



## ОРИГИНАЛЬНАЯ СТАТЬЯ



DOI: 10.26794/2220-6469-2022-16-2-51-63  
УДК 336.717.06(045)  
JEL G21

## Цифровой банкинг: смена парадигмы современных финансов

И.А. Зарипов

РЭУ им. Г.В. Плеханова, Москва, Россия

### АННОТАЦИЯ

Статья представляет собой авторский взгляд на современные проблемы, стоящие перед финансовым сектором Российской Федерации, в рамках перехода на цифровое обслуживание финансовых операций. Проблемы трансформации финансового сектора России обострились в связи с массовым переходом на дистанционные каналы взаимодействия из-за ограничений пандемийного периода. Автор исследует актуальные уязвимые точки цифровизации финансового сектора из-за усилившихся кибератак преступников и предлагает рекомендации по противодействию данным преступлениям. Приводятся доказательства необходимости пересмотра концепций и стратегий развития банков в связи с цифровизацией, совершенствования подходов к информационной безопасности. Автор приходит к выводу, что именно информационная безопасность является ключевым элементом процесса цифровизации банковской деятельности, а стабильность и надежность банковских институтов может быть обеспечена только совместными усилиями государства, банков и их клиентов.

**Ключевые слова:** цифровизация; финансовый сектор; банковские операции; цифровые финансы; информационная безопасность

**Для цитирования:** Зарипов И.А. Цифровой банкинг: смена парадигмы современных финансов. *Мир новой экономики*. 2022;16(2):51-63. DOI: 10.26794/2220-6469-2022-16-2-51-63

## ORIGINAL PAPER

## Digital Banking: Modern Finance Paradigm Shifting

I.A. Zaripov

Plekhanov Russian University of Economics, Moscow, Russia

### ABSTRACT

The article presents author's view on the current problems facing the banking system of the Russian Federation as part of the transition to digital banking services, especially aggravated due to the massive using of remote channels of interaction caused by the restrictions of the pandemic period. The author analyses the current problems of financial sector due to increased criminal cyber attacks and offers his recommendations to counter these crimes. There is evidence of the needs to revise the concepts and strategies of the development of banks in connection with digitalization, to improve approaches to information security. Finally, the author concluded that a key element in the process of digitalization of banking activities is information security, and the soundness of banking institutions can be ensured only by the joint efforts of the state, banks, and their customers.

**Keywords:** digitalization; financial sector; banking; digital finance; information security

**For citation:** Zaripov I.A. Digital banking: Modern finance paradigm shifting. *The World of the New Economy*. 2022;16(2):51-63. DOI: 10.26794/2220-6469-2022-16-2-51-63

## ВВЕДЕНИЕ

В настоящее время цифровой банкинг (Digital Banking, DB) — это модный тренд, о котором говорят банковские институты, представители ИТ-компаний, эксперты и чиновники. Действительно ли за цифровым банкингом будущее: т.е. цифровой банкинг сможет вытеснить с рынка традиционные банковские структуры, перевести их в «нишевое» положение? И какие основные угрозы может принести цифровизация банковскому сектору?

Цифровая революция способствовала развитию цифровых технологий в финансовом секторе, включая банковские операции — Digital banking. Эти тенденции, наряду с урбанизацией экономически активного населения, привели, прежде всего, к ускорению темпа жизни человека и изменению психологии массового клиента, который перестал воспринимать традиционные банки с их консервативными отделениями, очередями и часто неторопливым обслуживанием как нечто приемлемое лично для него. Благо, появились технологии и провайдеры, которые позволяют осуществлять все основные нужные клиентам банков операции на расстоянии в то время, когда удобно клиенту, а не в строго отведенные часы работы банковских филиалов и отделений. Эти новые возможности стали использовать и банки, разрабатывая и предлагая своим партнерам, контрагентам и клиентам мобильные приложения, усовершенствованные системы дистанционного обслуживания и интернет-банкинга. Имея смартфон или планшет и установив на него мобильное приложение, любой клиент может осуществить перевод, оплатить счета, проверить баланс, заказать новую пластиковую карту или заблокировать старую, даже открыть счет и оформить депозит. Поэтому функционал банковских отделений как универсальных финансовых хабов, где клиенты могли проводить все виды финансовых операций, уходит в прошлое.

Банковская отрасль стремительно меняется. Еще два года назад больше половины клиентов были готовы сменить банк, если закрывается их местный филиал. В настоящее время количество выразителей таких настроений снизилось и составляет меньше 1/5 от общего количества клиентов<sup>1</sup>.

<sup>1</sup> Accenture. North America Consumer Banking, 2015. Отчет по розничным банковским продуктам в Северной Америке, 2015. URL: <https://www.accenture.com/us-en/~media/Accenture/Conversion-Assets/Microsites/Documents17/Accenture-2015-North-America-Consumer-Banking-Survey.pdf#zoom=50> (дата обращения: 12.12.2021).

В настоящее время пересмотр функционала банка и банковской сети — одна из самых главных задач банковских учреждений. Владельцам и высшему руководству банковских институтов следует двигаться в фарватере современных тенденций, поэтому сейчас неприемлем старый взгляд на банковские отделения и филиалы как места, в которых денежные средства перемещаются между банком и клиентом. Ранее рост банковской сети, особенно в регионах, говорил о масштабности банковского бизнеса, существовали понятия «ключевой регион», «регион присутствия банка». Сейчас ситуация изменилась.

## ИЗМЕНЕНИЕ РОЛИ БАНКОВСКИХ ОТДЕЛЕНИЙ

В настоящее время нет потребности в существовании физического присутствия банковских подразделений в различных регионах страны, можно ограничиться лишь небольшим представительством банковского персонала, который бы функционально отвечал за техническую поддержку и консультировал клиентов. Банки сейчас отказываются и от такого представительства, перенеся техподдержку и взаимодействие с клиентурой в виртуальное пространство, иногда предлагая вначале услуги ботов или виртуальных помощников, которые позволяют решить наиболее простые и стандартные проблемы. Так, в США банковские структуры закрыли около трети филиалов по стране за последние пять лет, что позволило значительно (почти в половину) сократить операционные расходы и почти никак не отразилось на количестве привлеченных клиентов<sup>2</sup>. Что касается России, то, по оценке автора, минимальные расходы на открытие филиала банка обойдутся в 15 млн руб., а годовое содержание, при наличии минимального количества персонала, потребует еще около 10 млн руб.

Поэтому банки, сокращая отделения и развивая цифровые сервисы, имеют возможность снижать комиссии за обслуживание, уменьшать ставки по кредитам, т.е. предлагать своим клиентам более льготные условия. Это еще одно преимущество, которое предоставляют цифровые технологии.

В связи со снижением потребностей в широкой банковской сети банкирам придется решать, что делать с освободившимися площадями. Преждевременно говорить о полной ликвида-

<sup>2</sup> ABIATEC. URL: [www.abiatec.by](http://www.abiatec.by) (дата обращения: 08.12.2021).



ции банковских сетей в течение ближайших 15–20 лет — все-таки значительная часть клиентов предпенсионного и пенсионного возраста предпочитает пойти в банковское отделение и там путем живого общения с банковским сотрудником произвести платеж или получить наличные.

Кроме того, в любом обществе присутствуют консервативные настроения, постепенно трансформируемые в категорию «национальной традиции». Так, в США, Великобритании, Малайзии и странах — бывших колониях Великобритании клиенты до сих пор рассчитываются чеками, чего в банковской системе других стран никогда не было.

Безусловно, банковские отделения продолжают существовать и в будущем, хотя в некоторых странах (например, в Швейцарии) они превратятся в аналог элитарных клубов. Возможно, что на первый план будут выходить функции финансового советника или *private-banking*<sup>3</sup>. Банковские сотрудники отделений станут осуществлять консультации по различным экономическим вопросам, оказывая поддержку клиентам на протяжении всей жизни.

Известный банковский эксперт Ден Реймер также считает, что отделения не исчезнут. В рамках концепции цифровизации банковские отделения из главного канала взаимодействия становятся лишь одним из средств коммуникации, и в будущем из мейнстрима перейдут в нишевую, узкоспециализированную плоскость, станут дополнением к иным каналам цифрового банковского бизнеса. Но отделения все же будут исполнять некоторые функции: открытие счетов и их обслуживание (особенно для новых клиентов); консультирование (особенно по вопросам кредитов и новых сервисов), а также поддержка бренда банка [1].

Отметим, что в настоящее время совершенствуются технологии открытия счетов клиентам и без их физического присутствия. Современные программно-технические решения позволяют соблюдать все требования российского законодательства по идентификации клиента в рамках противодействия отмыванию криминальных доходов и финансированию терроризма, а также защиты персональных данных. Поэтому со временем кли-

ентам для открытия счета не нужно будет приезжать в отделение, а кредитную карту можно будет заказать через интернет, а банк, используя свои процедуры, проверит клиента и примет решение. Пин-код клиент получит через колл-центр, а карта будет активизирована через любой банкомат данного банка.

## ОСНОВНЫЕ ВОПРОСЫ ПРИ ПЕРЕХОДЕ НА ЦИФРОВОЙ БАНКИНГ

При переформатировании модели банка его руководству необходимо в Digital Banking найти ответы на следующие вопросы:

- Какое количество отделений нужно банку? Какие отделения будут построены на системе самообслуживания, а какие станут консультативными центрами и займутся продажами простых и транзакционных продуктов?

- Какое количество персонала нужно в головном офисе, консультативных центрах, точках продаж. Может быть, стоит часть функций передать на аутсорсинг? Как поступить с уже работающими сотрудниками? Надо ли значительно сокращать персонал или, может быть, переобучить ряд квалифицированных сотрудников на новую банковскую специальность?

- Каковы клиентские предпочтения? Стоит ли переориентировать отделения на более специализированные [филиалы для Private Banking, исламского (партнерского) банкинга и др.]?

- Какие технологии должны быть использованы в каждом отделении, и каким образом они будут коррелироваться с определенными группами клиентов?

- Какие другие способы взаимодействия с клиентами и контрагентами нужно использовать банку, и как интегрировать различные технологии, методики и продукты в единые цифровые системы банка?

От правильного ответа на данные вопросы зависит конкурентоспособность банка не только по отношению к другим финансовым институтам, но и к разным цифровым компаниям, постепенно, но все более активно заходящим на территорию банковской системы.

Итак, первое свойство цифрового банкинга — активное использование интернет- и иных цифровых технологий, ведущих к переформатированию отделений, филиалов традиционных банков — достаточно значимое, но не являющиеся основной тенденцией цифровизации.

<sup>3</sup> Private-banking — вид банковского обслуживания, ориентированный на предоставления комплекса банковских и финансовых услуг для состоятельной клиентуры, включая круглосуточного персонального менеджера (*concierge service*). Традиционно осуществляется в отдельных специально оборудованных банковских филиалах.

## ИЗМЕНЕНИЕ ПАРАДИГМЫ БАНКОВСКОГО ДЕЛА

Главное в современных процессах перехода на цифровой банкинг — изменение поведения банка, когда происходит общая трансформация парадигмы самого банковского дела. Цифровой банкинг означает, что банк сам приходит в те области, где есть клиенты. Кроме того, концепция цифрового банка предполагает, что банк будет развиваться в новых сферах, — именно в этих областях финансовый институт создает специальные возможности для различных групп клиентов. При этом он часто предлагает не только гибридные, транзакционные продукты, но и понятный и удобный для клиента технологический интерфейс с техническими решениями, нужными именно этой категории.

До эры новых технологий финансовый институт заявлял: «Вот я, вот моя продуктовая линейка, вот мои критерии по клиентам и условия, — будем рады видеть вас своими клиентами, если вы подойдете». Сегодня, в эпоху развития виртуальных систем, финансовый институт заявляет, что он самостоятельно может определить месторасположение клиента, приблизительно понял область его потребностей и готов в любое время предоставить комплекс услуг для комфортного использования.

В рамках новой концепции цифровых услуг банковские структуры, являясь своеобразными виртуальными посредниками, готовы предложить весь нужный клиенту комплекс услуг, не ограничиваясь только финансовыми операциями. При этом банк может создавать каналы взаимодействия с клиентами в информационных сервисах и социальных сетях, в электронном бизнесе и интернете вещей, в приложениях к мобильным устройствам, используя любую систему виртуального пространства, в которой клиенту могут потребоваться банковские услуги.

И хотя именно технологии Digital Banking являются теми средствами, которые положили начало этой новой концепции в банковском деле, все же главное, что изменился сам подход.

Цифровой банкинг ставит задачу охватить все области деятельности человека, — финансовые институты активно работают в мобильной сфере и в социальных сетях, но в остальных каналах банки пока находятся на стадии экспериментов. Проводится активная работа на уровне R&D<sup>4</sup>, идет

<sup>4</sup> R&D — Research&Development (англ.) — исследование и развитие — направление, отвечающее за аналитику и определение путей развития бизнес-структуры.

поиск решений, применение которых, полагаем, будет успешным.

Есть определенные возможности для банков и в новом направлении, называемом «интернет вещей», где финансовому институту надо найти варианты встраивания в цепочку взаимодействия устройств клиента.

## DIGITAL BANKING — НОВОЕ В РОЗНИЧНЫХ ОПЕРАЦИЯХ

Цифровой банк — это комплексная бизнес-стратегия, включающая все информационные каналы. Полагаем возможным отметить, что ситуация с переходом на цифровые технологии меняется так стремительно, что банковские институты, не начавшие процесс перехода, согласно новой концепции, отстанут настолько, что не смогут конкурировать с теми банковскими структурами, которые уже трансформируются из традиционных банков в экосистему по предоставлению комплекса всех виртуальных услуг, среди которых собственно банковские операции будут составлять лишь небольшую часть.

Цифровой банк — это следующая стадия в эволюции розничных банковских операций, включающих мобильные платежи, системы онлайн-займов (в том числе пиринговых) и депозитов, мобильный банкинг, MPOS<sup>5</sup>, системы персонального учета финансов (PFM).

Безусловно, банкам необходимо активно развивать и интернет-маркетинг, который позволит расширить охват клиентов, уже проведя сегрегацию их по группам, исходя из их потребностей.

Усилившаяся конкуренция в банковском секторе, который активно применяет цифровые технологии, привела к особой требовательности клиентов, особенно с точки зрения скорости и комфортности проведения банковских операций. У современных клиентов нового типа — Homo informaticus, людей поколения Z (Next Generation) — есть повышенные потребности и серьезные возможности искать свой идеал виртуального банка, поскольку эти клиенты хотят получить эксклюзивные банковские услуги, подобранные специально для них, в любой момент времени и нужные именно им. И такая потребность вполне объяснима, так как

<sup>5</sup> MPOS — mobile points of sale (англ.) — мобильная точка продажи — компактное устройство, представляющее собой подключенный к смартфону или планшетному компьютеру торговый терминал.



стиль жизни клиентов связан с интернет-средой и виртуальным пространством.

Традиционным банкам, которые хотят преуспеть в процессе перехода на новую цифровую платформу банковского обслуживания, уже недостаточно иметь просто официальный сайт в интернете и некое банковское приложение для мобильных систем Андроид и iOS. Подобные системы, отвечающие за лояльность потребителя и поддерживающие механизм продаж, во-первых, есть у всех без исключения средних и крупных финансовых структур, а во-вторых, уже не дают достаточно значимого прироста клиентской базы, поскольку не являются уникальным продуктам. Поэтому в современных условиях усиления конкуренции, как в банковском бизнесе, так и в онлайн-пространстве, банкам необходимо выработать новую уникальную концепцию построения информационной инфраструктуры и грамотно презентовать ее рынку.

В настоящее время большинство кредитных учреждений управляют классически отформатированными многоуровневыми процессами, предполагающими особый контроль. Но эти процессы в современных условиях позволяют удержать часть консервативных клиентов, а не привлечь новых с особыми потребностями в цифровых технологиях. При этом, даже если традиционные банки предлагают лишь отдельные цифровые услуги (например, мобильный банк или интернет-обслуживание с использованием дистанционного доступа через личный кабинет), этого уже недостаточно, поскольку невозможно полностью сконструировать комплексную модель цифрового банкинга для финансового института.

Большинство экспертов полагают, что заниматься созданием цифровой инфраструктуры без комплексного подхода непродуктивно. Новым игрокам достаточно затруднительно интегрироваться в существующее цифровое пространство, а тем более — сформировать свою уникальную цифровую инфраструктуру, достаточно гибкую и эффективно развивающуюся в соответствии с запросами и требованиями нового типа клиентов.

Пионерами цифрового банкинга стали глобальные банковские империи, начавшие инвестировать в цифровую стратегию ранее остальных банков, а также банки нового поколения, сразу построившие свою бизнес-стратегию как Digital банки. Именно они по праву заняли топовые места веду-

щих цифровых банков в рейтингах крупнейших консалтинговых компаний<sup>6</sup>.

Флагманам цифрового банковского рынка уже удалось добиться того, что взаимодействие банка и клиента осуществляется без участия сотрудников банка. Остальным финансовым институтам приходится удваивать и утраивать усилия, чтобы догнать своих конкурентов в этой сфере.

Кроме того, небанковские компании появляются на рынках традиционных банковских услуг (Google, Apple), развиваются поставщики финансовых продуктов нового поколения: Moven, Knab, Fidor Bank — на глобальном рынке; Instabank, Modulbank, Рокетбанк — в Российской Федерации<sup>7</sup>.

### РЕКОМЕНДАЦИИ БАНКАМ ПО РАЗВИТИЮ DIGITAL BANKING

Оптимальная, на наш взгляд, стратегия банка должна быть нацелена на такое обслуживание клиентов, при котором все операции проводятся быстро и удобно, а запросы обрабатываются в режиме реального времени, 24/7.

Для достижения этого следует синхронизировать все каналы обслуживания, четко ориентировать предложения продуктов на конкретного клиента, использовать сквозную обработку информации и постоянно коммуницировать с клиентами в режиме онлайн.

При этом, учитывая быстро меняющуюся ситуацию в мире цифровых технологий, надо предусмотреть гибкость как в ИТ-системах (позволяющую оперативно вносить изменения, корректировать и изменять услуги, каналы взаимодействия, банковские инструменты и продукты), так и в должностных инструкциях сотрудников банка и управленческих механизмах для того, чтобы быстро реагировать на изменяющуюся обстановку, не затягивая процесс принятия решений.

Для построения комплексной системы цифрового банкинга следует создать стандартный и бесперебойный механизм обслуживания клиентов в любом комфортном им канале. Зачастую клиенту одинаково удобно получить обслуживание

<sup>6</sup> Internet banking rank. Deloitte, Marksw Webb Rank & Report, 2016. URL: <https://markswwebb.ru/report/internet-banking-rank-2016/> (дата обращения 16.12.2021).

<sup>7</sup> Диасофт, BIAN: Digital banking как стратегическое направление развития современного банка. Сайт журнала «Банковские технологии». URL: <http://bosfera.ru/bo/ekspertiza-bian-i-diasoft-digital-banking-kak-strategicheskoe-napravlenie-razvitiya-sovremennogo> (дата обращения 15.12.2021).

как посредством дистанционных технологий (через выделенный сегмент на сайте банка или через мобильное приложение), так и в очном формате (через обращение к операционисту в отделении или через банкомат в торговом центре). При этом все каналы взаимодействия с клиентами должны быть интегрированы между собой, а также налажено взаимодействие с API<sup>8</sup> и с центральной (core) банковской системой.

Внутри Digital-платформы особое внимание должно быть уделено согласованности действий, и предусмотрена возможность для клиентов самим управлять предоставляемыми банками виртуальными услугами. Для современного клиента банка будет важно иметь возможность провести индивидуальную настройку каналов реализации банковских услуг с другими виртуальными системами: социальными сетями, поисковыми системами и пр. Подобные возможности банки могут предоставить, если будут использовать открытый интерфейс, позволяющий встраивать свои каналы обслуживания в информационные системы, используемые клиентом.

Банковская информационная система должна быть гибкой, легко изменяемой и настраиваемой, быстро менять саму структуру, удалять или добавлять программные компоненты, разработанные различными производителями, модернизировать и видоизменять их. Актуальной для развития современной Digital-платформы является концепция «Open API», т.е. открытого программируемого интерфейса, управляющего работой различных приложений в общей информационной системе. Именно использование банками подобной концепции позволит банковским структурам оперативно и комфортно взаимодействовать с клиентами, собирать и обрабатывать информацию об их потребностях, предлагая дополнительные услуги, нужные именно определенной категории клиентов.

### СОВРЕМЕННЫЕ ОСНОВНЫЕ ТРЕНДЫ РАЗВИТИЯ ЦИФРОВОГО БАНКИНГА

Цифровой банкинг становится в настоящее время темой для исследования в различных профессиональных сообществах, поскольку он находится на стыке финансов, ИТ-технологий, продаж,

как розничных, так и корпоративных. Руководитель Департамента Digital Banking компании Global Digital Banking Набенду Мисра (Nabendu Misra) выделил следующие актуальные тенденции в области наиболее востребованного канала взаимодействия тандема «банк-клиент» — банковских приложений [2].

#### Мобильные платежи, моментальная оплата

Идея о том, что телефон может использоваться как платежная карта, возникла давно, почти вместе с созданием смартфона. Тем не менее практическая реализация началась лишь недавно. Специальные чипы стали интегрировать в ряд смартфонов Android в 2013 г. Гаджет с подобным чипом мог быть использован как платежная карта. Операционные системы смартфонов и планшетов совершенствовались и в Android 4.4, — в 2014 г. была предложена технология, заменяющая владельцу расчетную карту (HCE — host card emulation). Почти все приложения на базе этой ОС и более поздних версий будут позволять осуществлять бесконтактные расчеты. Apple, начиная с iPhone 6, оснащает смартфоны специальным чипом. Новый метод оплаты Apple Pay, позволяющий осуществлять бесконтактные платежи, используя в качестве идентификатора отпечатки пальцев, облегчил банкам задачу при разработке своих приложений для iPhone.

Программное обеспечение, которое позволит пользователям оплачивать покупки бесконтактно, привязав дебетовые и кредитные карты, есть сейчас в активе многих компаний. Прогнозируется массовая замена пластиковых платежных инструментов на виртуальные (как это уже практикует PayPal). Компания Visa также предлагает онлайн-услуги в рамках программы «Цифровые решения Visa» (Visa Digital Solutions). Есть подобная система и у Mastercard.

Функция бесконтактной оплаты пользуется спросом у плательщиков, и банкам стоит включаться в это направление, иначе их место займут небанковские компании.

В настоящее время процессы цифровизации банковских услуг отечественных кредитно-финансовых институтов осуществляются в рамках дополнительных санкций США и стран ЕС, введенных ими в ответ на начало специальной военной операции России на Украине в феврале 2022 г. Санкции и прессинг ведущих западных государств вынудили уйти с российского рынка

<sup>8</sup> API — Application Programming Interface (англ.), программируемый интерфейс для приложений — программная оболочка, отвечающая за взаимодействие различных приложений в общей информационной системе.



или прекратить обслуживание российских клиентов крупнейшие мировые ИТ-компании, а также корпорации, оказывающие платежные услуги. Прекращение обслуживания россиян компаниями Apple, PayPal, Western Union, Visa, Mastercard, American Express, отключение от международной системы SWIFT некоторых российских банков заставило российские государственные и частные компании находить альтернативные платежные системы, которые позволят российским клиентам надежно проводить платежи внутри России и обслуживаться за рубежом. Внутри России ApplePay рекомендуется заменить на SberPay и использовать межбанковскую СБС (систему быстрых платежей). Одной из альтернатив Visa, Mastercard может стать совместный проект по выпуску международной пластиковой карты Национальной российской платежной системы «Мир» и китайской платежной системы UnionPay, поддержанный большинством российских банков. Заметим, что китайская национальная платежная система очень широко распространена в мире: ее карту принимают в 180 государствах. На настоящий момент выпущено более 3 млрд пластиковых карточек UnionPay<sup>9</sup>. Рассматриваются и иные варианты, с учетом существующих обстоятельств, в частности, рассматривается проект создания международной платежной системы, альтернативной системе SWIFT. Учитывая, что все страны Ближнего Востока, Китай, Индия, ЮАР, страны ЕвразЭС, а также ряд стран Латинской Америки поддерживают Россию, успех создания и функционирования подобной системы представляется вполне реальным.

### **Внедрение принципов компьютерных игр в банковском бизнесе**

Данная тенденция представляет собой применение принципов компьютерных игр к различным информационным каналам взаимодействия банка и клиента и заключается во внедрении таких опций, как получение баллов или предоставление особого статуса за депозит определенного уровня. Основная задача, которая решается банком, — мотивирование на регулярное открытие приложения, сайта, группы в социальных сетях. Эксперты считают, что в отличие от других цифровых инициатив данные усилия малоэффективны, поскольку трудно привязать клиента допол-

нительными баллами, однако, являясь финансово малозатратной, данная опция привлечения и удержания клиентов имеет право на существование и будет востребована частью клиентуры.

### **Мультизадачность в одном цифровом банковском продукте**

В настоящее время Digital Banking становится конкурентным преимуществом, и финансовые институты работают над выпуском узкозадачных цифровых продуктов, направленных на привлечение клиентов, но в рамках одного банковского приложения. Так, одной из особо востребованных услуг на фоне роста трудовой миграции является система денежных переводов. Традиционными лидерами индустрии были компании с историей: Western Union и Moneygram. Однако все изменилось, и в настоящее время большую часть рынка занимают онлайн-трансферы компаний Xendpay, Transfer Wise и Xoom за счет удобства их сервисов и выгодных тарифов. Финансовый институт может не только предусмотреть в своем фирменном приложении дополнительные функции для мобильных устройств, типа денежных переводов, оплаты коммунальных услуг, обмена валют, но и проводить различные рекламные кампании и исследования рынков.

Особые продукты могут быть предложены клиентам для проведения денежных переводов на территории отдельных стран (для России будут востребованы переводы в страны СНГ), пополнения электронных кошельков, операций с финансовыми инструментами и др.

### **Многоканальный банкинг (multichannel banking) – синхронизированное обслуживание клиентов в отделениях и в цифровой среде**

Финансовый институт, имея возможность отслеживать через свое приложение поисковую активность клиента, может оперативно готовить индивидуальное предложение, рассчитанное на конкретного клиента или узкую группу клиентов. При этом предложение может быть озвучено через любой канал взаимодействия. После очной консультации клиента в отделении банковские сотрудники могут приготовить соответствующий продукт и распространить его путем обзвона через колл-центры или через push-уведомления в приложениях.

<sup>9</sup> UnionPay. Официальный сайт. URL: <https://www.unionpayintl.com/ru/> (дата обращения: 18.04.2022).

Банкам нужна корректная и актуальная информация о своих существующих и потенциальных клиентах, поэтому им следует использовать максимальное количество полезной информации из профилей в социальных сетях и анализировать, какие банковские продукты можно им предложить.

#### Учет местоположения и действий клиентов

Месторасположение (локацию) любого человека, а тем более клиента, чей телефон банк знает, можно отслеживать посредством триангуляции (поиска и отображения телефона базовыми станциями через системы GPS или BLE<sup>10</sup>). Подобная информация востребована компаниями, которые могут готовить маркетинговые отчеты, ориентируя заказчиков услуг и рекламодателей на конкретную целевую аудиторию, что позволяет более целенаправленно работать с потенциальными клиентами, уже зная их базовые потребности и месторасположение. Представляют интерес любые данные по истории посещения разных сайтов, поисковым запросам, перемещениям, а также любые демографические данные, например семейное положение, состав семьи, наличие и возраст детей, социальный статус. Эта информация, не являясь по российскому законодательству персональными данными и поэтому находящаяся в открытом доступе, активно используется банковскими структурами в маркетинговых действиях [3].

Итак, доступ к виртуальным каналам по сбору и анализу любой информации расширяет возможности банковских структур, поскольку таким образом банки смогут лучше понять потребности своих клиентов, более точно выстроить различные клиентские профили, что даст им конкурентное преимущество и обеспечит коммерческий успех.

Однако есть еще один аспект, который важно учитывать при вовлечении в цифровой банкинг, — информационная безопасность.

### ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВЫХ ИНСТИТУТОВ — КЛЮЧЕВОЙ ЭЛЕМЕНТ DIGITAL BANKING

Переход на концепцию Digital Banking предполагает особую роль цифровых- и интернет-тех-

<sup>10</sup> BLE (*bluetooth low energy*) — Bluetooth с низким энергопотреблением, на основе которого, в частности, построена технология Apple iBeacon. Это способ определения местоположения пользователя с точностью до 10 метров, при этом щадящий батарею устройства.

нологий, что сопровождается значительными информационными и коммерческими рисками. При этом одной из главных проблем является угроза преступлений в киберпространстве.

Самыми серьезными по общему масштабу материальных потерь и морального ущерба признаются киберпреступления, целью которых являются отдельные банковские структуры и финансовый сектор страны в целом. Преступления направлены на счета и информационные системы кредитно-финансовых учреждений, злоумышленники стараются похитить финансовые ресурсы с корреспондентских счетов, в том числе и в системе Банка России.

На всех этапах реализации цифровых банковских операций — от разработки новых программных методик и технических решений до реализации банковских продуктов своим клиентам — руководство кредитных учреждений должно осознавать имеющиеся риски, прежде всего возможные уязвимости систем информационной безопасности. Часть банков задумывается об инвестициях в системы информационной защиты только на первичных этапах разработки новых систем. Однако, полагаем, такой подход нерационален. И наше мнение подтверждается реальными ситуациями, когда преступники уже на первых неделях после запуска проекта находят уязвимости в информационных банковских системах и совершают многомиллионные хищения. Только после этого, убедившись в незащищенности и недоработанности своих защитных механизмов, коммерческие банки вынуждены обращаться к разработчикам, которые, обладая успешным опытом создания надежных защитных систем, смогут обеспечить банкам комплексную постоянную информационную защиту.

В эпоху бурного развития информационных технологий, которые позволяют бизнес-структурам расширять спектр проводимых ими операций, охватывать больше клиентов и, соответственно, получать больше прибыли, вопросы информационной безопасности становятся ключевыми. Именно по тому, сколько внимания банки уделяют построению и совершенствованию систем защиты информации, можно судить о зрелости бизнеса. Серьезность подхода к вопросам раннего определения потенциальных угроз и своевременного реагирования на эти угрозы для банковских информационных систем определяется тем, на каком этапе привлекается служба информацион-



ной безопасности ко всем банковским процессам. Заметим, что в настоящее время современные крупные финансовые структуры уже обладают возможностью успешно решать задачи информационной защиты, используя своих штатных специалистов.

При этом необходимо отметить, что в области информационной безопасности есть две важные категории: угроза (потенциальный риск кибернападения) и атака (непосредственное нападение на информационную систему с целью хищения конфиденциальной информации и/или денежных средств). В случае, когда потенциальные угрозы не учитываются, незащищенные информационные системы будут атакованы, что приведет к серьезным, а иногда и катастрофическим финансовым потерям. При этом именно клиент зачастую несет большую часть потерь, поскольку он наименее защищен, хотя и связан с банками через дистанционные системы обслуживания. Поэтому банкам целесообразно начинать с защиты клиента, обеспечив его надежной системой информационной безопасности.

Ситуация с киберпреступлениями против банков и их клиентов остается напряженной, как в России, так и по всему миру. Ассоциация российских региональных банков сообщала, что за IV квартал 2015 г. киберпреступники похитили со счетов банков — участников Ассоциации — сумму, превышающую 1,5 млрд руб. [4]. В 2016 г. в России было зафиксировано не менее 8 крупных кибератак на информационные системы банковских структур. Только своевременные совместные действия сотрудников информационной защиты коммерческих банков и регулятора позволили снизить реальный ущерб с 5 млрд руб. до 300 млн руб.<sup>11</sup> Но кибератаки возможны и на защищенные системы Центрального банка Российской Федерации. В июле 2018 г. киберпреступники с помощью вирусной вредоносной программы сумели несанкционированно получить доступ к автоматизированному рабочему месту клиента Банка России (АРМ КБР) и похитить с корреспондентского счета 58 млн руб., распределив их по пластиковым картам клиентов в 22 крупнейших российских банка. В течение нескольких часов большая часть средств

была обналичена [5]. Массовый переход банков на онлайн-обслуживание клиентов в 2020–2022 гг., вызванный распространением пандемии коронавируса, значительно ухудшил ситуацию в области виртуальных преступлений против банковских структур. По экспертной оценке специалистов Сбера, потери банковской системы России от кибератак составляют порядка 600 млрд руб. в год<sup>12</sup>.

Киберпреступники продолжают совершенствовать свои знания и умения, постепенно приобретая специализацию в узких областях. Так, особой востребованностью в последнее время стали специалисты, готовые просканировать организационную и технологическую составляющую информационной системы банков и обнаружить все потенциальные уязвимости. На основе полученных данных киберпреступники готовы предоставить свои рекомендации по оптимальному взлому банковских систем и маскировке преступных действий. Подобные «экспертные» рекомендации уже стали предметом активной купли-продажи, в том числе, на уровне государств, не говоря уже о преступных сообществах [6].

Скачкообразно увеличилось количество преступлений по похищению денежных средств со счетов клиентов банков с помощью применения социальной инженерии и методов нейро-лингвистического программирования, когда преступники, получив часть персональных данных клиента банка путем общения по телефону, вынуждают его сообщить данные карты, получают доступ к счету или личному кабинету клиента и дистанционно похищают денежные средства с банковских счетов. Однако, учитывая общий масштаб хищений, за год достигший сотни миллиардов рублей, банки объединяют усилия по созданию систем противодействия подобным преступлениям (включая активные оперативные и профилактические мероприятия с подключением правоохранительных органов), формируют специальные подразделения и создают подробные инструкции для клиентов [7].

Несмотря на активную работу банковских структур совместно с Банком России в области противодействия виртуальным преступлениям, ситуация в области информационной банковской безопасности остается не только опасной, но и приближается к критическому уровню. В на-

<sup>11</sup> Аринтег (ARinteg). Актуальные решения по обеспечению информационной безопасности. 2016. Материалы X международной конференции АРБ. «Банковские карты: практика и трансформация» 14–15.04.2016 г. М.; 2016.

<sup>12</sup> Сбербанк. Официальный сайт. URL: [https://www.sberbank.com/common/img/uploaded/files/info/ir\\_presentation\\_march\\_2019\\_rus.pdf](https://www.sberbank.com/common/img/uploaded/files/info/ir_presentation_march_2019_rus.pdf) (дата обращения: 18.01.2022).

стоящее время киберпреступники, объединенные в организованные группы, направляют свои усилия на атаки банковской системы, особенно — информационной системы Банка России. Угрозам подвергаются уже не только клиентские счета, но и средства на корреспондентских банковских счетах. А это уже системная угроза!

Дополнительную угрозу представляют бывшие сотрудники банков, которые имели доступ к внутренней конфиденциальной информации, касающейся механизмов и процедур информационной безопасности, методов хранения и вывода денежных средств. Подобных специалистов становится больше в связи с планомерной работой Центрального банка Российской Федерации по оздоровлению банковской системы, в результате много банков лишается своих лицензий, и, соответственно, сотрудники этих банков — работы. Очевидно, что, зная информацию о внутренней банковской ИТ-инфраструктуре, злоумышленники становятся обладателями фактически безграничных возможностей: здесь и центральная АБС — Автоматическая банковская система банка (хранящая все данные о счетах клиентов), и автоматизированное рабочее место клиента Банка России — АРМ КБР (позволяющее переводить финансовые ресурсы с одного корсчета на другой), и интерфейс системы SWIFT (для взаимодействия с иностранными банками).

Одним из самых уязвимых мест остается именно АРМ КБР, поскольку программное обеспечение для всех АРМ КБР одинаково, и работа с ним строго регламентирована Банком России. Это и привлекает киберпреступников, так как они изучают системы, выбирают банк с наименее защищенной, подбирают методологию взлома, атакуют этот банк, получают доступ к средствам на корреспондентском счете и переводят их в несколько других банков. Потом, возможно, злоумышленники «расщепляют» средства на меньшие суммы, распределяют по карточным счетам розничных клиентов и обналичивают. Это одна из возможных схем кибератаки преступников с момента взлома информационной системы до получения денежных средств в свое распоряжение. В рамках противодействия киберпреступлениям против банков Центральный банк Российской Федерации разработал систему мер по безопасной работе с системой АРМ КБР [8].

В целом, можно посоветовать банкам три основных практических шага для защиты данного

слабого звена. Во-первых, выделить АРБ КБР в отдельный сетевой сегмент и максимально ограничить к нему доступ на сетевом уровне. Во-вторых, вывести хост их корпоративного домена (это крайне важно, так как безопасность домена поддерживать очень непросто). В-третьих, максимально ограничить происходящее внутри операционной системы у хоста АРМ КБР: только разрешенное программное обеспечение и только установленные заранее авторизованные процессы.

Полагаем, что ужесточение контроля со стороны регулятора, а также широкое информирование ИТ-специалистов банков о возможностях противодействия, привлечение правоохранительных органов и клиентов банков, включая розничных, к профилактическим мероприятиям по борьбе с киберпреступлениями может снизить их количество и интенсивность кибератак на финансовые структуры. Однако, исследуя текущую ситуацию в области обеспечения информационной безопасности в российском банковском секторе, есть возможность предположить, что общие усилия могут в ближайшее время привести к улучшению именно защиты АРМ КБР.

Но у киберпреступников останется немало возможностей реализовывать свои намерения и в других системах. По-прежнему много уязвимостей в системе международных межбанковских переводов SWIFT. Кроме того, злоумышленники, получив доступ к автоматической банковской системе (АБС), смогут фальсифицировать данные о платежах, затем направив их в АРМ КБР. При отсутствии дополнительных систем защиты, специальных защитных экранов между этими системами, и с учетом того, что АРМ КБР работает в автоматическом режиме, может снова возникнуть системная угроза.

Кроме того, надо иметь в виду, что внутри-российские и международные информационные каналы взаимосвязаны и взаимозависимы, поэтому уязвимость, например, в одной из систем переводов и платежей может негативно отразиться на информационной системе банка или несанкционированный доступ к банкомату одного банка может привести к незаконным списаниям со счетов клиентов в другом банке. Разнообразие имеющегося арсенала виртуальных атак снижает целесообразность противодействия им на последнем этапе.

Особенно обострилась ситуация с кибератаками в конце февраля 2022 г. Тогда все автоматические



системы российских государственных структур, АБС российских банков и сайты системно значимых компаний подверглись кибератакам в рамках развернутой против России кибервойны (гибридной войны) со стороны высокопрофессиональных и хорошо организованных хакерских групп по заказу США и ряда стран ЕС в ответ на начатую 24 февраля 2022 г. специальную военную операцию России на Украине. Международные хакеры, имеющие задачу нанести любой ущерб информационным системам российских финансовых и нефинансовых структур, зачастую направляют свои усилия по дестабилизации именно российского банковского сектора, понимая системную значимость банковской системы для общей экономической ситуации в России.

Именно сейчас в архисложных условиях многократно усиливается опасность киберугроз, возрастают риски и цена любой недоработки по построению системы противодействия преступлениям в киберпространстве. Поэтому в данных обстоятельствах так важно системно подходить к решению проблемы развития и совершенствования комплексных мероприятий по противодействию виртуальным киберпреступлениям — от контроля физического доступа к компьютерному и банковскому оборудованию до систем виртуальной защиты. Общее мнение экспертов таково, что невозможно построить абсолютно безопасную систему, исключаящую любое несанкционированное действие [9]. Но задача состоит в создании такой защиты, которую преступникам преодолеть технически сложно, дорого, долго, и, следовательно, это лишено для них практического смысла.

## ВЫВОДЫ

Цифровой банкинг, как в мире, так и в России, находится в начале развития, банки в этом бизнесе не обладают еще достаточным опытом, им, прежде всего, стоит начать с перестройки менталитета, вначале — у руководства, затем — у рядовых сотрудников. Финансовым институтам следует на данной стадии действовать достаточно оперативно, но вдумчиво, стараться перенять все лучшее у уже активных участников цифрового пространства. При внедрении новых технологий рекомендуется учитывать законодательные ограничения. При привлечении клиентов и отслеживании их потребностей полагаем важным найти «золотую середину» между навязчивостью и настойчивостью.

Перестройка системы банковского обслуживания, которая предусматривает переход на Digital Banking, предполагает, что для клиента банковский сервис станет удобнее, комфортнее, доступнее и безопаснее.

Финансовые институты по ходу включения в процесс дигитализации своего бизнеса должны становиться ближе к клиенту. Их основные функции изменятся: из кредитора и коллектора долгов банки трансформируются в финансового консультанта и помощника [10]. Такие метаморфозы повысят конкурентоспособность банковского сектора, а также привлекут к нему новых клиентов, в том числе из нового поколения Homo informaticus.

При этом полагаем, что без построения надежной и многоконтурной системы информационной безопасности банк не сможет защитить свои финансовые ресурсы и средства клиентов от киберпреступлений в цифровом пространстве. Кроме того, противодействие криминальным кибератакам должно происходить в рамках эффективного взаимодействия между государственными органами, финансовыми институтами и их клиентами разных категорий, включая розничных. Именно координация совместных и однонаправленных усилий всех перечисленных участников, построенная на принципах равного доступа к чувствительной информации, обеспечит защиту и будет способствовать развитию отечественного финансового сектора, включая региональные сегменты, что закрепит возможности совершения надежных и быстрых транзакций в цифровом формате.

Цифровые технологии не только принесли комфорт клиентам финансовых институтов, но и изменили уклад жизни большинства из них, их потребности и менталитет. Исходя из этого, банки из традиционных финансовых институтов превращаются в структуры, создающие новые цифровые бизнес-системы по оказанию услуг, лишь формально связанных с банковским ядром холдинга. Пример крупнейшего российского банка, оставившего от предыдущего названия лишь часть — «Сбер» и убравшего слово «банк», очень показателен и определяет лидирующее направление, в котором будут трансформироваться все банковские институты, включая региональные. По мере развития возникнут новые проблемы, откроются новые уязвимости, но это — естественный процесс эволюции, который будет определять развитие российского финансового сектора на ближайшие десятилетия.

Пока готовилась данная публикация, произошли события, которые кардинальным образом повлияли на прочность всю экономическую структуру Российской Федерации, в частности костяк экономики — финансовый сектор. Но, несмотря на планомерно вводимые США, ЕС и другими странами беспрецедентные экономические, финансовые и политические санкции, в также массовый уход ряда значимых и ведущих западных компаний с российского рынка, отечественный банковский сектор устоял, понеся относительно небольшие потери, показав наличие серьезного иммунитета к недружественным действиям внешних сил, механизмов снижения и нейтрализации внешних шоков, гибкости в принятии быстрых решений, а также продемонстрировав координацию совместных усилий с государственными надзорными

органами. По прогнозам известных экспертов, российская финансовая система будет вынуждена существовать в условиях западных санкций еще продолжительное время [11]. Поэтому необходимо использовать данный сложный период для развития своих собственных цифровых технологий (независимых от западных рынков платежных и расчетных систем), укрепления национальной валюты, продвижения цифрового рубля, обучения и повышения квалификации специалистов по цифровым банковским технологиям и информационной безопасности. Именно такой комплекс мер позволит поступательно развивать цифровые банковские услуги в России, обеспечив независимость и надежность отечественной банковской системе, несмотря на имеющиеся внешние ограничения и санкции.

### СПИСОК ИСТОЧНИКОВ

1. Реймер Д. Личный веб-сайт. URL: <http://denreymer.com/digital-banking-branch> (дата обращения: 10.12.2021).
2. Nabendu M. Global digital banking. LinkedIn. URL: <https://www.linkedin.com/pulse/future-digital-banking-2015-2016-nabendu-misra> (дата обращения: 06.12.2021).
3. Колезнева А. В. Технологии биометрической идентификации в банковских системах. *ПРО-Экономика*. 2018;(3):6.
4. Аитов Т. Выступление на панельной дискуссии “Мобильная безопасность и управление безопасности ИТ-инфраструктуры. Мат. Инфофорума 2016 (Москва, 4–5 февраля 2016 г.). М.; 2016:12–16.
5. Кондрашин М. Кибератаки на банки: тренды, уязвимости и роль регулятора. Сайт журнала «ПЛИАС». 27.07. 2018. URL: <https://plusworld.ru/professionals/kiberataki-na-banki-trendy-uyazvimosti-i-rol-regulyatora/> (дата обращения: 15.02.2022).
6. Петрова Е. В., Кузнецова Т. Е. Цифровизация банковской системы: цифровая трансформация среды и бизнес процессов. *Финансовый журнал*. 2020;12(3):91–101. DOI: 10.31107/2075-1990-2020-3-91-101
7. Пашковская И. В. Тенденции развития цифрового банкинга. *Актуальные проблемы и перспективы развития экономики: российский и зарубежный опыт*. 2019;(3):46–52.
8. Якубенко В. В. Финансовые технологии в обеспечении эффективности банковской деятельности. *Теория и практика общественного развития*. 2019;(1):72–76. URL: 10.24158/tipor.2019.1.13
9. Васильев И. И. Принципы организации кредитных организаций в условиях цифровых технологий. *Russian Economic Bulletin*. 2019;2(5):218–221.
10. Батаев А. В. Оценка мирового рынка облачных технологий в финансовой сфере. *Вектор экономики*. 2019;(6):91.
11. Ачаповская М. Цифровизация экономики как драйвер инновационного развития. *Банкаўскі веснік*. 2019;(3):52–58.

### REFERENCES

1. Reymer D. Personal website. URL: <http://denreymer.com/digital-banking-branch> (accessed on 10.12.2021). (In Russ.).
2. Nabendu M. Global digital banking. LinkedIn. URL: <https://www.linkedin.com/pulse/future-digital-banking-2015-2016-nabendu-misra> (accessed on 06.12.2021).
3. Kolezneva A. V. Application of biometric-based identification technologies in banking systems. *PRO-Ekonomika = PRO-Economics*. 2018;(3):6. (In Russ.).



4. Aitov T. Presentation at the panel discussion “Mobile security and IT infrastructure of security management”. In: Infoforum 2016 materials (Moscow, February 4–5, 2016). Moscow; 2016:12–16. (In Russ.).
5. Kondrashin M. Cyber attacks on banks: Trends, vulnerabilities and the role of the regulator. Website of the PLUS Magazine. July 27, 2018. URL: <https://plusworld.ru/professionals/kiberataki-na-banki-trendy-uyazvimosti-i-rol-regulyatora/> (accessed on 15.02.2022). (In Russ.).
6. Petrova E. V., Kuznetsova T. E. Digitalization in the banking industry: Digital transformation of the environment and business processes. *Finansovyi zhurnal = Financial Journal*. 2020;12(3):91–101. (In Russ.). DOI: 10.31107/2075–1990–2020–3–91–101
7. Pashkovskaya I. V. Trends in the development of digital banking. *Aktual'nye problemy i perspektivy razvitiya ekonomiki: rossiiskii i zarubezhnyi opyt*. 2019;(3):46–52. (In Russ.).
8. Yakubenko V. V. Financial technology used to provide banking efficiency. *Teoriya i praktika obshchestvennogo razvitiya = Theory and Practice of Social Development*. 2019;(1):72–76. (In Russ.). URL: 10.24158/tipor.2019.1.13
9. Vasilyev I. I. Principles of organization of credit institutions in the digital technological environment. *Russian Economic Bulletin*. 2019;2(5):218–221. (In Russ.).
10. Bataev A. V. Evaluation of the world market of cloud technologies in the financial sphere. *Vektor ekonomiki*. 2019;(6):91. (In Russ.).
11. Achapovskaya M. Digitalization of the economy as a driver of innovative development. *Bankauski vesnik = Bank Bulletin Journal*. 2019;(3):52–58. (In Russ.).

## ИНФОРМАЦИЯ ОБ АВТОРЕ / ABOUT THE AUTHOR



**Ильяс Абдулбарович Зарипов** — кандидат экономических наук, доцент ФГБОУ ВО «РЭУ им. Г.В. Плеханова», Москва, Россия

**Ilyas A. Zaripov** — Cand. Sci. (Econ.), Assistant Professor, Plekhanov Russian University for Economics, Moscow, Russia

[iliyas888@yandex.ru](mailto:iliyas888@yandex.ru)

<https://orcid.org/0000-0002-0261-6592>

*Конфликт интересов: автор заявляет об отсутствии конфликта интересов.*

*Conflicts of Interest Statement: The author has no conflicts of interest to declare.*

*Статья поступила 20.01.2022; после рецензирования 10.02.2022; принята к публикации 12.03.2022.*

*Автор прочитал и одобрил окончательный вариант рукописи.*

*The article was received on 20.01.2022; revised on 10.02.2022 and accepted for publication on 12.03.2022.*

*The author read and approved the final version of the manuscript.*