Как известно, Банк России перенес сроки исполнения по изменениям к Положению от 24.08.2016 № 552-П «О требованиях к защите информации в платежной системе Банка России» на начало 2019 года. Однако кредитным учреждениям уже сейчас стоит задуматься о том, как реализовать защиту электронных сообщений, направляемых в Банк России. Какие средства для этого существуют?

Как реализовать защиту электронных сообщений, направляемых в Банк России

Максим БОЛЫШЕВ, *компания R-Style Softlab, заместитель директора департамента банковского ПО RS-Bank*

Банк России переводит кредитные учреждения на новую технологическую схему обработки платежей, при которой электронные сообщения должны будут подписываться не в автоматизированном рабочем месте клиента Банка России (АРМ КБР), как это было ранее, а непосредственно в автоматизированной банковской системе (АБС) или в специально для этого предназначенной выделенной системе. Ответственность за целостность и неизменность передаваемых данных возлагается на автоматизированные системы банков.

Чтобы обеспечить выполнение требований регулятора, необходима дополнительная функциональность для сотрудника, ответственного за отправку документов в Банк России (для удобства будем называть ее АРМ). Принцип ее работы, как правило, такой: операционист готовит в АБС документ, формирует для него электронную подпись (ЭП) — защитный код (ЗК) и направляет ответственному за электронное взаимодействие с Банком России сотруднику. Тот после проверки ЗК визуально и (или) с помощью функции сверки проверяет документ, подписывает его ЭП — кодом аутентификации (КА), далее документ передается в АРМ КБР-Н (индекс «Н» от слова «новый») для сжатия, шифрования и отправки в Банк России.

Если же говорить о документах, пришедших из Банка России, то с ними еще проще — на прием остается та же схема, что и ранее: расшифровка, восстановление сжатого документа и проверка ЭП выполняются в АРМ КБР-Н, далее документ поступает в АБС, уже считаясь подлинным.

Максим БОЛЫШЕВ

Следуя требованиям Положения № 552-П, с целью обеспечения безопасности реализация АРМ должна позволять банку применять его в выделенном сегменте локальной вычислительной сети (ЛВС). Сотрудник банка должен работать с ним в специальном помещении, где приняты надлежащие меры по обеспечению безопасности.

Не все так просто

В некоторых ситуациях банк может остаться без поддержки российского законодательства или эти работы могут оказаться для него очень дорогими. Это может произойти, например, в следующих случаях:

— банк работает на АБС иностранного производства и разработчик не поддерживает изменения российского законодательства;

— банк использует АБС или данную функциональность собственной разработки;

— банк использует старую версию АБС, которая уже не поддерживается разработчиком;

— банк использует очень кастомизированную версию АБС.

Следуя требованиям Положения № 552-П, с целью обеспечения безопасности реализация АРМ должна позволять банку применять его в выделенном сегменте локальной вычислительной сети.

Как же тогда быть? Решение есть, и даже не одно.

Первый вариант — установить криптобиблиотеку, которая способна функционировать с любой АБС. Криптобиблиотека обеспечивает взаимодействие со СКАД «Сигнатура», а также подписание документов. Она формирует ЗК и КА электронных сообщений и пакетов сообщений УФЭБС. Все факты создания защитных кодов и кодов аутентификации будут отражаться в log-файле.

Для использования криптобиблиотеки необходимо, чтобы на рабочем месте пользователя была инсталлирована СКАД «Сигнатура» (к ней криптобиблиотека обращается за криптографическими преобразованиями). Кроме того, библиотеку следует зарегистрировать в ОС Windows, что позволит обеспечить доступ к ней из сторонних приложений как к COM-объекту. При этом потребуется небольшая доработка АБС, которая должна формировать пакеты документов и обеспечивать взаимодействие с криптобиблиотекой.

Второй вариант — установить систему автоматизации межфилиальных и межбанковских платежей, где необходимая функциональность также реализована. В этом случае банк сможет обеспечить передачу документов из собственной АБС в систему автоматизации межфилиальных и межбанковских платежей, в которой реализовано рабочее место пользователя, участвующего в подготовке электронных сообщений (ЭС) УФЭБС, передаваемых в Банк России. В АРМ банковский специалист будет выполнять ввод ЭС, генерировать для

них защитные коды, осуществлять их контроль с формированием для них кодов аутентификации.

Криптобиблиотека как ключевой элемент

Криптобиблиотека заслуживает отдельного внимания, так как именно она является ключевым элементом функциональности, необходимой для поддержки требований Положения № 552-П.

Криптобиблиотека не только реализует логику обработки электронной подписи, но и поддерживает интерфейс между экспортируемыми функциями и функциями, предоставляемыми криптосредством.

Функции криптосистемы реализует СКАД «Сигнатура». Она осуществляет обработку XML, формирует ЭП, осуществляет ее проверку, а также отвечает за поддержку ключевых носителей и работу с сертификатами ключей.

У криптобиблиотеки есть еще одна роль — служебная. Она обеспечивает поддержку локальных настроек, диагностирует ошибки и ведет журнал операций.

Криптобиблиотека не только реализует логику обработки электронной подписи, но и поддерживает интерфейс между экспортируемыми функциями и функциями, предоставляемыми криптосредством.

О безопасности начистоту

Ни для кого не секрет, что основной причиной преобразований в регламенте электронного взаимодействия между банком и регулятором стала недостаточная защищенность документов. Прежняя схема была не лишена лазеек, которыми охотно пользовались злоумышленники.

Вся функциональность по защите ЭС находилась в АРМ КБР, где осуществлялось наложение ЭП, а документы на подпись поставлялись в виде текстовых файлов. Злоумышленник мог положить во входной каталог свой текстовый файл, в АРМ КБР он подписывался, деньги в Банке России с корсчета банка списывались. По данным FinCERT, за период с октября 2015 г. по март 2016 г. по этой схеме хакерам удалось похитить из российских коммерческих банков 1,27 млрд руб.

Теперь ситуация изменилась: в новое АРМ КБР-Н Банка России электронные документы поступают уже с электронной подписью, которая гарантирует неизменность и целостность документа.

Однако на стороне банка лазейки для злоумышленника все-таки остались. Поэтому правильнее было бы обеспечить весь жизненный цикл документа с ЭП — от момента его ввода оператором или получения из внешней системы до выгрузки в Банке России. Разумеется, в случае передачи документов из системы в систему таких подписей может быть собрано несколько. Зато банк сможет быть уверен, что

Максим БОЛЫШЕВ

безопасности документов ничто не угрожает. В большинстве кредитно-финансовых учреждений на текущий момент такая схема работы с документами не внедрена, поэтому угроза не исчезла полностью, хотя нужно отметить, что безопасность стала выше.

Важный момент

Не будет лишним напомнить, что в нашем современном и динамично развивающемся мире технологии, используемые хакерами, тоже совершенствуются, и чтобы обезопасить себя от чуть более изощренного варианта увода денег с корсчета, необходимо использовать ЭП на протяжении всего жизненного цикла документов.

Заключение

В завершение статьи хотелось бы призвать всех к своевременному решению подобных вопросов. Не оставляйте их «на последнюю ночь», как обычно делают студенты перед экзаменом, поскольку цена ошибки на промышленном стенде очень велика, а любое изменение бизнес-процессов в банке — это дело непростое, требующее тщательного выбора решения и его аккуратного внедрения в текущую инфраструктуру с интеграцией со смежными системами. При этом требуется полноценное тестирование не только функциональности, но и быстродействия.