

Банки защищаются от хакеров

термин „войска“: у них строгая иерархия, их сообщество состоит из подразделений, они имеют серьезную конспирологическую защиту. Это очень серьезный, грамотный, обученный противник, который представляет большую угрозу для банковской системы, построенной на IT-платформах и электронных средствах. Поэтому обеспечение кибербезопасности входит в топ-3 главных проблем банковской системы, и с развитием технологий она будет вставать все более остро. Это надо принять и бороться с этим», — убежден первый заместитель председателя совета директоров АО «Альфа-банк» Олег Сысуев.

По его словам, «ничем другим, кроме как эффективными расходами на создание защитных систем, привлечение кадров, покупку специалистов, которые имеют опыт работы по этой специальности, проблему не решить».

По его словам, Альфа-банк накопил большой опыт борьбы с киберпреступностью, отбил немало хакерских атак: сейчас за обеспечение информационной безопасности и настройку софта кредитной организации отвечает большой штат специалистов в составе специального подразделения.

Не менее серьезно к обеспечению информационной безопасности подходит и Сбербанк. Заместитель председателя правления кредитной организации Станислав Кузнецов говорит, что Сбербанк решает проблему с помощью «белых» и «красных» хакеров, которые помогают отыскать и ликвидировать в системе уязвимые места.

«Они специально тестируют наши системы — и открыто, и скрытно. У нас это поставлено на промышленный поток, на этапах до внедрения, во время внедрения и после. Это требования современных стандартов. Мы должны опережать „инновационные“ попытки „плохих“ хакеров и создавать правильную защиту у себя», — говорит Станислав Кузнецов.

В 2017 году служба кибербезопасности кредитной организации пресекла более 300 тыс. попыток хищения средств физических и юридических лиц напрямую и с помощью вирусного ПО, предотвратив ущерб на сумму более 20 млрд руб. Интересно, что в 2016 году в Сбербанке было предотвращено попыток хищения на сумму около 16 млрд руб.

Поддержанию кибербезопасности способствует и сотрудничество банков с МВД, ФСБ и Интерпо-



Центробанк потребовал от кредитных организаций модернизации антивирусного программного обеспечения, которое должно быть настроено таким образом, чтобы информация о кибератаках отражалась одновременно со сведениями о клиентских операциях

лом. Например, Сбербанк с помощью штата квалифицированных специалистов формирует «базу данных» о мошенниках и передает ее в правоохранительные органы, которые проводят оперативно-разыскные мероприятия. В частности, в ноябре 2017 года эксперты дочерней структуры Сбербанка «Бизон» в составе группы Interpol Global Complex For Innovations в течение нескольких дней смогли выявить мошенническую подсеть на территории Китая.

В ситуацию включился регулятор

Реакцией на угрозу новых кибератак стала новая мера, введенная Центральным банком России. Регулятор добивается проведения модернизации антивирусного программного обеспечения в банках страны. В соответствии с требованиями Центробанка РФ, софт кредитных организаций должен быть настроен та-

ким образом, чтобы информация о кибератаках отражалась одновременно со сведениями о клиентских операциях. Свои требования регулятор основывает на том, что грамотно построенная система информационной безопасности в банках исключает возможность хакерского вмешательства при проведении операций. При слабой же защите происходит сбой в работе клиентских сервисов, и осуществить транзакцию становится невозможно.

Аналитик ГК «Финам» Леонид Делицын считает эту меру логичной, а роль ЦБ РФ в этой схеме работы с остальными банками — аналогичной роли правоохранительных органов в расследовании преступлений.

«Одно из требований ЦБ к банкам касается предоставления документации обо всех видах проникновения в информационную систему. Предполагается, что кредитные организации в случаях хакерских атак будут оформлять прото-

колы и направлять полные материалы об этих фактах в ЦБ, который будет работать подобно следователям, которые документируют место преступления и составляют отчеты. Это позволяет разрабатывать и внедрять типовые решения, в противном случае все средства банков уйдут на изобретение велосипедов», — убежден эксперт.

По информации Леонида Делицына, крупнейшие российские банки ежегодно тратят на IT более 10 млрд руб. в год. Но реальные расходы некоторых кредитных организаций на эти цели превосходят эту цифру примерно в десять раз: например, у Сбербанка они увеличились с 43 млрд до 102 млрд руб., у ВТБ — с 16 млрд до 40 млрд руб., включая контракты в сфере ИБ — с 800 млн руб. до 1,4 млрд руб. Таким образом, если ранее стандартные решения обходились банкам в 50–100 млн руб., то сейчас этих сумм явно недостаточно для обеспечения соответствия

стандартам ЦБ РФ и обеспечения должного уровня информационной безопасности.

«Так как революция в сфере финансовых технологий вынуждает банки ускорять ввод новых сервисов, а у разработчиков не всегда есть время для обеспечения безопасности операций и данных, отрасль может ждать волна консолидации. Регулятор рекомендовал около десятик специализированных поставщиков решений, которые могут настроить банкам систему информационной безопасности на аутсорсе, соответственно, банки увеличивают расходы», — объясняет аналитик.

Требование ЦБ РФ нацелено на создание в 2019 году нового национального стандарта по методике оценки соответствия защиты информации финансовых организаций. Предполагается, что он будет действовать с 1 июля 2019 года и определит методику защиты информации в банках. Авторы этой инициативы рассчитыв-

ают таким способом помочь банкам сформировать единый принцип работы системы информационной безопасности, сохранить свои данные, а значит, и доверие клиентов.

«В РФ на сегодняшний день пока нет единых национальных стандартов в области ИБ, обязательных для всех участников рынка. И это именно то, чего мы ожидаем от Центрального банка. Нам нужны стандарты, нам нужны правила, которые будут едины для всех кредитных учреждений и для всех сегментов рынка. Для примера — в упомянутом мной Евросоюзе уже достаточно давно приняты соответствующие законы, причем не только в рамках национальных законодательств, но и на уровне ЕС», — резюмирует Станислав Кузнецов.

По словам эксперта, выработка единого стандарта кибербезопасности — лишь часть большой работы по решению глобальной проблемы. Не менее важным в этом направлении является обмен информацией о киберугрозах и хакерских атаках между кредитными организациями, важной для предупреждения рисков.

«Например, в России до сих пор не существует единой системы, которая позволяла бы осуществлять (непосредственно между банками либо централизованно, через ЦБ) автоматизированный обмен информацией о скомпрометированных картах, паролях, фамилиях, телефонах и любых других деталях, необходимой для предотвращения мошенничества. У каждого из банков есть свой собственный стоп-лист, который никак не сопрягается со стоп-листами других кредитных организаций. Благодаря этому преступник может, например, многократно использовать один и тот же номер телефона для мошенничества, „работая“ по очереди с различными банками, — никто его не заблокирует. Резюмируя, скажу — сегодня две ключевые задачи обеспечения кибербезопасности банка — во-первых, защищать себя самого, свои системы, свое ядро, не допуская остановки процессов обслуживания, иными словами — не пропускать ударов „в самое сердце“, направленных на операционную систему, на базу данных, на ЦОДы с данными своих клиентов. И вторая задача — защищать клиентов при любых обстоятельствах, независимо от уровня их финансовой и компьютерной грамотности», — заключает Станислав Кузнецов.

Георгий Портнов

Сервисы для бизнеса, здоровья и повышения знаний

Сбербанк создает экосистему для предпринимателей

Не секрет: сегодня открыть бизнес и получить кредит стало намного проще, чем пару-тройку лет назад. Но только этим потребности предпринимателей не ограничиваются. Что нужно бизнесу, и что предлагают банки — в обзоре полезных сервисов Сбербанка и его партнеров.

ОТКРЫТЬ РАСЧЕТНЫЙ СЧЕТ

Первое, с чем сталкивается предприниматель — расчетный счет. Сбербанк предоставляет возможность резервирования счета, который будет действовать в течение 30 дней, без посещения банка. В течение указанного срока предпринимателю нужно прийти в банк и оформить счет. Для тех, у кого совсем нет времени приехать в банк, Сбербанк в Самаре и Волгограде тестирует проект, в рамках которого менеджер выезжает в удобное место и экономит время к предпринимателю. Этим способом уже воспользовались более тысячи компаний.

ВЫБРАТЬ ПАКЕТ УСЛУГ РКО

Сегодня бизнесу нужен не просто счет, а пакет услуг РКО, включающий как счет, так и платежи, самоинкассацию, бизнес-карту, снятие и внесение средств в банке и т. д. В Сбербанке каждый пакет услуг имеет четкое позиционирование. Так, «Легкий старт» предназначен для начинающего бизнеса, «Удачный сезон» — для организаций с невысокой транзакционной активностью и сезонным бизнесом, «Хорошая выручка» — для организаций с потребностью вносить наличные, а «Большие возможности» — для зрелых компаний с высокой активностью по платежам. Стоимость пакета пропорциональна объему включенных услуг, но при этом «Легкий старт» предлагает бизнесу самые нужные услуги... бесплатно!

ОФОРМИТЬ ОНЛАЙН-ФИНАНСИРОВАНИЕ

В определенный момент перед предпринимателем встает вопрос кредитования. До сих пор бытует мнение, что это долго, дорого и лучше с этим не связываться. Отнюдь! В Сбербанке малый бизнес может оформить кредит онлайн. Клиент банка может заполнить заявку в личном кабинете Сбер-

банк Бизнес Онлайн, а тот, у кого СББО-Ла нет — на сайте банка. Клиент, исходя из своих потребностей, выбирает вид кредита, загружает документы, выбирает наиболее подходящий офис и ждет звонка от менеджера. Онлайн-кредит дает не только колоссальную экономию времени, но и высокую «прозрачность» процесса: предприниматель отслеживает статус заявки, может вести онлайн-чат со всеми участниками процесса.

ВЫПУСТИТЬ КОРПОРАТИВНУЮ КРЕДИТНУЮ КАРТУ

Если бизнесу регулярно нужны небольшие суммы, то в этом поможет корпоративная кредитная карта без ограничения по оплате товаров и услуг. Карту ПАО Сбербанк отличают высокий лимит, умеренная комиссия за обслуживание и льготный 50-дневный период кредитования. Получить корпоративную кредитную карту можно при оформлении кредита «Доверие» (бесцелевой и беззалоговой кредит) или после оформления заказа на карту при наличии действующего расчетного счета (не менее 6 месяцев).

СЭКОНОМИТЬ НА БУХГАЛТЕРЕ

Сбербанк активно создает экосистему для предпринимателей, в которой традиционные финансовые услуги соседствуют с другими сервисами, которые необходимы бизнесу в решении ежедневных задач.

К примеру, вы можете представить предприятие без бухгалтера? Оказываться, это возможно. Сервис «Моя бухгалтерия» предлагает два варианта работы — «Моя бухгалтерия Онлайн», где предприниматель самостоятельно ведет финансовые дела, и «Моя бухгалтерия Аутсорсинг», в которой финансы заведует специалист на аутсорсинге. Наконец, есть еще «Бухгалтерия для ИП на УСН 6% без сотрудников» — онлайн-



сервис, который поможет подготовить все документы, клиенту останется только подтвердить их отправку.

...И НА ЮРИСТЕ

Без юридической защиты никуда. «Личный юрист» — это сервис дистанционной помощи для защиты интересов клиентов, где консультации оказываются по всем отраслям права (корпоративное, предпринимательское, административное и т. д.), а также по любым вопросам — от деловых до бытовых. Все консультации хранятся в личном кабинете, где их можно в любой момент прочитать или прослушать запись. Удобно!

Преимущества: такой «юрист» дешевле, чем в штате, экономит время, оперативен и работает 24 часа в день, что важно в экстренных ситуациях.

Консультацию можно получить множественным способом: по телефону 8-800-

775-73-09, через мобильное приложение, в личном кабинете, по электронной почте, в мессенджерах и т. д.

ВНЕСТИ ИЗМЕНЕНИЯ В ДОКУМЕНТЫ

Сервис «Внесение изменений в ИП и ООО» позволяет юристам и ИП самостоятельно подготовить полный пакет документов и произвести в режиме онлайн любые регистрационные действия, связанные с внесением изменений в ЕГРЮЛ и ликвидацией без привлечения юристов и без заверения документов у нотариуса. С помощью сервиса можно сменить наименование компании, изменить число участников ООО, сменить адрес, уставной капитал, ликвидировать ИП и т. д. Таким образом, компания экономит средства на содержании в штате юриста и время — документы готовятся за 15 минут.

ПОЗАБОТИТЬСЯ О ЗДОРОВЬЕ

Но почему мы только о бизнесе? Бизнес делают люди, а у них могут быть свои вопросы, например, по здоровью. Сбербанк предлагает воспользоваться сервисом телемедицины «Доктор рядом»*, который позволяет получить видеоконсультации врачей без посещения клиники. Зачем это нужно? Телемедицина — отличный способ, когда важно «второе мнение», когда визит в клинику кажется нецелесообразным, или когда на это просто нет времени. Для работодателя это отличная «фишка» в соцпакете и возможность сократить время отсутствия работников из-за их походов в больницу. Консультация может быть как по предварительной записи, так и срочная, когда врач ответит в течение 5 минут.

ПОВЫСИТЬ СВОИ ЗНАНИЯ

Сбербанк уже много лет сотрудничает с образовательной платформой «Деловая среда», в которой объединились ключевые поставщики образования, бизнес-школы, госорганы и эксперты. Здесь представлены материалы таких организаций, как «Высшая Школа Экономики», «Опора России», Федеральная налоговая служба и т. д. Информация для предпринимателей на платформе представлена в формате видео, статей и материалов на темы продаж, личной эффективности, управления риском, права, развития бизнеса и др. Наконец, в этом году Сбербанк совместно с правительством и одной из глобальных технологических компаний запустит проект по повышению знаний. Воспользоваться им смогут как действующие, так и начинающие предприниматели в Самаре, Саратове, Волгограде и Ульяновске. Проект предполагает как практические занятия с экспертами и наставниками, так и удаленные курсы.

* Услуга предоставляется ООО «Доктор рядом». Лицензия на осуществление медицинской деятельности №ЛО 77-01-013560 от 29 ноября 2016 г. Банк выступает партнером указанной организации.