УДК 004.056

Особенности использования мобильных устройств в работе защищенных корпоративных информационных систем

А. Ю.Бабиков[1], Д. И. Кардаш[2]

[1]babikov@hotbox.ru, [2]kardashdi@narod.ru

[1,2]ФГБОУ ВПО «Уфимский государственный авиационный технический университет» (УГАТУ)

Поступило в редакцию 22.12.2013

Аннотация. Рассмотрены вопросы организации информационной безопасности работы корпоративных информационных систем с использованием мобильных устройств. Приводятся результаты проведенного анализа мест возникающих уязвимостей. Предлагается методика внедрения мобильных устройств с учетом требований безопасности.

Ключевые слова. *Корпоративная информационная система; мобильное устройство; информационная безопасность; клиенты информационных систем*

В настоящее время осуществляется переход от бумажного к электронному делопроизводству. Однако при использовании электронного документооборота возникает ряд новых требований к обеспечению защищенности информации, предотвращению нарушения ее конфиденциальности и целостности.

Кроме этого, современный уровень развития вычислительной техники позволяет вводить в практику работы корпоративных информационных систем (КИС) широкий спектр мобильных устройств (МУ). Под ними понимаются нестационарные переносные устройства, например мобильные планшеты.

С недавнего времени стало возможным использование электронных цифровых подписей (являющихся одним из базовых механизмов КИС) в соответствии с ГОСТ на операционных системах МУ (iOS) [1]. В то же время для устройств под управлением Android решение данного вопроса представляется более сложным в силу фрагментарности устройств (большое количество различных устройств с различными версиями операционных систем); необходимости гарантирования отсутствия закладок, блокировки установки сторонних приложений, блокировки проникновения патогенного программного обеспечения с автоматическим обновлением программ.

При использовании МУ возникает ряд уязвимостей, которые в настоящее время парируются не полностью, однако уровень угрозы от них высок. Поэтому важно организовать процесс защиты информации при использовании МУ в КИС, что в настоящее время уже является практикой работы таких систем [2]. Следует заметить, что вопросы организации защиты работы МУ решены частично и недостаточно.

До недавнего времени при предъявлении требований СТР/СТРК отсутствие средств криптографической защиты информации вызывало сложности при использовании МУ для доступа к ресурсам корпоративных сетей. В силу этого в настоящее время актуальность приобретает разработка методики их использования в работе защищенных КИС.

ВИДЫ ИСПОЛЬЗУЕМЫХ В КИС МОБИЛЬНЫХ УСТРОЙСТВ

Современные КИС (при их реализации с помощью стационарных устройств) характеризуются информационной защищенностью за счет аппаратной реализации средств зашиты, грамотного проектирования сетевой инфраструктуры. Вместе с тем современные КИС характеризуются гетерогенностью, когда наряду со стационарными используются мобильные устройства.

При использовании МУ в КИС значимым является минимальность задержек при организации доступа к защищенной корпоративной информации, а именно – доступ к следующим типам данных:

- корпоративные информационные ресурсы;
- корпоративные терминальные сервера;
- web-порталы;
- библиотеки документов;
- сервера поддержки электронного документооборота;
- каналы цифровой передачи видеоинформации;
- информация серверов IP-телефонии и других средств коммуникации.

Наряду с преимуществами использования МУ они более уязвимы по сравнению со стационарными персональными компьютерами в силу следующих особенностей:

- при использовании публичных сетей встроенные средства защиты не всегда способны обеспечить требуемый уровень защищенности (например, в iPhone и iPad отсутствует встроенный сетевой экран);
- отсутствуют сертифицированные средства обеспечения безопасности;
- отсутствует официальная отечественная сертификация алгоритмов шифрования;
- отсутствуют сертификаты соответствия МУ требованиям ФСБ РФ и ФСТЭК РФ;
- последняя особенность усложняет использование МУ при подключении к КИС государственных органов и учреждений [3, 4].

В данных условиях организации вынуждены выбирать между отказом от использования МУ в КИС, или рисковать, разрешая их использование при отсутствии средств защиты. Любой из выбранных вариантов характеризуется финансовыми рисками и возможными потерями. Недопустимость этих последствий и определяет проблему использования МУ в КИС.

В настоящее время актуальны следующие платформы для мобильных устройств:

- iPhone, iPodTouch, iPad (операционная система AppleiOS);
- смартфоны и планшеты различных производителей (GoogleAndroid);
- Phone 7, Phone 8, RT (сосени 2012 года – Microsoft Windows);
- Blackberry (Playbook);
- мобильные PDA устройства (Symbian).

Исторически сложилось, что на Западе корпоративный сектор в большей степени использует устройства Blackberry. В России предпочтение в настоящее время отдают устройствам Apple и, в меньшей степени, устройствам на платформе GoogleAndroid.

Используемые средства связи – Wi-Fi-технологии либо технологии сотовой передачи данных посредством GPRS, EDGE, 3G, HSPA, LTE.

СТРУКТУРЫ ИНФОРМАЦИОННЫХ ПОТОКОВ

В современных КИС используются два основных типа клиентов, приведенных на рис. 1.

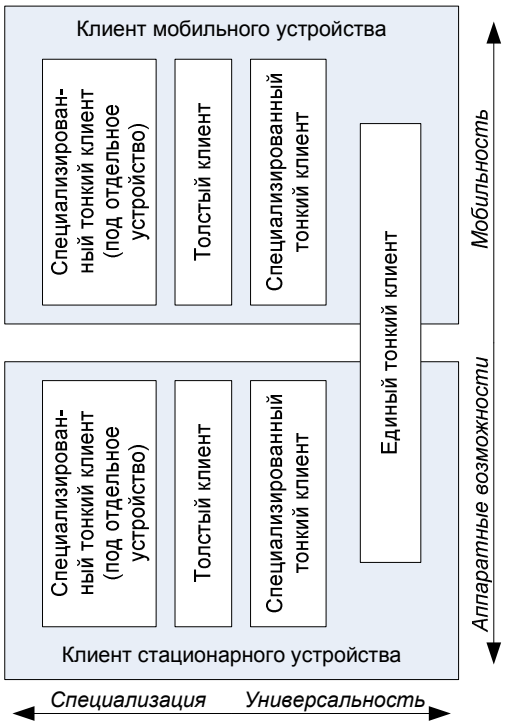

Рис. 1. Типы клиентов информационных систем

«Толстый» клиент, представляющий из себя программу, позволяющую работать с КИС и выполняющуюся на стороне клиента, характеризуется следующими достоинствами:

- возможность off-line-работы;
- лучшее использование аппаратных ресурсов (актуально для МУ);
- возможностью хранить информацию на устройстве, управлять и уничтожить при необходимости.

В случае отсутствия у злоумышленника толстого клиента подключение к серверу будет крайне затруднительно. Одновременно с этим он характеризуется следующими недостатками: специфичность (необходимость разработки под конкретную платформу или даже под конкретное устройство); сложность тестирования.

«Тонкий» клиент, представляющий из себя открываемую страницу в браузере и позволяющий работать с КИС, характеризуется универсальностью, но тем не менее, требует обеспечения совмести-мости для мобильных устройств. Наряду с этим ему присущи такие недостатки, как:

- необходимость адаптации под мобильные устройства;
- повышенные вычислительные затраты на стороне МУ;
- ограничения в выборе средств криптографической защиты.
- осуществление работы возможно только при наличии связи в on-line режиме.

Современные информационные системы реализуются на основе трехзвенной архитектуры (рис. 2), где нижний (первый) уровень ответственен за хранение данных системы, средний (второй) уровень отвечает за бизнес-логику информационной системы, а самый высокий (третий) уровень отвечает за взаимодействие с пользователем, то есть реализует интерфейс пользователя.

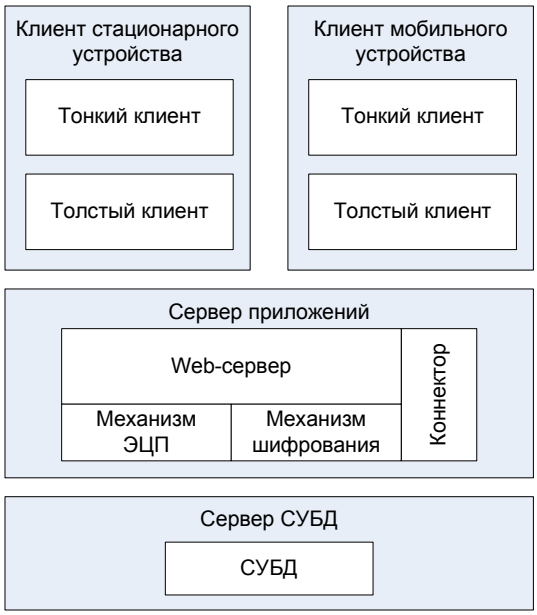

Рис. 2. Типовая архитектура информационных систем

Первый уровень трехзвенной архитектуры представлен системой управления базами данных (СУБД). Значимой функцией первого уровня является шифрование данных, хранимых в СУБД. Данная функция реализуется с помощью криптографических процедур. Наряду с ней используется механизм электронной цифровой подписи (ЭЦП), позволяющий фиксировать целостность хранимой документации. Она может быть полным аналогом собственноручной подписи должностного лица.

Второй уровень данной архитектуры представляет собой базу для реализации бизнес-логики работы КИС, ее функциональное наполнение. Именно эта часть архитектуры включает в себя модуль автоматизации документооборота. Очень важной компонентой среднего уровня являются интерфейсные коннекторы к другим операционным системам.

На первом уровне задача обеспечения информационной безопасности решается за счет:

- физической защиты цифровой обработки данных;
- организации корпоративной сети, использования межсетевых экранов;
- ограничения физического доступа, защиты от инсайдеров;
- осуществления резервного копирования информации;
- использования на уровне СУБД и ЭЦП типовых решений по обеспечению защиты информации.

На втором уровне для обеспечения информационной безопасности применяются сервер приложений и web-сервер. Здесь в большей степени безопасность информации обеспечивается грамотным построением КИС (установкой всех необходимых обновлений, закрытием портов, сменой паролей по умолчанию, отключением неиспользуемого функционала). Использование web-сервиса является достаточно новой частью информационной системы. Несмотря на наличие отработанных методов обеспечения информационной безопасности [5] для web-сервисов, простое заимствование этих методов в случае мобильного клиента не является оптимальной стратегией.

Третий уровень – это различные клиенты КИС (толстые и тонкие клиенты для стационарных и мобильных устройств). Обеспечение безопасности на третьем уровне заключается в защите среды передачи данных (шифрование, электронная подпись файлов), защите хранимых на устройстве данных (актуально для толстых клиентов), использование политик безопасности для клиентов.

Мобильные клиенты могут использоваться для работы с корпоративными web-сервисами. Этот подход может быть наиболее просто реализован [6]. Но при достаточно сложном функ-

ционале современных КИС, третий уровень архитектуры не может быть реализован только на тонких клиентах. В качестве причин этого можно указать:

1. Необходимость обеспечения возможности работы с КИС в off-line режиме (например, в самолете). Это может быть достигнуто только использованием толстых клиентов.

2. Ограничения мобильных клиентов в силу того, что они не поддерживают многие технологии (flash и др.).

3. Приложение в браузере требует заведомо большего процессорного времени, чем нативное приложение. Это приводит к увеличению времени эксплуатации МУ и канала информационного обмена.

4. Специфика решаемых задач (например, изображение векторной графики).

5. Малый размер МУ.

6. Низкая пропускная способность каналов связи.

Основные преимущества тонкого клиента – возможность обеспечить работу в off-line режиме, а также более гибкое управление информацией на устройстве (блокировка МУ в случае потери и др.).

МЕТОДИКА ВНЕДРЕНИЯ МОБИЛЬНЫХ УСТРОЙСТВ В ЗАЩИЩЕННЫЕ КОРПОРАТИВНЫЕ СИСТЕМЫ

Таким образом, можно предложить следующую методику внедрения МУ в КИС. Методика состоит из трех взаимосвязанных частей:

- выбор требований к модернизируемой КИС;
- реализация множества этапов внедрения МУ в работу КИС;
- проведение необходимых дополнительных работ.

Требования

Разработчик защищенной КИС с МУ должен выполнить следующий набор требований:

1. Использовать технологию «толстый клиент» с созданием нативного приложения под конкретную платформу.

2. Принять дополнительные меры по обеспечению безопасности устройства. Например, при помощи политик установления паролей, установки обновлений, запрета установки каких-либо посторонних программ и др.

3. Обязательное шифрование трафика во всех сетях (WiFi, GSM, LTE).

4. В случае если необходимо удостовериться в подлинности лица, работающего с системой, использовать технологию ЭЦП при помощи криптопровайдеров.

5. Обязательное ведение логов на серверной части действий клиента.

6. Проверка целостности информации при обмене данными, особенно в режиме off-line, обеспечение целостности информации, версионности.

7. Сведение к минимуму хранящейся на мобильном устройстве информации.

8. Шифрование всей корпоративной информации (в случае хранения ее на устройстве). Актуально для off-lineклиента.

9. Аутентификация пользователя, возможно, биометрически, либо иная двухфакторная авторизация (материальный носитель и пароль).

10. Резервирование устройств для обеспечения высокой надежности рабочих мест.

11. Ограничение доступа к данным клиента КИС, хранящимся в памяти устройства со стороны программ, сторонних программному обеспечению КИС.

12. Сжатие информации при передаче.

Этапы внедрения МУ

Для внедрения МУ в практику работы КИС необходимо последовательно осуществить следующие действия:

1. Построить списки имеющихся сертифицированных средств защиты информации для стационарных компьютеров.

2. Построить аналогичный предыдущему шагу список для МУ.

3. Выбрать алгоритмы шифрования и реализующего их программного обеспечения. Разработать способы обязательного шифрование сессий для работы с корпоративными ресурсами (электронной почтой, мессенджеры и т. д.);

4. Осуществить уничтожение контента, связанного с утерянными или украденными устройствами.

5. Сформулировать требования и осуществить установку парольной защиты, ввести практику регулярного обновления паролей и политик безопасности.

6. Разработать и внедрить практику блокировки устройства в случае их неиспользования.

7. Разработать способы (административные, программные и аппаратные) уничтожения информации на устройствах после определенного количества неудавшихся попыток разблокировки.

8. Осуществить защиту профайлов конфигурации КИС.

ЗАКЛЮЧЕНИЕ

Использование мобильных устройств в КИС является новым и перспективным средством для организации работы современных предприятий и организаций. Новизна их использования предполагает необходимость дополнительных научно-практических разработок в данной области. Можно сформулировать следующие направления дальнейших исследований, имеющих целью повышение информационной безопасности в со-временных КИС:

1. Разработка методики проверки и контроля совместимости обновлений программного обеспечения (чрезвычайно актуально для Android-устройств).

2. Выработка механизма взаимодействия в случае неустойчивой связи (успешно решается с помощью толстого клиента).

3. Создание платформонезависимого языка программирования для разработки программной реализации клиентов.

4. Разработка новых стандартов по обеспечению информационной безопасности эксплуатации МУ в КИС за счет повышения требований при помощи политик усиления безопасности.

5. Внедрение биометрической идентификации пользователей на МУ.

6. Организация практики хранения закрытого ключа на МУ (в карте памяти, внешнем контейнере, специальной Sim-карте).

7. Разработка методики использования криптопровайдера, сертифицированного ФАПСИ на конкретной платформе.

8. Расширение возможностей тонких и толстых клиентов (например, Android 4.0.3. и iOS не поддерживают популярную технологию «Flash»).

9. Создание методики автоматического управления корпоративными МУ (блокировка, стирание информации по запросу), регистрация сроков хранения информации.

10. Формализация требований к тонким клиентам: минимизация объема хранимой информации на МУ.

11. Защищенное сетевое соединение; логирование всех действий пользователя.

Использование предлагаемой методики, на ряду с решением в перспективе приведенных выше задач, позволит существенно повысить информационную безопасность КИС при их модификации современными МУ.

СПИСОК ЛИТЕРАТУРЫ

1. **Получено положительное заключение ФСБ России на ПК ViPNetClientiOS.** 2012. [Электронный ресурс].URL:http://www.infotecs.ru/press/news/15/7358 (дата обращения 10.10.2012).

2. **Digital Government: Building a 21st Century Platform to Better Serve the American People**. 2011. [Электронный ресурс]. URL:http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html (датаобращения 10.10.2012).

3. **ГОСТ Р ИСО/МЭК 27001-2006**. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2008. 32 с.

4. **ГОСТ Р ИСО/МЭК 15408-1-2008**. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. М.: Стандартинформ, 2008. 40с.

5. **Коржов, В.** Мобильные, но безопасные. — 2012. [Электронный ресурс]. URL: http://www.osp.ru/news/articles/2012/08/13012894(дата обращения 10.10.2012).

6. **Шепелявый Д**. Обеспечение безопасности Web-сервисов // Информационная безопасность. 2008. № 1.

ОБАВТОРАХ

Бабиков Александр Юрьевич, асс. каф. вычислительн. техники и защиты информации. Дипл. магистр техники и технологий (УГАТУ, 1999). Иссл. в обл. моделирования систем информационной безопасности.

Кардаш Денис Иванович, доц. той же каф. Дипл. инженер по вычислительн. машинам, комплексам, системам и сетям (УГАТУ, 1995). Канд. техн. наук по матем. и программн. обеспечению вычислительн. машин, комплексов и систем (УГАТУ, 2001). Иссл. в обл. систем искусственного интеллекта, интеллектуальн. отказоустойчивых систем управления, программн. обеспечения систем управления.

METADATA

Title: Features of using mobile devices in corporate information systems.

Authors: A.Y. Babikov[1], D. I. Kardash[2]

Affiliation:
[1,2] Ufa State Aviation Technical University (UGATU), Russia.

Email:[1]babikov@hotbox.ru.

Language: Russian.

Source: Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), Vol. 17, No. 2 (55), pp. 157-162,2013.ISSN 2225-2789 (Online), ISSN 1992-6502 (Print).

Abstract: Realization of information security organization for corporate information systems with use of mobile devices is discussed. The results of the analysis of vulnerabilitieslocations are given. The technique of mobile devices implementing uses security conditions.

Key words: Corporate information system; mobile device; information security; information system clients.

References (English Transliteration):

1. *The positive conclusion of the FSB Russia on PC ViPNet Client iOS*.(2012, Oct. 10),[Online], (in Russian), Available: http://www.infotecs.ru/press/news/15/
2. Digital Government: Building a 21st Century Plat-form to Better Serve the American People - 2011. [Online], (in Russian), Available: http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html.
3. *Information technology. Security techniques. Information security management systems. Requirements*, (in Russian),Federal standard R ISO/IEC 27001-2006, Moscow, Standatrinform, 2008.
4. *Information technology. Security techniques. Information security management systems. Evaluation Criteria for IT Security. Part 1: Introduction and general model*, (in Russian),Federal standard R ISO/IEC 15408-1:2008, Moscow, Standatrinform, 2008.
5. Korzhov, V(2012, Oct. 10) *Mobile but Secure*[Online],(in Russian), Available: http://www.osp.ru/news/articles/2012/08/13012894
6. Shepelyavy, D. *Securing Web-services* (in Russian), in "Information Security" No. 1, 2008.

About authors:

1. Babikov, Alexander Yuryevich, Assistant, Dept. of Computer Engineering and Information Security. Master of Technics& Technology (USATU, 1999).
2. Kardash, Denis Inanovich, Assoc. Prof., Dept. of Computer Engineering and Information Protection. (USATU, 1995). Cand. of Tech. Sci. (USATU, 2001).