Курманова Д.А.
Kurmanova D.A.
доцент, кандидат
экономических наук,
Башкирский
государственный
университет,
г. Уфа,
Российская Федерация

Султангареев Д.Р.
Sultangareev D.R.
аспирант,
Башкирский
государственный
университет,
г. Уфа,
Российская Федерация

Хабибуллина Л.Р.
Khabibullina L.R.
старший преподаватель,
заместитель декана
экономико-математического
факультета филиала
Башкирского государственного
университета
г. Нефтекамск,
Российская Федерация

УДК 336

DOI: 10.17122/2541-8904-2020-2-32-82-91

МОДЕЛИ УПРАВЛЕНИЯ РИСКАМИ ФИНАНСОВЫХ ТЕХНОЛОГИЙ

Киберинциденты продолжают движение вверх в рейтинге возможных угроз и занимают вторую позицию по значимости в ранжировании рисков в деятельности компаний (40 %). Пять лет назад они находились на пятнадцатой строчке. Подобно стихийному бедствию или пандемии, кибератака может оказать негативное влияние на сотни компаний, и число таких инцидентов растет. Так называемые «киберинциденты», когда хакеры вмешиваются в деятельность большого количества компаний, используя зависимости их общей интернет-инфраструктуры, происходят все чаще. Это отражает тот факт, что сегодняшний мир риск-менеджмента более изменчив, чем когда-либо. В то же время, в связи с вступлением в силу Общего регламента по защите данных (GDPR), который начал действовать в странах ЕС с мая 2018 года, уже стали реальными перспективы наложения большого количества и более крупных штрафов на компании, которые его не выполняют. Действия, предпринимаемые компанией в свете нарушения целостности данных, непосредственно влияют на окончательный размер такого нарушения, накладываемого на организации регулирующими органами по защите персональных данных. Репутационный ущерб неизбежен, если реакция на киберинцидент не адекватна.

Новые риски требуют новых инструментов, направленных на реакцию их потенциального воздействия и смягчения. В данной статье рассматриваются возможные риски финансовых технологий, обращается внимание на киберугрозы, частота которых растет, и предлагается модель выявления и оценки киберриска.

Ключевые слова: киберугроза, киберриски, киберинцидент, цифровизация, финтех, кибербезопасность, цифровая экономика.

FINANCIAL TECHNOLOGY RISK MANAGEMENT MODELS

Cyber incidents continue to move up in the rating of possible threats and occupy the second position in the ranking of risks in the activities of companies (40 %). Five years ago, they were on the fifteenth line. Like a natural disaster or pandemic, a cyber attack can have a negative impact on hundreds of companies, and the number of such incidents is growing. So-called "cyber incidents",

when hackers interfere with the activities of a large number of companies, using the dependencies of their shared Internet infrastructure, occur more often. This reflects the fact that today's world of risk management is more volatile than ever. At the same time, with the upcoming entry into force of the General data protection regulation (GDPR), which has been in effect throughout Europe since may 2018, the prospects of imposing more and larger fines on companies that do not comply with it have already become real. Actions taken by the company in light of a data integrity violation directly affect the final cost of such a violation. Reputational damage is inevitable if the response to a cyber incident is inadequate.

New risks require new tools to respond to their potential impacts and mitigate them. This article discusses the possible risks of financial technologies, draws attention to cyber threats, the frequency of which is increasing, and offers a model for identifying and evaluating cyber risks.

Key words: cyber threat, cyber risks, cyber incident, digitalization, FINTECH, cybersecurity, digital economy.

Развитию цифровой экономики, как перспективному направлению, отведена ключевая роль в укреплении национальной безопасности России. Переход России к цифровой экономике за последние пять лет потребовал финансовых ресурсов в объеме около 1 трлн рублей [5].

По оценкам Boston Consulting Group (BCG), последовательная цифровизация основных отраслей экономики России позволит к 2021 году создавать добавленную стоимость на сумму 5-7 трлн руб. в год, что сопоставимо с общими доходами российского бюджета от нефтегазового сектора (7,4 трлн руб. в 2014 г.) [10].

Информационные технологии внедряются во все сферы жизни человека, и финансовая сфера не осталась в стороне. Особое внимание участников рынка и государственных структур приковано к цифровизации финансовых услуг. На финансовом рынке появился новый сегмент – информационные технологии в финансовой сфере, или сокращенно – «финтех» (финансовые технологии).

По оценкам McKinsey, доля цифровой экономики в ВВП Российской Федерации сегодня составляет чуть менее 4 %. По этому показателю Россия занимает лишь 39-е место в мире [3]. При этом по уровню развития финансовых технологий Россия входит в пятерку мировых лидеров.

Одной из приоритетных задач в настоящее время является ликвидация барьеров, которые мешают передовым технологиям и инновациям успешно встраиваться в финансовую сферу, что может стать драйвером для повы-

шения эффективности в различных секторах экономики. Финансовая сфера становится более технологичной, растет спрос на автоматизацию и роботизацию бизнес-процессов, значительно увеличиваются объемные массивы данных и возможности их высокоточной обработки [4].

Современные российские банки в целях формирования конкурентных преимуществ активно развивают следующие направления: многоканальная доступность; персонализация; «вирусный» маркетинг; программы лояльности; помощь в управлении персональными активами; использование социальных сетей, веб-сервисов и мобильных приложений; интуитивно понятный интерфейс; понятное ценообразование. В связи с этим следует подчеркнуть весомую роль развития финансовых технологий в Российской Федерации крупных банков из топ-10, для которых характерно централизованное принятие решений под влиянием Центрального Банка Российской Федерации и готовность выделять инвестиции на развитие дорогостоящих наукоемких технологий.

Благодаря прогрессу в освоении информационных технологий начинают меняться финансовые и денежно-кредитные системы многих стран. Например, активный переход от оплаты наличными денежными средствами к безналичным онлайн-расчетам; от кредитов, выдаваемых банками или микрофинансовыми организациями, – к получению займа через онлайн-платформы от других физических лиц.

Цифровой сервис становится полноценным каналом обслуживания клиентов, который по существу заменяет посещение колл-центров банковских офисов.

По мнению специалистов [7], финтех представляет «динамично развивающийся сегмент на пересечении секторов финансовых услуг и технологий, в котором технологические стартапы и новые участники рынка применяют инновационные подходы к продуктам и услугам, в настоящее время предоставляемым традиционным сектором финансовых услуг».

Создание условий для развития финтех-проектов в России и их интеграция в существующую финансовую систему – основная цель созданной в 2016 году Ассоциации «Финтех Старт». Работа направлена на увеличение числа стартапов, использующих информационные технологии для совершенствования предоставления современных финансовых услуг, повышения прозрачности взаимодействия субъектов рынка с финансовыми организациями.

Банк России при участии Ассоциации «Финтех» запустил систему быстрых платежей (СБП), которая позволяет мгновенно переводить деньги между банками по простым идентификаторам: номеру телефона, адресу электронной почты, аккаунту в соцсети и др. [9]. Коммерческие банки также активно подключились к внедрению финансовых технологий (табл. 1).

Всемирный экономический форум в отчете «Глобальные риски – 2017» декларировал начало «четвертой индустриальной революции» на пересечении цифровых, биологических и физических технологий.

Четвертая индустриальная революция (Индустрия 4.0) – переход на полностью автоматизированное цифровое производство, управляемое интеллектуальными системами в режиме реального времени в постоянном взаимодействии с внешней средой, выходящее за границы одного предприятия, с перспективой объединения в глобальную промышленную сеть вещей и услуг.

Таблица 1. Программы банков в области развития финансовых технологий*

Банк	Программа поддержки финтех
Альфа Банк	ALFACAMP – долгосрочная программа поиска и развития стартапов, целью которой является реализация продуктов для онлайн-индустрии
Citibank / Ситибанк	- Первая программа-акселератор в 2013 году в Тель-Авиве, приняли участие более 300 стартапов; - «Citi Mobile Challenge» – виртуальный программный ускоритель, сочетающий виртуальную платформу с инкубатором
Commerzbank / Коммерцбанк	Основной инкубатор создан в 2013 году. Программа работает, принимая приглашения от стартапов
Barclays / Барклайс Банк	Предоставляет оборудование, средства и инструменты для стартапов. Вместе сTechStars Банк обеспечивает специальную программу поддержки для некоторых стартапов и предпринимателей
Банк России	Активно выступает за создание консорциума, объединившего бы всех участников финансового рынка, что позволило бы определить потенциал инноваций, объединить усилия инвесторов и оценку уровня риска, идущего от инноваций

*Составлено на основе [6]

Однако с внедрением финансовых технологий появляются новые, ранее не рассматривавшиеся риски, в дополнение к традиционным известным. При этом следует особо подчеркнуть риски, связанные с защитой данных, безопасностью, киберугрозами, а также риски бизнес-процессов [2]. Согласно докладу о глобальных рисках Всемирного

экономического форума 2019 года, мошенничество с данными и кибератаки являются четвертым и пятым глобальными рисками, с которыми сталкивается каждая организация. По своей значимости эти риски приравняются к экологическим проблемам. Большинство экспертов ожидают повышения

частоты кибератак, ведущих к краже денег и данных (82 %) и срыву операций (80 %).

В официальном ежегодном отчете о киберпреступности за 2019 год, опубликованном Cybersecurity Ventures, сообщается, что атаки хакеров во всем мире происходят каждые 14 секунд, а к 2021 году их частота возрастет до каждой 11 секунды.

Специалисты компании InfoWatch отметили, что за 2019 год в сеть утекло более 14 млрд конфиденциальных записей. Рост числа утечек во всем мире по сравнению с 2018 годов увеличился на 10 %, в России – более чем на 40 %.

С того момента, как финансовый сектор начал глобальное перемещение в Интернет, самой серьезной проблемой для сферы финансовых технологий является тема кибербезопасности, которая также стала одной из самых острых в мире. Именно на этой проблеме Центральный Банк Российской Федерации заострил свое внимание. Количество киберугроз неуклонно растет, в том числе связанных с кражей идентификационных данных. Требуется совершенно новый подход в управлении рисками кибербезопасности. Специалисты рассматривают идею формирования новой философии оценки рисков предоставления финансовых услуг в виртуальном пространстве.

События 2017 года, связанные с атаками программ-вымогателей WannaCry и Petya, вызвали нарушение работы значительного числа сервисов и нанесли финансовый ущерб большому числу компаний. Масштабная атака типа «отказ в обслуживании» на интернет-провайдера Дун в октябре 2016 года, также демонстрирует взаимосвязанность рисков и общую зависимость от совместной интернет-инфраструктуры поставщиков услуг и технологий. К такому выводу пришли эксперты Cyence Risk Analytics [1], компании в составе Guidewire, которая является партнером AGCS в оценке киберриска.

Перерыв в производстве, связанный с киберинцидентами, может быть вызван такими событиями, как атака программ-вымогателей, частота которых за последний год удвоилась, в ходе которых хакеры шиф-

руют файлы и требуют компенсацию за их разблокирование. Еще более частой причиной перерыва в производстве, связанного с киберинцидентами, может быть обычный отказ оборудования или ошибка персонала. Например, в феврале 2017 года сервис облачного хранения компании Amazon был недоступен в течение четырех часов, что оказало негативное влияние на ряд интернет-сервисов, сайтов других компаний. Поступила информация о том, что данное отключение было вызвано человеческой ошибкой. По оценке Cyence Risk Analytics, в результате компании из списка S&P 500, зависящие от сервисов Amazon, потеряли примерно \$150 млн [1].

Cyence Risk Analytics отмечает, что перерыв в производстве является одним из сильнейших факторов, причиняющих убытки компаниям после киберинцидента [1]. Например, согласно экспертным оценкам, в случае недоступности облачного сервиса у поставщика облачных услуг продолжительностью более 12 часов убытки могут составлять до \$850 млн. Соответственно, деятельности 50 тысяч компаний трех отраслей экономики (финансы, здравоохранение, розничная торговля) может быть нанесен серьезный ущерб.

Обеспечение кибербезопасности – серьезная проблема, требующая развития надлежащих инструментов ее выявления и устранения последствий на основе формирования модели выявления киберриска предоставления финансовых услуг. Модель угроз кибербезопасности включает в себя три направления – технологии, процессы, кадры. На стыке этих направлений появляются скрытые угрозы – «темная зона» для систем безопасности, специализирующихся на том или ином виде угроз.

Создание модели выявления киберриска предоставления финансовых услуг предусматривает решение следующих задач:

- построить модель выявления, которая даст объективное представление об уровне киберрисков; основная цель внедрения данной модели – не тратить ресурсы компании на снижение несущественных рисков, а

направить усилия на обработку рисков недопустимого уровня;

- выстроить простой и удобный процесс оценки, что особенно актуально для экспертов по кибербезопасности;

- учитывать мнения нескольких экспертов разных областей (в том числе сферы безопасности, бизнеса и информационных технологий) для получения объективного результата по выявлению рисков предоставления финансовых услуг;

- создать универсальную модель, подходящую для разных направлений деятельности в оценке всех идентифицированных киберрисков. При практическом применении модели такой подход позволит агрегировать результаты в единый рейтинг киберрисков для сравнения, анализа и оценки возможных рисков компаний.

При разработке модели выявления риска киберугроз в основу положена классическая формула риска, содержание которой определяется следующей зависимостью: вероятность инцидента, умноженная на ущерб от его реализации. Определен перечень риск-факторов, оказывающих влияние на эти два ключевых показателя: вероятность и ущерб.

На показатель вероятности влияют: перечень актуальных угроз; степень уязвимости, через которые эти угрозы могут быть реализованы; потенциал нарушителя и эффективность защиты.

На показатель ущерба, соответственно, оказывают воздействие критичность (недопустимость простоев) информационного актива; нарушение процесса; недовольство клиентов и партнеров и др. (рис. 1).

Рисунок 1. Система риск-факторов*

*Разработано авторами

Полноценная система менеджмента киберриска должна иметь инструменты автоматической реакции и предусматривать сценарии реагирования на любые потенциальные риски на всех уровнях бизнес-процессов

компании. Управление рисками – основа система защиты от киберугроз в компании, и для ее работы необходимо убедиться, что она вписывается в структуру управления компаний.

На основе проведенного исследования предлагается следующий алгоритм оценки киберриска.

Шаг 1. Формирование системы риск-факторов для оцениваемого вида риска. Для

каждого вида киберриска эксперты определяют перечень актуальных угроз, уязвимостей и мер защиты (рис. 2 и 3).

Риск-факторы, влияющие на вероятность				
Угроза (частота реализации)	Уязвимость (частота использования)	Потенциал нарушителя	Эффективность защитных мер	Вероятность
1 раз в день и чаще	1 раз в день и чаще	- Пользователь АС - Администраторы АС - Хакеры	Несущественная	Событие точно произойдет
От 1 раза в месяц до 1 раза в день	От 1 раза в месяц до 1 раза в день чаще	- Конкурирующие организации - Разработчики ПО и техники	Невысокая	Событие скорее всего произойдет
От 1 раза в год до 1 раза в месяц	От 1 раза в год до 1 раза в месяц	- Бывшие сотрудники - Третьи лица, привлекаемые по договору	Высокая	Событие возможно произойдет
Реже 1 раза в год	Реже 1 раза в год	- Лица без квалификации	Очень высокая	Событие скорее всего произойдет

Рисунок 2. Критерии оценки риск-факторов показателя вероятности*

*Разработано авторами

Шаг 2. Экспертная оценка риск-факторов. Предлагается оценить каждый риск-фактор по четырехуровневой шкале независимо от наличия и степени влияния различных групп факторов риска. Критерии критичности разработаны с учетом масштабов роста сегмента финтех. На этом же этапе определяется вес каждого риск-фактора, чтобы снизить влияние на итоговый показатель риска некритичных для него факторов.

Например: для риска утечки информации оценку ущерба от нарушения процессов можно не учитывать, а параметр «категория

информации» выступает как решающий, и его вес должен быть повышен. Далее оцениваем вес факторов по шкале от 1 до 9.

Шаг 3. Вычисление рейтинга киберриска. В этом шаге можно увидеть ключевое отличие предложной модели от уже существующих качественных методов. Ее преимущество перед классическим методом заключается в том, что можно объединить большое количество полученных мнений в одном значении рейтинга риска, тогда как классический табличный метод, где уровень риска находится на пересечении соответствующей строки вероятности и столбца ущерба, не

Риск-факторы, влияющие на ущерб					
Категория информации	Критичность АС	Нарушение процесса	Клиенты и партнеры	Регуляторы	Ущерб
Коммерческая тайна	Очень критичная	Сбои в нескольких процессах. Сворачивание процессов и направлений	Потеря доверия значительной части клиентов и партнеров. Появление судебных исков	Внеплановые проверки. Крупные штрафы до приостановки действия	Высокое воздействие
Банковская тайна. ПДн	Высоко критичная	Сбои в единичных процессах	Массовое недовольство о клиентов. Отток части клиентов и партнеров	Штрафы. Повышение внимания в виде писем и запросов	Среднее воздействие
Служебная информация	Критичная	Повлияет на скорость процессов, но не приведет к сбоям	Недовольство клиентов, не приводящая к оттоку	Предписание при проверках без наложения штрафа	Низкое воздействие
Обще-доступная информация	Не критичная	Не повлияет	Недовольство единичных клиентов (не VIP)	Без предписаний	Незначительное воздействие

Рисунок 3. Критерии оценки риск-факторов показателя ущерба*

*Разработано авторами

позволяет оперировать таким количеством мнений экспертов.

Для вычисления итогового рейтинга киберриска предложенная модель будет использовать матричный метод вычислений, агрегирующий все качественно-оцененные факторы в одно количественное значение. Это позволяет учесть общее количество уча-

ствующих в процессе экспертов и разброс их мнений, а также разницу в весах, что повышает объективность оценки.

Результат оценки — рейтинг риска R , выраженный числом от 0 до 1, и соответствующий ему уровень киберриска, приведены в таблице 2.

Таблица 2. Отличия дискретной и непрерывной шкал уровня риска*

Рейтинг риска	Низкий	Средний	Высокой	Критический
R	$R < 0,25$	$0,25 \leq R < 0,5$	$0,5 \leq R < 0,75$	$0,75 \leq R$

*Составлено на основе [8]

Пример результата оценки: рейтинги риска потери доступности сервиса и риска утечки информации — 0,51 и 0,63 соответственно. Уровень обоих видов риска высокий, но риск утечки информации более критичен.

Предлагаемая модель и алгоритм оценки киберрисков предоставляют возможность отслеживать динамику рейтинга даже при небольших изменениях в состоянии риск-факторов. Критерии оценки просты и доступны. Безусловно, как любой метод оценки, предлагаемая модель имеет ряд недостатков, которые заключаются в субъективности экспертного мнения. Решение проблемы видится в привлечении большого числа экспертов разных областей. В дальнейшем проблема будет полностью решена, когда экспертные оценки заменит аналитика больших данных на основе искусственного интеллекта. Второй недостаток предлагаемой модели заключается в необходимости формирования списка риск-факторов для каждой оценки. Сейчас на эту процедуру уходит значительная часть времени и трудозатрат сотрудников служб кибербезопасности. В перспективе возможно формирование базового перечня риск-факторов для наиболее критичных систем.

На данном этапе развития модели в приоритетные задачи команды кибербезопасности входят: использование аналитики больших данных (Big Data) вместо экспертных мнений в оценке риск-факторов; формирование базового перечня риск-факторов для наиболее критичных систем, что позволит оптимизировать процесс оценки.

Создание инструмента качественной оценки в виде рейтинга риска предоставляет возможность изучить зависимость динамики этого рейтинга и изменений показателей ущерба. Предлагаются основные направления, ведущие к количественной оценке киберрисков.

1. Прогноз величины ущерба. После того как сформируется достаточный объем статистики о динамике показателей, а также по причинам, по которым происходили скачки ущерба, возможно прогнозировать величину

ущерба от инцидентов. Тестирование на имеющихся исторических данных показало положительный результат. Например, в мае уровень киберриска повысился до высокого (изменение рейтинга с 0,44 до 0,53) по сравнению с апрелем. Есть статистика, на основании которой можно полагать, что при такой динамике в июне ожидается скачок ущерба в 100 млн рублей.

2. Модель Value-at-Risk (VAR). Следующий шаг — применение более прогрессивной модели Value-at-Risk, ранее не использовавшейся для оценки киберрисков. На основании статистики строится график распределения размеров ущерба и доходов. Показатель VAR характеризует максимальный ущерб компании в течение определенного периода, что позволит ответить на вопрос: «Какая сумма ущерба от реализации киберрисков гарантированно не будет превышена в течение следующего периода?» Точность такого прогноза будет достигать 95–99 %.

Предлагаемая модель процесса управления киберриском и принятия решений позволяет установить максимально допустимое значение риска и, как только результат оценки превысит пороговое значение, риск должен быть обработан.

Таким образом, с помощью предлагаемой модели оценки рисков финансовых технологий планируется обнаружить зоны концентрации высоких уровней риска в процессах и сформировать риск-ландшафт кибербезопасности. Актуальная информация о киберрисках будет регулярно предоставляться руководству финтех-компании для принятия стратегически важных решений. Полноценная система менеджмента киберриска должна иметь инструменты автоматической реакции и предусматривать сценарии реагирования на любые потенциальные риски на всех уровнях процессов компании. Чтобы понимать, куда наносить точечные удары, необходимо иметь информацию о текущем состоянии рисков в режиме реального времени.

Развитие процессов риск-менеджмента в сфере кибербезопасности позволит компании использовать удобные и безопасные сервисы, несмотря на растущий интерес со стороны

киберпреступников. Нацеленность на создание единой системы менеджмента киберрисков и универсальных метрик их оценки в дальнейшем приведет к обмену опытом с

другими компаниями и объединит усилия в борьбе с киберпреступностью.

Список литературы

1. Allianz риск барометр. Главные риски для бизнеса на 2018 г. [Электронный ресурс] Режим доступа: URL: <https://allianz.ru/ru/stuff/%d0%a0%d0%b8%d1%81%d0%ba%20%d0%91%d0%b0%d1%80%d0%be%d0%bc%d0%b5%d1%82%d1%80%202018.pdf>

2. Ajupov A.A., Kurmanova L.R., Kurmanova D.A., Abulguzin N.R. A comprehensive assessment of the financial security of banking system // International Business Management. – 2016. - № 10 (23). – P. 5620-5624. [Электронный ресурс] Режим доступа: URL: <https://www.elibrary.ru/item.asp?id=29469198>

3. Курманова Д.А. Финансовые технологии на розничном рынке банковских услуг // Вестник УГНТУ. Наука, образование, экономика. Серия экономика. – 2019. - № 1 (27) – С. 60-67.

4. Курманова Л.Р., Курбанаева Л.Х., Хадыев Т.И. Применение искусственного интеллекта в скоринговых системах российских банков // Инновационное развитие экономики. – 2019. - № 6 (54). – С. 41-48.

5. Russia Tries Rebranding Itself As A Digital Economy / Forbes [Электронный ресурс] Режим доступа: URL: <https://www.forbes.com/sites/kenrapoza/2018/06/11/russia-tries-rebranding-itself-as-a-digital-economy/#6092a9643314>.

6. Отчет о развитии отрасли Финтех в России 2017 [Электронный ресурс] Режим доступа: URL: <http://fintech-ru.com/развитие-отрасли-финтех-в-россии-2017>.

7. Регги де Феникс и Роджер Певерелли. Финансовые услуги. Перегрузка. Вызовы будущего для потребительского рынка банковских и страховых услуг [Электронный ресурс] Режим доступа: URL: <https://market.yandex.ru/product--reggi-de-feniks-i-rodzher-peverelli-finansovye-uslugi-perezagruzka-vyzovy-budushchego-dlia-potrebitelskogo-rynka-bankovskikh-i-strakhovykh-uslug/7787041?clid=703>

8. Осипова Т.Ю., Клименко Е.Н. Финансовые технологии, как оболочка инструментов финансов домашних хозяйств // Проблемы учета и финансов. – 2016. - № 4 (24). – С. 27-36.

9. ЦБ запустил новую систему денежных переводов по номеру телефона / Ведомости [Электронный ресурс] Режим доступа: URL: <https://www.vedomosti.ru/finance/articles/2019/01/28/792632-tsb-zapustil>

10. Цифровая Россия: новая реальность. Июль 2017 г. / DigitalRussia: anewreality. July 2017 [Электронный ресурс] Режим доступа: URL: <https://www.mckinsey.com/~media/McKinsey/Locations/E>.

References

1. Allianz risk barometer. The main risks to business for 2018 [Electronic resource] access Mode: URL: <https://allianz.ru/en/stuff/%d0%a0%d0%b8%d1%81%d0%ba%20%d0%91%d0%b0%d1%80%d0%be%d0%bc%d0%b5%d1%82%d1%80%202018.pdf>

2. Ajupov A.A., Kurmanova L.R., Kurmanova D.A., Abulguzin N.R. A comprehensive assessment of the financial security of banking system // International Business Management. – 2016. - № 10 (23). – P. 5620-5624. [Electronic resource] access Mode: URL: <https://www.elibrary.ru/item.asp?id=29469198>

3. Kurmanova D.A. Financial technologies in the retail banking market // Bulletin of the Ufa state petroleum technological University. Science, education, and Economics. Economy series- 2019. - № 1 (27) – P. 60-67.

4. Kurmanova L.R., Kurbanova L.H., Gadiev T.I. the Application of artificial intelligence in scoring systems of Russian banks // Innovative development of the economy. – 2019. - № 6 (54). – P. 41-48.

5. Russia Tries Rebranding Itself As A Digital Economy / Forbes [Electronic resource] access Mode: URL: <https://www.forbes.com/>

sites/kenrapoza/2018/06/11/russia-tries-rebranding-itself-as-a-digital-economy/#6092a9643314.

6. Report on the development of the FINTECH sector in Russia to 2017 [Electronic resource] access Mode: URL: <http://fintech-ru.com/development-industry-fintech-v-Russia-2017>.

7. Reggie de Phoenix and Roger Peverelli. Financial service. Reboot. Challenges of the future for the consumer market of banking and insurance services [Electronic resource] access Mode: URL: <https://market.yandex.ru/product-reggi-de-feniks-i-rodzher-peverelli-finansovye-uslugi-perezagruzka-vyzovy-budushchego-dlia-potrebitelskogo-rynka-bankovskikh-i-strakhovykh-uslug/7787041?clid=703>

8. Osipova T.Yu., Klimenko E.N. Financial technologies as a shell of household Finance tools // Accounting and Finance issues. – 2016. - № 4 (24). – P. 27-36.

9. The Central Bank has launched a new system of money transfers by phone number / Vedomosti [Electronic resource] access Mode: URL: <https://www.vedomosti.ru/finance/articles/2019/01/28/792632-tsb-zapustil>

10. Digital Russia: a new reality. July 2017 / Digital Russia: a new reality. July 2017 [Electronic resource] access Mode: URL: <https://www.mckinsey.com/~media/McKinsey/Locations/E>.