Владислав ЕРМАКОВ, МКБ: «Наша продуктовая команда достаточно зрелая в отношении вопросов безопасности и бизнес-рисков»

Беседовал: Станислав Комаров

В интервью NBJ Начальник управления развития дистанционного обслуживания МКБ Владислав Ермаков рассказывает о трансформации финансовой платформы кредитной организации, связанных с этим вопросах безопасности, а также о ходе реализации проекта «безбумажный банк» и внедрения PayControl.

NBJ: Владислав, каковы ваши ожидания от 2021 года? Куда движется МКБ в развитии каналов дистанционного банковского обслуживания?

В.ЕРМАКОВ: Вы же знаете – сейчас всё банковское сообщество упорно идёт по пути цифровизации. МКБ идёт в ту же сторону. И потому в 2021 году МКБ будет уже не просто банк, а, так сказать, финансовая платформа с элементами экосистемы.

NBJ: Что вы имеете в виду?

В.ЕРМАКОВ: Мы хотим удовлетворять не только финансовые, но и нефинансовые потребности наших клиентов. Да, мы пока не можем помочь клиенту МКБ забрать ребёнка из садика или сварить борщ. Но если он хочет поехать в отпуск, и ему нужно забронировать отель, купить ж/д или авиабилет – у нас есть сервис «МКБ Travel». Решил человек открыть своё дело и стать предпринимателем – наш сервис поможет подать документы на регистрацию в ФНС. Также уже есть юридические консультации, налоговый сервис. Специально для автовладельцев в ближайшее время запустим автомобильный сервис. Он поможет оплатить штрафы, оформить КАСКО и ОСАГО, записаться на ремонт и заправиться на АЗС. Кроме того, можно будет безопасно в защищенном контуре хранить данные из СТС и ПТС. При этом весь

«золотой стандарт банковских услуг» у нас в мобильном и интернет-банке, естественно, тоже сохранится.

NBJ: Бывает, что во вставшем на путь цифровизации банке идёт настоящая война «айтишников» и «безопасников». Первые стремятся сделать ДБО максимально простым и удобным, вторые – всё максимально обезопасить и тем самым усложнить. У вас те же проблемы?

В.ЕРМАКОВ: У нас вообще нет проблем (смеётся). Если серьёзно – мы прекрасно понимаем границы, в которых должны функционировать digital-сервисы и продукты. И как только у нас появляется идея внедрить новую «функцию», то в первую очередь мы идём к коллегам – «безопасникам».

Например, решили ввести возможность дистанционного подписания документов – и сразу же, ещё на берегу, договариваемся, как будем это делать.

Уже на первом этапе, когда наш специалист анализирует задачу, придумывает какое-то архитектурное и техническое решение, в работу включается специалист по информационной безопасности. Если он даёт «добро» на внедрение – мы передаём в разработку. Если накладывает вето – мы либо переделываем, либо вводим дополнительные механизмы защиты.

NBJ: И на этом взаимодействие заканчивается?

В.ЕРМАКОВ: Конечно, нет. Весь код, который написан по утверждённым требованиям, проходит, во-первых, ряд мероприятий, связанных с его статическим анализом, во-вторых, есть аудит, направленный на выявление проблемных мест. Соответственно, только когда безопасность даёт свою визу, мы выносим функцию «на бой».

Как видите, мы плотно взаимодействуем на всех этапах: первый – бизнес-анализ, второй – системный анализ, третий – разработка и выпуск фичей «на бой».

ЕЩЁ ОДИН ПРИМЕР – ЭТО ВНЕДРЕНИЕ PAYCONTROL. ЭТО РЕШЕНИЕ ДЛЯ ЭЛЕКТРОННОЙ ПОДПИСИ В СМАРТФОНЕ, КОТОРОЕ ПОЗВОЛЯЕТ КЛИЕНТАМ С ВЫСОКИМ УРОВНЕМ БЕЗОПАСНОСТИ И УДОБСТВА ПОДТВЕРЖДАТЬ СВОИ ОПЕРАЦИИ, СОЗДАВАЕМЫЕ В ЛЮБЫХ ЦИФРОВЫХ КАНАЛАХ

NBJ: Уже запущенные бизнес-процессы могут нести определённые риски?

В.ЕРМАКОВ: Департамент безопасности периодически проводит их аудит и выдаёт свои рекомендации. Например, внедрение СКЗИ – средств криптографической защиты информации – снижает риск того, что клиент подпишет кредит или проведёт операцию, а потом заявит, что этого не делал. Мы этим рекомендациям внимательно следуем, потому что business value от этих рисков нам понятен.

Мы и сами можем проявлять инициативу и обращаться в департамент безопасности, чтобы там был проведён аудит предложений о принятии тех или иных рисков.

NBJ: Проиллюстрируйте ваше взаимодействие конкретным примером...

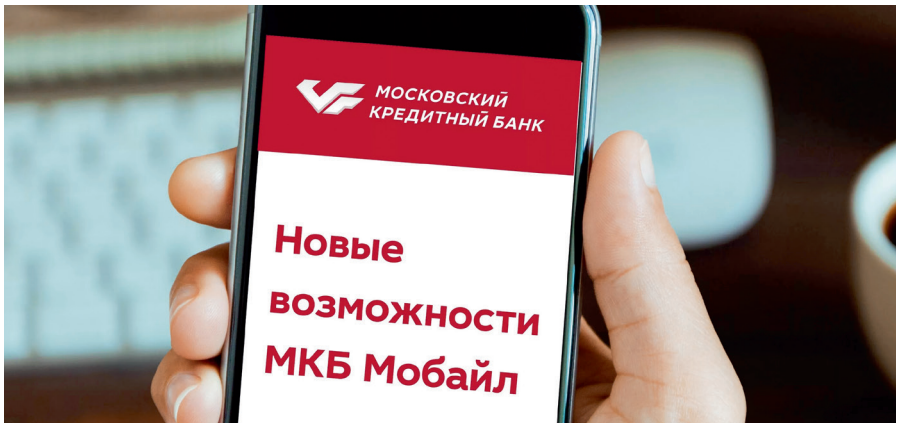
В.ЕРМАКОВ: В ходе пандемии сначала объявил Президент, а потом Банк России дал рекомендации по дистанционной реструктуризации кредитных договоров. Клиенты банков были вынуждены сидеть дома, у многих упали доходы, банкам было предложено пойти навстречу и изменить условия кредитных договоров тем, кто в этом крайне нуждался.

Мы совместно с коллегами из департамента информационной безопасности обсудили риски и в итоге внедрили новые бизнес-процессы по реструктуризации кредитов онлайн. Теперь новые кредитные договоры подписываем не цифровой, а простой электронной подписью.

Ещё один пример – это внедрение PayControl. Это решение для электронной подписи в смартфоне, которое позволяет клиентам с высоким уровнем безопасности и удобства подтверждать свои операции, создаваемые в любых цифровых каналах.

NBJ: А чем электронная подпись лучше привычных кодов из SMS?

В.ЕРМАКОВ: Это более безопасное и в то же время более выгодное решение для банка. Есть технологии



PAYCONTROL МЫ ВНЕДРИЛИ В АПРЕЛЕ 2020 ГОДА ТОЛЬКО НА 20% ОПЕРАЦИЙ, НО ЭТИ 20% ДАЛИ 80% ЭКОНОМИИ ИЗ-ЗА ОТКАЗА ОТ SMS

перехвата SMS злоумышленниками, что делает возможным совершение операции без желания и ведома клиента. В итоге клиент может оспорить операцию.

Кроме того, отправка SMS – это огромные расходы банка. У многих кредитных организаций данная услуга платная, 50–60 руб. в месяц, но эта плата не перекрывает расходов бизнеса. Так что отказ от SMS даёт элементарную экономию, и внедрение PayControl убило сразу двух зайцев: повысило безопасность операций клиентов и сократило расходы банка

NBJ: Кто был инициатором?

В.ЕРМАКОВ: И мы, и безопасники. Мы обратили внимание на это решение, поскольку хотели, в первую очередь, снизить расходы на SMS. И тут наши специалисты по информационной безопасности вышли на нас с инициативой внедрить решение для повышения защиты транзакций клиентов банка.

NBJ: Ваши ожидания от внедрения этого решения оправдались?

В.ЕРМАКОВ: Определённо! Судите сами: PayControl мы внедрили в апреле 2020 года только на 20% операций, но эти 20% дали 80% экономии из-за отказа от SMS. Сейчас внедряем PayControl в остальные бизнес-процессы, но базовый стандартный эффект, правило Парето (эмпирическое правило, названное в честь экономиста и социолога Вильфредо Парето, в наиболее общем виде формулируется как «20% усилий дают 80% результата, а остальные 80% усилий – лишь 20% результата», – прим. Ред.) у нас соблюдено в рамках уже первого запуска.

В итоге, решение и нам, и коллегам из информационной безопасности настолько понравилось, что мы расширяем его использование. У нас есть проект «безбумажный банк», в рамках которого переводим в онлайн подписание банковских документов, где раньше требовалась лишь «живая» подпись на бумаге. Например, договор о комплексном банковском обслуживании. Именно наши «безопасники» предложили делать «безбумажный банк» через PayControl. Сейчас приступили к этапу активной разработки. В скором времени можно будет даже кредитные договоры подписывать в мобильном банке без посещения офиса.

NBJ: А если клиент потом скажет, что не подписывал, откажется платить, и дело дойдет до суда? Вы видите такие риски?

В.ЕРМАКОВ: В случае судебных разбирательств мы можем посредством этого инструмента и технологий доказать, что клиент мобильной подписью подписал именно тот кредитный договор, который сохранился у нас в банке, что там соблюдены именно те сроки и та ставка, которые он увидел на экране. У безбумажного подписания кредитных договоров будет в итоге тройной эффект: мы повышаем эффективность продаж, экономим на «бумажных» и временных издержках, а также усиливаем наши позиции в ходе каких-то спорных моментов.

NBJ: Я правильно понимаю, что к переходу на безбумажные технологии и к внедрению мобильной подписи вас подтолкнула пандемия?

В.ЕРМАКОВ: Не совсем так. С одной стороны, работу над внедрением электронной подписи и «безбумажного банка» мы начали ещё в 2019 году, ещё до ввода ограничительных мер. Этот проект мы реализовывали чётко и последовательно. Но с другой стороны, наши эксперты из департамента безопасности, анализируя риски, связанные с пандемией и переходом на удалённый режим работы и обслуживания клиентов, действительно предрекали повышение активности кибермошенников и массовые атаки на счета клиентов. Чтобы избежать этих проблем мы повысили приоритет некоторых проектов в области безопасности, в том числе и проекта внедрения мобильной подписи. К слову сказать, результаты проекта позволили нам эффективно противостоять атакам финансовых мошенников, особенно с применением методов социальной инженерии. Можно сказать, что к испытаниям на прочность в эпоху пандемии наши цифровые каналы обслуживания были уже готовы.