Новые требования к безопасности СЭД

Какие новые требования к безопасности выдвигает рынок СЭД?

Начальник бюро делопроизводства, г. Архангельск

Е.Ю. Антошечкина,
главный специалист,
«ЭОС»

Информационная безопасность не является целью сама по себе: защиту информации необходимо обеспечивать исключительно в контексте эксплуатации защищаемой системы. Требования по информационной безопасности должны учитывать область и особенности использования объекта защиты (в нашем случае объектом защиты является СЭД и ее информационные ресурсы). То есть требования к обеспечению информационной безопасности СЭД определяются требованиями к ее функционалу и среде использования.

Среди современных тенденций рынка СЭД прежде всего следует отметить требования, связанные с обеспечением мобильности и оперативности использования СЭД.

Стремительный рост рынка мобильных устройств, наблюдаемый в течение последних нескольких лет, приводит к активизации спроса на решения для мобильных приложений на различных платформах (в частности, таких как Windows, Android, iOS) в области электронного документооборота. Также обращает на себя внимание существенное ужесточение требований ко времени выполнения тех или иных операций в СЭД (особенно это касается времени реакции на поступивший документ или информацию, выдачи и исполнения поручений). Если раньше время, отводимое на получение документа и принятие решения по нему, исчислялось днями, то сейчас часами и даже минутами.

Таким образом, наиболее актуальным требованием к современной СЭД можно назвать обеспечение оперативного доступа к информации для удаленных мобильных пользователей практически в любой точке земного шара. И основной задачей в области защиты информации становится обеспечение удаленного защищенного доступа к информационным ресурсам СЭД, тем более что в большинстве случаев доступ этот осуществляется по незащищенным каналам связи.

Большинство современных СЭД предоставляют возможность работы с мобильными приложениями, обеспечивая опе-

ративный доступ к информационным ресурсам с мобильных устройств (эти функции могут быть либо включены в возможности основного функционала СЭД, либо реализованы в виде дополнительных модулей).

Мобильные приложения могут содержать уязвимости, использование которых злоумышленниками может привести к весьма ощутимым потерям для организации, использующей СЭД.

Основными угрозами при использовании мобильных приложений являются сложность аутентификации и авторизации пользователя, получающего доступ к информации (что может привести к несанкционированному доступу к передаваемой/хранимой информации), и передача данных, в том числе и секретных, в открытом виде по незащищенным каналам связи (что может повлечь за собой нарушение конфиденциальности, а также целостности, авторства и аутентичности передаваемой/получаемой/хранимой информации).

В целях снижения риска возникновения подобных проблем следует для всех используемых мобильным приложением платформ принять меры по обеспечению достаточно надежного для данного приложения уровня информационной безопасности. В частности, необходимо обеспечить соответствие конфигурации серверной части мобильного приложения отраслевым стандартам информационной безопасности; обеспечить защиту серверной и клиентской частей мобильного приложения от программных уязвимостей и несанкционированного доступа к информации. Также нужно предусмотреть возможность (и необходимость) использования дополнительных средств обеспечения защиты.

В качестве дополнительных средств защиты могут использоваться, например, криптографические средства защиты информации для обеспечения конфиденциальности (шифрование), подтверждения авторства, целостности и подлинности информации (электронная подпись).

Следует также принимать во внимание, что для организации надежной защиты информации наряду с программно-аппаратной средой, используемой мобильным приложением, требуется проанализировать на предмет потенциальных уязвимостей логику работы самого приложения.

Учитывая необходимость оперативного доступа к системе и критичность ко времени отклика СЭД, нельзя допустить, чтобы реализация защищенного доступа к информации существенно снижала быстродействие СЭД, своевременную доступность ее информационных ресурсов. Должны быть предпри-

няты меры по обеспечению отказоустойчивости и доступности мобильного приложения. Учитывая, что пользователь мобильного приложения может находиться довольно далеко (зачастую в другом часовом поясе) от офиса, где установлена серверная часть приложения, немаловажно решить вопрос обеспечения синхронизации времени мобильного устройства и сервера.

Как правило, пользователями мобильных решений являются руководители высшего и среднего звена. Результат деятельности этих сотрудников весьма важен для организации, поэтому меры, обеспечивающие надежность использования мобильных приложений, не должны нарушать технологию работы системы и препятствовать ее эффективной эксплуатации.