ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

УПРАВЛЕНИЕ РИСКАМИ МОШЕННИЧЕСТВА ПРИ ОСУЩЕСТВЛЕНИИ ОПЕРАЦИЙ ПО БАНКОВСКИМ КАРТАМ И СИСТЕМАМ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ.

РЕФЕРАТ

УПРАВЛЕНИЕ РИСКАМИ МОШЕННИЧЕСТВА ПРИ ОСУЩЕСТВЛЕНИИ ОПЕРАЦИЙ ПО БАНКОВСКИМ КАРТАМ И СИСТЕМАМ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

ВКР (магистерская диссертация) состоит из введения, трех глав, заключения, библиографического списка, включающего 62 наименования. Работа включает 10 таблиц и 20 рисунков. Общий объем ВКР (магистерской диссертации) – 91 страница.

Ключевые слова: управление рисками мошенничества, банковские карты, система дистанционного банковского обслуживания, операция без согласия клиента

Цель исследования – научно обосновать и выявить наиболее эффективные инструменты, используемые коммерческими банками и Банком России для снижения риска несанкционированных (мошеннических) операций по банковским картам и системам ДБО, а также разработать рекомендации по управлению рисками при осуществлении операций по банковским картам и системам ДБО.

Научная новизна исследования заключается в разработке классификации операционных рисков по внутренним и внешним источникам их возникновения с указанием потерь, а также разработке методических рекомендаций для снижения риска мошенничества.

Практическая значимость диссертации заключается в возможности применения разработанных рекомендаций для эффективного управления рисками при осуществлении операций по банковским картам и системам ДБО коммерческими банками.

СОДЕРЖАНИЕ

Введение…….……..3

Глава 1. Теоретические аспекты управления операционными рисками в коммерческих банках

1.1. Понятие и классификация банковских рисков……8

1.2. Сущность и причины возникновения операционных рисков в коммерческих банках. Киберриск……...18

1.3. Развитие платежных систем в части внедрения технологий и стандартов для снижения рисков мошеннических операций……26

Глава 2. Исследование видов мошенничества и актуальных методов снижения рисков мошенничества по банковским картам и системам ДБО

2.1. Виды мошенничества с банковскими картами и системами ДБО.36

2.2. Методы Банка России и коммерческих банков по снижению рисков мошенничества…….……46

2.3. Мониторинг операций как главный инструмент коммерческих банков для предотвращения мошеннических действий…...……54

Глава 3. Управление инструментами, направленными на снижение риска мошенничества

3.1. Анализ мошеннических операций по статистике Департамента информационной безопасности Банка России……66

3.2. Оценка эффективности мониторинга карточных транзакций и систем ДБО на примере ПАО «СКБ-Банк»……71

3.3. Оптимизация управления инструментами, направленными на снижение риска мошенничества……..78

Заключение…...……... 84

Список используемых источников…….……86

ВВЕДЕНИЕ

Банковские карты являются универсальным, многофункциональным и высоко востребованным розничным продуктом, который на сегодняшний день составляет неотъемлемую часть широкого спектра предлагаемых услуг кредитными организациями. Постоянно расширяется инфраструктура приема и обслуживания банковских карт, развиваются маркетинговые и сервисные аспекты ведения бизнеса.

Актуальность темы исследования.

Наряду с высоким перечнем достоинств, банковские карты имеют и определенные недостатки, наиболее существенным их которых является их уязвимость перед несанкционированным воздействием со стороны третьих лиц с целью организации незаконного доступа к счету держателя и последующего хищения денежных средств. Проблема обеспечения безопасности проведения финансовых операций с использованием банковских карт и, в первую очередь – снижение риска мошенничества, по праву считается глобальной, поскольку в процесс ее решения вовлечены все участники мирового рынка платежных инструментов.

Отсутствие механизма предупреждения мошенничества с использованием банковских карт потенциально может привести к рискам банка-эмитента, связанным с прямыми финансовыми потерями, ухудшением деловой репутации и недоверием к предоставляемым продуктам со стороны клиентов. Принимая во внимание стремительные темпы развития рынка банковских услуг решение проблемы обеспечения комплексности и эффективности предпринимаемых мер по управлению риском мошенничества карточных транзакций и операций по системам ДБО является ключевым аспектом формирования политики безопасности, как на уровне отдельной кредитной организации, так и в масштабе всей банковской системы. Формирование системы управления этими процессами представляется актуальным как для коммерческих банков, так и для Банка России.

Актуальность исследуемой проблемы, а также ее практическая значимость и востребованность рассматриваемых вопросов определили выбор темы диссертации.

Цель исследования – научно обосновать и выявить наиболее эффективные инструменты, используемые коммерческими банками и Банком России для снижения риска несанкционированных (мошеннических) операций по банковским картам и системам ДБО, а также разработать рекомендации по управлению рисками при осуществлении операций по банковским картам и системам ДБО.

Для достижения поставленной цели были обозначены и решены следующие задачи:

- Раскрыть понятие операционные риски, в том числе киберриски и разработать классификацию операционных рисков, а также изучить историю развития платежных систем с направлением по снижению рисков мошеннических операций;
- Выявить механизмы организации несанкционированного доступа к системе ДБО клиента и к данным по карте со стороны третьих лиц для последующего совершения операции без согласия клиента;
- Исследовать текущий инструментарий Банка России и коммерческих банков на предмет снижения рисков мошенничества по банковским картам и системам ДБО, а также проанализировать данные Банка России по динамике операций без согласия клиентов за последние годы;
- Оценить эффективность используемых инструментов ПАО «СКБ-Банк» на предмет снижения рисков мошенничества по банковским картам и системам ДБО и разработать рекомендации по управлению рисками мошенничества коммерческим банкам при осуществлении операций по банковским картам и системам ДБО;

Объект исследования – коммерческие банки Российской Федерации.

Предмет исследования – управление рисками мошенничества при осуществлении операций по банковским картам и системам дистанционного банковского обслуживания.

Теоретической базой диссертации являются работы отечественных и зарубежных авторов, в которых рассмотрены банковские риски, а также приведена их классификация.

Теория управления рисками рассматриваются в работах Мягковой Т.Л., Коваленко О.Г., Медведевой О.Е., Богданкевича О.А, Шапкина А.С., Лаврушина О.И., Соколинской Н.Э., Казимагомедова А.А., Абдулсаламовой А.А., а также Тепман Л.Н., Эриашвили Н.Д. и др.

При изучении истории развития платежных систем и банковских картам на результаты работы повлияли научные труды таких авторов, как Голдовский И.М., Звонова Е.А., Эскиндарова М.А., Лямин Л.В., Пятиизбянцев Н., Пухов А.В, Ревенков П.В., Демчев И.А. и др.

Управление рисками при реализации дистанционного банковского обслуживания рассматривается авторами Юденков Ю.Н., Ермаков С.Л., Миндрова З.М., Герасимович А. М., Батаев А. В., Ревенков П.В, Лямин Л.В.

В современной научной литературе и трудах отечественных ученых проблематика совершенствования механизмов управления риском мошенничества с использованием банковских карт занимает определенное значение, однако глубина и степень разработанности данных исследований не удовлетворяют реалиям экономического мира с его постоянно меняющимися тенденциями.

Эмпирической базой исследования послужили официально опубликованные материалы и методические рекомендации ведущих Международных платежных систем MasterCard и Visa International, Национальной платежной системы «МИР», Банка России, исследования автора на тему киберрисков, статистические данные центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России и разработанные

им стратегические меры по снижению риска мошенничества, а также различные аналитические материалы, характеризующие развитие технологий снижения риска мошенничества.

Гипотеза исследования – несмотря на ежегодный рост несанкционированных операций, коммерческие банки грамотно используя инструменты для снижения рисков мошенничества по банковским картам и системам ДБО, могут уменьшить количество реальных несанкционированных операций.

Научная новизна исследования:

- Разработана классификация банковских операционных рисков по внутренним и внешним источникам их возникновения с указанием потерь;
- Систематизированы инструменты снижения риска мошенничества по каналу взаимодействия с клиентом;
- Разработаны методические рекомендации для снижения риска мошенничества при осуществлении операций по банковским картам и системам дистанционного банковского обслуживания.

Структура диссертации.

Работа состоит из введения, трех глав и заключения. Первая глава посвящена изучению операционных рисков, в том числе киберриска, а также изучению развития платежных систем в части внедрения технологий и стандартов для снижения рисков мошеннических операций. Помимо этого, в первой главе разработана классификации операционных рисков по внешним и внутренним источникам их возникновения с указанием потерь.

Во второй главе исследованы механизмы организации несанкционированного доступа к системе ДБО клиента и к данным по карте со стороны третьих лиц для последующего совершения операции без согласия клиента. Также во второй главе исследован текущий инструментарий коммерческих банков Российской Федерации и Банка России на предмет снижения рисков мошенничества по банковским картам и системам ДБО.

В третьей главе проведен анализ мошеннических операций по статистике Департамента информационной безопасности Банка России, также оценен эффект используемых инструментов ПАО «СКБ-Банк» на предмет снижения рисков мошенничества по банковским картам и системам ДБО. Помимо этого, разработаны рекомендации для оптимизации подхода к использованию инструментов коммерческих банков Российской Федерации и Банка России для снижения рисков мошенничества по банковским картам и системам ДБО.

Практическая значимость диссертации заключается в возможности применения разработанных рекомендаций для эффективного управления рисками при осуществлении операций по банковским картам и системам ДБО коммерческими банками.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМИ РИСКАМИ В КОММЕРЧЕСКИХ БАНКАХ

1.1. Понятие и классификация банковских рисков

Управление рисками является неотъемлемой частью организации банковской деятельности. Банк будет иметь успех в том случае, если принимаемые им риски разумны, контролируемы и находятся в пределах их финансовых возможностей и компетенции. Получение максимальной прибыли – стремление Банков, но при этом, стремление ограничивается возможностью понести убытки. Риск банковской деятельности означает наличие вероятности, что фактическая прибыль окажется меньше чем запланированная, ожидаемая. Чем выше ожидаемая прибыль, тем выше риск.

Банковский риск – это ситуативная характеристика деятельности банка, отображающая неопределенность ее исхода и характеризующая вероятность негативного отклонения действительности от ожидаемого. В этом определении имеются все понятия, необходимые для понимания банковских рисков – неопределенность ситуации принятия решения и вероятность негативного отклонения от планируемого.

Основными сущностными характеристиками риска являются:

а. вероятность риска – степень воздействия источника риска, каждый вид риска имеет нижние и верхние границы вероятности;

б. уровень риска – отношение величины ущерба к затратам на подготовку и реализацию риск-решения;

в. степень риска – качественная характеристика величины риска и его вероятности. Различают высокую, среднюю, низкую и нулевую степени;

г. приемлемость риска – вероятность потерь и того, что эти потери не превысят определенного уровня;

д. правомерность риска – вероятность риска находится в пределах нормативного для данной сферы деятельности уровня, который нельзя превысить без правовых нарушений.

Эффективность системы организации управления рисками большей частью зависит от классификации. Классификация риска – это распределение риска на особые группы по вполне определенным признакам для достижения поставленных задач. Научно-обоснованная классификация риска дает возможность четко определить роль каждого из рисков в общей системе классификации. Она создает возможности для эффективного применения соответствующих разнообразных методов, приемов, способов управления ими. Каждому из выявленных рисков соответствует своя собственная система методов оптимизации. В научной литературе можно увидеть разные варианты классификации банковских рисков.

Согласно Мягковой Т.Л., под рисками в банковской деятельности понимается ничем необусловленная возможность снижения величины доходов, увеличения расходов, уменьшения прибыли, снижения величины собственного капитала кредитной организации [31]. Это все в совокупности сказывается на неспособности банком расплачиваться по своим обязательствам вследствие любых факторов внутреннего и внешнего характера, которые влияют на результат деятельности экономического субъекта.

Как правило, банковские риски возникают ввиду обстоятельств, возникновение которых не зависит от самого коммерческого банка. Говоря конкретно, к этим обстоятельствам относятся нестабильность экономики страны, обострение ситуации на международных рынках, экономические санкции и т.д. Согласно Мягковой Т.Л., «банки всегда сравнивают риск предстоящего события, т.е. расчетную величину возможных потерь, связанных с таким событием с затратами, которые необходимы для минимизации негативных последствий данного события, если оно, конечно

же, произойдет. Также они могут сравнить данный риск с возможными выгодами, которые можно получить от возникновения такого события» [33].

Банковские риски несут в себе уровень потерь для деятельности любого коммерческого банка. Этот уровень можно минимизировать при условии возможности предвидения рисков.

Согласно Коваленко О.Г., риски, которые охватывают экономику отдельно взятого коммерческого банка, связаны с его конкретной деятельностью, умением эффективно управлять проходящими через него денежными потоками [18].

Переходя к классификации банковских рисков, отметим, что банковские риски разнообразны и их возникновение напрямую определяет сферу деятельности коммерческого банка.

Согласно Богданкевичу О.А., к основным банковским рискам относятся следующие риски:

- кредитный риск;
- страновой риск;
- рыночный риск;
- риск ликвидности;
- операционный риск;
- стратегический риск;
- риск потери деловой репутации банка [10]

Согласно Мягковой Т.Л., классификация банковских рисков осуществляется в соответствии с Таблицей 1.

Таблица 1 – Классификация банковских рисков [31]

Группа	Класс	Категория
Внешние банковские риски	Банковские риски операционной среды	Нормативно-правовые риски
		Риски конкуренции
		Экономические риски
		Страновой риск

Продолжение таблицы 1

Внутренние банковские риски	Банковские риски управления	Риск мошенничества
		Риск неэффективной организации
		Риск неспособности руководства Банка принимать целесообразные решения
	Банковские риски поставки банковских услуг	Технологический риск
		Операционный риск
		Риск внедрения новых финансовых инструментов
		Стратегический банковский риск
	Банковские финансовые риски	Риск процентной ставки
		Кредитный риск
		Риск ликвидности
		Внебалансовый риск
		Валютный риск
		Риск использования заемного капитала банка

Наряду с представленной классификацией банковских рисков, Мягкова Т.Л. приводит систему классификации банковских рисков:

- По времени возникновения (ретроспективные, текущие, перспективные);
- По степени (низкие, умеренные, полные). Степень банковского риска характеризуется вероятностью события, которое ведет к потере средств банком;
- По типу банка (специализированные, отраслевые, универсальные);
- По сфере влияния (внутренние и внешние);
- По основным факторам возникновения (политические и экономические);
- По составу клиентов (мелкие, средние и крупные);
- По характеру учета операций (риски по балансовым и по забалансовым операциям).
- По возможности регулирования (открытые и закрытые). Открытые риски банк не имеет возможности локализовать. Что касается закрытых рисков, то они регулируются путем проведения политики

диверсификации, т.е. путем широкого перераспределения кредитов в мелких суммах, предоставленных большому количеству клиентов при сохранении общего объема операций банка.

Согласно Тепман Л.Н. и Эриашвили Н.Д. классификация банковских рисков представлена в Таблице 2 [57].

Таблица 2 – Классификация банковских рисков [57]

Классификационный признак	Тип риска	Вид риска
По основному содержанию деятельности	Кредитный риск	
	Валютный риск	
	Процентный риск	
	Риск по формированию депозитов	
	Риск ликвидности	
	Репутационный риск	
	Риск неплатежеспособности (банкротства)	
	Операционные риски	Риск нарушения законодательства
		Риск противоправных действий или правонарушений сотрудников
		Риск нарушения администрацией банка или сотрудниками трудового законодательства
		Риск противоправных действий контрагентов
		Другие типовые операционные риски
По сфере возникновения	Внешние риски	Страновой
		Валютный
		Правовой (законодательный) риск
		Отраслевой риск
		Риск форс-мажорных обстоятельств
	Внутренние риски	Риски, связанные с видом банка
		Риски, связанные с характером банковских операций
		Риски, связанные со спецификой деятельности клиентов банка
По степени воздействия	Низкие	
	Умеренные	
	Полные	

Продолжение таблицы 2

По причине возникновения	Чистые	
	Спекулятивные	
По форме проявления	Системные	
	Несистемные	
	Открытые	
	Закрытые	

Рассмотрим подробнее конкретные виды рисков.

По области влияния риски делятся на внешние и внутренние, так как сфера деятельности коммерческого банка формируется под воздействием как внешних условий среды, так и внутренних факторов среды банковского учреждения. В связи с этим, внешние риски можно объединить по охвату территории и рычагам действия, а внутренние риски объединяются по характеру банковских операций, по составу клиентов банка и по типам коммерческих банков.

Внешние риски – это риски, практически не связанные с деятельностью банка или его контактной аудитории. По охвату территории они могут быть страновые и межстрановые, характеризующиеся высоким уровнем международного экономического сотрудничества, здесь можно говорить о мировых рисках. В частности, имеются ввиду экономические кризисы в отдельных регионах мира, которые отражаются и на вполне успешных в экономическом отношении странах.

В зависимости от источника воздействия среди внешних рисков можно отметить политико-правовые риски, экономические риски и природно-естественные риски.

Внутренние риски образуются в результате функционирования самих банков и их клиентов. В свою очередь, риски подразделяются на риски в основной и дополнительной деятельности кредитного учреждения. Первые относятся к самой распространённой группе рисков: кредитный, процентный, валютный и рыночный риски. Вторые включают в себя убытки по

формированию вкладов, риски по современным видам деятельности, риски банковских нарушений, риск уменьшения рейтинга.

По времени образования риски подразделяются на ретроспективные, операционные и перспективные. Деление рисков во временном диапазоне имеет огромное значение для планирования возможных для банка убытков. С учетом времени образования риска можно миновать наложением прошлых рисков и просчетов на будущую деятельность банка.

По степени (уровню) банковские риски можно подразделить на низкие, умеренные и полные. Уровень банковского риска характеризуется возможностью ситуации, ведущей к утрате банком ресурсов по этой операции, и может быть выражена в процентах или коэффициентах.

По признаку способа расчета риски могут быть комплексными и частными. В комплексный риск входит оценка и планирование размера риска банка, и выполнение экономических нормативов банковской ликвидности. Частный риск основывается на образовании шкалы коэффициентов риска или на взвешивании риска по конкретной банковской операции или группе.

В зависимости от вида банка риски банков делятся на специализированные, отраслевые и универсальные. По каждому из указанных рисков присутствуют все виды рисков, но возможность частоты их образования и особенности зависят от типа этого кредитного учреждения.

Выделяют также риски по составу клиентов (мелкие, средние и крупные), которые определяют уровень риска. Например, мелкий заемщик сильно зависит от непредсказуемости рыночных отношений, чем крупный. Вместе с тем большие кредиты, выданные только одному крупному клиенту, очень часто становятся причиной банкротств кредитных учреждений.

В зависимости от основных факторов образования банковские риски делятся на экономические и политические. При этом, политические риски – это риски, вызванные изменением политической ситуации, негативно влияющей на итоги деятельности предприятий (военные действия на территории страны, закрытие границ, запрет на вывоз или ввоз товаров и т.д.).

С другой стороны, экономические риски – это риски, вызванные негативными изменениями в экономике страны или банка. Они могут быть выражены сменой конъюнктуры рынка, уровня управления и т.д.

Процентный риск – это возможность утраты банком из-за превышения процентных ставок по депозитам над ставками по кредитам (либо резкого уменьшения маржи), а также из-за увеличения рыночных процентных ставок по ценным бумагам, который приводит к их удешевлению.

Портфельный риск – выражается в возможности утраты по отдельным типам ценных бумаг, а также по всем видам кредитов. Портфельные риски делятся на финансовые, риски ликвидности, систематические и несистематические, и прочие.

Валютный риск – это риск курсовых потерь, который связан с интернационализацией рынка банковских операций, образованием межгосударственных (совместных) предприятий и кредитных учреждений и разнообразием их деятельности и представляет собой вероятность денежных убытков в результате изменений валютных курсов.

Правовой риск – риск понесения убытков в результате различного применения норм законодательства судебными органами либо в результате невозможности исполнения контрактов вследствие нарушения законодательства или нормативных актов. Правовой риск включает в себя также риск применения надзорными органами штрафов или иных мер воздействия к кредитной организации, что позднее может привести к возникновению расходов в результате судебных рисков со стороны третьих лиц.

Кредитный риск - это риск невозврата кредитором основной суммы задолженности и процентов (в более широком смысле сюда относятся разные риски банка, связанные с невыполнением прочими участниками рынка своих долгов перед кредитным учреждением).

Риск ликвидности – риск, выражающийся в неспособности кредитной организации финансировать свою деятельность, то есть обеспечивать рост

активов и выполнять обязательства по мере их наступления без понесения убытков в недопустимых для финансовой устойчивости размерах.

Риск структуры капитала - означают, что при структуре капитала с большим удельным весом статей переоценки основных средств кредитное учреждение, вложившее крупные средства клиентов в кредитные операции со сроком погашения, превосходящим сроки привлечения ресурсов при изменении ситуации на рынке может понести как дополнительные затраты (в случае повышения стоимости ресурсов), так и стать банкротом.

Кроме того, исходя из возможностей регулирования выделяют открытые и закрытые риски. Открытые риски кредитное учреждение не может локализовать. Закрытые риски можно регулировать с помощью реализации политики диверсификации, следовательно, с помощью обширного перераспределения кредитов в суммах, предоставленных своим клиентам на фоне сохранения общего объёма операций банка; введения депозитных сертификатов; страхования кредитов и депозитов и др. Кроме того, отдельные специалисты-экономисты выделяют, кроме вышеперечисленных, некоторые иные категории банковских рисков.

Рыночный риск находится в тесной взаимосвязи с процентным и валютным рисками. Он означает риск возникновения убытков в связи с осуществлением кредитной организацией операций с балансовыми и внебалансовыми инструментами вследствие изменения рыночных цен, включая процентные ставки, валютные курсы и цены на финансовые инструменты.

Риск по формированию вкладов (ресурсной базы) – является тесно связанным с рыночными, процентными и валютными рисками. При создании ресурсной базы кредитное учреждение должно учитывать возможность роста затрат по привлечению ресурсов в случае корректировки ситуации на финансовом рынке. Депозитная политика кредитного учреждения имеет целью обеспечить банк ресурсами на время по назначенной цене для осуществления конкретных активных операций. Ее реализация означает

решение двух альтернативных задач: стабильность ресурсной базы и уменьшение затрат по ее формированию.

Риск упущенной выгоды – это убытки в связи с неосуществлением какой-либо операции.

Риски операционной среды объединяют в себе те риски, которые защищают интересы банка, при этом посредством которых над банком осуществляется контроль, а также те, которые вырабатываются инфраструктурой деятельности коммерческого банка: законодательный риск, правовые и нормативные риски, риски конкуренции, страновой риск.

Репутационный риск (риск потери деловой репутации) – риск, возникающий в результате негативного восприятия кредитной организации со стороны клиентов, контрагентов, акционеров, инвесторов, кредиторов, рыночных аналитиков, надзорных органов, что может негативно отразиться на способности кредитной организации поддерживать существующие и устанавливать новые деловые отношения и поддерживать на постоянной основе доступ к финансовым ресурсам, например, на межбанковском рынке.

Риски управления включают в себя риск мошенничества со стороны работников банка, риск неэффективной организации, риск невозможности руководства банка принимать оптимальные решения, риск того, что банковская система стимулирования не обеспечивает соответствующей мотивации. Риски этой категории вызваны низкой квалификацией банковских работников, корыстными задачами, преследуемыми сотрудниками банка. Риски, связанные с доставкой финансовых услуг, образуются в ходе предоставления банковских услуг и делятся на технологический, операционный, стратегический риски и риск внедрения новой продукции.

Технологический риск появляется в каждом отдельном случае, когда существующая система предоставления услуг становится менее эффективной, чем образованная.

Стратегический риск показывает возможность банка выбирать географические и продуктовые ниши, возможно доходные для банка в будущем, с учетом комплексной оценки операционной среды.

Кроме этого, согласно Тепману Л.Н. и Эриашвили Н.Д., риски, с которыми сталкиваются коммерческие банки при осуществлении своей деятельности, могут быть как чисто банковскими, так и общими. Чисто банковские риски непосредственно связаны с деятельностью коммерческого банка. Если говорить про общие риски, то они складываются в результате воздействия внешних факторов, которые не зависят от деятельности банка.

Классификации банковских рисков должны постоянно усовершенствоваться в зависимости от развития рыночных отношений, повышения качества обслуживания клиентов, применения новых информационных технологий в организации деятельности кредитных организаций.

Таким образом, были рассмотрены основные банковские риски и их классификации. Понятие и сущность операционных рисков автор рассмотрит в следующем параграфе, а также проведет их классификацию.

1.2. Сущность и причины возникновения операционных рисков в коммерческих банках. Киберриск

Так как банковское сообщество оказалось не готово к кризисам 2008 – 2009 гг., стандарты Базельского комитета направлены на повышение устойчивости банковских систем, при этом особое внимание уделяется операционным рискам. Базельский комитет предлагает определение операционного риска как риска потерь, ставших результатом неадекватных или неэффективных внутренних процессов, действий людей и технических систем или внешних событий [65].

Богданкевич О.А. определяет операционный риск как риск возникновения у банка потерь в результате несоответствия банковскому законодательству порядка и процедур совершения операций и других сделок, установленных внутренними документами банка, или их нарушениями сотрудниками банка в результате ошибок или некомпетентности. Операционный риск включает риск ошибок персонала, технологический, технический, методологический, учетный, правовой, управленческий, риск внутреннего и внешнего вмешательств, форс-мажорных обстоятельств и другие виды риска. [10]

В соответствии с Указанием Банка России «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы» от 15.04.2015 №3624-У, под операционным риском понимается риск возникновения прямых и непрямых потерь в результате несовершенства или ошибочных внутренних процессов кредитной организации, действий персонала и иных лиц, сбоев и недостатков информационных, технологических и иных систем, а также в результате реализации внешних событий [49].

Ранее правовой риск не включался в понятие операционного риска, в соответствии с Положением Банка России 716-П, правовой риск включен в понятие операционного риска и выделены следующие виды операционного риска [43]:

- риск информационной безопасности,
- риск информационных систем,
- правовой риск,
- риск ошибок в управлении проектами,
- риск ошибок в управленческих процессах,
- риск ошибок в процессах осуществления внутреннего контроля,
- модельный риск;
- риск потерь средств клиентов, контрагентов, работников и третьих лиц
- риск ошибок процесса управления персоналом,

- операционный риск платежной системы.

Киберриск является частью риска информационной безопасности и определяется как риск преднамеренных действий со стороны работников кредитной организации или третьих лиц с использованием программных средств, направленных на объекты информационной инфраструктуры кредитной организации в целях нарушения или прекращения их функционирования и создания угрозы безопасности информации, а также в целях несанкционированного присвоения, хищения, изменения, удаления данных и иной информации и нарушение режима доступа [43].

Классификация операционных рисков в зависимости от источников их возникновения представлена на Рисунке 1.

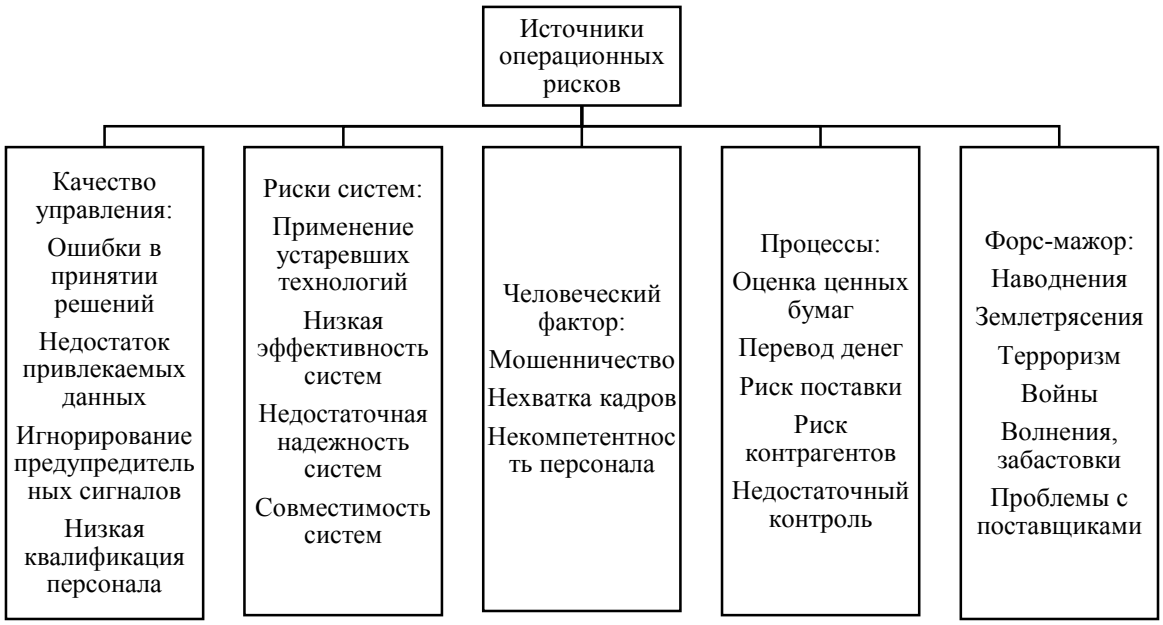

Рисунок 1 - Классификация операционных рисков [22]

Автором разработана классификация на основе критерия: внутренние и внешние источники возникновения операционных рисков.

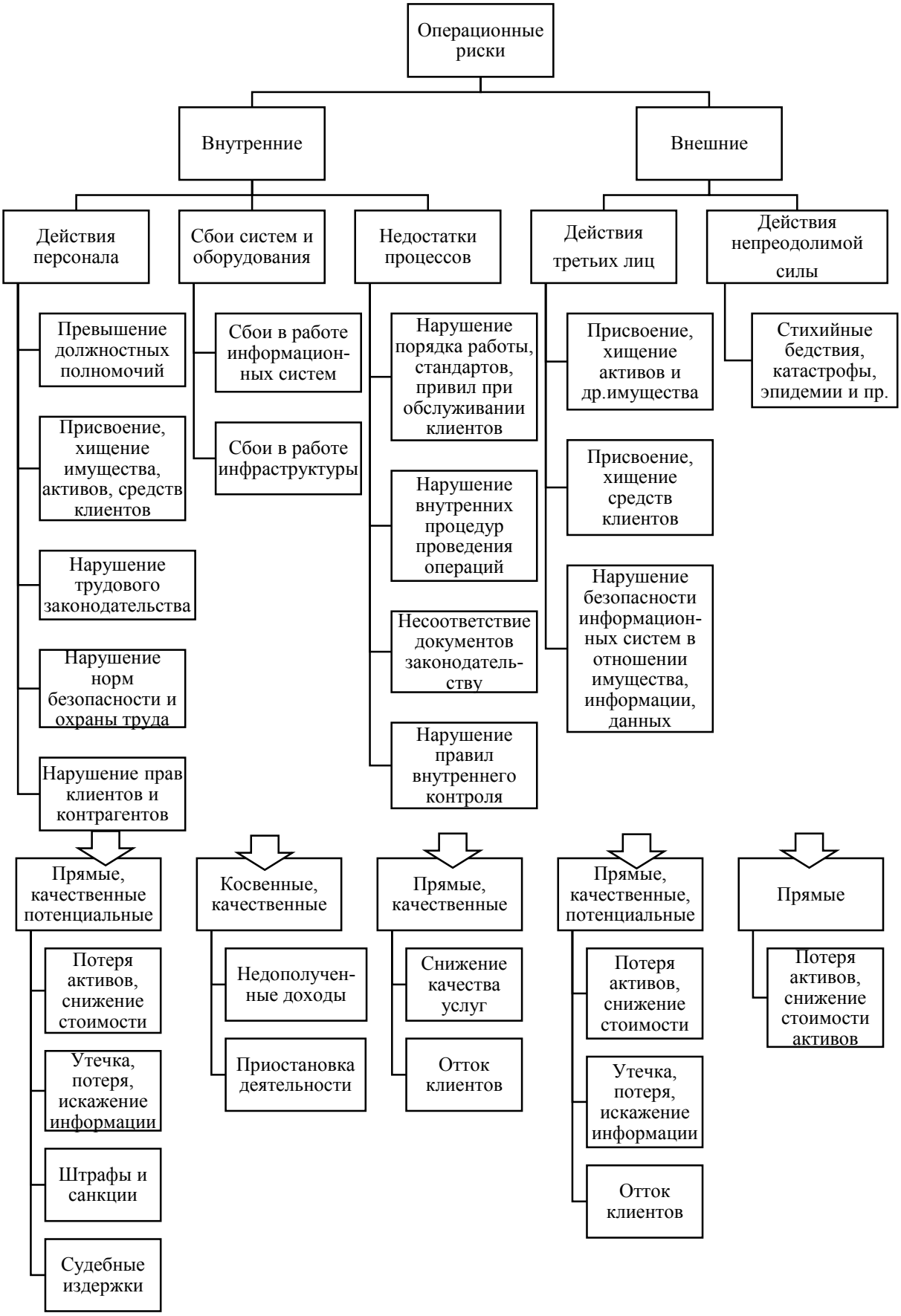

Рисунок 2 – Классификация операционных рисков[1]

[1] Составлено автором по: [22, 43, 65]

Реализация операционных рисков ведёт к прямым финансовым потерям или непрямым потерям. Прямые потери выражаются в денежном эквиваленте. Непрямые потери напрямую не выражаются в денежном эквиваленте, но влияют на финансовый результат посредством недополучения доходов по причине потери деловой репутации и уменьшения клиентской базы.

Виды потерь подразделяются в соответствии с Таблицей 3.

Таблица 3 – Виды потерь при реализации операционных рисков [43]

Прямые потери	Непрямые		
	Косвенные	Качественные	Потенциальные
1. Снижение (обесценение) стоимости активов. - потеря активов, - потеря наличных денежных средств в результате хищения или физического уничтожения; - обесценение стоимости кредита в результате начисления дополнительных резервов и пр. 2. Досрочное списание (выбытие, потеря, уничтожение) материальных и нематериальных, финансовых активов в результате реализации события операционного риска. 3. Денежные выплаты клиентам и контрагентам в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине третьих лиц, в том числе компенсированные кредитной организацией хищения средств клиентов и контрагентов. 4. Денежные выплаты работникам кредитной организации в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине кредитной организации. 5. Потери от ошибочных платежей, включающие: - потери в размере ошибочного платежа; - потери в виде уплаченных комиссий по проведению ошибочного платежа; - потери, связанные с поиском возможности возврата ошибочного платежа.	- недополученные доходы от приостановления или прекращения совершения операций, вызванных событиями операционного риска (например, приостановления или прекращения работы систем, оборудования); - неполученные доходы, связанные с непроведением отдельных сделок и операций по причине реализации событий операционного риска, не связанных с приостановлением и (или) прекращением совершения операций; - повышение стоимости заимствований, например, стоимости привлечения кредитных средств, в результате события операционного риска;	- возникновение источников других видов риска (например, кредитного риска, рыночного риска, риска ликвидности, риска потери деловой репутации, регуляторного риска, стратегического риска); - приостановку деятельности в результате события операционного риска (например, технологического сбоя); - отток клиентов; - неисполнение обязательств по сделке или неоказание услуги; - ограничения, приводящие к выполнению невыгодных для кредитной организации действий, накладываемые со стороны суда, исполнительных органов государственной власти, Банка России;	- потери (в том числе хищение) средств клиентов, контрагентов, работников и третьих лиц, которые не были компенсированы кредитной организацией, штрафы, наложенные на должностных лиц кредитной организации; - другие потенциальные потери.

Продолжение таблицы 3

6. Расходы (выплаты), связанные с решениями суда или представительством кредитной организации в судах по делам, связанным с потерями от реализации событий операционного риска 7. Штрафы, наложенные исполнительными органами государственной власти или Банком России. 8. Расходы на устранение последствий реализации события операционного риска, направленные на восстановление деятельности или на снижение потерь от реализовавшегося события операционного риска. 9. Отрицательный финансовый результат от невыгодных для кредитной организации сделок, совершенных по причине операционного риска. 10. Прочие потери, связанные с реализацией события операционного риска или устранением последствий события операционного риска.	- снижение рыночной стоимости акций кредитной организации или инструментов капитала кредитной организации по причине реализации события операционного риска; - потери, связанные с восстановлением ликвидности из-за оттока денежных средств по причине реализации операционного риска; - прочие потери, связанные с устранением последствий или снижением потерь от реализации операционного риска	- снижение качества предоставления услуг, выполнения операций (например, нарушение регламентированных сроков выполнения процессов и операций, установленных во внутренних документах кредитной организации); - утечку, потерю или искажение защищаемой, в том числе коммерческой, информации; - судебные акты (решения, определения, постановления), акты исполнительных органов государственной власти, Банка России, не связанные с уплатой штрафов; - снижение лимитов на межбанковское кредитование; - другие качественные потери.	

Рынок платежных карт и систем ДБО – перспективные сегменты банковского бизнеса в России. Их развитие – важнейший фактор в решении задач расширения доступности платежных услуг населению, сокращения наличных, развития безналичных расчетов, а также совершение большей части банковских операций дистанционно. Универсальный характер пластиковой карты, как платежного инструмента, позволяет успешно решать различные задачи в социальной, бюджетной сферах, в том числе, оказывать влияние на снижение уровня теневой экономики. Удобство и быстрота совершения операций в системе ДБО, при отсутствии необходимости посещения офиса банка, с учетом текущей ситуации в мире, а именно пандемии коронавирусной инфекции, повышает привлекательность данного

продукта. В связи с чем, происходит увеличение объема совершаемых операций с использованием банковских карт и систем ДБО, что влечет за собой потенциальные операционные риски. Рынок банковских карт, в виду своей массовости и доступности, наиболее подвержен операционному риску, по сравнению с другими направлениями деятельности банка, а доступ к денежным средствам на счете, привязанном к банковской карте, возможно получить с помощью системы ДБО.

Операционные риски при использовании банковской карты могут возникнуть в результате действий или бездействия разных субъектов, определяющих состояние рынка и условия деятельности банка на нем. Источниками риска могут являются непосредственные субъекты рынка: банки, эмитенты и эквайеры, держатели карт, карточные платежные системы, торговые предприятия, карточные мошенники, процессинговые центры.

Способы управления банковскими рисками – это методы воздействия банка на возможные риски с целью минимизации потерь от их осуществления. Именно в выработке основных подходов к оценке риска, определении допустимого его уровня и разработке соответствующей стратегии и состоит главная задача управления риском или риск менеджмента [16].

Выделяют следующие методы управления риском:

- Избежание (уклонение) риска
- Ограничение риска
- Снижение риска
- Трансфер (передача) риска, в том числе страхование
- Принятие риска

В соответствии с Указанием Банка России от 15 апреля 2015 г. N 3624-У «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы», кредитная организация должна создать систему управления рисками и капиталом путем реализации внутренних процедур оценки достаточности капитала, требования к которым установлены настоящим Указанием [49].

Для управления операционным риском банк устанавливает следующие процедуры:

- Идентификация операционного риска,
- Сбор и регистрация информации о событиях риска,
- Определение потерь и возмещений потерь,
- Количественная и качественная оценка уровня риска,
- Выбор и применение способа реагирования на операционный риск (изменения, вносимые в процессы; установление дополнительных способов контроля; обучение работников, в том числе участников процессов; применение автоматизированных решений; другие меры, направленные на уменьшение негативного влияния операционного риска),
- Мониторинг операционного риска.

В целях управления риском информационной безопасности, в том числе киберриска, банк должен определить функции структурного подразделения, ответственного за обеспечение информационной безопасности:

- Мониторинг риска,
- Ведение базы событий риска,
- Участие в реализации процессов, направленных на повышение эффективности управления риском,
- Оценка эффективности управления риском,
- Составление отчетов по событиям риска,
- Осуществление мониторинга сигнальных и контрольных значений показателей уровня риска,
- Участие в разработке внутренних документов;
- Информирование работников банка по вопросам управления риском;
- Осуществление других функций.

Таким образом, рассмотрев понятие операционных рисков, в том числе понятие киберриска, рассмотрев классификацию операционных рисков, предложенную в научных трудах, автором была разработана классификация

операционных рисков по внутренним и внешним источникам их возникновения, а также выявлены процедуры, необходимые для управления операционными рисками.

1.3. Развитие платежных систем в части внедрения технологий и стандартов для снижения рисков мошеннических операций

Платежная система – совокупность организаций, взаимодействующих по правилам платежной системы в целях осуществления перевода денежных средств, включающая оператора платежной системы, операторов услуг платежной инфраструктуры и участников платежной системы, из которых как минимум три организации являются операторами по переводу денежных средств. [44]

Рынок платежных карт представляет собой совокупность отдельных элементов безналичной платежной отрасли, которые осуществляют обслуживание операций с использованием карт и их эквивалентов (мобильные телефоны и иные электронные средства) без которых невозможно его функционирование, являются:

- Инструменты. К данной категории относятся платежные карты и их эквиваленты, используемые держателями карт при проведении платежной операции, а также задействованная при этом инфраструктура обслуживания: банкоматы, платежные терминалы и пр.
- Непосредственные участники. Стороны, задействованные в процессе обслуживания платежных операций, совершаемых при помощи карт. К ним относятся клиенты – держатели карт, торгово-сервисные предприятия, коммерческие банки, платежные системы.
- Другие институты. Совокупность институтов, которые напрямую не задействованы в платежных операциях, но взаимодействуют с

непосредственными участниками: разработчики программного обеспечения, правоохранительные органы и пр.

- Правила. Набор нормативно-правовых документов, регулирующих деятельность всех задействованных на рынке платежных карт участников на различных этапах их взаимодействия на всех уровнях (внутреннем, национальном и международном).

Самые известные и крупные международные платежные системы – это VISA и MasterCard.

Участниками платежной системы являются: Банк России, коммерческие банки и небанковские учреждения (включая клиринговые и расчетные центры).

К компетенции центральных банков относится управление рисками платежных систем. Центральный банк контролирует риск ликвидности, кредитный и системный риски платежной системы, осуществляет регулирование ликвидности ее участников, в том числе на основе функции кредитора последней инстанции, выступает как оператор платежной системы. Отсутствие должного внимания к любому из рисков и способов управления ими может привести к серьезным последствиям, выражающимся в дестабилизации расчетов в регионе или стране в целом вплоть до кризиса платежной системы. Когда банк принимает решение о вступлении в карточную ассоциацию, он тем самым подтверждает готовность следовать установленным платежной системой правилам, определяющим технические, юридические, организационные и финансовые аспекты его функционирования в системе безналичных расчетов, что фиксируется в договоре вступления в платежную систему. Правила являются очень подробными: в них описываются права и обязанности эмитентов и эквайеров, распределение расходов, связанных со случаями мошенничества, механизм урегулирования конфликтных ситуаций, возникающих между участниками рынка и т.п. За нарушение установленных правил и инструкций предусмотрены жесткие санкции. Контроль выполнения участниками правил

платежной системы производится специальным исполнительным органом – администратором платежной системы.

Карточные платежные системы через свои подразделения осуществляют поддержку функционирования инфраструктуры для осуществления платежных операций с использованием карт, обеспечивают процессинг, авторизацию, клиринг и взаиморасчеты по финансовым транзакциям между участниками, разрабатывают и продвигают инновационные платежные решения, обеспечивают глобальную поддержку держателей карт в экстренных ситуациях, предоставляют различного рода консалтинговые услуги и обучающие программы для партнеров по бизнесу и пр.

Благодаря стандартам и требованиям, предъявляемым карточными платежными системами к эмитируемым и программным продуктам, эмитентам, оборудованию и т.п., становится возможным согласованное проведение различного рода операций между участниками системы. Для информационного обмена между участниками предусмотрено распространение через справочно-информационные интернет системы необходимых для корректного ведения бизнеса справочных материалов, внутренних инструкций и приложений, таких как:

- полное описание предлагаемых платежной системой продуктов;
- руководства и методические рекомендации;
- требования к техническим характеристикам и дизайну;
- перечень комиссионных сборов, удерживаемых с кредитной организации за участие в системе, а также сроки и условия их взимания;
- приложения, позволяющие обслуживать уже запущенные банком карточные проекты и пр.

На национальном уровне регулирование сферы обращений платежных карт изначально определяется национальным опытом государства, складывается под воздействием политических, экономических, правовых, культурных и иных традиций. В современных условиях, для которых характерны динамичные изменения на финансовом рынке и быстрые темпы

внедрения инструментов безналичных расчетов, базирующихся на современных банковских технологиях, напрямую зависят от наличия адекватных правовых норм, действие которых защищено санкциями, обеспеченными государственным принуждением.

Как правило, регулирование, наблюдение и контроль за национальной платежной системой в целом и различными ее подсистемами на национальном уровне относятся к компетенции национального центрального банка. В рамках настоящего исследования представляется необходимым исследовать национальный опыт Российской Федерации в части регулирования рынка платежных карт.

В 2011 год был принят Федеральный закона 161-ФЗ «О национальной платежной системе», описывающего НПС и требования к ней, регулирующего порядок оказания через национальную систему платежных услуг и надзора за ней. Однако этот закон также не предусматривал обязательного создания национальной платежной системы и запрета на проведении российских платежей за рубежом.

В начале 2013 года Центробанком был создан реестр операторов платежных систем. В нем были перечислены все существующие на данный момент в России ПС и отмечены наиболее важные: Виза, Contact, МастерКард, Золотая Корона, а также платежные системы ВТБ и Сбербанка.

В марте 2014 года в ответ на присоединение Россией Крыма Visa и MasterCard заблокировали обслуживание карт, выпущенных несколькими российскими банками. Поэтому вопрос о создании национальной платежной системы в России стал актуальным. К закону «О национальной платежной системе» начали разрабатывать поправки, после принятия которых в России будут построены операционные центры и клиринговые платежные центры, а иностранным организациям будет запрещен доступ к данным о внутрироссийских платежных операциях. 27 марта 2014 года создание национальной платежной системы в России было одобрено Президентом РФ.

«Мир» – национальная платежная карта, разработанная в России. По карте «Мир» можно выполнять все привычные операции: снятие и внесение наличных, оплата покупок и услуг, в том числе в интернете.

Национальная система платежных карт (АО «НСПК») – это оператор платежной системы «Мир». НСПК обеспечивает выполнение операций по картам «Мир» и картам международных платежных систем. Все платежи, которые совершаются в России по картам российской и международных платежных систем, обрабатывает операционный платежный и клиринговый центр НСПК. Создавая российскую платежную систему, АО «НСПК» использует собственные разработки и технологии, которые соответствуют всем международным и российским стандартам.

Наличие развитой национальной системы платежных карт – это важный показатель соответствующего уровня развития экономики и финансовой системы и гарантии бесперебойности операций. Национальные платежные системы сформированы и успешно действуют в разных странах мира (Япония, США, Китай, Индия, Белоруссия и другие).

В соответствии с Правилами платежной системы Visa, участник платежной системы обязан осуществлять постоянный контроль и мониторинг операций с использованием банковских карт в целях выявления подозрительных операций и предотвращения мошеннической операций, а также сообщать о всех мошеннических операциях [55].

В связи с тем, что Оператор платёжной системы не оказывает услуг платёжной инфраструктуры (операционных и платёжных клиринговых услуг) и не реализует операционные процессы в платежной системе, участники платёжной системы самостоятельно:

а. Разрабатывают и реализуют порядок и мероприятия по противодействию осуществлению переводов денежных средств без согласия клиента в платёжной системе, в соответствии с требованиями Visa.

б. Получают и применяют полученную от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов

денежных средств без согласия клиента, в целях выявления в платёжной системе операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента.

в. Выявляют и используют информацию о технических данных, описывающих компьютерные атаки в целях противодействия осуществлению переводов денежных средств без согласия клиента.

г. При выявлении информации о технических данных, описывающих компьютерные атаки, направленные на информационную инфраструктуру участника платёжной системы или его клиентов, осуществляют мероприятия по противодействию осуществлению переводов денежных средств без согласия клиента.

д. Уведомляют Оператора платёжной системы о выявленной информации о технических данных, описывающих компьютерные атаки, а также о предпринятых и (или) предпринимаемых мерах для противодействия атакам и осуществлению переводов денежных средств без согласия клиента [55].

По мере того, как общемировой рынок платежных карт развивался, развивалась инфраструктура приема карт, увеличивалось число использования инструмента в повседневных расчетах, усиливалась степень интеграции новых технологий в платежный бизнес. Следующим серьезным шагом в эволюции платежного средства стало смещение интересов платежных систем с массового насыщения мирового рынка в сторону модели развития, ориентированной в большей степени на диверсификацию сопутствующих платежной системе услуг и повышение качества обслуживания конечных потребителей, в которой ключевое значение уделялось следующим аспектам:

- расширение функционала карты (покупки через интернет, мобильная коммерция, денежные переводы и пр.);
- развитие дополнительных приложений (бесконтактные платежи, оплата проезда в транспорте, бонусные программы и пр.);

- внедрение разнообразных элементов защиты в физическую оболочку карты, а также повышение безопасности карточных инфраструктур в целом (EMV-миграция, разработка единых стандартов функционирования и новых методов борьбы с мошенничеством и пр.);
- достижение большей надежности при аутентификации держателей карт (технология 3D-Secure, использование биометрической информации).

Параллельно с развитием платежных карточных систем и эмитируемых ими продуктов динамично развивались сопутствующие бизнесу области и направления, например, дистанционное банковское обслуживание.

Важнейшим условием массового распространения любого продукта на рынке, в том числе пластиковых карт, является наличие стандартов, определяющих их характеристики и функциональность. Одним из важнейших стандартов, разрабатываемых крупнейшими карточными платежными системами, применение которого для участников рынка постепенно становится обязательным, является международный стандарт для операций по картам с чипом, получивший название EMV.

Международные платежные системы, использовавшие традиционные магнитные карты, столкнулись с ростом карточного мошенничества, обусловленного сравнительной простотой подделки платежных карт, а также с необходимостью сделать свои карточные продукты более привлекательными для конечного потребителя за счет предоставления ему с их помощью дополнительных услуг помимо традиционной платежной функции.

В 1993 г. международные платежные системы Europay, MasterCard и Visa в лице представляющих их интересы компаний Europay International S.A., MasterCard International Incorporated и Visa International Service Association выступили с инициативой создания глобального проекта, основной целью которого является разработка и унификация международных спецификаций для дебетовых и кредитных чиповых карт, приложений и терминалов, который бы позволил повысить уровень безопасности транзакций по платежным картам.

Новый уровень безопасности позволил банкам-эмитентам карт перенести ответственность за утерянные средства таким образом, что с 1 января 2005 года торгующие организации или банки-эквайеры несут ответственность за мошеннические транзакции, совершенные при помощи систем, не поддерживающих стандарт EMV.

Чип имеет существенно более высокую степень защиты по сравнению с магнитной полосой. Секретный ключ чипа, идентифицирующий карту в банковских операциях, хранится в защищённой памяти, он записывается в память чипа на стадии изготовления, и его невозможно оттуда извлечь с помощью внешних устройств, не нарушая целостности самого чипа.

На текущий момент допустимо издание чиповых карт, содержащих в том числе и магнитную полосу на самой карте. Именно возможность провести транзакцию по чиповой карте, не используя собственно чип, является уязвимостью, используемой на данный момент технологии - то есть для успешной мошеннической транзакции достаточно скопировать магнитную полосу. Или, что даже более просто – для мошеннической операции в интернете достаточно знать полный номер карты, срок её действия, и значение кода CVV, которые просто текстом напечатаны на самой карте.

История 3DS началась больше 20 лет назад. В 1999 году Visa создала протокол безопасности 3D Secure, чтобы помочь торгово-сервисным предприятиям и банкам-эмитентам подтверждать (аутентифицировать) личность держателей карт при совершении покупок в интернете.

Для повышения безопасности расчётов в интернете система Visa ввела дополнительную меру безопасности, получившую название Verified by Visa, или VbV, так же называемая технологией 3-D Secure. Суть системы в том, что при оплате товаров или услуг в интернете необходимо ввести дополнительный проверочный код, который владелец карты получает от банка-эмитента карты.

Аутентификация плательщика осуществляется с помощью ввода дополнительного кода подтверждения. Проверочный код формируется банком-эмитентом и направляется плательщику в процессе оплаты. Он может

приходить в виде SMS или push-сообщения или выдаваться при получении карты.

Платёжная система VISA позволяет магазину проводить оплату для карт Visa по данным карты (номер карты, срок действия карты, код CVV), без необходимости подтверждения оплаты дополнительным проверочным кодом (технология 3-D Secure). Такой подход к оплате предполагает, что в случае спора по данной покупке магазин возьмет на себя риски, связанные с правомерностью оплаты и средства будут возвращены держателю карты. Таким образом, у магазина, поддерживающего технологию 3-D Secure есть выбор – дополнительно проверить покупку используя проверочный код, уменьшив риск возможного мошенничества, либо не использовать данную проверку, взяв на себя связанные с возможным мошенничеством риски.

Код CVV запрещено сохранять на любом из этапов осуществления покупки любым из участников платежной системы. Таким образом значительно снижается риск последующих мошеннических покупок при компрометации сохраненных платежных реквизитов карт, поскольку CVV попросту нигде не хранится. Такая мера безопасности позволяет удостовериться в том, что у покупателя есть физический доступ к карте при каждой покупке.

Совет по стандартам безопасности индустрии платежных карт (Payment Card Industry Security Standard Council) является главным международным регулирующим органом в сфере безопасности обращения платежных карт. Совет был создан в 2006 г. для разработки и продвижения единого набора требований к обеспечению безопасности данных (Payment Card Industry Data Security Standard, далее – PCI DSS), разработанного двумя годами ранее путем объединения требований программ по безопасности платежных систем Visa, MasterCard, American Express, Discover Card и JCB. Действие стандарта PCI DSS, содержащего двенадцать детализированных требований к обеспечению безопасности данных, объединенных в шесть областей контроля, обязательно для исполнения во всех организациях, задействованных в процессах передачи,

обработки и хранения данных держателей карт, примером которых являются банки-эмитенты, торгово-сервисные предприятия, принимающие карты к оплате, сервис-провайдеры и т.п. Каждые три года стандарт обновляется с учетом пожеланий участников платежной индустрии. Контроль за соответствием требований, изложенных в стандарте, лежит на ответственности платежных систем, которые определяют способы подтверждения требований PCI DSS и размер штрафных санкций за их несоблюдение. Минимальный уровень проверки представляет собой заполнение опросного листа самооценки (Self Assessment Questionnaire) организацией самостоятельно; для крупных организаций с большим объемом проходящих данных предусмотрено проведение ежегодного аудита с привлечением сертифицированного специалиста QSA и/или ежеквартального сканирования сети.

Таким образом, в данном параграфе было рассмотрено понятие платежная система, изучена история развития национальной платежной системы, а также рассмотрены внедренные технологии и стандарты для снижения риска мошенничества по картам.

В следующей главе автором будет исследованы различные виды мошенничества, произведена их классификация, а также выявлены актуальные методы снижения рисков мошенничества.

ГЛАВА 2. ИССЛЕДОВАНИЕ ВИДОВ МОШЕННИЧЕСТВА И АКТУАЛЬНЫХ МЕТОДОВ СНИЖЕНИЯ РИСКОВ МОШЕННИЧЕСТВА ПО БАНКОВСКИМ КАРТАМ И СИСТЕМАМ ДБО

2.1. Виды мошенничества с банковскими картами и системами ДБО

Проблема безопасности по-прежнему остро стоит перед банками и обществом. Сегодня каждому участнику процесса, использующему банковские карты, очевидно, что существует риск поломки оборудования, технологического сбоя, а также мошеннических действий со стороны злоумышленников. Все эти риски несут негативные последствия, как для банка, так и для клиента. Для последнего он заключается в потере денежных средств, а для банков – в финансовом риске и риске потери деловой репутации. Все это вынуждает банки постоянно совершенствовать систему по минимизации рисков, связанных с банковскими картами и системами ДБО.

Рассмотрим более подробно мошеннические схемы с использованием банковских карт.

а. Скимминг. С помощью сканирующего устройства – скиммера, который устанавливается на банкомат, считываются данные по карте с магнитной полосы, необходимые в дальнейшем для изготовления «белого пластика» – поддельной банковской карты. ПИН-код узнается с помощью расположенной недалеко видеокамеры или накладной клавиатуры.

б. Ливанская петля – вид мошенничества, когда в картоприемник вставляется устройство, которое удерживает карту от возврата её владельцу. Возле жертвы мошенничества появляется прохожий, который рассказывает о похожей ситуации и сообщает, что нужно набрать определенную комбинацию и ввести ПИН-код. Жертва мошенничества сообщает ПИН-код мошеннику, но после того, как комбинация не помогла, тот же самый человек советует

немедленно обратиться в банк. Тем временем карта изымается из устройства и с нее списываются денежные средства.

в. Фальшивые банкоматы. Мошенники производят фальшивые банкоматы или переделывают старые банкоматы, которые выглядят как настоящие. Такие банкоматы размещают в оживленных местах. После попытки снятия денежных средств, на дисплее появляется надпись, что денежных средств недостаточно или, что банкомат не работает. А мошенники тем временем скопировали данные с карты.

г. Фишинг – хищение персональных данных с помощью поддельных сайтов. Мошенники рассылают клиентам письма на электронную почту (или SMS-сообщениями или письмами в социальных сетях) со ссылкой на поддельный сайт, где клиент вводит конфиденциальные данные, которые становятся доступными мошенникам.

После нажатия соответствующей кнопки или клика по ссылке держатель банковской карты попадает на сайт, внешне напоминающий по дизайну известный сайт (сайт Банка, интернет-магазина). На поддельном сайте клиент вводит данные карты, номер карты, дату окончания и CVV код, либо вводит логин и пароль для входа в ДБО. После ввода данных, они становятся доступными мошеннику.

Существуют интернет-магазины, где для оплаты не обязателен ввод одноразовый пароль из SMS, достаточно знать номер карты, CVV код и дату окончания карты, чем пользуются мошенники.

д. Компрометация в торговой точке – оплата клиентом товара картой в терминале, далее получение доступа мошенниками к базе данных предприятия торговли и получение данных по картам.

е. Компрометация в торговой точке интернет-магазина, в котором осуществляется оплата клиентом товара с введением данных по карте. Данные по картам мошенники получают из компьютерной системы торговой точки, не имеющей необходимых средств безопасности для предотвращения несанкционированного доступа.

ж. При оплате за границей в мошенническом терминале, происходит считывание данных по карте, затем выпускается карта (белый пластик) с этими данными и происходят снятия в банкоматах

з. SMS-сообщения с психологическим воздействием на клиента для совершения необходимых мошенникам действий:

- SMS о блокировке карты клиента с указанием номера телефона, на который необходимо перезвонить;
- SMS о попадании родственника в неприятную ситуацию с просьбой перевода денежных средств;
- SMS о выигрыше, для получения которого необходимо сначала заплатить комиссию.

и. Мошенничество с использованием сервисов объявлений покупки и продажи товаров или услуг: «Авито», «Юла». Мошенники связываются с продавцом товара и направляют ему ссылку на поддельный сайт, где при вводе данных карты и одноразового пароля происходит перевод денежных средств мошеннику.

к. Клиенты попадают на поддельные сайты, набирая в строке поиска «покупка билетов», «оплата сотовой связи» и пр., где при вводе данных карты и одноразового пароля происходит перевод денежных средств мошеннику.

л. Мошенники взламывают страницы клиентов в социальных сетях и рассылают от имени пострадавшего письма с просьбой перевести денежные средства («в долг», «на лечение родственника»), указывая данные мошенника для получения денежных средств.

м. Заражение компьютера / телефона вирусным программным обеспечением при скачивании программ / приложений в интернете, которое передает данные по карте или данные для входа в систему ДБО мошенникам.

н. Реклама в интернете для моментального получения налоговых вычетов, выигрышей, для получения которых сначала нужно заплатить комиссию, почтовый сбор и пр.

о. Сговор с сотрудниками банка. Сотрудники банка, имея доступ к базам данных по клиентам, передают информацию мошенникам.

п. Сговор с сотрудниками предприятий торговли. Кассир при осуществлении оплаты по карте через терминал, может зафиксировать данные карты и передать мошенникам.

р. Дружественное мошенничество. Использование карты членами семьи, коллегами или друзьями, у кого есть доступ к данным по карте, известен ПИН-код или доступ к телефону и SMS-сообщениям, а также возможность входа в систему ДБО.

с. Кража / утеря карт. Рядом с картой может быть написан ПИН-код, либо можно осуществлять бесконтактную оплату в торговых предприятиях до 1000 рублей без ввода ПИН-кода.

т. Кража / утеря телефона. Возможность зайти в систему ДБО и совершать переводы, подтверждая их одноразовыми паролями, которые поступают на телефон (SMS-сообщение, PUSH-уведомление)

у. Социальная инженерия – хищение данных посредством воздействия на психику. В настоящее время, мошенники звонят клиентам, и путем психологического манипулирования получают конфиденциальные данные.

Например, представляются службой безопасности Банка и сообщают о несанкционированной операции по карте, при этом для остановки несанкционированного платежа, нужно назвать номер карты, дату окончания, CVV код, а также одноразовый пароль из SMS-сообщения. Таким образом, у мошенников есть все данные для осуществления перевода на свою карту. Либо просят сообщить данные, которых мошеннику достаточно для регистрации системы дистанционного банковского обслуживания, затем осуществляется вход в систему ДБО клиента и переводы со всех доступных счетов клиента на счета мошенников.

В данном случае решающим фактором является уровень критичности мышления в стрессовой ситуации. Стресс – это сильное эмоциональное потрясение [26], которое может иметь негативный характер (по карте клиента

прошла несанкционированная операция и нужно срочно её отменить), а может быть положительным и радостным (начислены дополнительные проценты / бонусы и их нужно срочно зачислить на карту, иначе они «сгорят»).

В 2019 г. в арсенале мошенников появился новый способ обмана клиентов. Технология подмены исходящего телефонного номера на номера, идентичные номерам контактных-центров банков, позволила им успешно выдавать себя за сотрудников служб безопасности банков. Обладая персональными данными, мошенники имитируют диалог с сотрудником банка, государственной структуры или иной организации. Исходя из предположения, что указанные данные могут быть известны только им, клиент поддается на обман, сообщая в конечном итоге кодовые слова, коды подтверждений и другую информацию, предоставляющую мошенникам возможность вывести со счетов клиента денежные средства.

Отличительная черта этого вида мошенничества – таргетированность на конкретные группы граждан: конечной целью злоумышленников является перевод средств жертв на их счета, при этом средства ее достижения варьируются.

Вариант получения доступа к звонкам и SMS-сообщениям клиента – установка переадресации звонков и SMS.

Для получения доступа к компьютеру или телефону клиента, чтобы войти в систему ДБО клиента, мошенники обманным путем устанавливают программы удаленного доступа и таким образом сами удаленно осуществляют все операции по переводу денежных средств.

Для хищения денежных средств методом социальной инженерии мошенникам достаточно владеть информацией о фамилии, имени и отчестве, а также о номере телефона физического лица, стальные необходимые данные мошенники получат при разговоре с клиентом.

Фактором, обусловливающим успешность хищения, является низкий уровень «компьютерной гигиены» жертвы. Переход по ссылкам из непроверенных источников на зараженные сайты, скачивание различных

приложений и бесплатных аналогов известных программ на мобильные телефоны, игнорирование установки антивируса и его предупреждений – все это делает возможным получение мошенниками логина и пароля от системы ДБО или данных по банковской карте.

Различные виды мошенничества автор систематизировала по каналу взаимодействия.

Таблица 4 – Систематизация видов мошенничества по каналу взаимодействия с клиентом

Канал взаимодействия	Вид мошенничества
Банкоматы	1. Скимминг 2. Ливанская петля 3. Фальшивые банкоматы
Предприятия торговли	1. Компрометация в торговой точке – оплата клиентом товара картой в терминале, далее получение доступа мошенниками к базе данных предприятия торговли и получение данных по картам 2. При оплате за границей в мошенническом терминале, происходит считывание данных по карте, затем выпускается карта (белый пластик) с этими данными и происходят снятия в банкоматах
Электронная почта	Письмо на электронную почту со ссылкой на мошеннический сайт, где клиент вводит конфиденциальные данные, которые становятся доступными мошенникам

Продолжение таблицы 4

Телефон	1. Звонок клиенту и путем психологического манипулирования получение конфиденциальных данных 2. SMS-сообщения с психологическим воздействием для совершения необходимых мошенникам действий
Сеть интернет (покупки в интернет-магазинах, работа с сайтами, социальные сети)	1. Сервисы объявлений покупки и продажи товаров или услуг: «Авито», «Юла» 2. Поддельные сайты Банков для получения конфиденциальных данных для входа в систему ДБО 3. Поддельные сайты оплаты билетов, связи и пр., для перевода денежных средств мошенникам 4. Взлом страницы в социальной сети и рассылка писем с просьбой перевести денежные средства 5. Заражение компьютера / телефона вирусным программным обеспечением при скачивании программ / приложений в интернете 6. Компрометация в торговой точке интернет-магазина – оплата клиентом товара с введением данных по карте,

Окончание таблицы 4

	далее получение доступа мошенниками к базе данных интернет-магазина и получение данных по картам 7. Реклама получения налоговых вычетов, выигрышей и пр., для получения которых сначала нужно заплатить комиссию, почтовый сбор и пр.
Через третьих лиц	1. Сговор с сотрудниками банка 2. Сговор с сотрудниками предприятий торговли, кассир может зафиксировать данные карты и передать мошенникам
Прямой доступ к карте / системе ДБО	1. Дружественное мошенничество 2. Кража / утеря карт (бесконтактная оплата до 1000 рублей) 3. Кража / утеря телефона

Из таблицы видно, что большинство мошеннических схем осуществляется в интернете, и попасть на них может любой человек.

В связи с развитием финансовых услуг, совершаемых в сети Интернет, тем более с учетом пандемии коронавирусной инфекции, в дальнейшем сохранится восходящий тренд совершения операций без согласия клиентов именно в этом канале (операции в сети Интернет без предъявления кары).

Итак, все рассмотренные мошеннические схемы позволяют выделить ряд рисков как для самих держателей, так и для банка-эмитента.

Определим риски для держателей банковских карт:

- финансовые. Любая жертва злоумышленников рискует потерять свои денежные средства.
- правовые (риски, связанные с судебными тяжбами). Держатель карты заключил договор с банком, который регулируется законами Российской Федерации. Даже если банк отказал в возврате денежных средств по несанкционированной операции, клиент может обратиться в суд. Однако следует иметь в виду, что от момента совершения несанкционированной операции до окончания судебного разбирательства пройдет длительное время. При этом, и в суде Банк может доказать, что клиент нарушил условия договора, предусматривающие необходимость сохранения конфиденциальности платежной информации.

При обращении в банк для опротестования операции, держатель карты должен доказать факт мошенничества. Для успешного рассмотрения заявления потребуется приложить копии всех документов, подтверждающих неправомерность операции. Это могут быть чеки, выписки по счету, копия заявления в полицию о факте мошенничества – все, что может подтвердить факт незаконности. По факту заявления служба безопасности банка также обязана провести проверку, собрать документальные подтверждения для признания спорной транзакции обоснованной или нет;

- поведенческие риски. Зачастую свою банковскую карту держатели передают третьим лицам: родственникам и знакомым. Однако последние в свою очередь могут не соблюдать мер безопасного ее использования, и персональные данные будут похищены;
- риск быть обманутым самими сотрудниками банка. Недобросовестные сотрудники Банка могут узнать у клиента данные по карте или логин и пароль к системе дистанционного банковского обслуживания под предлогом помощи клиенту.

Исходя из рассмотренных рисков держателям банковских карт следует соблюдать меры безопасности:

- закрывать клавиатуру при вводе ПИН-кода. Основное предназначение данного кода заключается в том, что он известен только владельцу банковской карты, поэтому любые действия, связанные с попыткой третьих лиц узнать его, являются мошенничеством;
- подключать услугу SMS-информирования. Данная услуга обслуживающего банка позволяет держателю карты мгновенно узнать о неправомерных действиях с картой, а значит, быстро отреагировать на них;
- пользоваться банкоматами, установленными в офисах банка. Кроме того, мошенникам труднее установить сканирующие устройства, поскольку в отделениях банков работают видеокамеры. Банкоматы, установленные в деловых и торговых центрах, на улицах, в большей степени подвержены мошенническим действиям;

Банки также несут ряд определенных рисков, связанных с мошенническими действиями:

- репутационный риск. Мошеннические операции снижают репутацию банков и в целом доверие клиентов при использовании банковской карты как удобного и безопасного инструмента. Именно поэтому уделяется большое внимание противодействию мошенничеству, как со стороны Банка России, так и со стороны кредитных организаций, так и со стороны платежных систем;
- финансовые. Возврат клиенту похищенных денежных средств, в том числе по решению суда.
- риск мошеннических действий со стороны клиента – держателя банковской карты. Нередки случаи, когда держатель карты находится в сговоре с мошенниками. Например, клиент сообщает в Банк о несанкционированном снятии со своей карты денежных средств, но при этом все необходимые данные были переданы третьим лицам умышленно. Отчасти поэтому банки проводят расследование, поскольку, если не будет доказана непричастность владельца карты к

снятию денежных средств с карты, банк обязан выплатить владельцу карты все похищенные денежные средства.

Таким образом, были рассмотрены различные виды мошенничества и произведена систематизация видов мошенничества по каналу взаимодействия с клиентом.

2.2. Методы Банка России и коммерческих банков по снижению рисков мошенничества

Коммерческие банки для снижения мошеннических операций:

- Осуществляют мониторинг операций клиентов по картам и системам ДБО, при этом меняют правила обработки операций при появлении новых видов мошенничества, создают эффективные скрипты для разговора с клиентом;
- При выявлении несанкционированной операции клиента, проводят мероприятия по минимизации повторных несанкционированных операций (блокировка карты, её перевыпуск, информирование клиента о причинах несанкционированной операции и мерах предосторожности);
- Направляют информацию в ФинЦерт об операциях без согласия;
- В режиме он-лайн передают информацию по электронной почте об операциях без согласия для возможности сохранения денежных средств;
- При направлении одноразового кода для подтверждения операции, добавляют в текст SMS-сообщения информацию о том, что никому нельзя сообщать одноразовый код, в том числе сотруднику банка;
- Информируют клиента о совершенной операции путем направления SMS-сообщения или PUSH-уведомления;
- Выдают памятки клиентам о безопасном использовании банковских карт;

- На официальных сайтах банки публикуют информацию о видах мошенничества, о способах защиты от мошенничества;
- Рассылают клиентам письма на электронную почту о безопасном использовании банковских карт и систем ДБО, о видах мошенничества;
- Реализуют возможность установки лимитов по операциям (на день, на месяц, на одну операцию);
- Реализуют возможность запрета осуществления операций в интернете.
- Предлагают клиентам приобрести полисы страхования;
- Осуществляют расследование инцидентов (по несанкционированным операциям) для выявления мошеннической схемы, для поиска торговых точек/банкоматов, где происходит компрометация данных;
- Проводят претензионную работу по заявлениям клиентов о совершении несанкционированной операции;
- Блокируют и перевыпускают карты при получении информации от платежных систем о компрометации карт;
- Работают в тандеме с операторами связи для выявления номеров телефонов, с которых звонят мошенники;
- Проводят мероприятия по безопасному использованию информации с банковскими картами сотрудниками банка (не имели доступа к ПИН-кодам карт, к полным номерам карт);
- Реализация виртуальной / цифровой карты для безопасного использования в сети интернет;
- Направляют информацию клиенту о входе (о неуспешной попытке входа) в систему ДБО по SMS или по электронной почте;
- Направляют в Банк России предложения по снижению мошеннических операций.

Часть рисков мошенничества по законодательству переложена на кредитные организации, то есть в случае проведения операции без согласия клиента, банк обязан вернуть денежные средства клиенту, при соблюдении условия, что клиент обратился в банк не позднее, чем на следующий день

после несанкционированного списания и он соблюдал порядок пользования картой. При этом, Банк должен выяснить, действительно ли операция была мошеннической или клиент нарушил правила безопасности пользования картой.

Если клиент приобретает полис страхования, то он должен понимать от каких рисков действует защита.

а. Если третьи лица незаконно получили денежные средства в результате [53]:

- использования карты после её утраты в результате грабежа или разбоя;
- получения карты и PIN-кода с применением насилия или угроз насилия и последующего снятия наличных в банкомате;
- подделки подписи и последующего получения наличных в любом банке;
- использования поддельной карты с действительными реквизитами для оплаты покупок и услуг либо снятия наличных в банкомате;
- фишинга, скимминга и подобных действий по получения информации с карты;
- хищения (грабежа, разбоя) наличных в течение двух часов с момента снятия их в банкомате.

б. Если клиент утратил карту вследствие:

- случайных механических повреждений или размагничивания;
- грабежа, разбоя, кражи;
- неисправности банкомата.

Таким образом, в случае, когда клиент сам сообщает мошенникам конфиденциальную информацию, полис страхования не действует. А с учетом данных, что около 70 процентов операций без согласия клиента осуществляется методами социальной инженерии, то все эти случаи страховка не покроет. Поэтому данный инструмент не является эффективным инструментом снижения риска мошенничества.

Автором рассмотрены и представлены в Таблице 5 методы разных коммерческих банков по снижению рисков мошеннических операций при осуществлении операций по картам и системам ДБО.

Таблица 5 – Методы коммерческих банков по снижению рисков мошеннических операций[2]

Наименование Банка	СКБ-Банк	УБРиР	Сбербанк	Альфа-банк	СитиБанк	Тинькофф
Осуществление мониторинга операций	Да	Да	Да	Да	Да	Да, совместно с операторам и связи
Наличие на сайте информации о мониторинге операций	Нет	Нет	Да, каким образом не указано	Да, с клиентом созванивает-ся сотрудник или высылается SMS	Да, указано что клиенту поступает SMS и с какого номера поступает SMS	Да, с клиентом созванива-ется сотрудник
Страхование карт	Нет	Есть	Есть	Есть	Нет	Есть
Информация о видах мошенничества	Есть	Есть	Есть	Есть	Есть	Есть
Памятка безопасного использования карт	Есть	Есть	Есть	Есть	Есть	Есть
Возможность установить лимиты	Есть, но на сайте нет информа ции	Есть	На сайте информация не найдена	Есть	На сайте информация не найдена	Есть
Виртуальная или цифровая карта	Да	Да	Да	Да	На сайте информация не найдена	Да
Какие методы минимизации мошенничества, кроме мониторинга		Предложение клиентам высылать подозритель-ное сообщение в банк, банк передаст мошеннечес-кие SMS в правоохрани-тельные органы	Предложение клиентам высылать номер телефона или сайт, который клиент хочет проверить. Если банк найдет совпадение в базе, то напишет что предпринять	Ограничение на осущес-твление определен-ных операциq по карте	- Предложение клиентам сообщить об угрозе -Информируют клиентов о том, что системы обнаружат, если смартфон клиента заражен вредоносной программой	Возмож-ность запретить операции в интернете

[2] Составлено автором по: [4,5,6,52,53,54]

По результатам было выявлено, что все исследуемые банки осуществляют мониторинг операций, но не у всех из них есть на сайте информация об этом. Только у КБ «Ситибанк» есть конкретная информация о том, что клиенту поступает SMS-сообщение и указано с какого номера оно поступает.

На X Международном форуме «Борьба с мошенничеством в сфере высоких технологий. ANTIFRAUD RUSSIA – 2019» главная дискуссия была на тему – «Банки, операторы связи и регуляторы – вместе или врозь против киберпреступников?» [66], на которой обсуждался вопрос взаимодействия банков и операторов связи при осуществлении мониторинга операций. В 2020 году АО «Тинькофф банк» стал первым российским банком, который протестировал и внедрил в свою антифрод-платформу технологию, разработанную крупнейшими операторами мобильной связи – Мегафоном, Tele2, МТС.

Также было выявлено, что на официальном сайте АО КБ «Ситибанк», на главной странице баннер красного цвета «Важная информация о безопасности», при нажатии на который открывается информация по всем вопросам безопасности и защите от мошенничества. На сайтах других банков не было обнаружено таких акцентов на безопасность. Также, на сайте АО КБ «Ситибанк» имеется важная информация для клиента о том, что банковские системы обнаружат, если смартфон клиента заражен вредоносной программой и клиент будет об этом уведомлен.

Таким образом, были рассмотрены методы разных коммерческих банков по снижению рисков мошеннических операций и выявлено, что коммерческие банки используют разные методы: такие как минимальный обязательный набор (мониторинг, размещение памятки о безопасном использовании карты), так и другие, позволяющие предотвратить хищение средств клиентов, а также совершенствуют уже имеющиеся методы снижения рисков мошенничества.

Банк России ставит перед собой задачи по противодействию кибератакам:

а. Организует и координирует деятельность банков в качестве центра компетенций по противодействию кибератакам:

- Собирает все инциденты в ФинЦерт,
- Проводит анализ инцидентов,
- Распространяет информацию об инцидентах другим банкам.

б. Координирует деятельность по блокировке несанкционированных переводов денежных средств в платежной системе Банка России.

в. Прекращает работу фишинговых ресурсов и ресурсов, распространяющих вредоносное программное обеспечение, телефонных номеров и SMS-рассылок, используемых в мошеннических целях [35].

г. Повышает финансовую грамотность населения.

Меры, принимаемые Банком России для минимизации риска мошеннических операций:

а. Внесение изменений в законодательство Российской Федерации в сфере обеспечения информационной безопасности кредитных организаций. После принятия необходимого закона, Банка России сможет блокировать фишинговые сайты.

б. Готовятся поправки в Федеральный закон 115-ФЗ, предусматривающие создание единого канала обмена между операторами связи и банками данными о мобильных устройствах и абонентах.

в. Повышение финансовой грамотности населения. Был создан ресурс «Финансовая культура», который способствует формированию финансовой культуры граждан.

г. Банк России рекомендует банкам повышать качество работы по доведению до клиентов информации о рисках использования электронных средств платежа. Указанную работу Банки должны проводить в соответствии с Положением Банка России №382-П: «Оператор по переводу денежных средств обеспечивает доведение до клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не

обладающими правом распоряжения этими денежными средствами, и рекомендуемых мерах по их снижению» [47].

д. Реализовано оперативное информирование банков об операциях без согласия клиентов по системе ФинЦерт.

В соответствии с Федеральным законом №167-ФЗ у банков есть обязанность проверять операцию на соответствие признакам, указывающим, что операция осуществляется без согласия клиента. В случае соответствия признакам, Банк обязан приостановить такую операцию, заблокировать электронное средство платежа и связаться с клиентом для подтверждения операции [42].

Существует две категории признаков операций, совершенных без согласия клиента, которые были установлены Банком России:

- Данные о получателях и параметрах устройства совпадают с данными из базы данных Банка России;
- Не типовая операция для клиента: сумма операции не совпадает с проведенными ранее, время проведения операций и т.д.

Осуществление проверки снижает риск проведения операции без согласия клиента. Но под психологическим воздействием клиент может подтвердить легитимность операции сотруднику банка. Если у банка есть информация об операции без согласия клиента или о попытке операции, то банк должен не позднее следующего рабочего дня сообщить о ней в Банк России.

После того как Банк России получает информацию об операции без согласия клиента, производится определение Банка, обслуживающего получателя, и по системе отправляется уведомление данного банка.

Если пострадавший клиент обратился в правоохранительные органы, то банк также заводит в систему номер обращения. Таким образом, в Банке России формируется возможность сопоставления фактов обращения граждан в полицию по операции без согласия, сведений о самих операциях и их

получателей. Данную информацию Банк России может направить в МВД России с целью повышения уровня раскрываемости преступлений.

Информирование банков об операциях без согласия является каналом оперативного уведомления, для этого автором была разработана схема представлена взаимодействия Банка России и коммерческих банком по операциям без согласия клиентов и представлена на Рисунке 3.

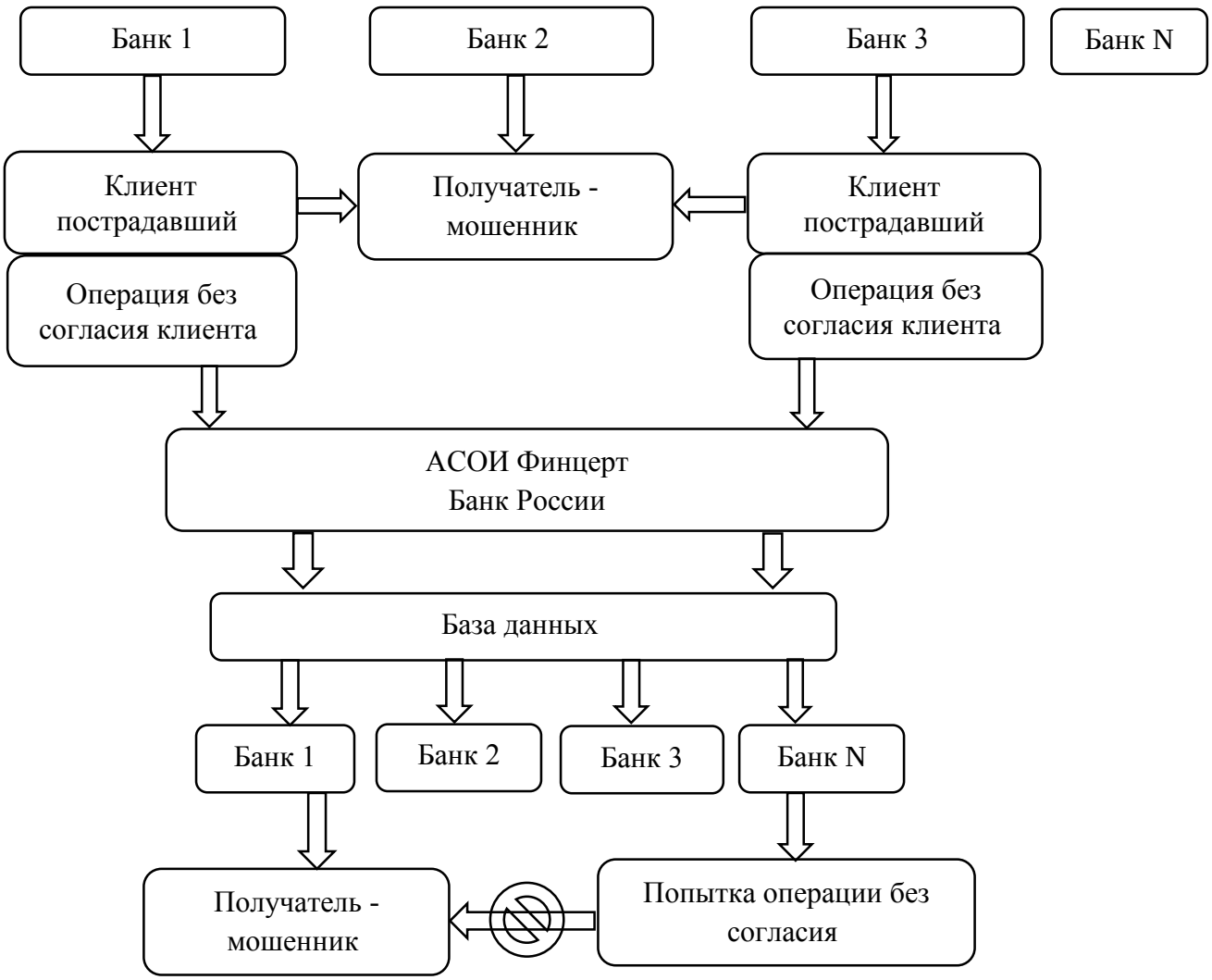

Рисунок 3 – Схема взаимодействия Банка России и коммерческих банков по операциям без согласия клиентов

Таким образом, используя автоматизированную систему обработки информации Финцерт, коммерческие банки получают оперативное уведомление по мошенническим операциям, а новые попытки несанкционированных операций будут предотвращены.

2.3. Мониторинг операций как главный инструмент коммерческих банков для предотвращения мошеннических действий

К современным технологическим решениям, используемым для противодействия мошенничеству, относятся системы мониторинга транзакций (СМТ).

Мошенничество с банковскими картами приводит к финансовым потерям и снижению доверия со стороны клиентов к данному банковскому продукту, поэтому важно осознать актуальность мер противодействия и разработать комплексный подход к решению проблемы для уменьшения рисков. Раннее обнаружение мошенничества и принятие адекватных и эффективных мер являются необходимыми условиями обеспечения безопасности ПСБК и должны проводиться в рамках мероприятий по управлению операционным риском в банке.

Общие требования к СМТ и задачи мониторинга транзакций в ПСБК.

- Мониторинг транзакций по банковским картам должен обеспечивать анализ всех авторизационных и клиринговых операций по банковским картам в ПСБК и принятие решений по подозрительным на предмет мошенничества операциям с целью уменьшения рисков.
- Система мониторинга транзакций является инструментом уменьшения рисков, связанных с проведением мошеннических операций по банковским картам, и должна быть составной частью комплексного подхода к обеспечению безопасности ПСБК банка.

Выбор той или иной СМТ банком-эмитентом должен основываться на анализе существующих рисков. Система должна использоваться для снижения финансовых потерь банка и держателей карт, снижения недовольства клиентов и повышения доверия к банку.

Основными целями мониторинга ИБ в организации являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных под заданные руководством цели.

Под транзакцией (или операцией) понимается одно из следующих определений:

- инициируемая держателем карты последовательность сообщений, вырабатываемых и передаваемых друг другу участниками системы для обслуживания держателей карт, при соблюдении свойств неделимости (должны выполняться все составляющие транзакции или не выполняться ни одна), согласованности (транзакция не нарушает корректности информации в базах данных), изолированности (отдельная транзакция не зависит от других), надежности (завершенная транзакция должна восстанавливаться после сбоя, а незавершенная – отменяться);
- единичный факт использования карты для приобретения товаров или услуг, получения наличных денежных средств или информации по счету, следствием которого является дебетование или кредитование счета клиента.

В соответствии с ранее приведенным определением мошенническая операция – операция с использованием банковской карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Мониторинг использует набор критериев и признаков (fraudulent pattern), позволяющих идентифицировать и своевременно пресечь несанкционированное использование карты.

Таким образом, СМТ в ПСБК являются одним из средств выявления и противодействия мошенничеству с банковскими картами. Существуют обязательные требования МПС к мониторингу, но они являются общими и в настоящее время недостаточными ввиду их принципиальной ориентированности на формирование регулярных отчетов, а не выявление мошенничества в реальном или близком к реальному времени.

Процесс обнаружения и предотвращения мошенничества не имеет начальной или конечной стадии, он выполняется непрерывно и включает в себя следующие подпроцессы:

- Мониторинг;
- Обнаружение;
- Принятие решений;
- Обучение.

Функция у всех антифрод-систем едина – выявлять и предотвращать мошенничество.

На основании таблицы, где произведена систематизация видов мошенничества по каналу взаимодействия с клиентом, по каждому каналу рассмотрим инструменты, которые позволят снизить риск мошенничества.

Таблица 6 – Инструменты снижения рисков мошенничества по каналу взаимодействия с клиентом

Канал взаимодействия	Инструмент снижения риска мошенничества
Банкоматы	Мониторинг операций, установка лимитов (ограничений в операции) на страну, повышение грамотности клиентов
Предприятия торговли	Мониторинг операций, претензионная работа, повышение грамотности клиентов
Электронная почта	Антивирус, повышение грамотности клиентов

Продолжение таблицы 6

Телефон	Мониторинг операций, вместе с операторами связи как Тинькофф, установка лимитов для пожилых клиентов на сумму, на оплаты и переводы в интернете, повышение грамотности клиентов
Сеть интернет (покупки в интернет-магазинах, работа с сайтами, социальные сети)	Мониторинг операций, установка запрета на операции в интернете
Через третьих лиц	Мониторинг внутреннего мошенничества, ограниченный доступ к данным по картам, мониторинг операций
Прямой доступ к карте / системе ДБО	Мониторинг операций, повышение грамотности клиентов

Таким образом, можно сделать вывод, что система мониторинга является самым актуальным инструментом для предотвращения операций без согласия клиента, управляя риском мошенничества.

Системы мониторинга транзакций по картам ранее не были настроены на отказ в операции, так как такая операция как перевод с карты на карту является моментальной и приостановить её нет возможности, можно либо разрешить перевод денежных средств, либо отклонить перевод. Ассоциация банков направила письмо в Банк России 10 января 2019 года, подготовив несколько вопросов по противодействию переводам денежных средств без согласия клиентов в рамках Федерального закона от 27.06.2018 №167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств». В частности, вопрос касался операций по картам, а именно отсутствия

технической возможности приостановления исполнения распоряжения. Банк России дал пояснения, что под термином «Приостановление исполнения распоряжения» следует понимать отказ в авторизации операции, в то время как «Возобновление исполнения распоряжения» означает обеспечение возможности проведения по запросу клиента авторизации операции, аналогичной приостановленной по сумме, валюте, получателю и назначению, при наличии доступного остатка денежных средств на банковском счете клиента, к которому привязана платежная карта клиента [39]. При этом, если банк откажет в авторизации операции, которая была легитимна, возникнет негативная реакция клиента. Поэтому возникают высокие требования к мониторингу операций в части максимально возможной точности определения мошеннический операций.

В рамках диссертационного исследования был проведен опрос, в котором приняло участие 50 человек. Были сформулированы гипотезы, часть из которых подтвердилась после обработки результатов опроса. Результаты опроса с количественным значением и процентным соотношением приведены в Таблице 7.

Гипотеза 1. Существует разнообразие мошеннических схем в пространстве интернет, значит большое количество клиентов – держателей банковских карт осуществляет оплаты с использованием карты в интернете.

Гипотеза 2. В текущее время мошенничество по картам очень распространено, значит много владельцев карт должно сталкиваться с разными видами мошенничества. Поэтому необходимо работать в направлении минимизации рисков мошенничества.

Гипотеза 3. По данным ФинЦерт 69% составляют операции без согласия клиента, совершены методами социальной инженерии, которые совершаются путем обзвона держателей карт, значит большое количество респондентов должны ответить, что им звонили мошенники.

Гипотеза 4. Банки должны обеспечить доведение до клиентов информации о возможных переводах без согласия клиента. Банк России

выделил пять признаков, по которым можно распознать мошенников и направил банкам рекомендации проинформировать клиентов об этих о признаках, значит большое количество респондентов должны были получить информацию.

Гипотеза 5. Держатели карт не понимают рисков при небезопасном использовании карты, значит могут не выполнять условия по безопасному использованию карты, что влечет возможность осуществления несанкционированной операции.

Таблица 7 – Вопросы и ответы респондентов с процентным соотношением

1 У Вас есть пластиковая банковская карта?	Значение	в %
Да	50	100%
Нет	0	0
2 Как Вы используете карту:	Значение	в %
В банкомате	32	64%
Оплачиваю покупки в магазинах	41	82%
Оплачиваю за поездки в транспорте	18	36%
Оплачиваю в интернете (покупки в интернет-магазинах, оплата гос. пошлин, оплата коммунальных услуг, услуг связи, покупка авиа и жд. билетов, переводы с карты на карту и пр.)	44	88%
3 Вы используете интернет-банк (система дистанционного банковского обслуживания)?	Значение	в %
Да	44	88%
Нет	6	12%
4 Вы когда-либо сталкивались с мошенническими действиями в отношении Вас?	Значение	в %
Да, звонили мошенники и запрашивали данные по карте/паспортные данные/логин пароль для входа в интернет-банк и пр.	27	54%
Да, оплачивал(а) в интернете за авиа/жд билеты / за сотовую связь / в интернет магазине, но оплата не прошла	1	2%
Да, были списания с карты без моего согласия, но не понятно как мои данные стали известны мошенникам	1	2%
Да, продавал(а) на Авито/Юле, произошло списание по карте, а не зачисление на карту	0	0
Карта была утеряна/ украдена и были списания денежных средств	0	0

Продолжение таблицы 7

Да, другой вид мошенничества по карте	5	10%
Да, другой вид мошенничества по системе ДБО	0	0
В соц.сетях просили в долг со взломанной страницы друга	12	24%
Нет, не сталкивался(ась)	14	28%
5 Если была мошенническая операция	Значение	в %
Денежные средства были списаны, и банк мне их вернул	4	8%
Денежные средства были списаны, и банк мне их не вернул (я не обращался(ась) / отказал в возмещении)	0	0
Была попытка операции, но денежные средства не списались с карты	3	6%
Не было списаний с карты без моего согласия	43	86%
6 Подключена ли у вас услуга СМС-информирования по карте?	Значение	в %
Да	37	74%
Нет	13	26%
7 Звонили ли Вам сотрудники банка для подтверждения операции? (не мошенники)	Значение	в %
Да	13	26%
Нет	26	52%
Я не знаю кто звонит, мошенники или не мошенники, не беру трубку/не отвечаю	5	10%
Затрудняюсь ответить	6	12%
8 Если Вам позвонят и представятся сотрудником безопасности и попросят подтвердить операцию, Ваши действия:	Значение	в %
Подтвержу, если реально совершал операцию, но более никаких данных сообщать не буду	10	20%
Ничего не скажу, перезвоню в контакт-центр своего Банка с вопросом кто звонил	28	56%
Ничего не скажу / никуда звонить не буду / не отвечу на звонок	10	20%
Затрудняюсь ответить	2	4%
9 Поступала ли Вам из банка информация о видах мошенничества, о безопасном использовании карты (по электронной почте / по СМС)?	Значение	в %
Да	16	32%
Нет	26	52%
Затрудняюсь ответить	8	16%

Окончание таблицы 7

10 Если Вы оставите карту в магазине или потеряете, а нашедший карту Вам её вернёт, Ваши действия?	Значение	в %
При обнаружении утери сразу заблокирую карту, после того как карта будет у меня – разблокирую карту	13	26%
При обнаружении утери сразу заблокирую карту и обращусь в Банк для перевыпуска карта	33	66%
Затрудняюсь ответить	4	8%

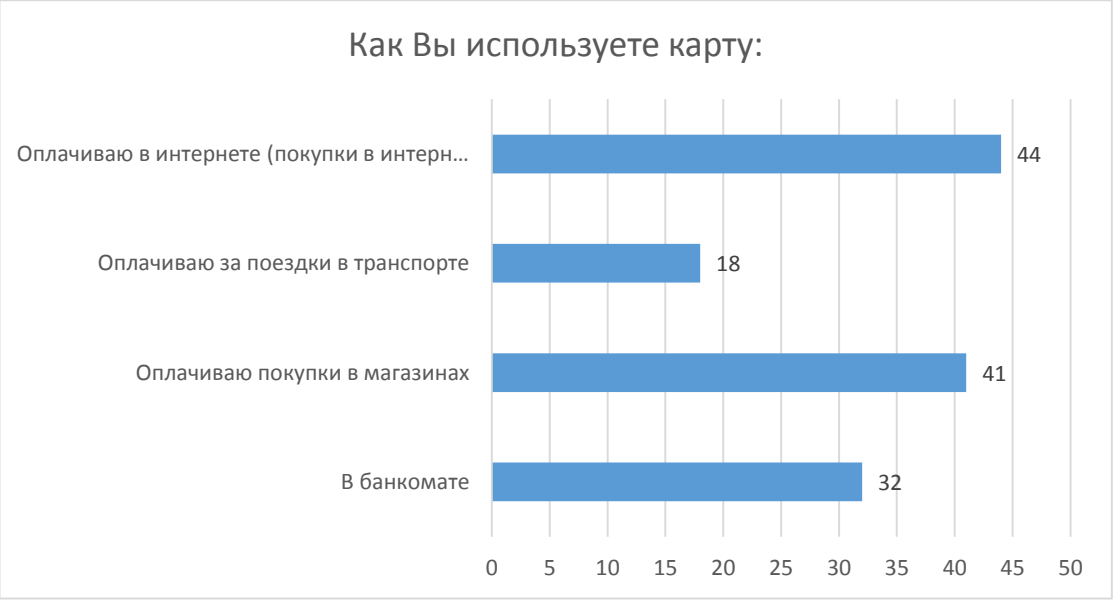

Рисунок 4 – Ответы на вопрос 2

Максимальное количество человек ответили (88% из всех респондентов), что осуществляют оплаты в интернете, следовательно, основной фокус на разнообразие мошеннических схем целесообразно осуществлять именно в интернет. Гипотеза 1 подтвердилась.

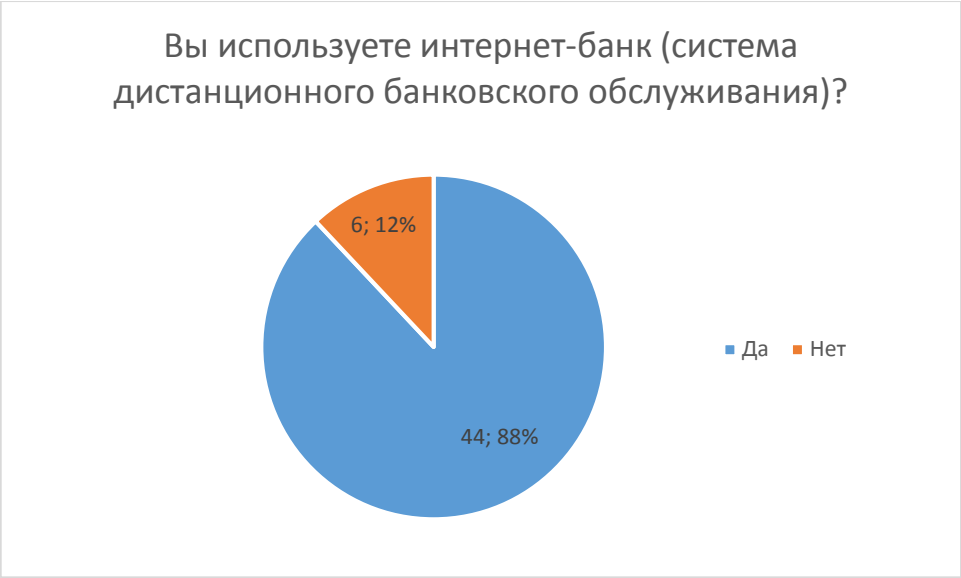

Рисунок 5 – Ответы на вопрос 3

Рисунок 6 – Ответы на вопрос 4

Более 70% респондентов ответили, что сталкивались с мошенническими действиями, 28% респондентов ответили, что не сталкивались с мошенничеством, значит гипотеза 2 подтвердилась.

Больше половины (54% из всех респондентов) ответили, что им звонили мошенники и запрашивали данные по карте/паспортные данные/логин пароль для входа в интернет-банк и пр., значит гипотеза 3 подтвердилась.

86% респондентов утверждают, что не было списаний с карты без их согласия, при этом только 28% сообщили, что не сталкивались с

мошенничеством, значит большая часть респондентов понимает, что столкнулись с мошенничеством и не сообщает никому свои личные данные.

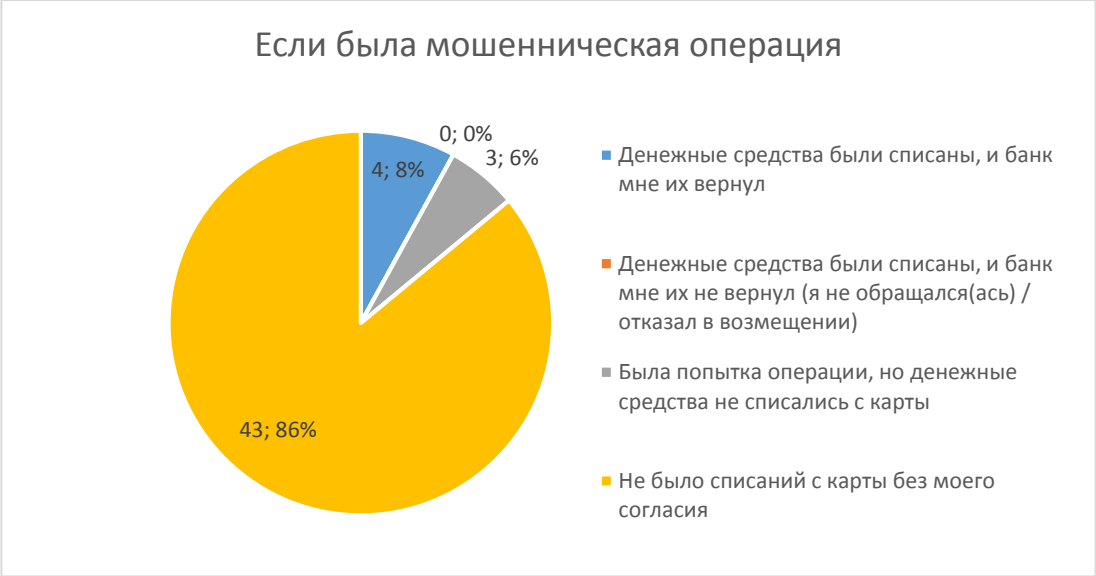

Рисунок 7 – Ответы на вопрос 5

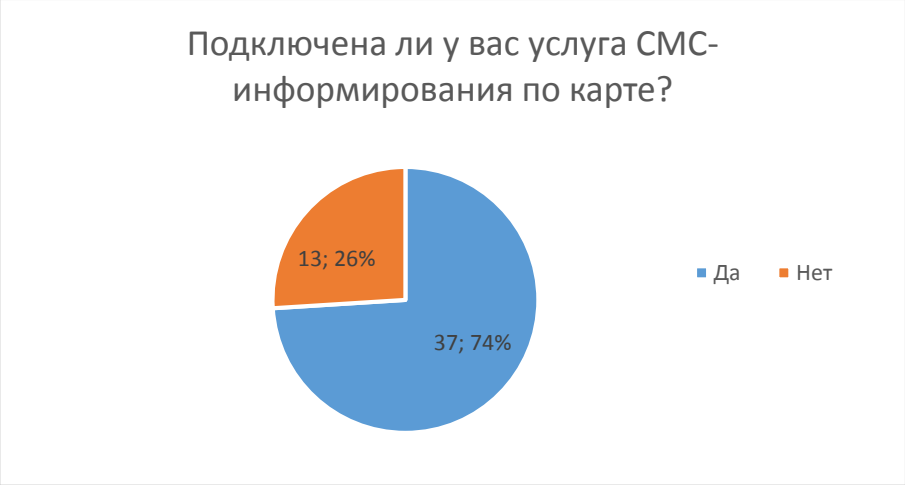

Рисунок 8 – Ответы на вопрос 6

SMS-информирование является одним из инструментов раннего обнаружения списаний денежных средств без согласия клиента. Как видно из ответов респондентов, не все держатели карт пользуются данным инструментом.

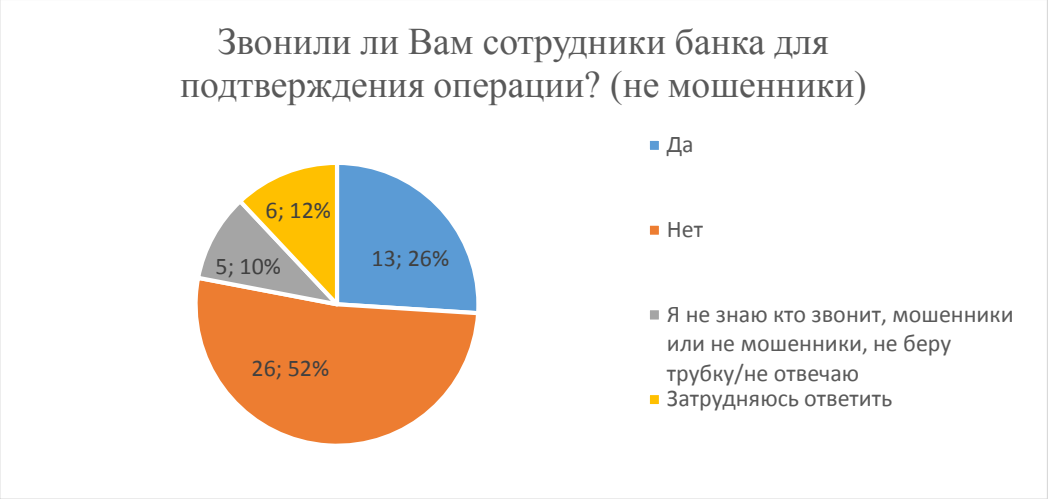

Рисунок 9 – Ответы на вопрос 7

Рисунок 10 – Ответы на вопрос 8

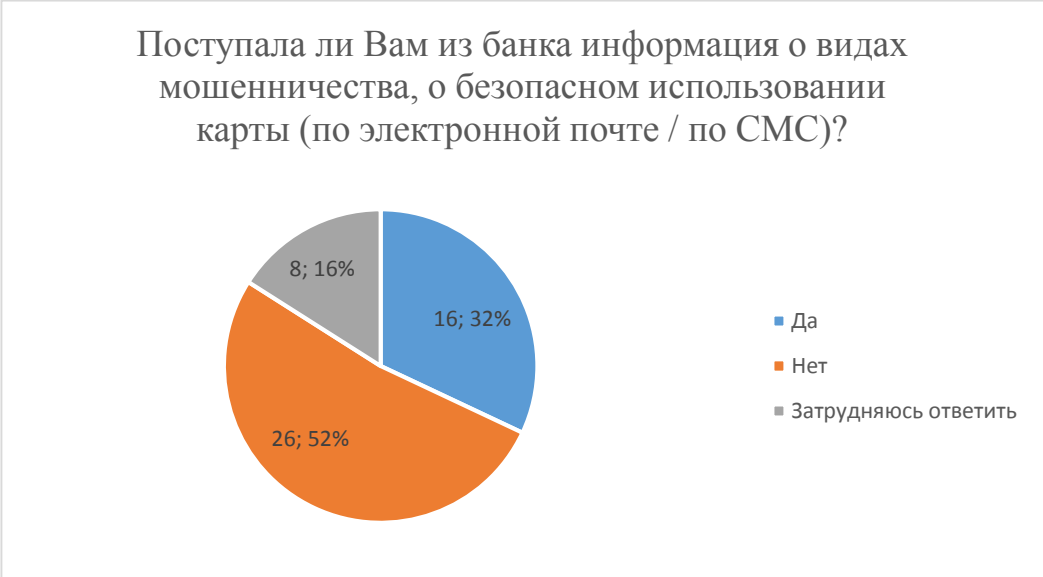

Рисунок 11 – Ответы на вопрос 9

На вопрос о поступлении респондентам информация из банка о видах мошенничества, о безопасном использовании карты (по электронной почте / по SMS), только 32% ответили утвердительно, значит не все банки выполнили рекомендации Банка России, значит гипотеза 4 не подтвердилась.

Рисунок 12 – Ответы на вопрос 10

Держатели карт должны безопасно использовать карту и в случае утери она может быть скомпрометирована, то есть данные по карте (номер карты, дата окончания карты, CVV код) стали доступны третьим лицам, что влечет возможность осуществления несанкционированной операции. При этом 26% респондентов сообщили, что при возврате карты, разблокируют её. Таким образом, гипотеза 5 подтвердилась.

Таким образом, во 2 главе были изучены различные виды мошенничества, произведена систематизация видов мошенничества по каналу взаимодействия с клиентом, а также изучены методы коммерческих банков и банка России по снижению рисков мошенничества, в том числе представлена схема взаимодействия Банка России и коммерческих банком по операциям без согласия клиентов.

ГЛАВА 3. УПРАВЛЕНИЕ ИНСТРУМЕНТАМИ, НАПРАВЛЕННЫМИ НА СНИЖЕНИЕ РИСКА МОШЕННИЧЕСТВА

3.1. Анализ мошеннических операций по статистике Департамента информационной безопасности Банка России

В 2018 г. для упрощения процесса информационного обмена, а также повышения его оперативности и защищенности Банком России была создана автоматизированная система обработки инцидентов (АСОИ Финцерт). В соответствии с требованиями Федерального закона №167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» от 27.06.2018 в Банке России создана база данных о случаях и попытках осуществления переводов денежных средств без согласия клиента и обеспечена возможность получения данных из этой базы для всех организаций, являющихся операторами по переводу денежных средств, операторами услуг платежной инфраструктуры, операторами платежных систем.

Признаки операций, которые должны быть приостановлены банком из-за того, что могут проводиться без согласия клиента, содержатся в приказе регулятора. Этот документ утвержден Банком России в развитие закона № 167-ФЗ, направленного на противодействие несанкционированным операциям и защиту клиентов банков от хищения средств кибермошенниками.

По данным, полученным из форм обязательной отчетности об инцидентах информационной безопасности, официально представляемых кредитными организациями в Банк России, и данным, полученным в рамках информационного обмена, организованного Финцерт Банка России, на территории России и за ее пределами объем несанкционированных операций с использованием платежных карт, эмитированных российскими кредитными

организациями, в 2018 г. составил 1,384 млрд руб. (в 2017 г. – 0,961 млрд руб., в 2016 г. – 1,08 млрд руб., в 2015 г. – 1,14 млрд руб.)

Удельный вес таких операций в общем объеме операций с использованием платежных карт, эмитированных российскими кредитными организациями, в 2018 г. составил 0,0018% (1,8 коп. на 1000 руб. переводов). При этом лимиты допустимого удельного веса несанкционированных переводов денежных средств, установленные европейской службой банковского надзора (EBA), составляют 0,005% (5 евроцентов на 1000 евро переводов).

В соответствии с Положением Банка России 716-П отношение суммы денежных средств, по которой получены уведомления клиентов о несанкционированном переводе (списании) денежных средств, за отчетный период нарастающим итогом с начала календарного года к общей сумме переводов за этот же период, контрольное значение должно быть не более 0,05 процентов, сигнальное значение - не более 0,005 процента [43].

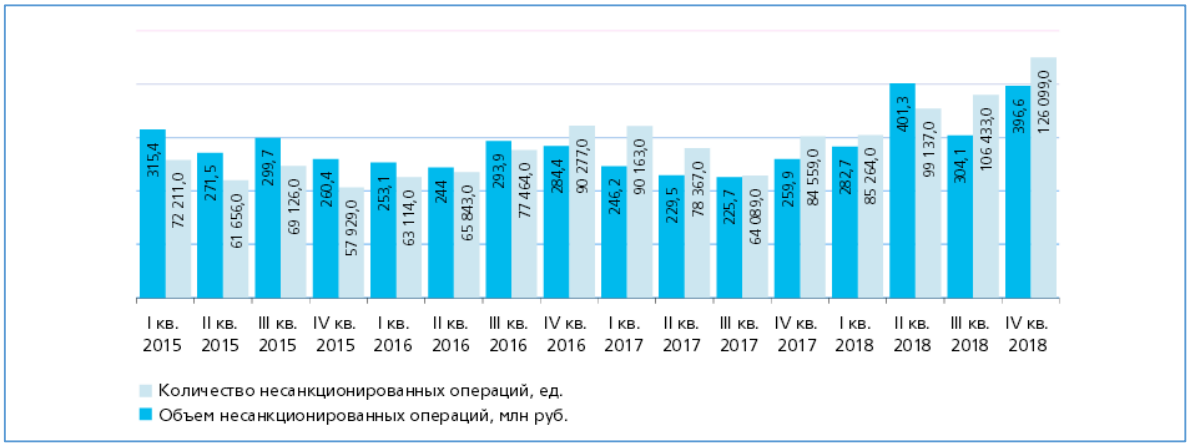

Рисунок 13 – Количество и объем несанкционированных операций с использованием платежных карт с 2015 по 2018 гг.

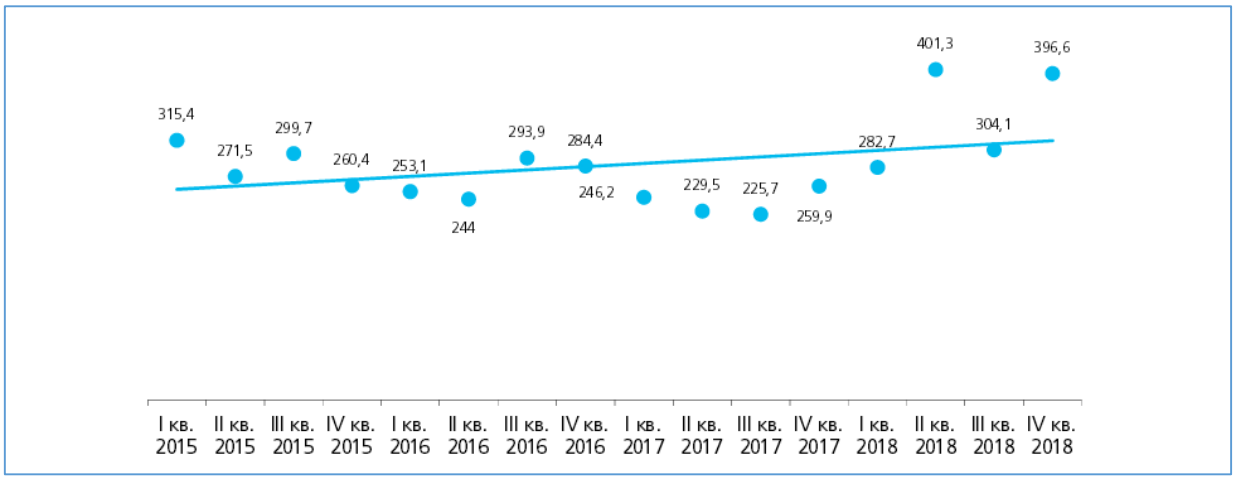

Рисунок 14 – Тренд объема несанкционированных операций с использованием платежных карт с 2015 по 2018 гг.

Рисунок 15 – Динамика несанкционированных операций с использованием платежных карт в разрезе их проведения (млн.руб.) с 2015 по 2018 гг.

По данным Банка России, в 2019г. количество операций, которые были совершены без согласия клиентов (с использованием ЭСП физических и юридических лиц) составляет 6 426,5 млн. рублей. Количество таких операций – 576 566 единиц. 69% этого количества операций было совершено с использованием методов социальной инженерии (побуждения клиентов к самостоятельному проведению операции путем обмана или злоупотребления доверием) [36].

Банки возместили клиентам 935 млн. руб., около 15%.

Рисунок 16 – Соотношение возмещенных клиентам денежных средств (в процентах)

Текущий невысокий уровень возмещения зависит от того, что среди операций, совершенных без согласия клиентов высокий процент социальной инженерии, так как при данном виде мошенничества клиент нарушает условия договора с кредитными организациями, предусматривающие необходимость сохранения конфиденциальности платежной информации. Банк России планирует рассмотреть вариант изменения процедуры возврата денежных средств пострадавших клиентов.

Повышение безопасности финансовых услуг является задачей, которую Банк России реализует в интересах как их потребителей, так и самих кредитных организаций.

Операции без согласия клиента с использованием ЭСП можно поделить на 3 вида:

- операции через терминалы, банкоматы
- операции в Интернете – оплата товаров и услуг
- операции в системе ДБО

Сумма хищений через банкоматы и терминалы составляет более 525 млн. руб. (возвращено 54,4 млн. – 10%). Сумма хищений в интернете составляет 2 971,3 млн. руб. (возмещено 653,2 млн. руб.). Сумма хищений по системам дистанционного обслуживания составляет 2 227 млн. руб. (возмещено клиентам 162,3 млн.)

За первые три квартала 2019 и 2020 гг. данные по операциям без согласия клиентов представлены в таблице 8.

Таблица 8 – Количество и суммы операций без согласия клиентов за 1,2,3 кварталы 2019 и 2020 гг.

Год	2019 год			2020 год			
Квартал	1 квартал 2019	2 квартал 2019	3 квартал 2019	1 квартал 2020	2 квартал 2020	3 квартал 2020	Прирост / снижение (в %)
Кол-во операций, ед.	124 788	113 250	163 310	169 501	192 336	180 352	35
Сумма, тыс.руб.	1 329 773	1 793 765	1 901 770	1 406 345	2 171 236	2 506 593	21
Банкоматы, терминалы, ед.	8 095	9 904	10 494	11 273	9 434	10835	11
Сумма, тыс.руб.	157 097	112 534	134 760	111 316	127 789	200 525	9
CNP-транзакции, ед.	73 819	66 957	109 664	123 617	152 857	137 764	65
Сумма, тыс.руб.	669 609	926 876	838 743	603 964	1 122 144	1 182 367	19
Операции в ДБО, физические лица ед.	42 015	34 308	42 326	34 035	29 238	31 195	-20
Сумма, тыс.руб.	397 537	559 837	742 919	460 013	728 055	944 614	25
Операции в ДБО, юридические лица ед.	859	2 081	826	576	807	558	-48
Сумма, тыс.руб.	105 530	194 518	185 347	231 052	193 248	179 085	24

По полученным данным можно увидеть, что количество операций без согласия клиентов и сумма операций за 2020 год гораздо выше, чем в 2019 году. Количество операций без согласия за три квартала 2020 возросло на 35% по сравнению с тремя кварталами 2019 года. Только за третий квартал 2020 года сумма похищенных денежных средств составляет более 2,5 миллиардов рублей.

Также видно, что высокий рост по операциям в интернете. Количество операций без согласия за три квартала 2020 года возросло на 65% по сравнению с тремя кварталами 2019 года.

Видно, что операций без согласия в ДБО физических лиц гораздо больше, чем в ДБО юридических лиц, хотя средняя сумма операции по

операции без согласия в ДБО юридических лиц выше, чем операция без согласия в ДБО физических лиц. Однако при снижении количества операций без согласия в ДБО юридических лиц в 2020 году на 48% по сравнению с аналогичным периодом 2019 года, сумма похищенных денежных средств возросла на 24%.

Если рассматривать операции в ДБО физических лиц, то можно наблюдать тенденцию к снижению. Количество операций без согласия за три квартала 2020 года снизилось на 20% по сравнению с тремя кварталами 2019 года. Это говорит о том, что банки эффективно используют такой инструмент, как мониторинг операций, что подтверждает гипотезу исследования о возможности уменьшения количества несанкционированных операций.

Операцию по карте нет возможности приостановить для того, чтобы связаться с клиентом, а можно лишь отклонить авторизацию. А операцию с банковского вклада в системе ДБО приостановить можно, до тех пор, пока сотрудник банка не получит от клиента подтверждения операции.

В связи с развитием финансовых услуг, совершаемых в сети Интернет, тем более с учетом пандемии коронавирусной инфекции, в дальнейшем сохранится восходящий тренд совершения операций без согласия клиентов в канале операции в сети Интернет без предъявления кары и по системам ДБО, и соответственно тема снижения рисков мошенничества по банковским картам и системам ДБО, является актуальной и востребованной.

3.2. Оценка эффективности мониторинга карточных транзакций и систем ДБО на примере ПАО «СКБ-Банк»

В соответствии с Федеральным законом 167-ФЗ, Банк может приостановить операцию и заблокировать карту клиента, в случае отсутствия связи с клиентом для подтверждения операции.

Если данные о получателе перевода содержится в базе данных Банка России о случаях и попытках хищений, Банк должен принять решение о приостановке операции. Второй признак – это совпадение информации о параметре устройства, используемом для совершения перевода в системе ДБО, с информацией о параметрах устройств из базы данных. Еще один признак – это несоответствие характера, объема, а также параметров совершаемых транзакций операциям, которые обычно проводит клиент. Такие параметры, как время, день и место осуществления операции, а также сумма операции и периодичность. При этом регулятор не устанавливает для банков порядок выявления таких транзакций. Параметры проверки Банки выбирают самостоятельно в рамках реализуемых ими систем управления рисками.

В случае определения операция как потенциальной операции без согласия клиента, то банк должен связаться с клиентом для её подтверждения. При этом, если связаться с клиентом не удалось, банк вправе приостановить такую операцию на срок до двух суток.

Появление новых форм мошенничества, в т. ч. большой рост мошенничества с использованием социальной инженерии, доля которого, согласно отчету Финцерта Банка России за 2018 год, составила порядка 97% от всех случаев мошенничества, заставляет пересматривать подходы к мониторингу операций по картам и системам ДБО.

Кросс-канальное мошенничество является самым актуальным трендом 2018-2019 гг. Принцип кросс-канального мошенничества заключается в том, что, воздействуя на клиента приемами социальной инженерии, мошенники получают доступ практически ко всем инструментам, которые клиент использует для совершения банковских операций: карты, система ДБО, мобильное приложение и используют одновременно все возможные каналы для хищения средств. Появление этого типа мошенничества обусловлено тем, что даёт возможность мошенникам узнать сумму всех денежных средств клиента и где они хранятся (карточные счета, вкладные счета) и при отсутствии денежных средств на карте клиента, вывести денежные средства

со вклада клиента. Мошенники реализуют сценарии, предусматривающие одновременную активность сразу во многих каналах банковского обслуживания. При этом мониторинг операций отдельно в каждом из этих каналов зачастую не даст возможности выявить подозрительное операции клиента, так как по отдельности такие операции могут выглядеть вполне законно. И только в совокупности операций в разных каналах, будет создана четкая картина мошенничества.

Даже если клиент никогда не пользовался системой ДБО, не устанавливал на телефон мобильное приложение, мошенник может сделать это за него, узнав у клиента необходимые для этого данные: номера карт, договоров, паспортные данные, одноразовые пароли. А дальше – непосредственно совершать вывод средств, используя все возможные транзакционные каналы: переводы со счетов, с карт, оплаты в интернете, сервисы токенизированных операций Apple Pay, Samsung Pay и др.

В случае, если мошенник смог войти в систему ДБО под учетными данными клиента и зная, что множественные повторяемые операции в одном и том же канале легко выявляются, он совершает именно операции в разных каналах. При этом он совершает «нефинансовые» действия – сброс/смена паролей, смена/назначение ПИН-кода, выпуск виртуальных карт, принятие кредитного предложения и т. д.

Таким образом, если система мониторинга останется «моноканальной», она попросту не сможет выявить все перечисленные триггеры, как финансовые, так и нефинансовые, в их связи и последовательности. Только одновременный мониторинг всех каналов предоставления банковских услуг, причем с привязкой именно к клиенту, а не к конкретному счету или карте, которых может быть много у одного клиента, способен выявить сложные модели поведения мошенников, а значит, и оперативно предотвратить хищения.

До 2019 года реализованный функционал мониторинга карточных транзакций в ПАО «СКБ-Банк» строился на выявлении подозрительных

операций путем обработки всех карточных транзакций по определенному набору правил. Правила оптимизировались, реализовывались новые правила в соответствии с потребностями заказчика. При этом, недостаточно гибкое программное обеспечение, не позволяло использовать те возможности, которые имеются у существующих антифрод систем. Так, например, не был реализован кросс-канальный мониторинг. При этом, формировалось большое количество ложных срабатываний, что увеличивало нагрузку на сотрудников отдела мониторинга и снижало эффективность работы.

По данным за 2015 – 2020 гг. динамика подозрительных операций составила:

Рисунок 17 – Количество подозрительные карточных операций, тыс. шт. за 2015-2020 гг.

Рисунок 18 – Количество операций без согласия клиентов в ПАО «СКБ-Банк», шт. за 2019-2020 гг.

Количество подозрительных карточных транзакций в 2019 году сократилось в связи с совершенствованием алгоритмов выявления подозрительных карточных операций с целью снижения ложных срабатываний.

При этом, в 2019 году количество операций без согласия клиента по сравнению с 2018 годом возросло на 63%. По сравнению с 2019 годом, в 2020 году количество операций без согласия выросло еще на 26%.

В 2018 году стал актуальным вопрос о внедрении новой антифрод системы.

Одним из направлений компании, в которой заказана новая антифрод система, является информационная безопасность и разработка решений для обеспечения безопасности коммерческих и государственных организаций. Компания специализируется на построении комплексных систем безопасности, защите облачной инфраструктуры, управлении инцидентами, а также системах противодействия мошенничеству. Антифрод система является общеаналитической кроссканальной платформой. Продукт полностью соответствует актуальным требованиям законодательства РФ по противодействию мошенничеству.

Особенности антифрод системы: Обработка событий в режиме реального времени; использование платформы Big Data вместо привычных реляционных систем управления базами данных; использование самообучаемых математических моделей, позволяющих выявлять подозрительные действия в автоматическом режиме; проведение расследований инцидентов информационной безопасности, связанных с выявленными аномалиями; прогнозирование потенциальных аномалий.

Данное решение используется в ПАО «СКБ-Банк» для мониторинга операций в системах дистанционного банковского обслуживания. Является эффективным и достаточно гибким в плане реализации новых правил и настройки существующих потребностей заказчика. Также, с 2020 года данное решение стало использоваться и для мониторинга карточных транзакций, с дальнейшим формированием кросс-канального мониторинга.

Динамика количества подозрительных операций по картам за последние четыре года представлена на Рисунке 19.

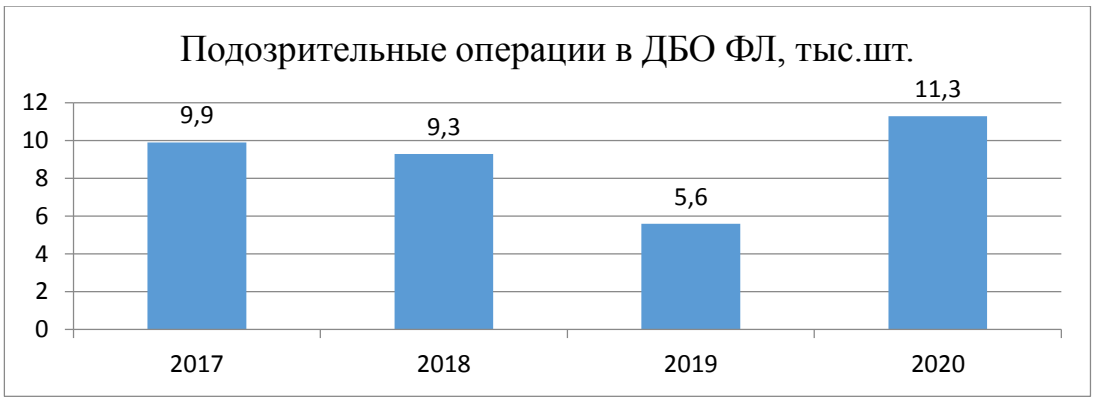

Рисунок 19 – Динамика подозрительных операций в ДБО физических лиц, тыс. шт., за 2017-2020 гг.

Рост числа подозрительных операций в ДБО возник по причине разработки новых правил в связи с появлением новых схем мошенничества.

Количество выявленных операций без согласия клиентов (сколько всего операций без согласия и сколько их них было предотвращено) представлено на Рисунке 20.

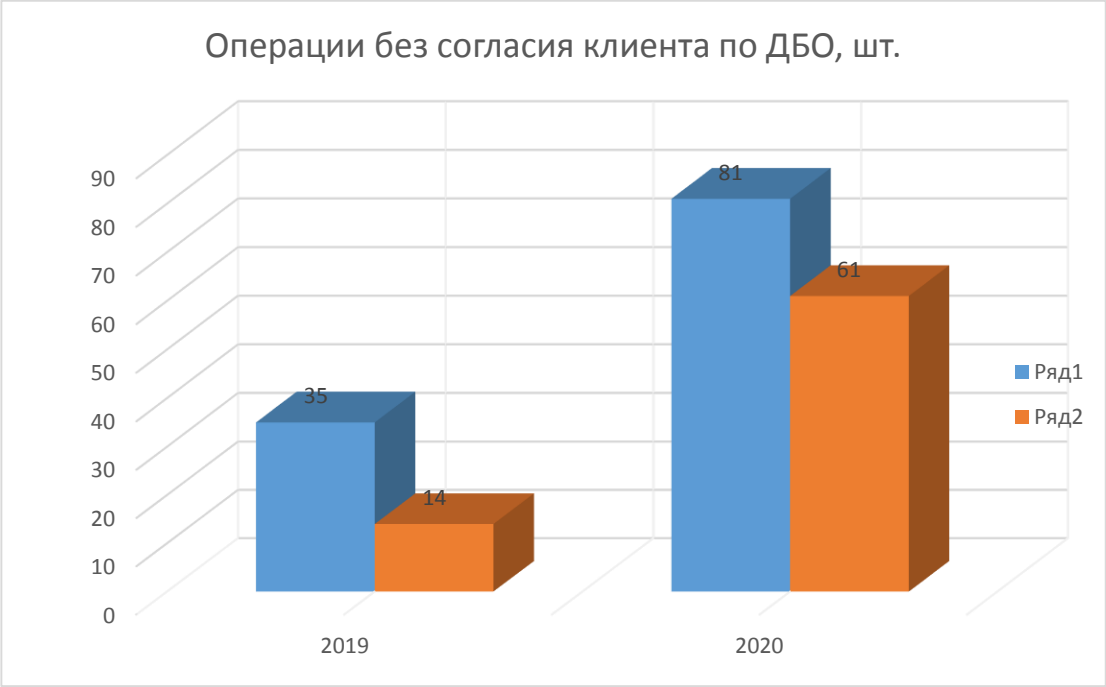

Рисунок 20 – Количество попыток операций без согласия и количество предотвращенных операций за 2019-2020 гг.

В 2019 году предотвращено 14 операций без согласия клиентов по системе ДБО, денежные средства сохранены на сумму свыше 3 миллионов рублей. В 2020 году предотвращена 61 операция без согласия клиента, что в 4

раза больше, чем в 2019 году; на сумму свыше 6 миллионов рублей, что в 2 раза больше, чем в 2019 году.

Таблица 9 – Количество и суммы операций без согласия клиентов и предотвращенных операций в ПАО «СКБ-Банк» за 2019-2020 гг.

Год	2019		2020	
	Количество	Сумма, руб.	Количество	Сумма, руб.
Проверено подозрительных транзакций	417 312	4 087 360 625	204 515	3 435 274 839
Операции без согласия	603	12 527 887	763	16 559 488
Проверено подозрительных платежей	5 628	443 068 423	11 323	1 082 022 726
Операции без согласия	35	3 366 822	81	6 818 927
Предотвращено операций без согласия	14	3 053 966	61	6 120 802

В случае, если осуществляется мошенническая операция с карты, то при попадании в систему мониторинга, по признакам несанкционированной операции, должна быть приостановлена, но с учетом того, что технически мгновенный перевод с карты приостановить нет возможности, авторизация должна быть отклонена. В случае, если авторизацию банк не отклонит, то мошенническая операция будет проведена, а также проведены все последующие операции, пока банк не получит от клиента информацию, что операция является несанкционированной и карта не будет заблокирована. Поэтому разрабатывать и внедрять антифрод систему мониторинга операций необходимо с учетом данного фактора.

Операцию (за исключением мгновенных переводов) по системе ДБО можно приостановить до тех пор, пока банк не получит от клиента

подтверждения операции, а также можно приостановить все последующие операции. При этом, операцию можно возобновить, получив подтверждение клиента. Мониторинг операций в системе ДБО является также более эффективным, потому что банк имеет в распоряжении больше параметров по операции, таких как геолокация, IP-адреса, данных об удаленном подключении, данных по смене логина и пароля и прочее.

На основании представленных данных, можно сделать вывод о том, что количество операций без согласия клиентов ежегодно растет, при этом мониторинг ПАО «СКБ-Банк» является эффективным средством предотвращения операций без согласия, так как предотвращает около 90% по сумме всех попавших в мониторинг попыток операций без согласия клиента в системе ДБО.

3.3. Оптимизация управления инструментами, направленными на снижение риска мошенничества

В ходе диссертационного исследования были выявлены проблемы при использовании инструментов, направленных на снижение риска мошенничества по картам и ДБО.

Таблица 10 – Проблемы при использовании инструментов снижения риска мошенничества и возможные варианты их решения

Инструмент	Проблема	Решение	Итог
Монито-ринг операций	Ошибки сотрудников мониторинга	Обучение сотрудников мониторинга, повышение квалификации	Больше предотвращенных операций без согласия

Продолжение таблицы 10

	Не верно отработало правило / операция не отразилась как подозрительная	Анализировать причины не попавших в мониторинг операций без согласия клиента	Исправление ошибок / доработка системы
	В правила не заложена новая схема мошенничества	В Финцерт в инциденте сделать обязательным заполнение поля схема мошенничества и рассылать банкам	Предупреждаю-щий фактор для возможности изменить правила мониторинга в других банках
	Клиент подтверждает операцию, при этом она является явно мошеннической	Разработать скрипты для сотрудников мониторинга, в моменте проводить расследование для дальнейшей работы с клиентом	Больше предотвращенных операций без согласия
	Низкая грамотность клиента	При выявлении операции без согласия клиента, информировать клиента о причинах, мерах предосторожности. Информировать клиентов при выявлении новых схем мошенничества (по SMS, по электронной почте)	
	Не подключение / отключение SMS-информирования клиентами	Информировать клиента о неполучении клиентом сообщений при операции без согласия	Быстрое реагирование клиента на операцию без согласия

Окончание таблицы 10

Финцерт	Денежные средства быстро переводят на другую карту или кошелек либо снимают в банкоматах	Доработать ФинЦерт для моментальной блокировки карты, куда зачислены денежные средства по мошеннической операции	Возможность сохранить денежные средства на карте мошенника.
	Не найден конечный получатель денежных средств	Доработать ФинЦерт для заведения куда были переведены денежные средства (цепочка) и блокировать карту мошенника	Предотвращение для других банков. Возможность сохранить денежные средства на карте, куда денежные средства были переведены.
	Открытие карт мошенниками в разных банках	Запрет открытия карт мошенникам в других банках и при обнаружении в своем банке открытых карт – их закрытие	Предотвращение для других банков
	Не известен номер карты и банк, куда зачислены денежные средства, так как операция прошла через банк-посредник	В правила платежной системы добавить обязанность банков предоставлять в переводе номер карты получателя	Пропадет необходимость уточнять по электронной почте номер карты получателя у банка-эквайера
Претензи-онная работа	Нет регламентирован-ного процесса возврата денежных средств клиенту, если денежные средства сохранены на карте мошенника	Законодательно закрепить возможность возврата денежных средств со счета мошенника	Возможность возвращать клиентам похищенные денежные средства

Такой инструмент как добавление в текст SMS-сообщения информации о том, что никому нельзя сообщать одноразовый код, может быть не эффективен, так как мошенники, разрабатывая схемы, опираются на знание банковских технологий и предлагают клиенту сообщить данные роботу.

Информирование клиента о совершенной операции путем направления SMS-сообщения или PUSH-уведомления не будет покрывать все случаи мошенничества, по причине того, что услуга SMS-информирования платная и не все клиенты её подключают.

Памятки о безопасном использовании банковских карт, которые выдаются клиентам при выдаче карты, а также информация о видах мошенничества и о способах защиты от мошенничества, публикуемая на официальных сайтах банков также не является эффективным инструментом, по причине того, что не все клиенты ответственно отнесутся к тому, что нужно эту информацию изучить.

Когда банки осуществляют рассылку клиентам писем на электронную почту о безопасном использовании банковских карт и систем ДБО, о видах мошенничества, есть процент клиентов, у которых нет электронной почты или они о ней не сообщили в банк.

Информацию о возможности установки лимитов по операциям клиентам необходимо донести, она не является обязательной при открытии карты. Также, как и возможность запрета осуществления операций в интернете. По мнению автора, именно установка запрета операций в интернете является эффективным инструментом по снижению риска мошенничества, в случае если запрет устанавливать при оформлении карты в офисе банка с получением информации от клиента – намерен он пользоваться картой в интернете или нет. Таким образом, если будет установлен запрет на операции в интернете – операция без согласия клиента по карте не пройдет, пока ограничение не будет снято. Либо не подключать отдельным категориям клиентов возможность осуществлять операции в интернете по умолчанию, подключение должно быть

инициировано владельцем карты по факту возникновения необходимости в совершении операции.

Таким образом, для снижения рисков, связанных с мошенническими действиями по банковским картам и системам ДБО, банкам предлагается выполнять следующие действия.

- При использовании системы мониторинга операций, совершенных по картам и операций, с использованием систем ДБО, учитывать кросс-канальное мошенничество, на постоянной основе отслеживать новые схемы мошенничества и вносить изменения в правила работы системы мониторинга, разрабатывать новые скрипты для общения с клиентами, а также проводить постоянное повышение квалификации сотрудников;
- Работать с операторами связи по выявлению номеров мошенников;
- Не подключать пожилым людям возможность осуществлять операции в интернете по умолчанию, подключение должно быть инициировано владельцем карты по факту возникновения необходимости в совершении операции;
- При выдаче карты клиенту направлять в SMS-сообщении или на электронную почту клиенту информацию о мошенничестве;
- Обучать клиентов, а также сотрудников банка, безопасному использованию банковских карт и систем ДБО. Предлагается использовать методы тестирования клиентов на знание безопасного использования карты и системы ДБО, с предоставлением результатов тестирования. Для прохождения тестирования стимулировать клиентов, например, повышенным кэшбэком за покупки или бесплатным обслуживанием карты на определенный период. Сотрудникам в обязательном порядке всем проходить тестирование;
- При отключении клиентом SMS-информирования или отказе от подключения направлять информацию клиенту о том, что если по карте будут совершаться несанкционированные операции, то клиент сможет оперативно карту заблокировать.

Меры, которые по мнению автора, требуется предпринять Банку России для снижения риска проведения операций без согласия клиента:

- Доработать законодательство таким образом, чтобы при сохранении ДС на счете мошенника, была упрощенная процедура их возврата.
- Доработать законодательство таким образом, чтобы при обнаружении Банком подозрений на мошеннические действия своего клиента, у Банка была Возможность заблокировать карту и запросить подтверждающие документы по операциям у клиента.
- Доработать законодательство таким образом, чтобы запретить закрытие счета клиента – мошенника, до проведения всех необходимых процедур по проверке и/или возврату денежных средств пострадавшим клиента.
- Доработать АСОИ Финцерт по мгновенной блокировке карты и направлении информации не в банк-эквайер, а в банк-получатель денежных средств.
- В правила платежной системы добавить обязанность банков предоставлять в переводе номер карты получателя.
- Возложить ответственность на операторов сотовой связи отслеживать исходящие звонки или SMS-сообщения с одного номера на разные номера и блокировки таких номеров.
- Не давать возможности мошеннику открывать карты и подключать системы ДБО в других банках, если уже в одном банке имеется информация о мошенничестве.

ЗАКЛЮЧЕНИЕ

Процесс управления рисками мошенничества по банковским картам и системам ДБО является очень важным для кредитных организаций, при этом не будет одного концептуального решения на несколько лет, в связи с многообразием видов мошеннических схем и созданием практически ежедневно новых схем мошенничества.

В теоретической части диссертации были рассмотрены различные виды банковских рисков и их классификация, более подробно рассмотрены операционные риски, в том числе понятие киберриска, а также процедуры, необходимые для управления операционными рисками. Также была разработана классификация операционных рисков по внутренним и внешним источникам их возникновения с указанием потерь.

Учитывая то, что мошенничество с банковскими картами осуществляется практически с момента их возникновения, в работе были рассмотрены внедренные ранее технологии и стандарты для снижения риска мошенничества по картам.

Изучению актуальных методов снижения рисков мошенничества посвящена вторая глава диссертации – были изучены различные виды мошенничества, произведена их систематизация по каналу взаимодействия с клиентом, представлена схема взаимодействия Банка России и коммерческих банком по операциям без согласия клиентов и выявлен основной инструмент коммерческих банков по снижению рисков мошенничества при осуществлении операций по банковским картам и системам ДБО – мониторинг операций.

Процесс управления рисками динамично развивается: Банк России планировал повышать финансовую грамотность населения, и недавно заработал сайт «Финансовая культура», а школьники изучают основы безопасности на уроках информатики. Коммерческие банки в 2019 году на форуме AntiFraud Russia обсуждали взаимодействие банков и операторов

сотовой связи, а в 2020 году Тинькофф банк внедряет технологию в свою антифрод-платформу, разработанную совместно с крупнейшими операторами мобильной связи.

В рамках диссертационного исследования был проведен опрос по использованию респондентами банковских карт и систем ДБО, а также мошенническим действиям в отношении респондентов; были получены результаты опроса, которые подтвердили часть выдвинутых гипотез, в том числе большой процент респондентов сталкивался с мошенническими действиями и в основном это звонки на сотовые телефоны, что в дальнейшем обуславливает такой высокий процент социальной инженерии.

В третьей главе проведен анализ мошеннических операций по статистике Департамента информационной безопасности Банка России, по результатам которого можно утверждать, что проблема мошенничества по картам и системам ДБО на текущий момент является острой, а тема по снижению рисков мошенничества актуальной, в связи с постоянным ростом количества и сумм мошеннических операций. Также была рассмотрена система мониторинга операций на примере ПАО «СКБ-Банк» и её эффективность.

Помимо этого, были разработаны рекомендации для оптимизации подхода к использованию инструментов коммерческих банков Российской Федерации и Банка России для снижения рисков мошенничества по банковским картам и системам ДБО.

Подводя итог работы, можно сделать следующее заключение, что при взаимодействии всех институтов, участвующих в описанных процессах, с использованием ими различных инструментов и их модернизации, борьба с мошенническими действиями в отношении владельцев карт и систем ДБО будет эффективной.

Таким образом, поставленные задачи были выполнены и цель исследования достигнута.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Аксенов А.П. Дистанционное банковское обслуживание/Аксенов А. П. и др. - Москва: КноРус: ЦИПСиР, 2010. 165с.
2. Аляев Д.А. Банковские риски при операциях с кредитными картами // Российское предпринимательство. 2010. №9.
3. Аляев Д.А. Тенденции управления рисками в российских банках на современном этапе // Вестник Алтайского государственного аграрного университета. 2009. №6.
4. АО «Альфа-Банк»: [сайт]. – URL: https://alfabank.ru/ (дата обращения 05.02.2021).
5. АО КБ «СитиБанк»: [сайт]. – URL: https://www.citibank.ru/russia/main/rus/home.htm (дата обращения 05.02.2021).
6. АО «Тинькофф банк»: [сайт]. – URL: https://www.tinkoff.ru/ (дата обращения 05.02.2020).
7. Банк России: [сайт]. – URL: http://cbr.ru (дата обращения 05.02.2021).
8. Батаев А. В. Оценка безопасности дистанционного банковского обслуживания в России // Молодой ученый. 2017. №10.
9. Богданкевич О.А. Организация деятельности коммерческих банков, Минск : ТетраСистемс, 2011. 144с.
10. Герасимович А.М. Анализ дистанционного обслуживания клиентов в банковской деятельности. –МОСКВА: Атика, 2015. 368с.
11. Голдовский И.М. Банковские микропроцессорные карты. М.: Альпина Паблишерз, 2010. 686с.
12. ГОСТ Р 57580.1-2017 Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер: [сайт]. – URL: http://docs.cntd.ru/document/1200146534 (дата обращения 31.01.2021).

13. Жуков Е.Ф. Банковский менеджмент : учебник / Е.Ф. Жуков. – 2-е изд., перераб. и доп. – Москва : Юнити, 2016. 255с.
14. Звонова, Е. А. Международный финансовый рынок. Учебник и практикум / под ред. Е.А. Звоновой, М.А. Эскиндарова, Москва. ЮРАЙТ, 2017. 454с.
15. Зюкин, А.А. Банковские риски / А.А. Зюкин. – Москва : Лаборатория книги, 2010. 45с.
16. Ковалев П. П. Банковский риск-менеджмент / П. П. Ковалев. - Москва : Финансы и Статистика, 2009. 300с.
17. Коваленко, О. Г. Сущность и классификация банковских рисков / О. Г. Коваленко, О. В. Игонина. // Молодой ученый. 2016. №12(116).
18. Козодаева А.Н., Обыденнова А.С. Способы совершения мошенничества с использованием банковских карт // Ученые записки Тамбовского отделения РоСМУ. 2019. №13.
19. Казимагомедов А.А. Банковские риски: учебное пособие / Казимагомедов А.А., Абдулсаламова А.А. - Москва : КноРус, 2020. 259с.
20. Кутафьева, Л. В. Классификация банковских рисков // Молодой ученый. 2013. №10 (57).
21. Лаврушин О.И. Банковские риски: учебник / коллектив авторов; под ред. О.И. Лаврушина, Н.И. Валенцевой. 3-е изд., перераб. и доп. - М.: КНОРУС, 2016. 292с.
22. Лаврушин О.И. Оценка финансовой устойчивости кредитной организации: учебник / коллектив авторов; под ред. О.И. Лаврушина, И.Д. Мамоновой . - М.: КНОРУС, 2011. 304с.
23. Левашов М.В., Овчинников П.В. Эффективность классификаторов для выявления фрода в финансовых транзакциях. // Вопросы кибербезопасности, 2019. №5(33)
24. Лямин Л.В, Пятиизбянцев Н., Пухов А.В, Ревенков П.В. и др. Мошенничество в платежной сфере. / Бизнес-энциклопедия. Интеллектуальная литература, 2016. 345с.

25. Мальцева Ю.А. Психология управления: учеб.пособие / Ю.А. Мальцева, О.Ю. Яценко. – Екатеринбург: Изд-во Урал. ун-та, 2016. 92 с.
26. Маркова О. М. Банковские операции: учебное пособие / О. М. Маркова. – Москва: Юрайт. 2017. 544с.
27. Международная платежная система Mastercard: [сайт]. – URL: https://www.mastercard.ru/ (дата обращения 01.02.2021).
28. Миндрова З.М. Проблемы и перспективы развития дистанционного банкинга в России //Сети и бизнес. 2015. № 3.
29. Мягкова Т.Л. Банковское дело / Т.Л. Мягкова – Саратов: Ай Пи Эр Медиа 2015. 212с.
30. Национальная платежная системы МИР: [сайт]. – URL: https://mironline.ru/ (дата обращения 15.01.2021).
31. Национальная система платежных карт: [сайт]. – URL: https://www.nspk.ru/cards-mir/security/about-fraud/ (дата обращения 15.01.2021).
32. О банках и банковской деятельности. Федеральный закон от 02.12.1990 №395-1
33. Обзор несанкционированных переводов денежных средств за 2018 год. // Банк России: [сайт]. – URL: https://www.cbr.ru/Content/Document/File/62930/gubzi_18.pdf (дата обращения 10.01.2021).
34. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год. // Банк России: [сайт]. – URL: https://www.cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf (дата обращения 10.01.2021).
35. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств I и II кварталы 2019 – 2020 годов https://www.cbr.ru/analytics/ib/review_1q_2q_2020/ (дата обращения 27.01.2021)

36. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств III квартал 2019 и 2020 годов https://www.cbr.ru/analytics/ib/review_3q_2020/ (дата обращения 27.01.2021)
37. Об отдельных вопросах, связанных с противодействием осуществлению переводов денежных средств без согласия клиента. Письмо Банка России от 07.12.2018 № 56-3-2/226
38. Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента. Положение Банка России от 17.04.2019 № 683-П
39. Об эмиссии платежных карт и об операциях, совершаемых с их использованием. Положение Банка России от 24.12.2004 №266-П
40. О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств. Федеральный закон от 27 июня 2018 г. №167-ФЗ
41. О требованиях к системе управления операционным риском в кредитной организации и банковской группе. Положение Банка России от 08.04.2020 № 716-П
42. О национальной платежной системе. Федеральный закон от 27.06.2011 №161-ФЗ
43. О памятке «О мерах безопасного использования банковских карт». Письмо Банка России от 02.10.2009г. № 120-Т
44. О рекомендациях по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети "Интернет". Письмо Банка России от 05.08.2013 N 146-Т
45. 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. Положение Банка России от 09.06.2012 №382-П

46. О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков. Положение Банка России от 03.10.2017 № 607-П
47. О требованиях к системе управления рисками и капиталом кредитной организации и банковской групп. Указание Банка России от 15.04.2015 №3624-У
48. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России 01.09.2018 – 31.08.2019. // Банк России: [сайт]. – URL: https://www.cbr.ru/Content/Document/File/84354/FINCERT_report_20191010.PDF (дата обращения 05.02.2021).
49. О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации. Указание Банка России от 8 октября 2018 г. N 4926-У
50. ПАО КБ «УБРиР»: [сайт]. – URL: https://www.ubrr.ru/ (дата обращения 05.02.2021).
51. ПАО «Сбербанк»: [сайт]. – URL: https://www.sberbank.ru (дата обращения 05.02.2021).
52. ПАО «СКБ-Банк»: [сайт]. – URL: https://skbbank.ru/ (дата обращения 05.02.2021).

53. Правила платежной системы Виза (Visa Payment System Operating Regulations): [сайт]. – URL: https://www.visa.com.ru/content/dam/VCOM/regional/cemea/russia/media-kits/documents/vpsorr-21.11.19.pdf (дата обращения 05.02.2021).
54. Тепман Л. Н. Управление банковскими рисками: учебное пособие / Л. Н. Тепман, Н. Д. Эриашвили. – М.: ЮНИТИДАНА, 2017. 311с.
55. Финансовая культура: [сайт]. – URL: https://fincult.info/article/kak-bystro-raspoznat-moshennika/ (дата обращения 05.02.2021).
56. Фомичев, А.Н. Риск-менеджмент: Учебник. – М.: Дашков и К°, 2016. 371с.
57. Шубин К.А. Банковские карты и платежные системы самообслуживания // Вестник. 2018. №10.
58. Шапкин, А.С. Экономические и финансовые риски: оценка, управление, портфель инвестиций / В.А. Шапкин, А.С. Шапкин. 9-е изд. - М. : ИТК «Дашков и К», 2013 . 544 с
59. Юденков Ю.Н. Интернет-технологии в банковском бизнесе: перспективы и риски: учебно-практическое пособие / Ю.Н. Юденков, Н.А. Тысячникова, И.В. Сандалов, С.Л. Ермаков;п предисл.чл.-корр РАН А.С.Сигова. – 2-е изд.,стер. – М.: КНОРУС, 2016. 320с.
60. Ягупова Е.А. Палий М.В. Мошенничество с банковскими картами и методы их противодействия в России // Символ Науки. 2017. №01-1/2017
61. International Convergence of Capital Measurement and Capital Standards. A Revised Framework, Basel Committee on Banking Supervision, далее - Базель II http://safbd.ru/sites/default/files/basel.pdf
62. X Международный форум «Борьба с мошенничеством в сфере высоких технологий. ANTIFRAUD RUSSIA – 2019» [сайт] – URL: https://vipforum.ru/conferences/antifraud_russia/archive/antifraud_russia_2019/ (дата обращения 14.02.2021).