информационные технологии

«ВТБ станет открытой площадкой»

Рынок превращается в соревнование экосистем. Помимо поиска ответа на этот стратегический вызов весь финансовый сектор вынужден решать и тактическую задачу: как обеспечить бесперебойную работу во время пандемии. О том, как технологически для этого меняется ВТБ, рассказал заместитель президента-председателя правления банка **Вадим Кулик**.

— интервью —

ПРЕДОСТАВЛЕНО ВТБ

— Компании все чаще говорят о бизнесе в будущем времени. О том, что ждет клиентов через 10, 30 или 50 лет — как будто задачи современников уже решены. На что вы нацелены?

— В основе впечатлений клиента о бренде — эмоция в точке контакта: она часто является драйвером решения о взаимодействии с банком. О чем мы в первую очередь думаем? О клиентском опыте — в нем все аспекты взаимоотношений с клиентом: цены и ценности, профессионализм и эмпатия, высокотехнологичность и экологичность. Каков клиентский опыт сейчас? Каким он должен быть через год? Отвечая на эти вопросы, мы проектируем наши действия на среднесрочную перспективу. Этот опыт складывается из нескольких компонентов. Помимо цены, узнаваемости, качества продукта есть удобство, атмосфера, скорость и устойчивость сервиса. Все такие факторы в совокупности и составляют клиентское впечатление.

Есть идеальная картина, к которой стремятся бренды и о которой мечтают клиенты. Сервис 24/7, где каждый вопрос можно решить на 100%, без «бумажек», без погрешностей, за секунду и в один клик. Понятно, что пример экзальтированный — сейчас такого ни у кого нет. Но это горизонт, к которому двигаются все банки. В частности, ВТБ. Возможно ли одномоментно построить такую платформу? Нет. Наступит ли счастье быстро? Нет.

— Чего не хватает для счастья?

— Один из тормозов — требования документальных подтверждений для ряда операций. Конечно, уже есть передовые инструменты, позволяющие клиенту совершать операции в моменте и без неудобных шагов. Появилось предзаполнение полей в разных, в том числе кредитных, процессах, совершенствуется электронная подпись, вводится биометрия, внедряются всевозможные удобства для подтверждения, освобождающие от документов, сканов и фотографий.

В текущем году мы поднялись на первые строчки ведущих рейтингов. Finalta, мировой лидер сравнительной аналитики, признала за ВТБ первое место среди российских банков по числу обновлений. The Banker выбрал ВТБ лучшим трансакционным банком Центральной и Восточной Европы. В рэнкинге фонда «Сколково» и компании VR Bank ВТБ переместился с 15-го на 2-е место по уровню цифровизации банков страны.

До идеала еще далеко, но наши прорывы уже налицо. Сбои еще бывают, но мы работаем над их сокращением, и многое нами уже сделано, в частности в рамках открытой в конце прошлого года программы «Надежность». Это комплекс проектов и инициатив, направленных на обеспечение высокой доступности и непрерывности наших операций. Уже на первом году реализации программы мы идем быстрее плана и вдвое сократили время простоев при увеличении плотности поставок нового функционала на 27%. Большие общебанковские релизы мы сейчас внедряем раз в месяц, а более локальные — практически каждую неделю.

— Как это удалось?

— Во многом за счет работы над инфраструктурой. Мы много занимались переработкой старой архитектуры и запуском новых производственных платформ. Обновили оборудование, перестроили сети. В ноябре у нас запускается новая омниканальная платформа. Кроме того, банк также изменил формат сотрудничества с вендорами — разработчиками и поставщиками ПО. Теперь мы не покупаем готовые решения, а сотрудники компаний-вендоров, работая в составе наших команд, создают новые продукты и сервисы именно для ВТБ.

— Вы сразу восприняли пандемию как вызов или сначала растерялись из-за неожиданного карантина и вынужденной удаленки?

— Растерянность была в первый момент, но мы ее быстро преодолели. Ранее менеджеры ВТБ, включая меня, были противниками удаленки, считали, что из-за отсутствия живого контакта уйдет командный дух и энергия коллектива, пострадает мотивация и дисциплина. Но в начале апреля мы внедрили огромное запланированное обновление разных систем банка, потом темп не сбавляли. Всего за две недели в совершенно новых условиях нам надо было выстроить новую инфраструктуру, поставить огромные комплексные элементы, отрежиссировать виртуальные команды — в релизе в апреле участвовал «оркестр» из 853 человек. Мы справились, у нас почти нет отставаний по проектам. Если посмотреть на наш портфель внедрений, то перенести пришлось всего 1%, и то ненадолго — максимум на два месяца.

— Вы сами придумали, как это сделать, или воспользовались сторонним опытом? Скажем, некоторые крупные компании обратились к удаленке задолго до пандемии.

— Мы во все вникали самостоятельно. Не было времени изучать сторонний опыт и обращаться за помощью. Понятно, что есть известный опыт и свои заготовки, что на бегу мы с кем-то что-то обсуждали, но сделали все сами. Хотя сейчас мне трудно представить, каким образом мы так быстро и эффективно справились. За две недели пришлось, представьте, в десять раз увеличить мощность каналов, найти оборудование для развертывания удаленных мест — а оно оказалось в дефиците. За период пандемии мы почти в десять раз увеличили число удаленных рабочих мест — сейчас их около 35 тыс. Мы видим, что удаленная работа при грамотной организации бывает эффективнее очной. Думаю, мы вряд ли полностью вернемся в старый формат.

— Как вам удается в условиях удаленки удерживать и развивать команду? Ведь сложно работать на бытовом уровне: дети на «каникулах», бабушки в «изоляции», компьютеры «летят» и т. п.

— Это комбинация элементов. Во-первых, всесторонне организуем труд с помощью технологий, всячески поддерживаем. У нас развернут хелп-деск, есть система всевозможных предупреждений, оперативная техподдержка. Во-вторых, мы активно стимулируем рабочий драйв, вовлеченность, создаем возможности для снятия стресса. Мы постоянно общаемся: на связи в Telegram, на протяжении года у нас шел письменный сериал, мы выпускаем видеоблог и комиксы о производственных проблемах. Блог называется «Они тоже человеки», где герои — сотрудники банка — рассказывают о своей обычной жизни вне работы. Я сам часто обращаюсь к коллективу по видео. То есть сотрудники, несмотря на удаленку, вовлечены в единый живой организм.

Все понимают важность каждой секунды. Если раньше у меня было 10–12 встреч в день: комитетов, переговоров, митингов, то сейчас по видео — 20–22. Рабочий график уплотнился вдвое, и качеству это только в плюс.

— Как быть с Agile? На этой методике в последнее время многое строилось. Не нивелирует ли ее удаленка?

— За год мы сильно перестроили процессы. Над созданием и внедрением новых продуктов теперь работают стримы, которые состоят из более чем 1100 команд разработки. Каждая команда идет к своей цели, и каждый участник команды имеет свою зону ответственности, осознает свой вклад в результат проекта, программ, реализацию стратегии цифровой трансформации банка. Удаленка тут ничего не изменила.

— В современном мире конкурировать с сотрудниками начинают роботы. Какие банковские работы может полностью заменить искусственный интеллект? Что в ВТБ здесь внедрено и планируется?

— Искусственный интеллект нужен для удешевления процессов, снижения издержек и комиссий для клиентов, экономии времени. За этот год ВТБ существенно расширил сферу его применения. В частности, мы внедрили во внешнюю эксплуатацию целую серию аналитических платформ, более 70 моделей. Что это сразу дало банку? В той же рознице при тех же рисковых параметрах мы стали выдавать на 18% больше кредитов. Мы много работаем над биометрией, компьютерным зрением и роботизацией, с помощью которой убирается рутинный труд сотрудников. Мы выращиваем одного цифрового сотрудника примерно раз в три недели: один робот — один тип операции. Это хорошая скорость. Банки в большинстве внедряют такого за месяц-два.

— Где у вас трудятся цифровые сотрудники?

— Цифровые сотрудники сделали ВТБ лидером программы кредитования с господдержкой. Кредиты в рамках этой программы надо было выдавать день в день — это требовало срочной автоматизации целого ряда процессов. Мы встроили цифровых сотрудников, которые условно перебивают документы, перекладывают данные системы в систему, и добились нужной скорости.

— Видите ли вы в будущем конкуренцию со стороны финансовых сервисов глобальных цифровых корпораций, например Facebook и Google?

— Тут двояко. Эту конкуренцию принято, с одной стороны, демонизировать, а с другой, наоборот, недооценивать. Главное, держаться посередине, и нам пока это удается. Такой конкуренцией нельзя пренебрегать, но и не надо впадать в панику. Молодежь тяготеет ко всему, что предлагают гиганты. Наверное, сегмент платежей через мессенджеры, поисковики, соцсети все-таки довольно сильно ими узурпируется. Но у молодежи в массе нет высоких рисков, кроме процессов проведения платежей. Психология же человека такова, что с возрастом по мере накопления средств он тяготеет к стабильности, которую давала и продолжит давать банковская лицензия. Это не отменяет того, что нам как финансовому институту нужно быть максимально удобными и максимально дешевыми, чтобы за платежи конкурировать.

— Что вы думаете об экосистеме как экономическом институте? Эффективно ли делать банк частью чего-то гораздо большего?

— Для нас это вызов. В такой стратегии, безусловно, есть выигрышные стороны, но есть и недостаток — это закрытая площадка с единым брендом. Я полагаю, что эффективнее, если у каждого элемента будет свой бренд. ВТБ планирует стать открытой площадкой — встраивать свои приложения в другие компании, открывать для них свои системы.

— Что скажете о законе о защите персональных данных? Еще до пандемии сложилось впечатление, что никаких секретов ни от кого особо нет. Что предпринимает в этой сфере ВТБ?

— Банки жестко следят за исполнением законодательства о банковской тайне и защите персональных данных. Утечка — это трагедия. Тайна — базис банковского института. Без нее он фактически теряет смысл, потому что теряется доверие. Я скажу больше. Законодательство настолько жесткое, что ограничивает возникновение кросс-индустриальных продуктов на основе обезличенных данных, которые на самом деле являются мощным драйвером новой экономики. Полагаю, на уровне закона возможность объединения продуктов разных игроков на стыке индустрий все же вскоре появится — там на практике не требуется никакая персонификация.

— Вы строите какие-то дополнительные системы защиты клиентской информации?

— Несомненно. И новые создаем, и выявляем слабые места действующих систем, так называемые элементы внесистемного обмена. Также жестко ограничиваем доступ сотрудников к информации, которая не касается их прямых обязанностей, не влияет на их работу. Сотрудник, совершая операцию, видит только сессию, которая ему нужна сейчас.

Интервью взяла Юлия Полякова

Небезопасная дистанция

— COVID-19 и кибербезопасность —

С переходом компаний на удаленную работу выросло не только количество инцидентов информационной безопасности (ИБ), но и масштаб их последствий. Число возможных точек проникновения хакеров в организацию стало равно числу сотрудников, работающих удаленно, а, например, взлом домашнего роутера превратился в угрозу безопасности корпорации. Компании стали внедрять системы мониторинга действий сотрудников и автоматизированные ИБ-решения, распространяющиеся по подписке. Если в первые месяцы удаленки многие пользовались бесплатными решениями вендоров, то сейчас компании перестраивают IT-платформы исходя из того, что их сотрудники могут работать дистанционно всегда.

Пожертвовать безопасностью ради скорости

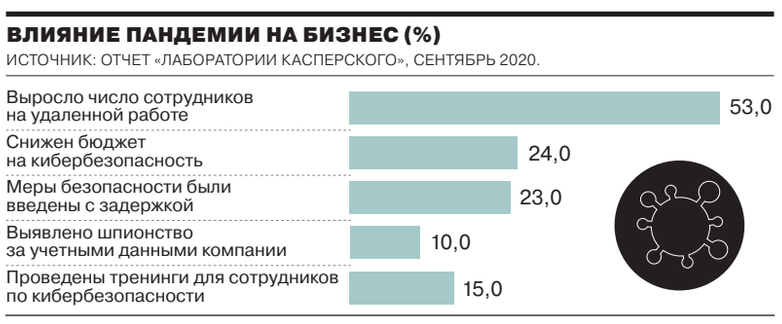
Во втором квартале 2020 года число атак выросло на 59% по сравнению с аналогичным периодом прошлого года, следует из данных Positive Technologies. Апрель и май стали рекордными по числу успешных кибератак. 11% компаний впервые организовали удаленный доступ в апреле, а значит, на периметре 11% компаний появились новые сервисы, которые злоумышленники, конечно же, попытались атаковать, говорит директор экспертного центра безопасности Positive Technologies Алексей Новиков. Хакерские боты начинают подбирать данные для доступа к новому сервису в среднем через шесть-десять часов после его появления, отмечает он.

Переход на удаленную работу был очень быстрым с точки зрения мобилизации IT и не всегда безопасным из-за принесения безопасности в жертву скорости, согласен руководитель практики информбезопасности Accenture в России Андрей Тимошенко. Большинство компаний урезало почти все инвестиции, и покупка консалтинга в сфере ИБ пошла «под нож» в первых рядах, подтверждает руководитель группы по оказанию услуг в области кибербезопасности КПМГ в России и СНГ Илья Шаленков. Это можно объяснить тем, что риски ИБ для бизнеса неочевидны, так как штрафы за невыполнение требований в России, в отличие, например, от ЕС, незначительные, полагает Андрей Тимошенко.

Только 7% промышленных компаний по всему миру признали, что принятая ими ранее стратегия кибербезопасности оказалась достаточно эффективной и во время пандемии, следует из результатов опроса «Лаборатории Касперского». Для остальных организаций перевод на удаленку стал стресс-тестом. Многие воспользовались бесплатными лицензиями вендоров в области ИБ для быстрого «наращивания» бастионов защиты, благо почти все вендоры предлагали свои продукты для использования во время карантина на безвозмездной основе, отмечает Алексей Новиков. Если в первые месяцы удаленки компании жили на переходной архитектуре и инфраструктуре, то сейчас многие организации не только понимают, но и уже ведут проекты по пересмотру IT-платформ и систем обеспечения ИБ под новые реалии, когда очень большая часть сотрудников работает удаленно всегда, говорит партнер EY, руководитель группы услуг по технологическим рискам в СНГ Николай Самодаев.

ВЛИЯНИЕ ПАНДЕМИИ НА БИЗНЕС (%)

ИСТОЧНИК: ОТЧЕТ «ЛАБОРАТОРИИ КАСПЕРСКОГО», СЕНТЯБРЬ 2020.



Автоматизация в тренде

Главной ценностью в условиях ограничения на передвижения в реальности стала максимальная автоматизация процессов и функций ИБ, констатируют эксперты. Речь идет о таких направлениях, как автоматизация реагирования на инциденты безопасности по заранее предопределенным сценариям и «умная» аналитика ИБ: автоматический анализ больших объемов данных с использованием методов машинного обучения, уточняет он.

В условиях массовой удаленной работы стирается грань между периметрами защиты информационных активов, меняется ландшафт угроз и рисков, а присутствие в офисе специалистов ИБ в условиях карантинных ограничений зачастую также лимитировано. Поэтому единственный выход для поддержания качественной системы защиты — это «умная» автоматизация процессов и функций ИБ.

Еще одной тенденцией за время карантина стал рост спроса на услуги ИБ как сервиса. В подписочной модели у клиентов есть возможность оплачивать фактически потребляемые сервисы, а внедрение и обслуживание решений помогает существенно сэкономить время и трудозатраты, поясняет руководитель департамента информбезопасности Softline Дмитрий Васильев.

В первую очередь передача ряда функций ИБ на аутсорсинг касается так называемых рутинных операций, второй основной сегмент — это сложные высокотехнологичные услуги, которые компаниям сложно и дорого реализовывать внутренними силами, отмечает Николай Самодаев. Сегмент SecaaS (безопасность как услуга) показывает существенный рост в России и в мире, и пандемия не окажет существенного влияния на эту тенденцию, потому что сегмент рынка в стадии бурного роста, уточняет руководитель направления «Информационная безопасность» КРОК Андрей Заикин.

Кроме того, за время карантина возрос интерес компаний к решениям по контролю активности пользователей и рабочего времени сотрудников, отмечают Андрей Тимошенко и Дмитрий Васильев. К традиционным задачам контроля обеспечения ИБ добавились задачи мониторинга эффективного использования рабочего времени, уточняет Николай Самодаев. Такие решения фиксируют, совершает ли пользователь какие-либо действия в системах или он просто залогинился и пошел заниматься своими делами, контролируют использование корпоративного интернета, а если речь о банке со своим процессинговым центром, то отслеживается и количество покупок, совершаемых в рабочее время.

Слабое звено

Рост числа удаленных подключений заметно усилил риски внешних проникновений: для компаний, которые перевели в онлайн взаимодействие с клиентами, большую опасность представляют DDoS-атаки, которые способны вывести сайт из строя на время, достаточное, чтобы потенциальные покупатели перешли к конкурентам, предупреждает Дмитрий Васильев.

Число атак с переходом на удаленную работу изменилось не так радикально, как их успешность и последствия, полагает технический директор Trend Micro в России и СНГ Михаил Кондрашин. В условиях, когда сотрудники ИБ были заняты переводом штата на надомный режим работы, у компаний стало существенно меньше ресурсов для проведения расследований потенциальных инцидентов. А взлом домашней сети удаленного сотрудника означает возможность атаковать сеть у него на работе, подчеркивает господин Кондрашин. По данным Trend Micro, число атак на домашние роутеры в 2020 году выросло почти на 15%. «Это очень тревожная тенденция, ведь скомпрометированный домашний роутер в условиях удаленной работы сотрудников угрожает и их работодателям»,— отмечает Михаил Кондрашин.

Люди — самое слабое звено любой организации, а работающие на удаленке и сталкивающиеся каждый день со стрессом и проблемами с мотивацией становятся еще более простым инструментом в руках мошенников, подтверждает Андрей Тимошенко. По его словам, с переходом на удаленку выросло число атак с целью вымогательства с использованием вирусов-шифровальщиков. Такие атаки распространяются в основном через вредоносные письма, когда неподготовленные в вопросах ИБ сотрудники открывают вложения или кликают на ссылки в письмах от непроверенных источников.

В первом полугодии требуемые злоумышленниками суммы выкупа выросли, тогда как общее число инцидентов, связанных с программами-вымогателями, в мире снизилось более чем втрое по сравнению с тем же периодом 2019 года, отмечает Михаил Кондрашин, добавляя, что это указывает на более точный выбор жертв. Причем стремление компаний СМБ к экономии приводило к тому, что, сталкиваясь с требованием выкупа, организации не сообщали об этом в правоохранительные органы, пытаясь справиться своими силами, чтобы быстрее решить проблему, отмечает Андрей Тимошенко.

Работа над ошибками

По данным «Лаборатории Касперского», 79% россиян, перешедших на работу из дома, не получали никаких конкретных рекомендаций по защите от киберугроз. При этом поведение сотрудников на удаленке стало более рискованным с точки зрения кибербезопасности — например, 60% российских сотрудников в хоум-офисах смотрят контент для взрослых с гаджетов, используемых для решения рабочих задач, а ведь «клубничка» часто эксплуатируется злоумышленниками как приманка для внедрения вредоносного ПО и реализации мошеннических схем, отмечают в компании.

Топ ошибок удаленных сотрудников традиционен, однако в новых условиях их критичность приобретает новое качество, отмечает Алексей Новиков. Пользователи используют нестойкие и одинаковые пароли, вводят учетные данные, не удостоверившись в надежности ресурса, выдают информацию о себе, которая может помочь подобрать пароль, рассказывает он. Во-вторых, пользователи нередко скачивают на личные устройства вредоносное или потенциально вредоносное ПО, используют нелицензионный софт, который, как правило, имеет «специальный» вредоносный функционал — и здесь причина также кроется в невысокой осведомленности в вопросах информационной безопасности, указывает господин Новиков. Кроме того, культура патчменеджмента на стороне пользователей отсутствует даже чаще, чем в корпоративном секторе: частный пользователь часто не следит за антивирусной защитой своих устройств, не устанавливает обновления безопасности, отмечает он. Все это в совокупности предоставляет широчайшие возможности для атаки даже не слишком высококвалифицированного злоумышленника, предупреждает эксперт.

Юлия Степанова