DOI: 10.17117/na.2016.12.02.056

<http://ucom.ru/doc/na.2016.12.02.056.pdf>

Поступила (Received): 19.12.2016

Кудинов В.А., Солнцев С.П., Куликов Г.С., Грачев Н.С. Организация защиты мобильных соединений на примере подключения к системе электронного документооборота

Kudinov V.A., Solntsev S.P., Kulikov G.S., Grachev N.S.
Securing mobile connections on the example of the connection
to the electronic document management system

В статье рассмотрена и исследована специфика защиты мобильных подключений на примере доступа к электронному документообороту через информационную сеть. На основе проведенных исследований предоставлен примерный перечень необходимых программных продуктов для обеспечения полноценной защиты

Ключевые слова: документооборот, информационные технологии, защита, информация

In the article reviewed and investigated the specificity of protection of mobile connections in the example of access to the electronic document via the network. Based on these studies provided an approximate list of the necessary software to provide full protection

Key words: document, information technology, protection, information

Кудинов Виктор Александрович

Бакалавр

Московский технологический университет
г. Москва, пр. Вернадского, 78

Kudinov Victor Alexandrovich

Bachelor

Moscow technological university
Moscow, Vernadskogo ave., 78

Солнцев Сергей Павлович

Бакалавр

Московский технологический университет
г. Москва, пр. Вернадского, 78

Solntsev Sergey Pavlovich

Bachelor

Moscow technological university
Moscow, Vernadskogo ave., 78

Куликов Георгий Сергеевич

Бакалавр

Московский технологический университет
г. Москва, пр. Вернадского, 78

Kulikov Georgiy Sergeevich

Bachelor

Moscow technological university
Moscow, Vernadskogo ave., 78

Грачев Никита Сергеевич

Бакалавр

Московский технологический университет
г. Москва, пр. Вернадского, 78

Grachev Nikita Sergeevich

Bachelor

Moscow technological university
Moscow, Vernadskogo ave., 78

Введение

Не покидая рабочего места можно решить многие задачи, но необходимость доступа к системе электронного документооборота (СЭД) остается и по

сей день, например, чтобы в различных командировках отсутствие руководящей должности не приводило к остановке работы с документами. СЭД – автоматизированная многопользовательская система, сопровождающая процесс управления работой иерархической организации с целью обеспечения выполнения этой организацией своих функций [1].

Исследование объекта и предложения по его защите

У многих СЭД есть различные мобильные клиенты, которые реализуются или как «тонкий» клиент или как мобильное приложение. «Тонкий» клиент – это, как правило веб-приложение, которое переносит все или большую часть задач по обработке информации на сервер [2], то есть на мобильном устройстве пользователь работает с ним через веб-браузер, а значит минусом является отсутствие возможности работы онлайн. Плюсом же такого решения является меньшая трудоемкость разработки. А мобильное приложение имеет возможность работы оффлайн, кроме того, оно эргономичнее браузера.

Требования безопасности

При мобильном доступе к СЭД информация покидает периметр, выходит из вычислительной сети организации и может быть перехвачена. Кроме того, появляется внешняя точка доступа в периметр, что может быть использовано для атаки на внутреннюю сеть.

Например, для защиты информации в системах, используемых в органах государственной власти, должны применяться «средства шифрования по ГОСТ», то есть российские средства шифрования – сертифицированные средства криптографической защиты информации (СКЗИ). Далее рассмотрим подходы к решению указанных задач по защите информации с мобильного аппарата с использованием сертифицированных СКЗИ.

Защита данных, передаваемых по сети

Данные, передаваемые по сети, защищаются за счет использования одного из протоколов – SSL/TLS или IPSec, которые шифруют данные, передаваемые по сети. Оба протокола могут использовать одни и те же криптографические алгоритмы для шифрования трафика, поэтому безопасность практически идентичная в обоих случаях. Возможность построения защищенного канала дает дополнительную защиту при передаче данных и позволяет организовать более качественное обслуживание за счет оперативного доступа ко всем ресурсам [3].

Сегодня в России есть ряд сертифицированных средств организации защищенного SSL/TLS-подключения с сертифицированными СКЗИ, например, от компаний «StoneSoft», «Checkpoint» и «Trusted TLS». Также доступны VPN-решения, примером может служить система ViPNet от российской компании «Инфотекс».

Защита периметра сети

Для защиты периметра сети лучше всего подходит эшелонированная защита, которую можно построить путем размещения шлюзов доступа мобильных устройств в демилитаризованных сегментах сети (ДМЗ), то есть таких

сегментах сети, которые содержат общедоступные сервисы и отделяют их от частных [4]. Эти сегменты отделены от Интернета и внутренней сети передачи данных межсетевыми экранами, а шлюзы поддерживают аутентификацию каждого подключения по цифровому сертификату. В качестве дополнительного средства защиты можно организовать такой режим, когда канал между шлюзом в ДМЗ и сервером СЭД внутри корпоративной сети будет однонаправленным и обеспечит передачу данных только по запросам сервера СЭД, что исключает атаку извне.

При описанном сценарии работы внутренний сервер устанавливает непрерывное соединение с ДМЗ и поддерживает его для получения данных от мобильных устройств. Такой подход не требует открытия входящих портов на межсетевых экранах, что минимизирует риски сетевой безопасности.

Защита данных и особенности поддержки сертифицированных СКЗИ на мобильном устройстве

Для обеспечения защиты локальных данных на мобильном устройстве может использоваться зашифрованная область, где хранится конфиденциальная информация. Это означает, что прочитать данные не удастся даже в случае, если устройство окажется в руках злоумышленника и данные будут похищены.

Особенностью использования сертифицированных СКЗИ на популярных мобильных платформах iOS и Android является то, что (в отличие, например, от ОС Windows) эти средства нельзя встроить на системный уровень ОС – так, чтобы ими могли пользоваться все приложения. В ОС от Microsoft есть возможность установить в систему криптопровайдер (CSP); в iOS и Android приходится встраивать его в каждое приложение. Для реализации применения сертифицированных СКЗИ на мобильном устройстве подойдет продукт компании «Крипто-Про» – «КриптоПРО CSP».

Доступ к зашифрованным областям памяти мобильного приложения, организация защищенного канала связи и аутентификация пользователей в приложении осуществляются с использованием ключа пользователя, размещенного в криптографическом контейнере. Ключевые контейнеры защищаются пин-кодом. Поскольку аутентификация пользователей в приложении организована с помощью цифрового сертификата, необходимо также контролировать актуальность сертификата, периодически обращаясь к удостоверяющему центру. Чаще всего сертификат отзывается при завершении срока его действия или же при увольнении сотрудника.

Расшифровка информации из зашифрованной области должна производиться на короткий промежуток времени и только по запросу пользователя, а по завершении работы расшифрованные данные должны быть удалены из памяти. Также следует применять технологии очистки памяти, при которой области памяти не просто очищаются, но и многократно перезаписываются случайными данными, чтобы избежать возможности восстановления блоков расшифрованной информации. В качестве дополнительной меры усиления безопасности могут использоваться отчуждаемые носители для хранения ключевой информации [5].

Для операционной системе Apple выпускаются специальные считыватели смарт-карт, они подключаются по Bluetooth или через специальный разъем. Так же применяются специальные токены со встроенным Bluetooth модулем и микрочипом, что удобно, потому что не требует дополнительных считывателей. Есть множество различных решений на рынке, таких как смарт-карта и риддер для мобильных устройств «Алладин Р.Д.». При использовании подобных устройств для доступа к информации необходимы одновременно само устройство с установленным программным обеспечением, токен и пин-код, зато это обеспечивает многофакторную аутентификацию.

Контролировать целостность исполняемых модулей так же очень важно, так как теоретически устройство может быть подвержено различным вирусам. Чтобы избежать подобных проблем, очень важно иметь сертифицированное программное обеспечение для сравнения контрольных сумм и проверки целостности кода приложения, операционной системы и модулей защиты информации. В случае несовпадения контрольных сумм с эталонными программа должна прекратить свою работу и уничтожить всю важную информацию, включая криптографические ключи.

Встраивание сертифицированных СКЗИ в приложения – достаточно трудоемкая задача. Если защита данных на устройстве обеспечивает организационными мерами, то для защиты канала связи сейчас на рынке доступны два средства построения VPN-подключений с шифрованием данных по ГОСТ: «VipNet Client» и «Защищенный Туннель». Эти программные продукты поддерживают мобильные операционные системы iOS и Android, то есть покрывают большую часть мобильных устройств, применяющихся сегодня в государственных и коммерческих организациях. При использовании этих программ могут потребоваться изменения в настройках подключения, в остальном же мобильный клиент работает в привычном для него режиме.

Заключение

Сейчас на рынке есть достойные отечественные программные продукты, способные надежно защитить данные или канал их передачи за периметр локальной компьютерной сети организации, такие как «КриптоПРО CSP», «ViPNet», «Защищенный Туннель» и т.д.

При должном финансировании и правильной квалификации обслуживающего персонала использование сотрудниками организации мобильных устройств при удаленной работе – не препятствие для конфиденциальности служебных данных. Хотя и специальные продукты обеспечивают безопасность работы с СЭД вне рабочего места с достаточной надежностью, стоит отметить, что необходимость должной квалификации пользователя так же не переоценена. Пользователь должен как минимум понимать общую схему и принципы защиты служебной информации на мобильном устройстве.

Список используемых источников:

1. Свободная энциклопедия «Википедия».

URL: https://ru.wikipedia.org/wiki/Система_автоматизации_документооборота

2. Свободная энциклопедия «Википедия». URL: https://ru.wikipedia.org/wiki/Тонкий_клиент

3. Информационный центр. URL: http://ic-dv.ru/uslugi/zawiwennyj_elektronnyj_dokumentoorot/
4. Свободная энциклопедия «Википедия». URL: [https://ru.wikipedia.org/wiki/DMZ_\(компьютерные_сети\)](https://ru.wikipedia.org/wiki/DMZ_(компьютерные_сети))
5. Открытые системы СУБД. URL: <http://www.osp.ru/os/2014/03/13040837/>
6. Даниленко А.Ю., Павлова Н.С. Методика и средства работы с системами электронного документооборота через WEB-браузер // Сборник трудов ИСА РАН. М.: УРСС, 2003.

© 2016, Кудинов В.А., Солнцев С.П., Куликов Г.С.,
Грacheв Н.С.

Организация защиты мобильных соединений на
примере подключения к системе электронного
документооборота

© 2016, Kudinov V.A., Solntsev S.P., Kulikov G.S.,
Grachev N.S.

Securing mobile connections on the example of the
connection to the electronic document management
system