реальной действительности лишь в том случае, когда будут учтены расчеты, подтвержденные обоснованными возможностями, опирающимися на достигнутые технико-экономические показатели с учетом тенденций их роста. Изменения этих тенденций сразу отразятся на прогнозных результатах. С учетом вышесказанного прогнозирование производительности труда – это процесс непрерывного наблюдения за развитием факторов роста производства и своевременного внесения каких-либо изменений в результаты прогноза.

Литература

1.Авкопашвили, П.Т. Увеличение производительности предприятия как причинный фактор диверсифицирования продуктов / П.Т. Авкопашвили // В сборнике: Современные проблемы и перспективные направления инновационного развития науки сборник статей по итогам Международной научно-практической конференции. – 2017. – С. 9–11.

2.Деружинский, Г.В. Рынок труда инвестиционно-привлекательного региона: особенности его функционирования в современных посткризисных условиях / Г.В. Деружинский, Т.Г. Строителева // Экономика устойчивого развития. – 2012. – № 1 (9). – С. 79–83.

3.Молочников, Н.Р. Трудовой потенциал в системе управления предприятием: проблемы и практика реализации в условиях инновационной экономики / Н.Р. Молочников Н.Р., Е.Е. Пономаренко Е.Е. // В сборнике: Россия: тенденции и перспективы развития Ежегодник. Институт научной информации по общественным наукам Российской академии наук; Ответственный редактор В.И. Герасимов. – 2018. – С. 305–307.

4.Титова, О.В. Современные подходы к планированию производительности труда на промышленных предприятиях / О.В. Титова // Финансовая экономика. – 2018. – № 7. – С. 351–353.

УДК 336.71

А.Р. Базилевич, Д.В. Зиринова, И.В. Рындина, Е.И. Сорокина

ОСНОВНЫЕ ПРОБЛЕМЫ РАЗВИТИЯ ИНТЕРНЕТ-БАНКИНГА В ДЕЯТЕЛЬНОСТИ КОММЕРЧЕСКИХ БАНКОВ

A.R. Bazilevich, D.V. Zirinova, I.V. Ryndina, E.I. Sorokina

BASIC PROBLEMS OF DEVELOPMENT OF INTERNET BANKING ACTIVITIES OF COMMERCIAL BANKS

Ключевые слова: Интернет-банкинг, дистанционное обслуживание, интерфейс, информационные технологии, фрод-мониторинг, дистанционные каналы, финансовый супермаркет, банковское обслуживание.

Keywords: Internet banking, remote service, interface, information technology, fraud monitoring, remote channels, financial supermarket, banking.

Интернет-банкинг стремительно входит в банковский сектор и из новой услуги трансформируется в обыденную. Банки преподносят наличие развитой системы дистанционного обслуживания в качестве конкурентного преимущества. Однако, как считает ряд авторов, рост количества систем банковского обслуживания существенно опережает качество, поэтому функционирование дистанционных каналов обслуживания сопряжено с существованием ряда проблем [3,5].

Еще в начале XXI века банковские транзакции осуществлялись в основном за счет физического взаимодействия субъектов финансового сектора и пользователями [4]. В настоящее время в Российской Федерации отсутствует четко сформулированная законодательная база, регулирующая деятельность банков, предоставляющих услуги клиентам дистанционным способом. Отсутствует специально разработанное законодательство. Одним из основных факторов, останавливающих развитие информационных технологий в российском банковском секторе является недостаточная правовая база использования электронных аналогов отчетных и платежных документов, использованных при заключении торговых сделок, подписании договоров и соглашений. Документы с живой печатью банка являются приоритетными при предоставлении необходимой стороне сделки. К тому же сделки с использованием электронных каналов связаны с риском и для продавцов товаров и услуг, и для банков, выступающих в качестве продавцов банковских продуктов и услуг, и для покупателей по причине слабой законодательной базы и минимальной судебной практики в сфере электронного документооборота. Пострадавшей стороне, будет проблематично доказать правоту, если договор заключен в виртуальном пространстве. По причине неразвитости законодательной базы пользователи данных систем защищены не законом. Отечественные системы дистанционного банковского обслуживания довольно активно развиваются. Однако количество систем значительно опережает их качество. То есть запускаемые сервисы являются недоработанными, в них присутствует минимальный набор функций, сервисы являются недостаточно защищенными. В таких случаях иногда проще и безопаснее приехать в отделение банка и совершить необходимую операцию. На текущем этапе, по мнению Юсуповой О.А. «первоочередная роль в составе задач электронного бизнеса банка принадлежит маркетингу – привлечение клиентов через сеть, допродажи через интернет-банк и мобильные приложения, обслуживание и взаимодействие с клиентами через мессенджеры, e-mail, sms, социальные сети» [7]. Наиболее явной проблемой, сдерживающей развитие удаленных сервисов обслуживания, является информационная безопасность. Задача повышения уровня безопасности является приоритетной для большинства банков. Банки постоянно занимаются совершенствованием каналов предоставления дистанционного банковского обслуживания, однако злоумышленники работают над взломом данных систем. Поэтому процесс не останавливается, экономические преступления совершаются. Причем совершаются не только мошенниками-одиночками, но и группами лиц, в том числе международными.

Стандартная система защиты информации в системах дистанционного банковского обслуживания обычно представляет собой средства отбора подозрительных операций, встроенные в дистанционный канал. Система основана на контроле платежных реквизитов. В настоящее время сервисы снабжаются средствами записи с функцией контроля информации об устройствах, с которых был осуществлен платеж. Помимо этого в системе присутствуют алго-

ритмы, осуществляющие автоматическую проверку подозрительных операций, основанных на ранее обнаруженных случаях фрода. Стандартные механизмы защиты сервисов: использование криптографического ключа, усиленная аутентификация не избавляет от осуществления мошеннических операций, но способствует их уменьшению.

Развитие каналов дистанционного банковского обслуживания является удобным не только для клиентов, но и для мошенников. В дистанционной среде мошенники получают возможность перемещать денежные средства, полученные преступным путем, при этом имеют минимальный иск обнаружения себя. Тем более что не все клиенты контролируют остатки на своих счетах, операции по счетам, оставляют в свободном доступе сеансовые ключи для входа в дистанционные каналы. Многие банки используют в своей деятельности системы фрод-мониторинга, которые защищаются на основе бизнес-логики событий. Например, система может быть настроена таким образом, что при перечислении крупных сумм с карты одного банка на карту другого банка, при наступлении определенных событий, произойдет блокировка карты, с которой был осуществлен перевод. Безопасность системы зависит и от банка, и от клиента. Банк несет ответственность за комплексное применение мер безопасности к системе в целом, а клиент несет ответственность за доступ к системе с его рабочего места. Банк, в свою очередь, разрабатывает системы таким образом, чтобы утечка информации сводилась к минимуму, они создают продукты призванные защитить ключи электронной подписи клиента и саму процедуру подписания платежных документов в программе. Злоумышленники работают в двух направлениях. С одной стороны, если их целью является поиск небольших сумм денежных средств, то они идут по пути наименьшего сопротивления: занимаются поиском ключей от конкретного личного кабинета, ведь зачастую эти данные не скрываются клиентом: хранятся либо на персональном компьютере, либо записаны в личных данных, либо сохранены в компьютере, который находится в свободном доступе. По сути, клиент самостоятельно провоцирует злоумышленников на совершение мошеннических действий.

С другой стороны, если целью мошенников является похищение крупных денежных сумм, то объектом будет выступать не конкретный клиент, а сервер. По результатам исследования, проведенного в 2016 г. компанией Intercede, 58% потребителей не скрывают логины и пароли от личных кабинетов мобильных и интернет приложений. Информация распространяется среди знакомых, родственников, друзей. То есть клиенты самостоятельно подвергают риску свои персональные данные. В настоящее время большинство людей используют множество паролей от личных кабинетов, почты, сервисов. По причине их многообразия потребители используют автозапоминание, которое присутствует в программе. Это чревато тем, что при попадании гаджета в руки злоумышленников все личные данные будут раскрыты. Однако защита постепенно повышается. Это происходит за счет устройств, направленных на хранение ключей электронной цифровой подписи. С устройств подпись направляется в банк посредством доверенных каналов. Однако по мере совершенствования серверов, мошенники начинают искать В настоящее время специалисты в области ИТ и информационной безопасности работают над созданием максимально безопасных устройств и сервисов, чтобы свести к минимуму риски работы с удаленных каналах обслуживания.

Атаки на системы дистанционного банковского обслуживания с каждым годом растут, в последнее время специалисты занимаются решением проблемы несанкционированных платежей, которые злоумышленники совершают двумя способами: либо незаконно овладев ключами пользователя, либо проникнув в систему и подменив реквизиты платежного поручения. Однако инфраструктура системы дистанционного банковского обслуживания также нуждается в дополнительной защите, ведь если web-интерфейс системы «клиент-банк» разработан без учета факторов безопасного программирования, то это будет привлекательно для мошенников. Своевременно установленные обновления, рекомендованные разработчиком услуг, способствуют повышению безопасности системы. Довольно часто уязвимости находятся в операционной системе, по этой причине кредитные организации переносят контролирование и подписание платежных документов в замкнутую внутреннюю среду на внешнем устройстве, в котором подмена документов невозможна. Многие банки переходят на технологии двухфакторной аутентификации, при которой ключ хранится на eToken или на смарт-карте, то есть является неизвлекаемым.

Банки заинтересованы в обеспечении безопасности счетов своих клиентов, потому как от этого зависит репутация банка, клиентопоток. Согласно Федеральному закону № 161-ФЗ «О национальной платежной системе» банки, осуществляющие операции обязаны возместить клиенту убыток по операции, осуществленной без его согласия, в случае, если докажут, что клиент нарушил порядок использования средства электронного платежа, что повлекло совершение операции без ведома клиента [1]. Одним из методов мошенничества является фишинг, которые заключается в том, что мошенники овладевают информацией, касательно банковской карты пользователя, используя при этом методы социальной инженерии: обзвон, рассылка смс-сообщений от имени банка. Либо создают интернет страницы, переходя на которую пользователи самостоятельно оставляют персональные данные, не подозревая о том, что страница является мошеннической. В последнее время все более актуальной является проблема хищения ключей электронных цифровых подписей, которые предоставляют возможности к списанию средств со счетов клиентов злоумышленниками, по этой причине разрабатываются различные устройства, сводящие к минимуму утечку информации из системы, например SafeTouch, предоставляемый ПАО «Сбербанк». Современный мир виртуальных технологий дает возможность компаниям, занимающимся электронной коммерцией предоставлять услуги вне зависимости от географии присутствия, у компании не возникает необходимость иметь собственное территориальное представительство в стране оказания услуг и быть зарегистрированными в этом государстве.

По причине того, что операторы, оказывающие электронные банковские услуг могут быть частным центром обработки-хранения информации и не являться кредитными организациями, следовательно, информация по электронным кошелькам пользователей системы не подпадает под термин «банковская тайна». Согласно ст. 26 Федерального закона «О банках и банковской деятельности» под банковской тайной понимается информация об операциях, о счетах и вкладах клиентов и корреспондентов, которую банк не может передавать третьим лицам, за исключением случаев, предусмотренных законом, т.е. это юридический принцип в законодательстве, в соответствии с которым банк в лице доверенных лиц не имеет права разглашать сведения, полученные в ходе проведения аудита либо другого взаимодействия, в том числе сведения, полученные в ходе профессиональной деятельности сотрудников.

Информация может относиться к коммерческой тайне (обладатель коммерческой тайны самостоятельно определяет, какая информация подпадает под эту категорию), в отличие от банковской, которая регламентирована законом. А соответственно и ответственность лиц за разглашение информации о владельцах, операциях и счетах существенно отличается. Ярким примером являются казино, которые перенесли работу в электронное пространство и в настоящее время используют электронные банковские системы и пластиковые карты для осуществления операций с денежными средствами. Помимо выше перечисленных проблем существует проблема окупаемости. Внедрение и развитие электронных систем влекут неизбежные финансовые затраты на разработку технологий, приобретение оборудования, программного обеспечения, средств защиты информации, а также внутреннюю перестройку организационных вопросов в работе банка. Окупаемость нововведений происходит не мгновенно. Недостаточная грамотность населения и недоступность восприятия интерфейса широкими слоями населения. Восприятие технологий пользователями разнится, поэтому интерфейс должен быть максимально простым и удобным, для расширения масштаба применения, чтобы пользоваться услугой могли разные категории граждан: и молодежь и пенсионеры.

К тому же система должна работать бесперебойно. Технические сбои, профилактические работы, неактуальная информация способны вызывать недоверие со стороны клиентов. Существующие в настоящее время проблемы предоставления услуг через дистанционные каналы обслуживания определяют дальнейшее развитие системы. Риски защиты информации, недоверие со стороны клиентов, тормозят дальнейшее совершенствование системы дистанционного банковского обслуживания. Необходимо провести совершенствование системы в Российской Федерации для улучшения его качества, с целью защиты данных и привлечения новых клиентов. Еще два-три года назад банки фокусировались на развитии интернет-банкинга, потому как большинство клиентов при управлении финансами использовали именно этот сервис. За последний год ситуация изменилась: аудитория интернет-банка перестала расти, а мобильного банкинга, наоборот, с каждым годом увеличивается на 30-40%. Отразим проблемы развития электронных банковских услуг на рис. 1.

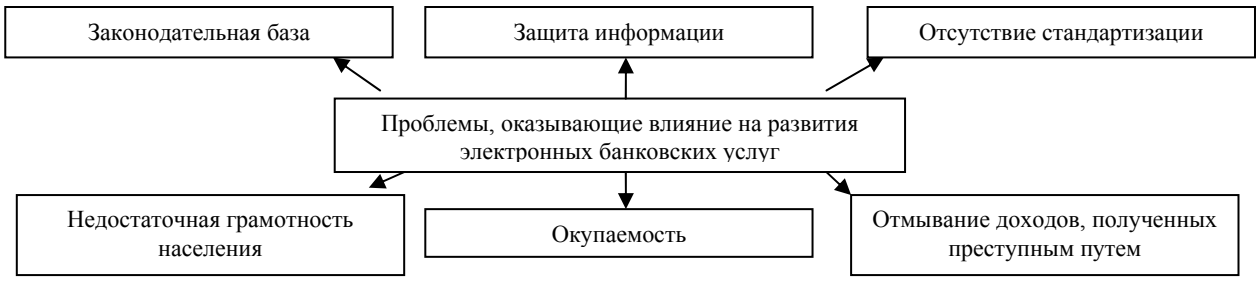

Рис. 1. Основные проблемы, оказывающие влияние на развитие электронных банковских услуг

Говоря о перспективах развития дистанционного банковского обслуживания, следует отметить, что на сегодняшний день одним их главных трендов является омниканальность. То есть все удаленные каналы должны присутствовать в одном месте, для того, чтобы клиент, начав серию операций, довел её до конца. Однако интегрированы все услуги должны быть в одной среде банка. Банки должны предоставлять комплекс услуг, стремиться к созданию финансового супермаркета. Важнейшим аспектом в сфере дистанционного банковского обслуживания является реализация банковских продуктов. Например, в интернет – банке клиент имеет возможность оставить заявку на кредит: ипотечный автокредит или потребительский. Однако у клиента остается необходимость посетить офис банка для завершения операции. В настоящее время набирает обороты концепция digital banking (цифровой банкинг или диджитализация). Банки внедряются в жизнь потребителей через мобильные устройства, интернет, социальные сети и т.д.

В настоящее время банки перестали оказывать исключительно исторически сложившиеся банковские функции. Наблюдается формирование финансовых супермаркетов. Под финансовым супермаркетом, по мнению И.Е. Смирнова, понимают подразделение, которое имеет возможность предложить полный спектр финансовых услуг, в том числе страховых, инвестиционных, консультационных [6]. Основная задача финансового супермаркета состоит в предоставлении максимального количества сопутствующих услуг собранных в одном месте, что, безусловно, является удобным для клиента в плане экономии времени и комфорта совершения операций. Большинство кредитных организаций активно развивается в данном направлении. Уже сейчас на сайтах многих банков предоставляются услуги по возврату налоговых вычетов, услуги по поиску и подбору туров для путешествий, поиску и покупке авиа и ЖД билетов, услуги страхования, а также возврату НДС с покупок за границей. Коммерческие банки ведут активную политику расширения области присутствия через сервисы дистанционного обслуживания. Выпускаются пластиковые карты через сайты банков, быстрыми темпами внедряются сервисы по доставке пластиковых карт до конечного пользователя, минуя офисы кредитных организаций. Например, в 2016 г. банк ПАО «Сбербанк» открыл собственную инновационную лабораторию «Сбербанк Цифровые технологии». В ней будет выстроен полный цикл разработки продуктов, от этапов исследования пользовательских интерфейсов, разработки программного обеспечения до внедрения и продвижения готовых продуктов.

Каждый развивающийся современный банк стремится развивать дистанционные сервисы обслуживания и привлекать всё больше пользователей. Создав, собственную лабораторию по разработке банковских продуктов и услуг ПАО «Сбербанк» мгновенно внедряет инновации в свою деятельность, постоянно отслеживая новые тенденции в развитии рынка дистанционных банковских продуктов и услуг. Так, вышла новая версия приложения для физических лиц «Сбербанк-Онлайн 3.0», в котором находят отражение самые современные услуги: перевод денежных средств контакту из телефонной книги, перечисление денежных средств переносом одной вкладки на другую и др.

Однако ПАО «Сбербанк» на данный момент предоставляет не полный перечень услуг, нельзя сказать, что он является полноценным финансовым супермаркетом. Помимо этого, все операции: приходные и расходные, осуществляемые через банковский счет, автоматически находят отражение в статьях налоговой декларации. Бухгалтеру необходимо внести незначительные коррективы по операциям, осуществленным наличным способом и декларация готова к отправке в Налоговые органы. Вся отчетность, передаваемая в государственные структуры, а также все документы, проводимые через банковский счет, архивируются и хранятся на серверах банка, доступ к которым имеют владельцы электронных цифровых подписей, данный процесс представлен нами на рис. 2.

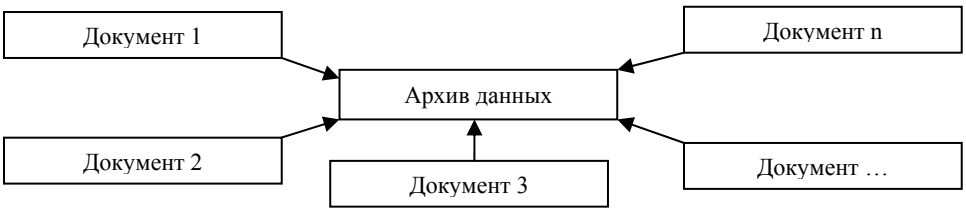

Рис. 2. Архивирование документации

Таким образом, внедрение выше перечисленных функций способствует упрощению ведения бизнеса для индивидуальных предпринимателей и собственников бизнеса, значительно сокращается время на формирование отчетности и других бухгалтерских документов. Затраты на введение данного функционала потребуются на этапе разработки. В последствии затраты окупятся за счет комиссионных сборов банка за предоставление данных услуг.
В результате, предложенные услуги привлекут новых клиентов, готовых оплачивать удобство предложенных сервисов. К тому же услуги предполагают наличие доступа к персональным данным клиентов и хранению информации о них в облачных структурах банка.

Таким образом, клиент заинтересован в долгосрочном сотрудничестве с банком. Сервисы отслеживания информации сводят к минимуму совершение операций, направленных на легализацию доходов, полученных преступным путем. Однако функционирование финансового супермаркета имеет и отрицательные стороны. Комплексное обслуживание клиента требует наличие квалифицированных сотрудников, разбирающихся в множестве продуктов. Такие сотрудники стоят дороже. К тому же необходимо время и деньги для того, чтобы обучить действующих сотрудников тем областям продаж, с которыми раньше они не сталкивались. Движущей силой развития рынка дистанционного банковского обслуживания будет являться конкуренция, которая заставляет кредитные организации развивать сервисы максимально удобные для клиентов, чтобы привлечь дополнительный поток клиентов. В связи с вышесказанным можно отметить, что процесс развития продуктов на базе систем Интернет-банкинга требует тщательной проработки в части расчетов экономической эффективности и окупаемости таких проектов для банка.

Литература

1.Федеральный закон от 27.06.2011 N 161-ФЗ (ред. от 28.11.2018) «О национальной платежной системе».
2.Федерального закона от 02.12.1990 N 395-1 (ред. от 26.07.2018) «О банках и банковской деятельности».
3.Буркова А.Ю. Дистанционное банковское обслуживание: преимущества и риски // Юридический справочник руководителя. 2015. № 6.
4.Козырь Н.С., Толстов Н.С. Интернет банкинг в РФ: состояние и перспективы развития // Экономика: теория и практика. 2013. № 4. С. 37-44.
5.Попов В.В. Интернет-банкинг. Российский рынок дистанционного банковского обслуживания // Перспективы развития информационных технологий. 2016. № 29. С. 78-82.
6.Смирнов И.Е. Новое в технологиях электронных финансовых услуг // Организация продаж банковских продуктов. 2014, №2.
7.Юсупова О.А. Интернет-банкинг как направление диджитализации банковского бизнеса: состояние, проблемы, перспективы // Финансовая аналитика: проблемы и решения. 2016. № 34. С. 12-25.

УДК 684:65

В.А. Беспалько, Н.В. Вахрушева, К.С. Савина

СОВРЕМЕННЫЕ ПОДХОДЫ К РЕАЛИЗАЦИИ И АНАЛИЗУ ЭФФЕКТИВНОСТИ МАРКЕТИНГОВОЙ СТРАТЕГИИ

V.A. Bespalko, N.V. Vahrusheva, K.S. Savina

MODERN APPROACHES TO IMPLEMENTATION AND ANALYSIS THE EFFECTIVENESS OF MARKETING STRATEGIES

Ключевые слова: торговые сети, индикаторы эффективности, учет деятельности, маркетинговая деятельность, маркетинговая стратегия, анализ эффективности, стратегическое планирование, стратегия инновации.

Keywords: trading networks, performance indicators, activity accounting, marketing activity, marketing strategy, efficiency analysis, strategic planning, innovation strategy.

Стратегическим планированием считается организация и содействие в ведении политики организации, которая направлена на достижение поставленных целей и на поиск возможностей для маркетинга. Разработка стратегического планирования подразумевает его долгосрочность, он состоит из определенных моментов: выдвигается долговременная цель стратегического маркетинга; выдвигается стратегия маркетинга; наблюдаются и вычленяются хозяй-