

59. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России за период с 01 июня 2015 г. по 31 мая 2016 г. [Электронный ресурс]. – Режим доступа:http://www.cbr.ru/StaticHtml/File/14435/FinCERT_survey.pdf

60. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России 1 июня 2016 – 1 сентября 2017 [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/StaticHtml/File/14435/GUBZI-4.pdf

61. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопастности Банка России 1 сентября 2017 – 31 августа 2018 [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf

62. Рейтинг интернет-банкинга физических лиц 2017 [Электронный ресурс]: официальный сайт. – Режим доступа: http://markswebb.ru/e-finance/internet-banking-rank-2017/

63. Рейтинг интернет-банкинга юридических лиц 2017 [Электронный ресурс]: официальный сайт. – Режим доступа: http://markswebb.ru/e-finance/internet-banking-rank-2017/

64. Рейтинг мобильного банкинга физических лиц 2017 [Электронный ресурс]: официальный сайт. – Режим доступа: http://markswebb.ru/e-finance/mobile-banking-rank-2017/

65. Центральный банк Российской Федерации [Электронный ресурс].– Режим доступа: http://www.cbr.ru.

ПРИЛОЖЕНИЯ

Приложение 1

Классификация инноваций

№ п/п	Классификационный признак	Виды инноваций
1	По причинам зарождения	– реактивные – стратегические
2	По функциональному назначению	– основные – обеспечивающие
3	По инновационному потенциалу и степени новизны	– радикальные – комбинаторные – модифицирующие
4	По степени воздействия на деятельность банка	– точечные – системные
5	По отношению к разработчику	– нововведения, разработанные собственными силами – нововведения, приобретенные у стороннего разработчика
6	По распространенности на рынке	– лимитированные – не лимитированные
7	По территориальному распространению, заимствованию или адаптации	– зарубежные – отечественные
8	По временному аспекту	– сверхновые и новые – оперативные (текущие, краткосрочные) – перспективные
9	По технологическим параметрам	– продуктовые – процессные (технологические)

Приложение 2

Динамика объема платежей, поступивших в кредитные организации за 2013-2017 гг. по способам поступления, млрд. руб.

	Годы					Темп роста 2017 г./ 2013 г., %
	2013	2014	2015	2016	2017	
платежные поручения:	428129,7	503139	500989,3	491488,5	517117,2	120,8
от юридических лиц	420923	495427,5	494000,3	483760,3	507769,6	120,6
от физических лиц	7206,7	7711,5	6989	7728,2	9347,6	129,7
Через сеть интернет	285352,4	353105,6	373106,1	372422,7	413497,7	144,9
от юридических лиц	284250,9	351392,6	371387,1	370368,1	410970,6	144,6
от физических лиц	1101,5	1713	1719	2054,6	2527,1	229,4
посредством сообщений с использованием абонентских устройств мобильной связи:	4,7	6,3	20,8	53,3	121,3	2580,9
от юридических лиц	-	-	-	-	-	-
от физических лиц	4,7	6,3	20,8	53,3	121,3	2580,9

Приложение 3

Динамика количества платежей, поступивших в кредитные организации за 2013-2017 гг. по способам поступления, млн. ед.

	Годы					Темп роста 2017 г./ 2013 г., %
	2013	2014	2015	2016	2017	
платежные поручения:	1274,8	1315,6	1360,0	1431,9	1510,5	118,5
от юридических лиц	1058,2	1083,4	1106,7	1183,2	1276,0	120,6
от физических лиц	216,6	232,3	253,2	248,7	234,6	108,3
Через сеть интернет	747,5	840,1	961,3	1097,5	1254,9	167,9
от юридических лиц	671,0	747,3	873,1	1009,9	1147,5	171,0
от физических лиц	76,5	92,8	88,2	87,5	107,4	140,4
посредством сообщений с использованием абонентских устройств мобильной связи:	3,4	4,7	12,0	23,3	37,4	1100,0
от юридических лиц	-	-	-	-	-	-
от физических лиц	3,4	4,7	12,0	23,3	37,4	1100,0