Рынок мобильного банкинга: факторы роста и механизмы защиты

Самодостаточная мобильность

Чтобы ориентироваться в технологических изменениях в отрасли, банкам и поставщикам решений для них важно понимать, какие технологии актуальны на данный момент. «Б.О» провел исследование, показывающее, что банки внедряли недавно, что устанавливают сейчас и к чему только готовятся

Текст
ДМИТРИЙ СЛОБОДЕНЮК,
КОММЕРЧЕСКИЙ ДИРЕКТОР ARINTEG

Эксперты едины во мнении, что один из ключевых мировых трендов — развитие возможностей интернет-банкинга и мобильных сервисов для управления счетами. Что вполне оправдано, если учесть результаты исследования аналитического агентства Markswebb Rank & Report по эффективности сервисов мобильного банкинга физических лиц: 10,8 млн. человек в России пользуются сервисами мобильного банкинга. Сегодня топовые российские банки ведут активную работу по развитию сервисов мобильного банкинга. Основной идеей этой работы становится расширение платежных возможностей и внедрение дополнительных удобных опций.

Таким образом, мобильный банк становится еще более эффективным инструментом, способствующим расширению клиентской базы. Очевидно, что с точки зрения конкурентного преимущества разработка полнофункционального мобильного банкинга становится очень актуальной.

Ключевым препятствием для популяризации этого решения оставалась недостаточная надежность системы двухфакторной идентификации клиентов мобильного банкинга. По сути, передача пароля третьим лицам или разглашение учетной информации клиента, утеря средств доступа к приложениям демонстрировали уязвимость системы безопасности.

Сегодня разработана и широко используется многофакторная модель защиты информации. Это так называемая сильная аутентификация, состоящая из нескольких механизмов защиты, ее реализация требует четкого проектирования и постоянной поддержки.

Для защиты критичных информационных данных компания ARinteg в качестве наиболее эффективных средств аутентификации выделяет токены с использованием криптографии и технологии открытого ключа (PKI). Инфраструктура PKI основана на аппаратных решениях и защищена микроконтроллером, что обеспечивает безопасность ключа поль-

зователя даже при работе в уязвимой среде. В процессе строгой аутентификации участвуют два фактора: во-первых, наличие USB-токена, Secure MicroSD-токена или смарт-карты, а во-вторых, знание PIN-кода для выполнения криптографических операций внутри токена. Помимо логических данных при строгой аутентификации используются и биометрические данные владельца токена, что исключает использование устройства без его владельца.

Безопасное хранение информации, паролей и ключей доступа обеспечивает новое поколение смарт-карт, USB- и MicroSD-токенов. Эти модели выполнены на защищенном смарт-карточном микроконтроллере и поддерживаются в продуктах мировых вендоров. Смарт-карты выполняют двух- и трехфакторную аутентификацию с поддержкой биометрии по отпечаткам пальцев. Новое поколение токенов сегодня очень актуально, поскольку обеспечивает безопасный доступ ко всем информационным системам организации: веб-порталам, «облачным» приложениям, системам электронного документооборота и т.д. Это позволяет управлять компанией без инцидентов безопасности и поддерживать эффективное взаимодействие сотрудников. Инфраструктура открытых PKI-ключей поддерживает систему юридически значимого электронного оборота, так как является средством усиленной квалифицированной подписи, полностью соответствующим требованиям ФЗ-63 и приказу ФСБ №796 к средствам электронной подписи. Платформа смарт-карт организована для решения задач в различных сегментах экономики и поддерживается различными информационными системами.

На качественно новый уровень информационную безопасность выводит использование уникальных физических данных пользователей. Так, в качестве одного из факторов аутентификации в PKI-системах выступают отпечатки пальцев. Важным видится тот факт, что хранение цифровых образцов биометрической информации сотрудников происходит в защищенной области смарт-карты. Таким образом, цифровые образцы никуда не пересылаются, и доступ к ним имеет исключительно держатель карты. Этот факт имеет большое значение при доступе пользователей к критически важной информации, поскольку подтверждает неотчуждаемость токена от его владельца. Стоит отметить высокую стойкость к атакам и низкую вероятность подделки биометрических данных.

За метод строгой аутентификации на базе токенов выступает и психологическая сторона вопроса. Так, сотрудники существенно внимательнее относятся к биометрическому носителю парольной информации. Объясняется это очень просто — токен персонализирован, а значит, все действия с его использованием будут производиться от лица его владельца и отслеживаться в системе.

Рынок показывает высокий рост использования и расширения функционала мобильного банкинга. Эта тенденция очень удобна финансово-кредитным учреждениям, поскольку позволяет значительно расширять свое присутствие без развертывания филиальной сети. Благоприятное влияние на нее оказывает и высокое качество средств многофакторной аутентификации. Ведь от того, насколько надежно защищены данные клиентов, зависит уровень их доверия, а следовательно и эффективность организации в целом.

Для защиты критичных информационных данных компания ARinteg в качестве наиболее эффективных средств аутентификации выделяет токены с использованием криптографии и технологии открытого ключа (PKI)

Сегодня уровень информационной безопасности меняет расстановку сил на рынке дистанционного банковского обслуживания, позволяет вывести мобильный банкинг в самостоятельный финансовый сервис. Темпы роста мобильного банкинга весьма ощутимы, не менее активно развиваются и сопутствующие сегменты рынка. Одновременно спрос населения на услуги дистанционного обслуживания показывает важность развития этого направления. Финансовые учреждения не могут игнорировать ни существующую рыночную ситуацию, ни новейшие технологические разработки, поэтому многие инвестируют в развитие мобильного банкинга. Б.О

СПРАВКА Б.О

Компания ARinteg — ведущий российский системный интегратор и поставщик IT-решений в сегменте информационной безопасности. Компания реализует свои услуги на базе разработок ведущих мировых производителей по направлениям:

- Создание комплексных систем информационной безопасности
- Внедрение инфраструктурных решений
- Аудит и консалтинг в области IT и ИБ
- Поставка программного обеспечения
- Сопровождение и поддержка технических решений

ARinteg обладает высшими партнерскими статусами крупнейших российских и зарубежных разработчиков программного и аппаратного обеспечения. ARinteg имеет все необходимые лицензии ФСТЭК и ФСБ для работы в области информационной безопасности на российском рынке.