

УДК 339.13

С. В. Губарьков

ФГАОУ ВО Дальневосточный федеральный университет, Владивосток,
e-mail: gsv20031973@mail.ru

В. Г. Белкин

ФГАОУ ВО Дальневосточный федеральный университет, Владивосток,
e-mail: belkin.vg@mail.ru

Е. Б. Гаффорова

ФГАОУ ВО Дальневосточный федеральный университет, Владивосток,
e-mail: gafforova.eb@dvfu.ru

В. В. Соколенко

ФГАОУ ВО Дальневосточный федеральный университет, Владивосток,
e-mail: val.sokolenko@gmail.com

ВЛИЯНИЕ ИНТЕРНЕТА ВЕЩЕЙ НА БАНКОВСКИЕ УСЛУГИ И МАРКЕТИНГОВЫЕ КОММУНИКАЦИИ КРЕДИТНОЙ ОРГАНИЗАЦИИ

Ключевые слова: банковские услуги, интернет вещей, маркетинговые коммуникации, мобильный банкинг, финансовые услуги, облачные вычисления, big data, искусственный интеллект, риски, маркетинговая стратегия.

В статье выполнен анализ особенностей влияния интернета вещей на формирование банковских услуг и маркетинговые коммуникации кредитной организации. Выделены четыре важных технологических решения, направленных на цифровизацию банковского бизнеса: облачные вычисления, большие данные, искусственный интеллект и интернет вещей. Обосновано, что мобильный банкинг является самым популярным видом дистанционного банковского обслуживания, осуществляемого с помощью интернета вещей. Описаны восемь основных рисков, которые необходимо учитывать для успешного запуска новых банковских продуктов, основанных на использовании потенциала интернета вещей. Сформулированы три основные задачи по совершенствованию маркетинговых коммуникаций СберБанка.

S. V. Gubarkov

Far Eastern Federal University, Vladivostok, e-mail: gsv20031973@mail.ru

V. G. Belkin

Far Eastern Federal University, Vladivostok, e-mail: belkin.vg@mail.ru

E. B. Gafforova

Far Eastern Federal University, Vladivostok, e-mail: gafforova.eb@dvfu.ru

V. V. Sokolenko

Far Eastern Federal University, Vladivostok, e-mail: val.sokolenko@gmail.com

IMPACT OF THE INTERNET OF THINGS ON BANKING SERVICES AND MARKETING COMMUNICATIONS OF THE CREDIT ORGANIZATION

Keywords: banking services, internet of things, marketing communications, mobile banking, financial services, cloud computing, big data, artificial intelligence, risks, marketing strategy.

The article analyzes the features of the influence of the Internet of things on the formation of banking services and marketing communications of a credit institution. Four important technological solutions aimed at the digitalization of the banking business have been identified: cloud computing, big data, artificial intelligence and the Internet of things. It is substantiated that mobile banking is the most popular type of remote banking service carried out using the Internet of things. Eight main risks are described that must be taken into account for the successful launch of new banking products based on the use of the potential of the Internet of things. Three main tasks are formulated to improve SberBank's marketing communications.

Введение

Многие потребности клиентов банков в настоящее время основаны на использовании потенциала интернета вещей. Сущность интернета вещей или IoT (Internet of Things) проявляется не только в объединении разных устройств в единую сеть, но, прежде всего, в трансформации бизнеса и создании инновационных товаров и услуг.

В банковской сфере с помощью интернета вещей кредитные организации повышают конкурентоспособность путем снижения затрат и создания новых банковских продуктов. В значительной степени это касается повышения качества банковских услуг, совершенствования логистических схем и оптимизации складских запасов, использования искусственного интеллекта для снижения человеческого фактора при выдаче кредитов и т.д.

С помощью IoT создаются такие новые банковские продукты, как «цифровые каналы обслуживания клиентов и платежи», «доставка продуктов на дом», «устройства для создания системы «умный» дом», что обеспечивается за счет формирования и развития бесшовных каналов коммуникации, совершенствования мобильного банкинга и т.п.

В процессе оказания банковских услуг коммерческие банки уделяют большое внимание особенностям поведения клиентов. Одним из факторов, влияющих на это поведение, является активное использование клиентами потенциала интернета вещей. В этой связи, коммерческому банку очень важно постоянно заниматься мониторингом динамично изменяющихся потребностей клиентов и оперативно совершенствовать систему маркетинговых коммуникаций.

Цель исследования: изучить особенности влияния интернета вещей на формирование банковских услуг и маркетинговые коммуникации кредитной организации.

Материал и методы исследования

В процессе исследования были использованы следующие методы: индукции, дедукции, сравнения, группировки, экспертных оценок и системный анализ. Теоретические аспекты применения интернета вещей в банковском бизнесе широко исследованы в научных трудах российских и зарубежных ученых: И.Г. Дежиной, А.К. Пономарева, Д.В. Лаконцева, Е.А. Крук, М.В. Федорова,

М. Абрамовой, Дж. Синки, П. Роуз и др. Вопросы использования потенциала маркетинга в банковской сфере при выстраивании маркетинговых коммуникаций отражены в работах И.Т. Балабанова, В.Г. Белкина, Г.И. Белоглазова, Л.И. Вотинцевой, Д.В. Гайдунько, В.Э. Гордина, С.В. Губарькова, Е.Ф. Жукова, В.В. Иванова, Н.П. Кетовой, А.И. Ковалева, И.В. Корнеевой, О.И. Лаврушина, Т.Н. Лобанова, Л.С. Марковой, О.В. Никитенко, М.А. Пономаревой, С.Ю. Старостина, Е.С. Стояновой, Ю.С. Стрельцова, В.М. Усскина, Э.А. Уткина и др. [1-4].

Результаты исследования и их обсуждение

Понятие «интернет вещей» впервые прозвучало в 1999 году: изобретатель Кевин Эштон обозначил этими словами мир, в котором человек перестанет быть «устройством ввода» для информации, распространяемой через интернет, уступив эту роль электронике. Новые технологии передачи данных и типы сенсоров действительно позволили создавать сети физических объектов, взаимодействующих между собой [5].

В банковской сфере использование потенциала интернета вещей началось с активного распространения мобильного банкинга. За последние несколько лет мобильный банкинг стал чуть ли не основным способом коммуникации клиента и банка. Люди все реже ходят в банковские офисы, так как через мобильные приложения сегодня можно воспользоваться практически любой банковской услугой. В настоящее время, наша жизнь без мобильного телефона с «выходом в интернет» кажется немыслимой, однако, сами по себе мобильные устройства и сети никогда не породили бы интернет вещей. Перемещение данных с устройств в базы данных, через обширные компьютерные сети, обслуживающие предприятия и частных лиц – это потенциально сложный, дорогой и трудоемкий процесс.

Среди организаций, предложивших свои версии архитектуры IoT, можно выделить Международный союз электросвязи (МСЭ), Всемирный форум IoT (Internet of Things World Forum, IoTWF), Европейскую комиссию, а также исследовательские агентства, подобные IoT Analytics. Эталонная модель, предложенная МСЭ, отражена на рис. 1 [6].

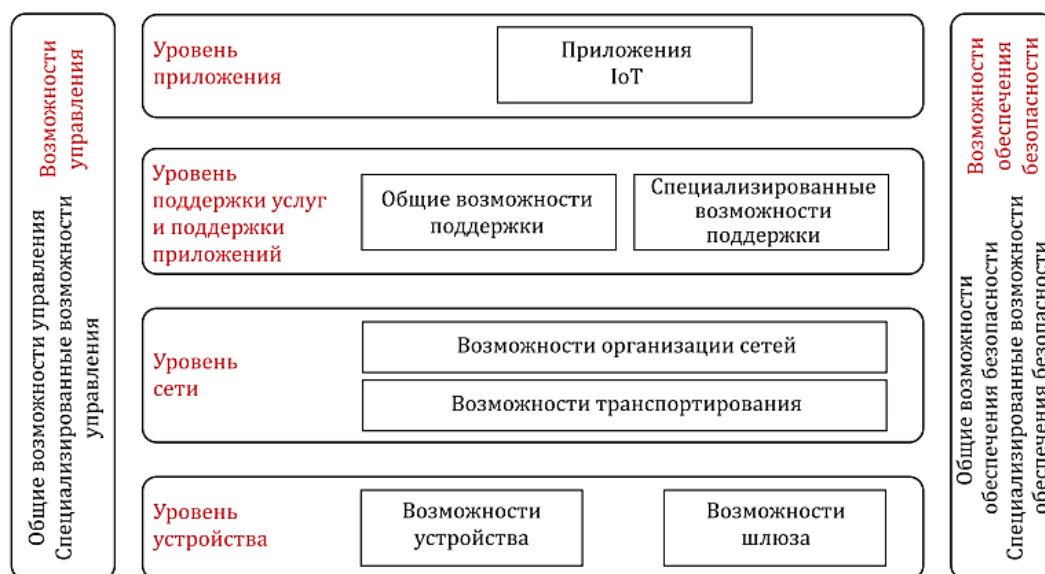


Рис. 1. Эталонная модель IoT, МСЭ-Т Y.2060

Данная модель включает в себя четыре уровня, а также возможности управления и обеспечения безопасности, которые связаны с этими уровнями. Кредитные организации преимущественно используют схему, предложенную МСЭ, но без выделения функции управления.

Рынок банковских услуг претерпевает изменения, компании вынуждены стремительно меняться в условиях цифровой трансформации. У такого исхода было как минимум две предпосылки: *цифровизация* – создание приложений, компьютеров и искусственного интеллекта – и *интернет*, который перевел все бизнес-процессы в онлайн-среду, кардинально изменил их и повысил тем самым продуктивность компаний, сумевших приспособиться к новым условиям.

В работе «Цифровая трансформация. Как выжить и преуспеть в новую эпоху» Томаса Сибела, крупнейшего специалиста в области информационных технологий, представлены четыре важнейших технологических решения, необходимых для цифровизации банковского бизнеса: облачные вычисления, большие данные, искусственный интеллект/машинное обучение и интернет вещей [7].

Облачные вычисления. При помощи облачных вычислений компании избавляются от необходимости конфигурировать и управлять ресурсами самостоятельно: облачные технологии делают все за них, предоставляя удобный доступ к программам, компьютер-

ным сетям и серверам. Облачными ресурсами может владеть как сама организация, так и третья сторона, предоставляющая сервис за плату, как, например, Amazon Web Service.

Ранее для этих же целей использовались корпоративные дата-центры, но по мере развития технологий стало понятно, что это не совсем эффективно, ведь чем больше серверов и прочих управляемых объектов в инфраструктуре компании, тем сложнее налаживать между ними коммуникацию. Облачные технологии показали эффективные и более или менее надежные, безопасные для данных результаты, из-за чего многие IT-директора признались, что имеет смысл отказаться от частных дата-центров в пользу облачных хранилищ. Облачные сервисы существуют по 4 основным моделям, функционал и различия которых наглядно продемонстрированы в схеме (рис. 2).

В зависимости от задач бизнеса имеет смысл комбинировать модели, где-то обращаясь к внутренним ресурсам, а где-то – к услугам сторонних сервисов. Такой подход позволяет снизить зависимость от единственного провайдера и извлечь максимум пользы из разных облаков. Например, для хранения данных можно использовать Microsoft Azure, AWS – для вычислений, IBM Watson – для машинного обучения, и Google Cloud – для распознавания изображений. Таким образом, создается мультиоблако, или гибридное облако, обеспечивающее широкий выбор возможностей [8].



Рис. 2. Модели облачных сервисов

Большие данные (big data). Информация в разном виде была важна всегда, но в эпоху цифровой информации особенно. Многим приложениям с искусственным интеллектом (ИИ) требуются огромные массивы данных, чтобы обучить и усовершенствовать алгоритмы машинного обучения. Сам термин «big data» появился еще в начале 2000-х годов. Тогда всю поступающую в компанию информацию обрабатывали специалисты вручную, делали выводы о ситуации в целом. Но, к сожалению, такой подход даже на заре развития больших данных был неэффективен: на обработку информации уходило слишком много времени и ресурсов.

Сейчас же эта проблема, будь она не автоматизирована, стояла бы особенно остро, так как в связи с цифровой трансформацией данных становится только больше – сейчас их объемы измеряются зеттабайтами (1 зеттабайт данных поместится на 250 миллиардах DVD-дисков). Конечно, в режиме реального времени отслеживать изменения, проделывая эту работу человеческими ресурсами, невозможно. Отсюда появилась необходимость в сервисах, а именно облачных технологиях, которые обладают всеми возможностями для проведения быстрых вычислительных операций и хранения данных.

Таким образом, big data и сервисы, при помощи которых информацией можно управлять, дают огромный толчок для развития интернет-банкинга.

Искусственный интеллект – это третья технология цифровой трансформации. В это понятие входят научные и технические дан-

ные, необходимые для создания разумных машин и компьютерных программ. Одна из главных и самых широких подгрупп ИИ, применяемых во многих сферах жизни и в бизнесе особенно, – это машинное обучение. Под этим термином понимают набор алгоритмов, которые самообучаются за счет решения аналогичных задач и постоянной обработки больших данных.

Благодаря алгоритмам машинного обучения появились возможности, которые ранее казались невозможными. На основе входных данных об условиях полета и записях последнего технического обслуживания и выходных данных о количестве случаев поломки двигателя алгоритм может предупредить о возможной неисправности самолета и даже предсказать ее причину. Чтобы сделать это, больше нет необходимости в соответствующих специалистах – достаточно лишь наличие всех данных в достаточном для анализа объеме.

ИИ – удивительная технология с безграничными возможностями, открыть и развить которые еще только предстоит. В полной мере она еще не охватила банковский бизнес, однако отдельные элементы, такие как машинное обучение, уже повсюду применяются – например, в алгоритмах поисковых систем и предложениях, которые всплывают при оформлении определенной категории услуг в мобильном приложении банка.

Интернет вещей (IoT). Последняя движущая технология цифровой трансформации – интернет вещей, позволяющий подключить к интернету любое устройство. Потенциал IoT заключается в том, что

вычисления становятся еще более простыми и доступными, микропроцессоры – более дешевыми и эффективными, а сети – высокоскоростными.

Жесткая конкуренция в банковском секторе диктует банкам свои условия. Клиентам мало иметь возможность просто получить банковский продукт, их интересует качество предоставляемой услуги и временные затраты на её получение. Не менее важно, чтобы банковская услуга обладала нужными характеристиками и могла в конечном итоге удовлетворить все потребности клиента.

Для банка, в свою очередь, важна конкурентоспособность банковской услуги, которая в отличие от качества, определяет комплекс потребительских и стоимостных характеристик банковской услуги, определяющих её успех на рынке.

Для успешного запуска банковских продуктов, основанных на использовании потенциала интернета вещей, необходимо просчитать все возможные риски, связанные с безопасностью хранения данных, автоматизацией процессов, возникновением технологических сбоев и не только. Британская страховая группа RSA выделила восемь рисков, которые необходимо учитывать при выводе нового банковского продукта на рынок.

1. Риск кибератак. Сегодня кибератаки являются одной из главных проблем цифровой среды. По данным RiskBased Security, глобальные затраты на решение последствий от киберпреступности будут расти на 15% в год в течение следующих пяти лет, достигнув 10,5 трлн долларов ежегодно к 2025-му (по сравнению с 3 трлн долларов в 2015 году) [9].

2. Риски, связанные со сменой сотрудников. Этот риск, согласно описанию RSA, связан с динамичным характером рынка труда и гиг-экономикой (этот термин описывает модель трудоустройства, при которой нанимают сотрудников на временные позиции). Возникает риск утечки данных временными сотрудниками, которые работают part-time или привлекаются только для проектов.

3. Технологические риски. Этот обширный тип рисков связан с постоянными изменениями в управлении новыми цифровыми бизнес-операциями. Многие организации ежедневно сталкиваются со сбоями в работе ИТ-систем из-за неточных тестирований новых решений.

4. Защита данных. В цифровом бизнесе высоки риски, связанные с защитой персональных данных. К ним относится кража или утечка любых конфиденциальных данных – финансовая информация клиентов, исходный код собственной продукции, данные подрядчиков.

5. Соответствие объема данных новой технологии. Риски, связанные с несоответствием новой технологии объему создаваемых данных. Из-за несоответствия этих параметров могут произойти сбои.

6. Риск, связанный с работой с третьими лицами. Бизнес-партнеры, поставщики, другие третьи лица, с которыми вы сотрудничаете, далеко не всегда следуют тем же правилам безопасности, что и вы. Поэтому стоит заранее продумать безопасность передаваемых данных и прописать все договоренности официально.

7. Автоматизация. Учитывая масштабность потенциальных угроз и нехватку специалистов для их смягчения, автоматизация процесса устранения неполадок необходима. Но в то же время это может привести к большим сбоям. Автоматизация предоставляет возможности для новых кибератак (например, атака Stuxnet, сорвавшая ядерную программу целой страны).

8. Неустойчивость. Высокий риск недоступности проведения бизнес-операций после сбоя. Из-за уязвимости программных обеспечений требуется долгое время на восстановление работы, которая вынужденно приостанавливается.

Таким образом, рисками, которые исходят от устройств интернета вещей, пренебрегать не стоит. Несмотря на то, что большинство из них на данный момент не обладают большими вычислительными мощностями, не хранят и не передают критичную информацию (кроме некоторых исключений), IoT-устройства предоставляют новые возможности злоумышленникам для проникновения за периметр предприятия. С их помощью можно организовывать DDoS-атаки или несанкционированный сбор и передачу данных, которые в дальнейшем могут использоваться для организаций атак на инфраструктуру предприятия. Что касается личных устройств интернета вещей, в особенности тех, которые работают с данными о состоянии здоровья (фитнес-браслеты, кардиостимуляторы и т.д.) каждый пользователь должен понимать, что эта информация в любой момент может стать

известна третьим лицам. Безопасность IoT-устройств не должна и не может ограничиваться одним отдельным инструментом или механизмом. Основной принцип защиты предприятий от рисков, которые могут нести устройства интернета вещей, заключается в использовании нескольких уровней защиты: защита периметра, шифрование каналов связи, аутентификация пользователей, обеспечение целостности данных, патч-менеджмент, защита от инсайдеров. При этом стоит помнить, что не существует единого решения для всех устройств в организации – у некоторых из них достаточно долгий срок эксплуатации, и их безопасность нужно обеспечивать в течение всего жизненного цикла: от ввода в эксплуатацию до утилизации.

Чтобы противостоять растущим угрозам в ландшафте IoT, при разработке ядра IoT и проектировании архитектуры следует придерживаться подхода, основанного на безопасном проектировании [5]:

1. Встроенная безопасность и конфиденциальность: из-за продолжающихся сбоев, вызванных IoT в потребительском, корпоративном и государственном секторах, соблюдение принципов безопасности и конфиденциальности в соответствии с принципами проектирования должно быть обязательным для повышения конфиденциальности и безопасности потребителей и укрепления доверия потребителей к IoT-устройствам. Этот целостный подход позволяет IoT-ландшафту на платформах бизнес-индустрии интегрировать конфиденциальность в саму ткань ИТ-систем, сетевой инфраструктуры, бизнес-процессов и проектных спецификаций.

2. Единые руководящие принципы безопасности: децентрализованный и распределенный характер систем IoT делает критически важным наличие единых и хорошо разработанных руководящих принципов безопасности (позволяющих шифрование при передаче и в состоянии покоя) и установление доверия между подключенными устройствами с помощью безопасного централизованного сертификата и управления ключами.

3. Проверка соответствия для третьих сторон: участие сторонних сервисов может привести к новым нарушениям безопасности, что делает жизненно важным оценку соответствия и проверки работоспособности задействованных компонентов сервисов.

Российская банковская сфера отражает типичный рынок монополистической конкуренции, на котором присутствует дифференциация продукта (банковские услуги отличаются неоднородностью и различными характеристиками). Отличие банковской сферы от товарно-материальной сферы заключается в специфике банковских услуг, предлагаемых клиентам. Для поддержания конкурентоспособности в условиях рынка монополистической конкуренции банку необходимо формировать систему маркетинговых коммуникаций, направленных на формирование позитивного имиджа, оперативное размещение рекламы в целевых аудиториях и продвижение новых банковских продуктов на рынке. Все это способствует достижению одной из важных задач банковского маркетинга – поиск оптимальных способов удовлетворения потребностей клиентов.

В силу вышесказанного, становится очевидным, что коммерческому банку для повышения эффективности коммуникативной политики необходимо больше внимания уделять имиджевой составляющей, где оптимальными инструментами являются телевидение и Интернет-площадки. С учетом стоимости обозначенных инструментов приоритетное значение в настоящее время приобретает Интернет-реклама, как менее дорогая и более масштабная по охвату населения. Развитие маркетинговых коммуникаций коммерческого банка направлено на одновременное развитие коммуникаций, формирующих имидж банка, и коммуникаций, обеспечивающих оптимизацию процесса обслуживания клиентов с учетом их потребностей.

Для повышения конкуренции банкам, функционирующим на рынке монополистической конкуренции, во многом приходится полагаться на эффективность маркетинговых коммуникаций. Учитывая стремление клиентов банка активно применять потенциал интернета вещей при получении банковских услуг, становится очевидным необходимость совершенствования коммуникативной политики банка с учетом особенностей и рисков, возникающих при использовании IoT-устройств.

СберБанк, как флагман российского банковского сектора, достаточно активно использует потенциал интернета вещей, как при создании новых банковских продуктов, так и при формировании своей

экосистемы. В основе маркетинговой стратегии СберБанка находится постоянное совершенствование отношений с клиентами в рамках реализации принципов маркетинга взаимодействия.

В 2020 году Сбер закончил этап создания Platform V и запустил масштабную миграцию своего core-бизнеса на новую платформу. Все новые сервисы запускаются только на новой платформе. Не только банковский бизнес, но и дочерние компании используют компоненты Platform V. Это касается главного связующего звена экосистемы – объединяющих элементов, таких как единый идентификатор клиента (SberID), единый продуктовый каталог и другие. Кибербезопасность в СберБанке обеспечивается компанией по стратегическому управлению цифровыми рисками BiZone [10].

Пандемия ускорила продажи финансовых продуктов онлайн. Продажи продуктов в интернет-банке позволяют клиентам продолжать пользоваться услугами СберБанка даже в режиме самоизоляции: выдача кредита с подписанием договора онлайн; выпуск цифровых карт; выпуск кредитной карты в цифровом формате. Одним из главных последствий пандемии является более активное использование онлайн-сервисов в повседневной жизни россиян. Например, доля онлайн-транзакций в общих потребительских расходах по итогам февраля 2021 года составила 11,8%, что на треть выше прошлогоднего показате-

ля (8,7% в феврале 2020 года). По оценке Сбера, такое изменение перенесло порядка 1 трлн руб. клиентов в Интернет только за период с апреля по декабрь 2020 года включительно. На рис. 3 представлена доля онлайн-операций в общем объеме безналичного торгового оборота СберБанка за 2020-2021 гг. [11].

Повышение качества обслуживания клиентов является одной из основных задач коммуникационной политики банка. Наибольший отклик дает непосредственный контакт с потребителями, личное общение в подразделениях банка. Именно в этих взаимодействиях грамотно обученный персонал пытается выстроить цепочку индивидуального подхода к каждому клиенту, установления дружественного контакта с целью дальнейшего пролонгирования отношений и для разрешения проблем потребителей. Помимо вышеуказанных коммуникаций, важнейшей областью взаимодействия с клиентами является решение проблемы очередей в операционных офисах банков. В рамках решения данной задачи в СберБанке был запущен краудсорсинговый проект – «Очереди.НЕТ!», основной задачей которого стало сокращение времени пребывания посетителей в очереди до 10 минут. Стремясь сделать обслуживание более удобным, современным и технологичным, СберБанк с каждым годом все более совершенствует возможности дистанционного управления счетами клиентов [12].



Рис. 3. Доля онлайн-операций в общем объеме безналичного торгового оборота СберБанка за 2020-2021 гг.

Выводы

Таким образом, можно заключить, что коммерческим банкам для повышения конкурентоспособности необходимо реализовать как минимум четыре важнейших технологических решения, направленных на цифровизацию банковского бизнеса: облачные вычисления, большие данные, искусственный интеллект/машинное обучение и интернет вещей.

В настоящее время мобильный банкинг является самым популярным видом дистанционного банковского обслуживания, осуществляемого с помощью интернета вещей. Однако, нормативно-правовое регулирование деятельности банков в сфере дистанционного банковского обслуживания, в том числе, с помощью IoT-устройств, нуждается в совершенствовании.

Для успешного запуска новых банковских продуктов, основанных на использовании потенциала интернета вещей, необходимо учитывать восемь основных рисков, связанных с: кибератаками, сменой сотрудников, возникновением технологических сбоев, безопасностью хранения данных, соответствием объема данных новой технологии, работой с третьими лицами, автоматизацией процессов, неустойчивостью.

Чтобы противостоять растущим угрозам в ландшафте IoT, при разработке ядра IoT

и проектировании архитектуры следует придерживаться подхода, основанного на безопасном проектировании и учитывающего встроенную безопасность и конфиденциальность, единые руководящие принципы безопасности и проверку соответствия для третьих сторон.

В числе основных задач по совершенствованию маркетинговых коммуникаций СберБанка, в том числе, с учетом влияния интернета вещей, следует отметить:

- активное развитие экосистемы, в которой клиент удовлетворяет потребность в нефинансовых услугах и одновременно мотивируется к получению финансовых услуг банка;
- внедрение системы корпоративной социальной ответственности, в рамках которой банк максимально учитывает интересы целевой аудитории и особенности используемых клиентами IoT-устройств, а далее предлагает многовариантный подход к выбору способов удовлетворения потребностей клиентов;
- внедрение высокотехнологичных разработок СберБанка и компаний его экосистемы в сферах кибербезопасности, транспорта, робототехники, видеосвязи, управления коммерческой недвижимостью и складской логистикой, что позволяет снижать цифровые риски при использовании IoT-устройств.

Библиографический список

1. Банки России: современный инструментарий и виртуальные технологии развития: учебник / коллектив авторов; под ред. д-ра экон. наук, профессора В.Г. Белкина; д-ра экон. наук, профессора Л.И. Вотинцевой. Владивосток: Изд-во Дальневост. ун-та, 2021. 359 с.
2. Губарьков А.С., Губарьков С.В. Особенности поведения российских потребителей на рынке банковских услуг // Управление и экономика народного хозяйства России: сборник статей Межд. научно-практич. конф. (17–18 марта 2021 г., г. Пенза). Пенза: РИО ПГАУ, 2021. С. 92-98.
3. Губарьков С.В., Егосин В.С. Технология создания новых банковских продуктов: актуальные проблемы и перспективы развития // Вестник Алтайской академии экономики и права. 2021. № 5 (часть 2). С. 175-180. DOI: 10.17513/vaael.1702.
4. Губарьков С.В., Ким А.Г., Губарьков А.С. Способы совершенствования ценовой политики для корпоративных клиентов коммерческого банка // Вестник Алтайской академии экономики и права. 2021. № 7. Ч. 1. С. 17-23. DOI: 10.17513/vaael.1775.
5. Губарьков С.В., Гончар К.Г. Интернет вещей в финансовой индустрии: проблемы безопасности // Инновационные аспекты развития науки и техники. 2021. № 6. С. 111-118.
6. Лидеры Всемирного форума по Интернету вещей анонсировали эталонную модель IoT и Кадровый консорциум IoTWF. [Электронный ресурс]. URL: https://re-port.ru/pressreleases/lidery_vsemirnogo_foruma_po_internetu_veshei_anonsirovali_ytalonnuyu_model_iot_i_kadrovyy_konsorcium_iotwf/ (дата обращения: 05.06.2022).

7. Карнаух В.К. На пути к цифровому обществу. Рецензия на книгу Т. Сибела «Цифровая трансформация. Как выжить и преуспеть в новую эпоху» // Управленческое консультирование. 2021. № 9 (153). С. 145-149.
8. Сравнение услуг облачных провайдеров: Microsoft Azure, AWS или Google Cloud. [Электронный ресурс]. URL: <https://la.by/blog/sravnenie-uslug-oblachnyh-provayderov-microsoft-azure-aws-ili-google-cloud> (дата обращения: 05.06.2022).
9. Кибербезопасность 2021-2022. Тренды и прогнозы. [Электронный ресурс]. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-2021-2022-trendy-i-prognozy/> (дата обращения: 06.06.2022).
10. ИТ-бюджет Сбербанка в 2020 году установил новый рекорд. [Электронный ресурс]. URL: <https://news.myseldon.com/ru/news/index/251024045> (дата обращения: 7.06.2022).
11. COVID полностью изменил потребительский рынок: российские покупатели не хотят возвращаться в оффлайн. [Электронный ресурс]. URL: <https://oborot.ru/news/rossiyane-stali-bolshe-tratit-v-internete-i131818.html> (дата обращения: 8.06.2022).
12. Кетова Н.П. Оказание услуг коммерческими банками: использование потенциала маркетинга, выстраивание взаимодействий с клиентами // Вестник Адыгейского государственного университета. Серия 5: Экономика. 2015. № 3 (165). С. 261-271.