УДК 391:519.7:510.5

Анпилогов С.С., Волошин А.Л.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ПЛАНШЕТНЫХ КОМПЬЮТЕРОВ APPLE IPAD2 ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Аннотация:

Рассмотрены штатные механизмы защиты информации планшетного компьютера Apple iPad2. Проведен анализ способности реализованных механизмов защитить конфиденциальную информацию пользователей планшетного компьютера Apple iPad2 при ее обработке, хранении или передаче в распределенных государственных или коммерческих организациях. Проанализирована возможность эффективного использования реализованных механизмов защиты в правовом поле Украины. Предложены пути практического применения планшетного компьютера Apple iPad2 для криптографической защиты конфиденциальной информации или построения комплексных систем защиты информации в информационно-телекоммуникационных системах разного целевого назначения.

Анотація:

Розглянуто штатні механізми захисту інформації планшетного комп'ютера Apple iPad2. Проведено аналіз спроможності реалізованих механізмів захистити конфіденційну інформацію користувачів планшетного комп'ютера Apple iPad2 при її обробці, зберіганні або передачі в розподілених державних або комерційних організаціях. Проаналізовано можливість ефективного використання реалізованих механізмів захисту в правовому полі України. Запропоновано шляхи практичного застосування планшетного комп'ютера Apple iPad2 для криптографічного захисту конфіденційної інформації або побудови комплексних систем захисту інформації в інформаційно-телекомунікаційних системах різного цільового призначення.

Abstract:

Considered established mechanisms to protect information tablet Apple iPad2. The analysis of the ability to implement mechanisms to protect the confidential information of users Tablet PC Apple iPad2 in its handling, storage or transmission of the distribution of public and commercial organizations. The possibility of effective use of protection mechanisms implemented in the legal field of Ukraine. The ways of the practical application of the Tablet PC Apple iPad2 for cryptographic protection of sensitive information, or build complex systems of information security in information and telecommunication systems of different purpose.

Введение

Бурное развитие информационных технологий не оставило без внимания государственный и корпоративный сектора, внеся большое разнообразие в средства вычислительной техники, мобильной связи, хранения данных и т.д. Большинство указанных технологий на сегодняшний день объединил в себе так называемый планшетный компьютер, – устройство, которое появилось на отечественном рынке не так уж давно, однако обладает довольно большой популярностью. Это связано как с широкой функциональностью этого изделия, так и с высокой эргономичностью и практическим удобством использования. Планшетные компьютеры по принципу практического использования принципиально отличаются от персональных компьютеров, поэтому многие аналитики относят планшетные компьютеры к устройствам так называемой

“посткомпьютерной” эпохи, которые проще и понятнее привычных персональных компьютеров и со временем могут вытеснить эти компьютеры с ИТ-рынка [1]. Исходя из этого, многие коммерческие организации рассматривают использование планшетных компьютеров в качестве штатных устройств обработки корпоративной информации. Как следствие этого, эти устройства в полном объеме могут быть задействованы для хранения и обработки конфиденциальной информации этих коммерческих компаний (в том числе, персональных данных сотрудников, бизнес-планов, отчетов о финансовой и хозяйственной деятельности). Это приводит к необходимости обеспечения защиты такой информации от несанкционированного доступа к ней злоумышленников (см, например, [2 – 4]), а отсутствие в доступной печати простых и понятных практических руководств по обеспечению защиты информации в планшетных компьютерах делает эту задачу достаточно нетривиальной.

Данная статья посвящена общему обзору механизмов защиты наиболее распространенного на сегодняшний день планшетного компьютера iPad2 производства компании Apple. Она не претендует на полное и исчерпывающее техническое описание реализованных механизмов защиты, а содержит лишь только их общую характеристику и основные принципы работы. Более детальное и конкретное описание тех или иных средств защиты информации заинтересованный читатель может получить на веб-сайте компании Apple (http://www.apple.com). Отдельное внимание уделено особенностям использования описанных механизмов защиты в рамках действующего законодательства Украины в сфере защиты информации.

1. Характеристика штатных механизмов защиты планшетного компьютера iPad2

На отечественном рынке планшетный компьютер iPad2 представлен двумя модельными модификациями – с 3G модулем и без него, а также с различным объёмом памяти (16, 32, 64 Гб). Устройство iPad2 работает под управлением операционной системы iPhone Operating System (iOS) версии 4.3.5 (build 8L1).

Однако какой бы объем памяти не поддерживал компьютер iPad2 (16, 32, 64 Гб), в любом случае в ней может храниться большой объём информации с ограниченным доступом, будь то персональные данные или конфиденциальная информация организации или предприятия. Без принятия мер безопасности в случае утери или кражи устройство iPad2 сможет предоставить посторонним людям полный доступ к электронной переписке, контактам, расписанию календаря, фотографиям и видео, да и любым другим файлам, хранящимся в памяти.

Для обеспечения надлежащего уровня безопасности необходимо правильно настроить устройство в соответствии с принятой в организации политикой безопасности информации. Не отличаясь особо в этом плане от других устройств вычислительной техники, безопасность на компьютере iPad2 – это баланс между удобством использования и степенью защищенности от несанкционированного доступа. То есть, чем удобнее пользоваться устройством, тем меньшую защиту оно обеспечивает. Однако это устройство при всей своей высокой эргономичности способно обеспечить достаточно высокий уровень безопасности конфиденциальной информации. Так, оно реализует механизмы шифрования данных при передаче через незащищенную среду, использует механизмы аутентификации пользователей для доступа к хранимой информации, а также

обеспечивает шифрование всех данных в памяти устройства. Изделие iPad2 также обеспечивает защиту от несанкционированного доступа с использованием пароля доступа, который к тому же может быть установлен удаленно. И если устройство попадет в чужие руки, пользователи или ИТ-администраторы могут инициировать команду удаленного стирания всей информации, хранящейся в его памяти. Перейдем к более подробному рассмотрению механизмов защиты устройства iPad2.

Профили безопасности устройства

Прежде всего, необходимо отметить, что пользовательская настройка механизмов защиты изделия iPad2 возможна как путем индивидуальной настройки устройства, так и применения (настроенного ранее) профиля конфигурации. Профили конфигурации могут быть применены на устройстве iPad2 двумя путями: удаленно и локально [5 – 7].

Для реализации *удаленного варианта* применения профилей конфигурации необходимо, чтобы устройство было настроено для обмена данными с серверами Microsoft Exchange, Exchange ActiveSync и синхронизировалось с ними по беспроводному протоколу [8]. В этом случае применение профиля безопасности осуществляется автоматически без участия конечного пользователя. В *локальном варианте* применение профилей конфигурации осуществляется при помощи приложения iTunes. Это приложение входит в штатный комплект прикладного программного обеспечения устройства iPad2 и предназначено для синхронизации устройства с персональным компьютером.

При необходимости профиль конфигурации может содержать требования по возможности удаления используемого профиля только при наличии административных прав, а также запрещать удаление действующего профиля без полного стирания содержимого памяти устройства.

Настройки профиля безопасности хранятся в XML-файле, который в частности содержит ограничения на использование прикладного программного обеспечения, настройки протоколов обмена данными Virtual Private Network, Wi-Fi, учетные записи электронной почты, учетные данные для работы iPad2 с корпоративными программными системами. Профиль безопасности при необходимости может быть защищен от несанкционированного доступа. Для этого используются механизмы электронной цифровой подписи и шифрования в порядке, определенном в IETF RFC 3852 [9]. В частности, для шифрования информации применяются широко распространенные за рубежом криптографические алгоритмы шифрования 3DES и AES-128.

Настройки ограничений на использование прикладного программного обеспечения позволяют ограничить круг приложений (и, как следствие, возможных функций), доступных пользователю устройства iPad2. Управляя этими ограничениями, можно определить набор доступных пользователю функций. Как правило, эти ограничения связаны с использованием сетевых приложений, таких как Safari (веб-браузер), YouTube (клиент сервера хранения видеофайлов) и iTunes Store (клиент сервера доступных приложений Apple). Этими ограничениями также можно контролировать ряд других действий, например, наложить запрет на установку пользовательских приложений. Дополнительно к указанным ограничениям возможно настроить приложение iTunes для запрета доступа к данным, необходимым для обновления и установки приложений.

Защита данных, хранимых в памяти компьютера

Совместно с шифрованием данных, передающихся через незащищенную среду, изделие iPad2 обеспечивает шифрование данных, хранящихся в его памяти [5, 7].

В устройстве применяется аппаратное шифрование с использованием криптографического алгоритма шифрования AES-256. Механизмы шифрования всегда включены и не могут быть отключены пользователем. Кроме того, также может быть зашифрована и резервная копия данных, создаваемая приложением iTunes. Для защиты данных, обрабатываемых приложениями сторонних разработчиков, изделие iPad2 поддерживает соответствующий программный интерфейс, позволяющий разработчикам использовать указанные встроенные аппаратные средства шифрования. Также устройство iPad2 поддерживает возможность использования криптографических алгоритмов шифрования AES (с разными длинами ключей), RC4 и 3DES. Аппаратная реализация алгоритма шифрования AES и алгоритма хеширования SHA1 позволяет значительно увеличить производительность использующих их приложений.

Если устройство iPad2 потеряно или украдено, администратор корпоративной сети или владелец устройства может осуществить удаленное стирание данных и отключить устройство. Под удалением данных в этом случае понимается удаление ключа шифрования, которым зашифрованы данные, хранящиеся в памяти устройства. После этого все зашифрованные данные становятся недоступны. Если устройство iPad2 настроено на обмен данными с серверами Microsoft Exchange, Exchange ActiveSync, администратор корпоративной сети может послать команду удаленного стирания с помощью консоли управления Exchange (Exchange Server 2007) или веб-инструмента мобильного администрирования Exchange ActiveSync (Exchange Server 2003 или 2007). Пользователи сервера Exchange Server 2007 могут также осуществить удаленное стирание данных непосредственно с помощью приложения Outlook Web Access [6, 7].

Устройство iPad2 также можно настроить для автоматического удаления данных после определенного количества неудачных попыток ввода пароля доступа. Максимальное количество таких неудачных попыток ограничено десятью. Этот механизм служит надежной защитой против попыток подбора пароля с целью получить доступ к устройству. По умолчанию в изделии iPad2 используется простой цифровой пароль (4 цифровых символа), но при желании пользователь может настроить изделие на использование более сложного буквенно-цифрового пароля произвольной длины, что существенно уменьшает риск его подбора.

Ко всему прочему пользователь может установить период времени, после которого при отсутствии активности с его стороны происходит автоматическая блокировка устройства. Время простоя может быть задано в широких пределах, но маленький интервал будет доставлять неудобства (пользователь вынужден будет постоянно вводить пароль), а большой интервал времени будет бесполезен.

Защита каналов связи

Устройство iPad2, являясь планшетным компьютером, поддерживающим беспроводные технологии связи, предоставляет возможность пользователям получить доступ к корпоративным сетям из любой точки мира. Часто при этом передается конфиденциальная информация, поэтому защита этой информации при передаче через незащищенную среду очень важна для пользователей. Идя навстречу таким пожеланиям, изделие iPad2 предлагает защищенные технологии обмена данными в Wi-Fi и сотовых (3G) сетях передачи данных [5, 7].

На сегодняшний день во многих корпоративных средах используются технологии виртуальных частных сетей (virtual private network (VPN)). Изделие iPad2 интегрируется с широким спектром часто используемых VPN-технологий за счет поддержки сетевых протоколов IPSec, L2TP и PPTP. Поддержка этих протоколов обеспечивает высокий уровень IP-шифрования для передачи конфиденциальной информации. Устройство iPad2 позволяет осуществлять обмен данными через сетевые прокси-серверы, а также разделение туннелированного IP-трафика общественных или частных сетевых доменов.

Кроме того, для безопасного доступа к использованию VPN-технологий изделие iPad2 использует надежные методы аутентификации пользователей. Проверка подлинности осуществляется с использованием сертификатов открытых ключей, соответствующих требованиям X.509. Это позволяет предоставить пользователям упрощенный доступ к информационным корпоративным ресурсам и является жизнеспособной альтернативой использованию аппаратных идентификаторов (токенов). Также эти сертификаты открытых ключей позволяют пользователю устройства iPad2 воспользоваться технологией VPN On Demand, что делает процесс аутентификации прозрачным и в то же время обеспечивает защищенный доступ к соответствующим сетевым службам [8].

Для корпоративных систем, требующих двухфакторной аутентификации, устройство iPad2 может быть интегрировано с платформами RSA SecurID и CRYPTOCard.

Дополнительно изделие iPad2 поддерживает защищенные протоколы обмена данными SSL (версии 3) и TLS (версии 1), широко использующиеся на сегодняшний день для защиты данных, передающихся в сети Интернет. Прикладное программное обеспечение изделия (в частности, веб-браузер Safari, календарь, клиент электронной почты) использует эти механизмы в автоматическом порядке для организации зашифрованного канала связи между изделием iPad2 и соответствующими корпоративными серверами.

Для защищенного доступа к беспроводным Wi-Fi-сетям и аутентификации устройство iPad2 поддерживает технологию WPA2. Эта технология обеспечивает шифрование передаваемой информации (в том числе, паролей доступа) с использованием криптографического алгоритма AES-128. Поддержка устройством протокола аутентификации, определенного в IEEE 802.1x, позволяет легко применять его в широком диапазоне устройств, использующих протокол аутентификации RADIUS.

Безопасность операционной системы

Операционная система iPhone OS (iOS), используемая в устройствах iPad2, ориентирована на использование механизмов безопасности на уровне ядра [7]. Так, система предполагает «изолированный» подход к запуску приложений, поэтому работающие приложения не могут получить доступ к данным других приложений. С точки зрения безопасности такой метод разграничения доступа к данным для процессов достаточно эффективен. В то же время для конечного пользователя этот подход неудобен в связи с тем, что для предоставления некоторому приложению доступа к файлу другого приложения необходимо сначала сопоставить этот файл такому приложению с использованием приложения iTunes. Операционная система iOS обеспечивает недоступность системных файлов, ресурсов и самого ядра для пользовательских приложений.

Для защиты установленных приложений от модификации, а также от использования нелегитимного («пиратского») программного обеспечения в операционной системе используются механизмы проверки электронной цифровой подписи на устанавливаемых программных продуктах. Так, приложения, входящие в комплект поставки, подписываются электронной цифровой подписью компании Apple. Приложения сторонних разработчиков подписываются электронной цифровой подписью их разработчиков, проверка этой подписи осуществляется с использованием сертификатов открытых ключей, выпущенных компанией Apple. Это гарантирует, что устанавливаемые приложения не были подделаны или модифицированы злоумышленником. Кроме того, проверка электронной цифровой подписи проводиться каждый раз перед запуском приложения. Это позволяет убедиться в том, что приложение не было модифицировано с момента его последнего запуска. Система iOS имеет защищенную логическую структуру, которая обеспечивает хранение учетных данных пользователя в приложениях и сетевых службах в зашифрованном виде.

Тем не менее, допускается использование пользовательских или самостоятельно разработанных приложений. Для этого разработчик прикладного программного обеспечения должен являться членом интернет-сообщества iDP (iPhone Developer Portal). Подписав с помощью специально разработанной утилиты Provisioning profile разработанное приложение, разработчик получает возможность его запуска и отладки на устройстве iPad2.

2. Известные уязвимости планшетного компьютера iPad2

Несмотря на наличие разнообразных описанных выше механизмов защиты, устройство iPad2 обладает своими уязвимостями. Здесь не рассматриваются угрозы, связанные с человеческим фактором (короткой длиной пароля, отсутствием пароля вообще, утерей/кражей устройства злоумышленниками и так далее), а внимание уделяется возможностям обхода механизмов защиты, не зависящих от пользователя.

Единственным известным на сегодняшний день способом программного взлома устройство iPad2 является так называемый джейлбрейк (англ. jailbreak). Сущность этого способа заключается в локальной или удаленной модификации прошивки устройства, после которой пользователи и прикладное программное обеспечение получают полный доступ к его файловой системе. Использование джейлбрейка позволяет устанавливать прикладное программное обеспечения без проверки его целостности и аутентичности (в обход механизмов электронной цифровой подписи, описанных в п. 1.4).

Не останавливаясь на деталях практического применения джейлбрейка (а заинтересованный читатель может получить пошаговое руководство по его практическому осуществлению, например, в материалах [10]), отметим только, что на сегодняшний день известно два типа джейлбрейка (используется терминология, принятая в соответствующих интернет-сообществах):

- привязанный джейлбрейк (требуется применять джейлбрейк каждый раз заново после перезагрузки устройства iPad2, при этом установленные приложения переустанавливать не надо);
- отвязанный (как противоположность привязанному) джейлбрейк (отсутствует необходимость повторного применения джейлбрейка).

В настоящее время отвязанный джейлбрейк реализован для iOS до версии 4.3.3 включительно. Для более новых версий операционных систем пока реализован лишь привязанный джейлбрейк [11].

Судя по доступной информации, на данный момент ведущими интернет-сообществами активно ведутся работы по взлому системы iOS версии 5.x и реализации отвязанного джейлбрейка [12, 13]. Учитывая печальную статистику по взлому предыдущих версий этой операционной системы, приходится констатировать, что преодоление механизмов защиты пятой версии этой системы является только вопросом времени.

3. Особенности применения планшетного компьютера iPad2 для защиты информации в правовом поле Украины

Исходя из изложенного выше, можно констатировать, что устройство iPad2 имеет широкий набор механизмов защиты, позволяющих обеспечить защиту как пользовательских данных при хранении их в памяти устройства, так и информации, передающейся по незащищенным каналам связи между устройством и соответствующими корпоративными серверами. Это свидетельствует о возможности эффективного применения данного изделия для защиты конфиденциальной информации и информации, необходимость защиты которой установлена законодательством, в том числе при построении комплексных систем защиты информации в распределенных корпоративных информационно-телекоммуникационных системах.

При этом, однако, необходимо учитывать требования действующих в Украине нормативно-правовых актов в сфере криптографической и технической защиты информации, определяющих порядок применения с целью обеспечения безопасности информации тех или иных механизмов защиты.

Так, *Положение о порядке разработки, производства и эксплуатации средств криптографической защиты информации*, утвержденное приказом Администрации Госспецсвязи Украины от 20.07.2007 № 141 (с изменениями), разрешает к применению для криптографической защиты информации только средства, имеющие сертификат соответствия или положительное экспертное заключение по результатам государственной экспертизы в сфере криптографической защиты информации ([14, п. 4.1]). Аналогично обстоит ситуация в сфере технической защиты информации. Так, *Правила обеспечения защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах*, утвержденные постановлением Кабинета Министров Украины от 29.03.2006 № 373, обязывают использовать при построении комплексных систем защиты информации средства защиты информации с подтвержденным соответствием ([15, п. 21]). По данным веб-сайта Государственной службы специальной связи и защиты информации (www.dstszi.gov.ua), регулярно публикующего перечни криптосредств и средств технической защиты информации, прошедших сертификацию или государственную экспертизу, изделие iPad2 на момент подготовки статьи не имело ни одного из указанных документов.

Более того, организации, желающей взять на себя труд организовать проведение одной из приведенных процедур подтверждения соответствия, следует помнить о том, что в средствах криптографической защиты информации должны применяться криптографические алгоритмы и протоколы, являющиеся национальными стандартами Украины или рекомендованные Администрацией Госспецсвязи ([14, п. 2.12]). Ни один из

перечисленных выше криптографических алгоритмов шифрования (3DES, AES), к сожалению, к таковым не относится. Этот факт играет очень важную роль при построении комплексных систем защиты информации, так как согласно принятой практике, использование в указанных системах средств криптографической защиты, реализующих иностранные криптоалгоритмы, не допускается.

Немало практических вопросов вызывает и применение устройства iPad2 для защиты информации от несанкционированного доступа. Так, данное устройство содержит весьма упрощенные (по сравнению с операционными системами «классических» электронно-вычислительных машин) механизмы управления пользователями и их правами доступа. В частности, здесь нет привычных пользователю операционных систем семейства Microsoft Windows механизмов регистрации в одной системе нескольких пользователей и управления правами их доступа, например, к объектам файловой системы. Нет также классического разделения пользователей на группы административных и обычных пользователей. Указанные особенности делают неприменимыми ряд положений нормативных документов системы технической защиты информации (в частности, [16, 17]), касающихся, как минимум, обеспечения конфиденциальности и целостности пользовательских данных. Вообще, тема соответствия механизмов защиты устройства iPad2 требованиям нормативных документов системы технической защиты информации в Украине является достаточно глубокой и требует дополнительного изучения. В силу ограничений на объем авторы планируют детально раскрыть указанные вопросы в отдельной статье. Здесь же следует ограничиться декларацией обеспокоенности авторов относительно правомочности применения описанного выше набора механизмов защиты устройства iPad2.

Чтобы ситуация не казалась читателю настолько безнадежной, в заключение отметим, что описанные выше механизмы защиты являются штатными (базовыми) средствами изделия iPad2. Это означает, что заинтересованная организация может заказать разработку (или разработать своими силами) прикладное программное обеспечение, отвечающее требованиям отечественной нормативной базы в сфере защиты информации. Это, в частности, касается и криптографических алгоритмов (протоколов), и прохождения сертификации (государственной экспертизы в сфере криптографической и/или технической защиты информации), и выделения ролей администратора и пользователей, и управления правами пользователей по доступу к защищаемой информации. Примером для разработчика таких специализированных приложений могут служить известные системы защиты информации от несанкционированного доступа серии «Гриф», «Лоза», «Рубеж», а также криптографические системы защиты сетевых соединений класса «Криптосервер», «CryptoLink» и другие.

Только в этом случае, на наш взгляд, возможно полноценное (и, как следствие, эффективное) легитимное использование устройства iPad2 в государственном и корпоративном секторах Украины.

Выводы

Широкий набор функций, удобный и понятный пользователю графический интерфейс, малые массо-габаритные показатели определили большую популярность устройства iPad2 в сегменте ИТ-устройств современного отечественного и международного рынков. Однако при широком внедрении подобных устройств не следует забывать о необходимости защиты информации, обрабатываемой, передаваемой и

хранимой в этих изделиях. Наличие широкого спектра штатных механизмов защиты информации в устройстве iPad2 предполагает возможность эффективного решения задачи его интеграции в защищенные распределенные корпоративные информационно-телекоммуникационные системы. Однако попытка анализа соответствия характеристик механизмов защиты этого изделия требованиям отечественной нормативной базы в сфере защиты информации вызывает серьезные опасения по поводу широкого применения этих устройств как с целью защиты информации от несанкционированного доступа, так и с целью криптографической защиты передаваемых через незащищенную среду данных. Возможным путем решения этой проблемы является разработка прикладного программного обеспечения, отвечающего требованиям действующего законодательства (см., например, [16, 17]), и последующее проведение его государственной экспертизы в сфере криптографической и/или технической защиты информации.

Детальному анализу соответствия штатных механизмов защиты устройства iPad2 от несанкционированного доступа требованиям отечественных нормативных документов системы технической защиты информации авторы планируют посвятить отдельную статью.

Литература:

1. *iPad*. Руководство пользователя для программного обеспечения iOS 4.2 [Электронный ресурс] // Режим доступа: http://manuals.info.apple.com/ru_RU/iPod_touch_iOS4_User_Guide_RS.pdf. – Название с экрана.

2. *Закон* Украины “Об информации” // Відомості Верховної Ради України. – 1994. – № 16.

3. *Закон* Украины “О защите информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах” // Відомості Верховної Ради України. – 1994. – № 31.

4. *Правила* обеспечения защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах, утвержденные постановлением Кабинета Министров Украины от 29.03.2006 № 373 // Офіційний вісник України. – 2006. – № 13.

5. *Horwath J.* iPad Security Settings And Risk Review For iOS 4.X / J. Horwath [Электронный ресурс] // Режим доступа: http://www.sans.org/reading_room/whitepapers/apple/ipad-security-settings-risk-review-ios-4x_33826. – Название с экрана.

6. *Bradley T.* 30 days with the iPad / T. Bradley [Электронный ресурс] // Режим доступа:http://www.pcworld.com/businesscenter/article/234994/30_days_with_the_ipad.html. – Название с экрана.

7. *iPad* in Business Security Overview [Электронный ресурс] // Режим доступа: http://www.apple.com/ipad/business/docs/iPad_Security.pdf. – Название с экрана.

8. *iPhone* OS. Enterprise Deployment Guide. Second Edition, for Version 3.2 or later [Электронный ресурс] // Режим доступа: http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf. – Название с экрана.

9. *IETF* RFC 3852. Cryptographic Message Syntax (CMS) [Электронный ресурс] // Режим доступа: http://www.ietf.org/rfc/rfc3852.txt. – Название с экрана.

10. *Джейлбрейк* своїми руками [Электронный ресурс] // Режим доступа: http://jailbrake.ru. – Название с экрана.

11. *iPad* [Электронный ресурс] // Режим доступа: http://ru.wikipedia.org/wiki/IPad. – Название с экрана.

12. *Непривязанный* джейлбрейк iOS 5 готов? [Электронный ресурс] // Режим доступа: http://ukrainianiphone.com/10/10/2011/38693. – Название с экрана.

13. *Jailbreak* iOS 5 на Windows с помощью Sn0wbreeze 2.8. Инструкция [Электронный ресурс] // Режим доступа: http://www.macdigger.ru/iphone-ipod/jailbreak-ios-5-na-windows-s-pomoshhyu-sn0wbreeze-2-8-instrukciya.html. – Название с экрана.

14. *Положение* о порядке разработки, производства и эксплуатации средств криптографической защиты информации, утвержденное приказом Администрации Госспецсвязи Украины от 20.07.2007 № 141 (с изменениями).

15. *Нормативный* документ системы технической защиты информации «НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», утвержден приказом Департамента специальных телекоммуникационных систем и защиты информации Службы безопасности Украины от 28.04.1999 № 22.

16. *Нормативный* документ системы технической защиты информации «НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу», утвержден приказом Департамента специальных телекоммуникационных систем и защиты информации Службы безопасности Украины от 28.04.1999 № 22.