Инсайдерские угрозы мобильной консьюмеризации ИТ и защита от них

Оглавление:

Введение

Проникновение потребительской электроники и программных продуктов в корпоративные информационно-вычислительные системы является одной из основных тенденций современных ИТ, влияние которой на уровень инсайдерских угроз корпоративной ИБ в ближайшей перспективе принципиально возрастет.

Развитие этого процесса **консьюмеризации** корпоративных информационных технологий (ИТ), как окрестил его Дуглас Нил из Computer Sciences Corporation[1], и его важнейшего аспекта – использования в бизнесе персональных мобильных устройств: смартфонов, КПК и завтрашних «Мобильных Интернет Устройств» (Mobile Internet Devices) – определяются воздействием нескольких ключевых факторов:

- прогресса микроэлектронных, а также телекоммуникационных технологий;
- опережающего развития потребительской электроники;
- определяющего социального явления – прихода в корпоративный бизнес подросшего поколения «Цифровых Аборигенов» (Digital Natives)[2].

Воспитанное на компьютерных играх, виртуальной Интернет-реальности и изощренное в использовании электронных новинок это поколение продвигается сегодня на все уровни корпоративной иерархии, включая руководство, и внедряет в практику бизнеса свои «ширпотребовские» компьютерные привычки и инструментарий (gadgets), при этом *фундаментально трансформируя* концепции управления и способы организации корпоративных ИТ.

---

[1] "On the Edge: Exploring Next-Generation Digital Disruptions", Computer Sciences Corporation, May 6, 2002 (http://www.csc.com/newsandevents/news/1750.shtml)

[2] "On the Horizon", NCB University Press, Vol. 9 No. 5, October 2001, Marc Prensky (http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf)

Для мировой индустрии ИБ это означает, что в ближайшие 2-3 года следует ожидать значительных изменений в методах управления и средствах реализации корпоративной информационной безопасности (ИБ), связанных с кардинальным ростом производительности и функционала персональных мобильных устройств и соответствующим изменением профиля угроз безопасности информации. Чтобы успешно отражать эти новые угрозы, отрасль должна создать эффективные решения для каждого аспекта ИБ оконечных вычислительных устройств (Endpoint Security).

Мобильный аспект консьюмеризации ИТ

Если оценивать «аппаратную» сторону консьюмеризации ИТ, то совершенно очевидно, что ее основным акселератором станут именно персональные мобильные устройства. Несмотря на довольно ограниченный набор корпоративных мобильных приложений (электронная почта, чаты, реже – мониторинг присутствия), смартфоны и КПК уже доказали свою эффективность не только для личного использования, но и как средство повышения производительности труда. Например, согласно результатам обзора “Mobile Messaging Market Trends, 2007-2010", опубликованного исследовательской компанией Osterman Research, в прошлом году в Северной Америке 15% всех сотрудников компаний использовали в своей работе мобильные устройства[3]. Результаты опроса ИТ-профессионалов американского корпоративного сектора на web-портале TechTarget позволяют уже в 2008 году прогнозировать рост этого показателя до 25%[4].

Дальнейшее ускорение корпоративной «мобилизации» обусловлено несколькими факторами:

- Во-первых, закон Мура продолжает действовать, что наглядно подтвердила выставка потребительской электроники 2008 International Consumer Electronics Show в Лас-Вегасе[5], где компания Интел анонсировала 16 новых процессорных чипов на базе 45-наномикронной технологии.

- Во-вторых, мир вступает в эпоху повсеместных высокоскоростных беспроводных коммуникаций, сочетающих глобальную популярность Wi-Fi с быстрорастущей инфраструктурой коммерческих мобильных сетей 3-го поколения 3G/HSPA, насчитывающей более 160 операторов в 73 странах[6]. Принципиально ускорит этот процесс «инъекция» мобильного WiMAX, приготовленная компанией Интел для всех ноутбуков на базе их новой платформы Montevina, что к 2010 году обеспечит 750 миллионам их владельцев[7] готовность к мобильному высокоскоростному доступу в Интернет.

- В-третьих, вторжение Intel на рынок однокристальных вычислительных систем (System-On-Ship) с их чипом Moorestown, обладающим уникальной производительностью и на порядок меньшим энергопотреблением по сравнению с существующими аналогами, по сути, заставит разработчиков мобильных ОС стандартизовать и консолидировать индустрию, тем самым создав условия для бурного развития корпоративных прикладных программ для мобильных устройств. Новое поколение однокристальных систем действительно сделает мир

---

[3] "Mobile Messaging Market Trends, 2007-2010", Osterman Research, Inc., October 2007 (http://www.ostermanresearch.com/or_mm07es.pdf)
[4] "Mobile phone beats out smartphone as device of choice", Copyright: 2007 TechTarget (http://searchmobilecomputing.techtarget.com/originalContent/0,,sid40_gci1278692,00.html)
[5] CES 2008: Intel Debuts 16 New Processors Based on 45nm Silicon Technology http://blog.wired.com/gadgets/2008/01/ces-2008-intel.html
[6] Official HSPA web-site (http://hspa.gsmworld.com/networks/)
[7] http://www.wimax-vision.com/newt/l/wimaxvision/article_view.html?artid=20017463390

«ультрамобильным» вне зависимости от того, под управлением какой мобильной ОС он будет «работать» – Windows XPe, Ubuntu, Mac OS X, Android, или Windows Mobile.

Угрозы мобильной консьюмеризации

Нет сомнений в том, что консьюмеризация корпоративных ИТ скоро сделает «мобильной» большую часть работников, каждый из которых будет использовать либо личное, либо «казенное» мобильное устройство. И, весьма возможно, предложенная компанией Yankee Group для условий консьюмеризации Дзэн-подобная модель *кооперативного* управления ИТ-процессами[8] действительно окажется оптимальной для повышения производительности труда.

Однако, с точки зрения информационной безопасности, задача управления поведением работников в условиях использования приложений на базе социальных сетей или потребительской электроники, очевидно, не может основываться на созерцании и постижении, поскольку просто нереалистично ожидать *кооперативного поведения* и *самодисциплины* от халатных, забывчивых или, хуже того, злонамеренных сотрудников.

Неисправимый «человеческий фактор» многократно усугубляется техническим прогрессом: ведь те же самые технологические достижения, которые определяют прогресс консьюмеризации, одновременно ведут к резкому росту рисков ИБ, поскольку создают предпосылки для развития таких негативных процессов, как разработка вредоносного мобильного ПО и – что еще более насущно – ***рост утечек конфиденциальной корпоративной информации через персональные мобильные устройства работников***.

«Дорожная карта» мобильного malware

Типичный размер флэш-памяти современных мобильных устройств (4-8GB) уже достаточен для хранения и работы стандартных операционных систем (ОС). Значительное повышение их производительности с одновременным снижением на порядок энергопотребления, связанное с выпуском компанией Интел ее нового чипа Moorestown, уже запустило цепную реакцию развития индустрии мобильных ОС и корпоративных приложений.

Этот быстрый процесс, в свою очередь, сделает прибыльной разработку *коммерческих* вредоносных программ для мобильных устройств. Из сегодняшнего «прототипного» состояния эта отрасль киберпреступности перейдет к поставке «продуктов коммерческого качества», увеличив таким образом вероятность атак на мобильные устройства и их заражения, как минимум, до уровня современного персонального компьютера (ПК), напрямую подключенного к Интернет.

Насколько скоро это станет реальностью, зависит, прежде всего, от сфокусированности производителей мобильных ОС на развитии их потенциально огромного рынка. Маловероятно, однако, что реальные проблемы начнутся мгновенно, поскольку «целевой рынок» для коммерческих вредоносных программ должен развиться до уровня, достаточного для того, чтобы оправдать вложения в их разработку. В этой связи значимых событий в данной области следует ожидать не ранее второй половины 2009 года.

[8] "Zen and the Art of Rogue Employee Management", Yankee Group, August 6, 2007 (http://www.yankeegroup.com/pressReleaseDetail.do?actionType=getDetailPressRelease&oldId=24)

Утечка данных через мобильные устройства

С другой стороны, нарастающая угроза утечек корпоративных данных через персональные мобильные устройства неизбежна и насущна.

Неизбежна, поскольку определенные стороны человеческой натуры не переделать: никуда не денутся случайные ошибки, халатность и злой умысел. Кроме того, терять и красть смартфоны и КПК в будущем тоже будут.

Насущна эта угроза потому, что реальна прямо сейчас, а новые технологии ее многократно умножат. Именно поэтому готовность к ее отражению столь важна уже сейчас.

Каков же масштаб этой угрозы сегодня, когда ИТ консьюмеризация только начинается? Ситуация с информационной безопасностью мобильных устройств неутешительна:

- По оценкам исследовательской компании In-Stat[9] только в США в 2007 году пропало более 8 млн. мобильных телефонов. Что же касается владельцев смартфонов, то для них – как правило, в большей степени допущенных к конфиденциальной информации – вероятность пропажи мобильного устройства на 40% выше.

- Очередное – 2007 года – обследование компьютерной преступности и безопасности "2007 CSI Computer Crime and Security Survey", проведенное Computer Security Institute[10] и FBI, выявило, что причиной 7% общего размера финансового ущерба американских корпораций из-за инцидентов ИБ стала потеря персональных или конфиденциальных данных в результате краж мобильных устройств.

- Согласно статистике[11] британского Министерства внутренних дел, 2% индивидуальных владельцев мобильных телефонов ежегодно становятся жертвами телефонных воров.

Проекция этой сегодняшней статистики на прогнозы роста рынка мобильных устройств[12], сделанные Тимом Бояриным (Tim Bajarin), президентом компании Creative Strategies, заставляет сделать вывод об опасной перспективе дальнейшего роста проблем корпоративного сектора с информационной безопасностью мобильных устройств: около 5 млн. смартфонов будут утеряны или похищены в 2008 году, а к 2010 году эта цифра возрастет до 14 млн, что станет причиной, соответственно, 14% и 21% общих финансовых потерь корпоративного бизнеса от всех типов инцидентов в области ИБ.

Механика «мобильных» утечек

В общем случае, утечка данных через мобильное устройство является двухэтапным процессом:

(1) сначала данные неконтролируемым образом передаются с информационного ресурса на корпоративном сервере или ПК на мобильное устройство;

---

[9] In-Stat research “Mobile Security 2007: End Users Are Losing It” (#IN0703622MBM) (http://www.instat.com/abstract.asp?id=229&SKU=IN0703622MBM);
“Mobile Security Still a Misunderstood Issue”, Hardware Zone, 27 April 2007 (http://hardwarezone.co.th/news/view.php?id=7153&cid=5)

[10] "2007 CSI Computer Crime and Security Survey", September 13, 2007, Computer Security Institute (http://www.gocsi.com/forms/csi_survey.jhtml)

[11] “Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey” (http://uk.sitestat.com/homeoffice/homeoffice/s?rds.hosb1007pdf&ns_type=pdf&ns_url=%5Bhttp://www.homeoffice.gov.uk/rds/pdfs07/hosb1007.pdf%5D)

[12] Creative Strategies (http://www.creativestrategies.com/downloads.php); “Tech Predictions for 2008”, PC Magazine, 28.12.2007 (http://www.pcmag.com/article2/0,2704,2241562,00.asp)

(2) затем эти данные бесконтрольно «уходят» с этого устройства куда-то наружу.

Соответственно, для борьбы с таким двухэтапным процессом существующие решения по защите от утечек данных (Data Leakage Prevention – DLP) строятся как два слоя компонентов:

(1) Первый слой включает DLP-компоненты на серверах, ПК или установленных в сети выделенных аппаратных комплексах, которые предотвращают утечку данных с корпоративных ресурсов на мобильные устройства посредством перехвата и фильтрации данных во всех используемых коммуникационных каналах.

(2) Второй слой состоит из средств защиты информации (СЗИ), работающих *резидентно* на мобильных устройствах и предотвращающих утечку данных с этих устройств.

Резидентные DLP-компоненты мобильных устройств

Анализ функций современных СЗИ, резидентно работающих на мобильных устройствах, приводит к выводу, что сегодня существует единственный *действительно эффективный* механизм защиты от утечек их данных: это криптографические средства, обычно реализуемые по технологии полного шифрования диска и – реже – файлового шифрования или шифрования виртуальных дисков. Такие средства блокируют доступ к любым данным в зашифрованной встроенной памяти и на съемных флэш-картах украденных или потерянных мобильных устройств.

Несмотря на стремление некоторых производителей представить технологию «удаленного уничтожения данных» (*remote data wiping*) как еще один надежный механизм защиты от утечек, на самом деле, на это решение нельзя полагаться, потому что первое, что сделает любой охотник за информацией со смартфоном, это выключит его и вынет карту памяти для чтения на другом устройстве, куда сигнал из корпоративного центра о «полной терминации» данных поступить не сможет.

Что касается всех прочих резидентных СЗИ мобильных устройств – FW, VPN, Device/Port Control, Anti-Virus/Anti-Malware, IDS, Application Control, NAC, User/Device Authentication – то они не предназначены для *информационной* фильтрации данных и не способны детектировать их утечки в исходящем с устройства трафике.

Даже недавно появившиеся Anti-Spam[13] модули работают в противоположном направлении, защищая мобильное устройство от попадания нежелательных данных *на него*.

Мобильная криптография – не панацея

Несмотря на то, что криптография может полностью защитить от утечек данных на пропавших мобильных устройствах, она не является панацеей против всех типов «мобильных» утечек.

Например, при штатной работе устройств прикладные программы работают с хранимыми в ОЗУ устройства нешифрованными данными, и ничто не мешает пользователям случайно или намеренно отослать эти данные из активного сетевого приложения – электронной почты, web-браузера, чата – куда-нибудь за пределы организации.

[13] SMS Spam Filtering в продукте Mobile Security 5 производства компании Trend Micro.

Например, невнимательный сотрудник может переслать субподрядчику ранее полученное электронное письмо с инструкциями по доставке товара клиенту, не обратив внимания на то, что письмо содержит приложение с персональными данными клиента, которые запрещается передавать третьей стороне.

Кроме того, для обеспечения неприкосновенности частной информации в условиях консьюмеризации, то есть, «двойного» – личного и производственного – применения мобильных устройств, работники, по всей видимости, будут полагаться на криптографические решения от работодателей еще меньше, чем сейчас. То есть, рассчитывать на 100% применение корпоративного шифрования на мобильных устройствах в будущем просто нереально – напротив, скорее всего, оно сократится по сравнению с сегодняшней ситуацией, когда только 55% компаний в США применяют криптографию для защиты хранимых данных[14].

Таким образом, не следует переоценивать эффективность резидентного шифрования как универсального механизма защиты от утечек данных с персональных мобильных устройств.

Это означает, что и сегодня, и в обозримом будущем *исключительную важность будут иметь решения по защите от неконтролируемой передачи корпоративных данных на мобильные устройства*.

Защита от утечек на мобильные устройства

Современные мобильные устройства могут получать данные по каналам трех типов: через сетевые приложения, съемные карты памяти и локальные коммуникации с персональным компьютером для синхронизации (Local Sync).

Сегодня на рынке предлагается множество продуктов и решений для защиты от утечек данных на мобильные устройства через сетевые приложения – такие, как почта, web-браузеры, чат, передача файлов. Реализованные как серверные программные компоненты или специализированные сетевые аппаратные комплексы эти решения используют технологии протокольной и контентной фильтрации, а также контроля типов файлов и доказали свою высокую эффективность.

Аналогичные проверенные технологии фильтрации контента и типов файлов интегрированы в продукты управления доступом к локальным интерфейсам и портам компьютеров (Endpoint Device/Port Control), обеспечивая таким образом надежную защиту от утечек данных через съемные карты памяти.

«Унесенные Sync'ом» – серьезная проблема корпоративной ИБ

Принципиально важным обстоятельством является то, что современные DLP-решения (Data Leakage Prevention) реализованы как *канально-специфичные*.

В то же время, программы локальной синхронизации мобильных устройств также *специфичны* и *не используют* протоколы сетевых приложений. С технической точки зрения, это означает, что существующие решения по контентной фильтрации и детектированию типов файлов *не могут контролировать* поток данных в каналах локальной синхронизации мобильных устройств.

[14] "Enterprise@Risk: 2007 Privacy & Data Protection Survey", Deloitte & Touche LLP and Ponemon Institute LLC (http://www.deloitte.com/dtt/cda/doc/content/us_risk_s%26P_2007%20Privacy10Dec2007final.pdf)

Единственная возможная «заглушка» средствами контроля доступа к локальным интерфейсам – это *полностью блокировать* подсоединения мобильных устройств к компьютеру на уровне USB портов. К сожалению, подключение мобильных устройств к не-USB портам *не детектируется* большинством современных продуктов Endpoint Device/Port Control.

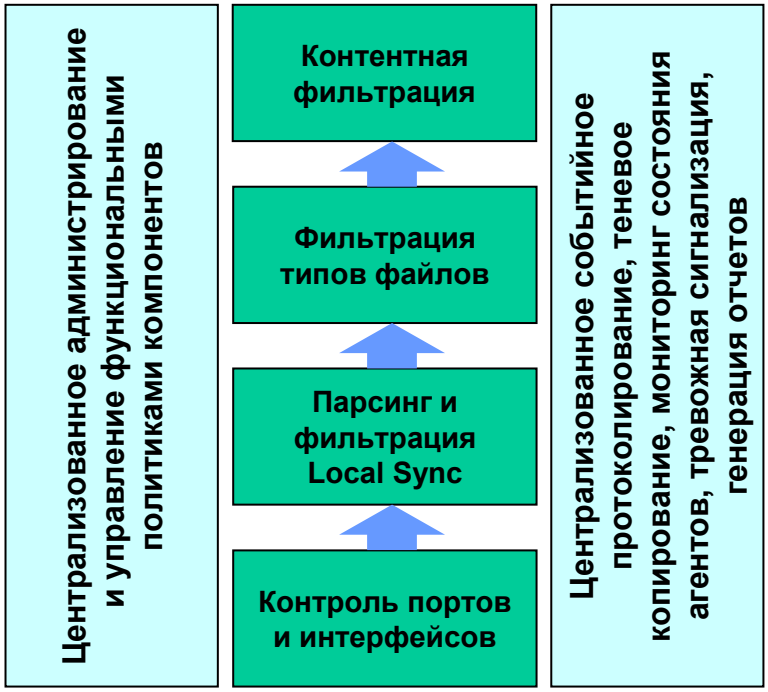
В результате корпоративные пользователи стоят перед выбором: либо полностью блокировать локальные подключения мобильных устройств и какое-либо их использование в производственных целях, либо испытывать судьбу и рисковать корпоративными данными каждый раз, нажимая на кнопку Sync.

Сложившийся дефицит контроля каналов локальной синхронизации мобильных устройств уже сегодня воспринимается корпоративными пользователями как серьезная угроза безопасности информации. Бездействие может превратить эту угрозу в одну из главных инсайдерских проблем ИБ предприятий по мере внедрения потребительской электроники в их информационные технологии.

Поэтому задачей первостепенной важности для отрасли ИБ является создание ***комплексного решения защиты от утечек данных через каналы локальной синхронизации мобильных устройств***.

Архитектура решения по защите от утечек через каналы локальной синхронизации мобильных устройств

Архитектура решения защиты от утечек через каналы Local Sync представляет собой стэк интегрированных механизмов информационной защиты, объединяющий компоненты Endpoint Device/Port Control, Local Sync Application Parsing and Object Filtering, File Type Filtering, and Content-Based Filtering.



В этом стэке каждый уровень контролирует «свои» целевые типы параметров соединений и данных, блокирует или фильтрует запрещенные элементы, детектирует и маркирует типы объектов для контроля другими функциональными механизмами, а затем пропускает классифицированный поток данных к следующему уровню стэка.

В частности, компонент *Device/Port Control* детектирует и контролирует локальное подсоединение мобильного устройства, тип интерфейса (USB, Bluetooth, IrDA, COM), тип устройства (Windows Mobile, Palm, Symbian,..) и – если возможно и необходимо – его модель и уникальный идентификатор.

Результаты передаются компоненту *Local Sync Parsing*, который осуществляет протокольный анализ потока данных, детектирует его объекты (files, pictures, calendars, emails, tasks, notes,..), фильтрует запрещенные типы и пропускает остальные к детектору типов файлов.

Компонент *File Type Filtering* распознает типы полученных файлов, удаляет из потока запрещенные политикой и передает разрешенные на вход компонента *Content-Based Filtering,* который осуществляет *информационную* фильтрацию, удаляя те части человеко-понимаемых данных, которые не соответствуют установленной политике ИБ предприятия.

Безусловно, полное решение на базе такой архитектуры должно включать необходимые *обеспечивающие компоненты* для централизованного администрирования и управления на базе политик, мониторинга состояния агентов, событийного протоколирования и аудита, теневого копирования и генерации отчетов.

Ключевым компонентом всей архитектуры является модуль парсинга и фильтрации протоколов локальной синхронизации, поскольку он реализует специфику канала данного типа и позволяет под- и надстраивать прочие функциональные компоненты стэка.

При наличии этого основного модуля остальные архитектурные компоненты могут быть интегрированы в решение достаточно быстро, поскольку их реализации для других типов каналов передачи данных на мобильные устройства уже существуют, хотя и не адаптированы для контроля данных локальной синхронизации.

DeviceLock – базисная платформа контроля Local Sync

Используя уникальную патентуемую технологию, компания Смарт Лайн Инк реализовала в своем программном продукте DeviceLock базисные компоненты информационной защиты каналов локальной синхронизации, обеспечивающие основные функции предотвращения утечек данных на уровнях контроля соединений, детектирования и фильтрации типов передаваемых данных.

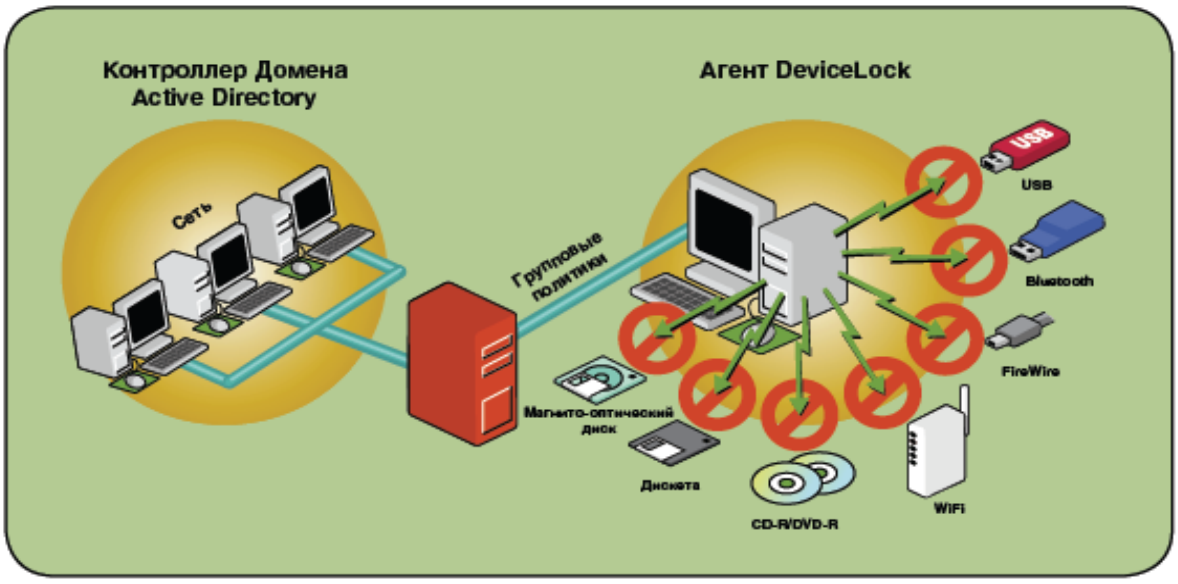
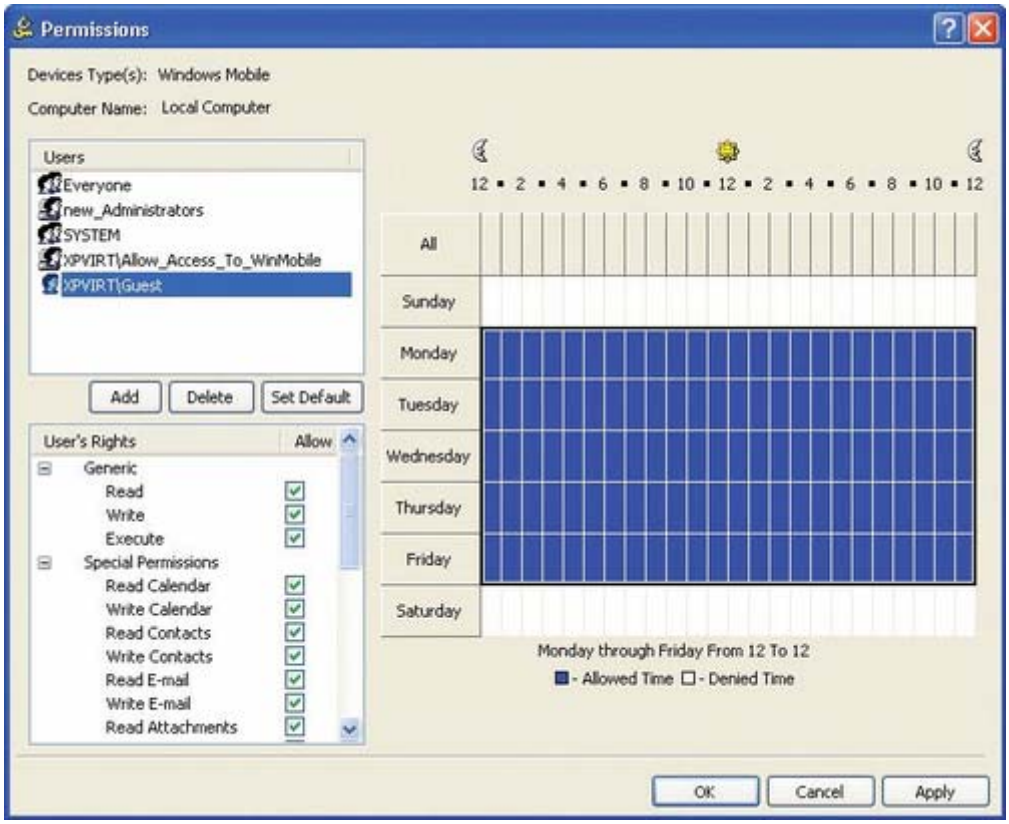


Рис. 1. Схема работы DeviceLock

Сегодня DeviceLock является единственным продуктом на российском и мировом рынках ИБ, который поддерживает контроль локальной синхронизации для платформ Windows Mobile® 5, Windows Mobile® 6 и Palm® OS, фильтруя протоколы Microsoft ActiveSync, Windows Mobile Device Center (WMDC) и HotSync с гранулированностью фильтрации до типов их объектов – files, pictures, calendars, emails, tasks, notes и т.д.

С помощью DeviceLock на определенном компьютере или всех компьютерах какого-то подразделения предприятия одному сотруднику или их группе можно разрешить подключать их персональные мобильные устройства и синхронизировать, например, содержимое календарей, списка задач и почтовые сообщения, но запрещено синхронизировать файлы, графические объекты и заметки. При этом все прочие пользователи корпоративной информационной системы на данных компьютерах не смогут провести локальную синхронизацию их мобильных устройств, однако, им это может быть разрешено на других компьютерах корпоративной сети – например, на их рабочих станциях – в соответствии с централизованно задаваемой политикой. Кроме того, DeviceLock поддерживает использование временного расписания при задании политик синхронизации: например, рядовым сотрудникам она может быть разрешена только в рабочее время с понедельника по пятницу, а руководству компании – в любое время.



DeviceLock детектирует и позволяет контролировать присутствие мобильного устройства на любом порту и интерфейсе: USB, COM, IrDA, Bluetooth. В случае подключения мобильного устройства через USB порт обеспечивается контроль доступа к конкретным моделям и отдельным устройствам (по их серийным номерам).

Кроме того, администраторы безопасности предприятий и организаций, использующих DeviceLock, имеют возможность удаленно управлять инсталляцией и исполнением приложений на мобильных устройствах.

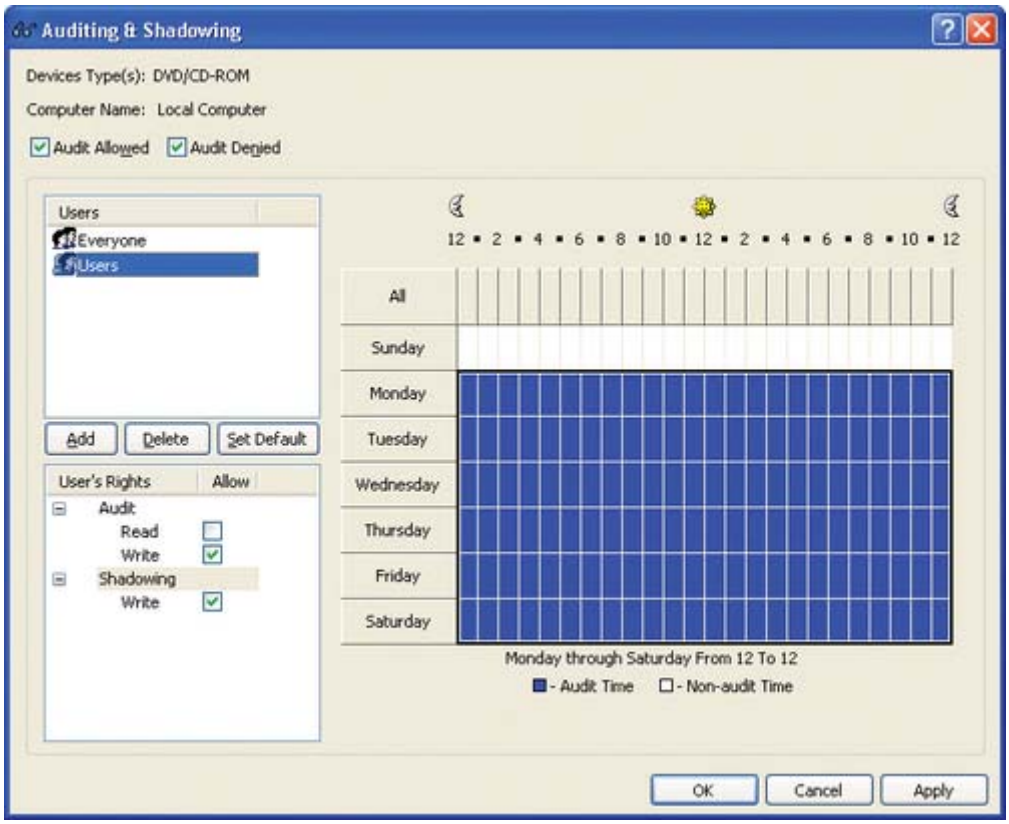
Гибкое управление политиками синхронизации всех агентов DeviceLock, установленных на защищаемых компьютерах корпоративной сети, а также всем комплексом

административных операций по обеспечению их полного жизненного цикла обеспечивается централизованно либо с выделенной платформы управления на базе одного или нескольких компонентов DeviceLock Enterprise Server, либо, если в организации используется платформа системного управления Microsoft Active Directory®, через ее групповые политики (Group Policy Objects), для чего предоставляется специальная GPO-оснастка – DeviceLock Group Policy Manager (GPM), полностью интегрированная в инфраструктуру Microsoft AD.

Принципиальные преимущества DeviceLock GPM состоят в том, что его пользователи не должны выделять дополнительные финансовые и трудовые ресурсы на установку и эксплуатацию отдельной серверной платформы для управления агентами DeviceLock, и, что не менее важно, масштабируемость DeviceLock GPM полностью определяется масштабом развернутой в организации Microsoft AD, таким образом автоматически обеспечивая потребности владельца.

Другой уникальной по значимости для пользователей характеристикой DeviceLock по контролю каналов локальной синхронизации является поддержка детального событийного протоколирования и теневого копирования с автоматическим централизованным сбором и хранением всех данных, передаваемых на мобильные устройства, в базе данных DeviceLock Enterprise Server. При этом политики сбора данных аудита и теневого копирования задаются централизованно с консоли DeviceLock Group Policy Manager или DeviceLock Enterprise Server – в зависимости от того, применяется ли у пользователя платформа Microsoft Active Directory.

Для решения задач аудита и расследований инцидентов информационной безопасности, включая обеспечение доказательной базы, в DeviceLock Enterprise Manager встроены удобный инструментарий централизованного просмотра событийных журналов и информации в базе данных теневого копирования, а также средства генерации отчетов.



Используя программный продукт DeviceLock, предприятия и организации всех типов и масштабов имеют возможность централизованно, оперативно, гибко и экономично контролировать локальные коммуникации между персональными мобильными устройствами сотрудников и рабочими станциями в корпоративной сети, таким образом повышая производительность труда персонала через его мобильность и ограничивая при этом риски информационной безопасности, связанные с неконтролируемым использованием мобильных устройств.

Компания Смарт Лайн Инк имеет четкие перспективные планы дальнейшего развития DeviceLock в интересах его многочисленных пользователей по всему миру и продолжает интенсивную работу по преобразованию базисного решения по контролю Local Sync в полнофункциональную платформу защиты от утечек данных через персональные мобильные устройства.

О компании Смарт Лайн Инк

Разработчик DeviceLock – ЗАО “Смарт Лайн Инк”. Основанная в 1996 году, российская компания Смарт Лайн Инк (SmartLine Inc) занимается разработкой программного обеспечения для администрирования компьютерных сетей. Качество и надежность продуктов Смарт Лайн Инк подтверждают более 50 тысяч клиентов в 80-ти странах мира – государственные, военные, медицинские, образовательные, крупнейшие финансовые и коммерческие учреждения, а также компании малого и среднего бизнеса. Программное обеспечение Смарт Лайн Инк установлено на более чем 2 000 000 компьютерах. В число клиентов компании входят Центральный Банк РФ, Сбербанк России, ОАО "Силовые машины", ВТБ 24, Российская государственная библиотека, BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank. Смарт Лайн Инк – международная компания с офисами в Лондоне, Милане, Москве, Ратингене (Германия) и Сан Рамоне (штат Калифорния, США). Основной офис разработки программных продуктов Смарт Лайн Инк находится в Москве.

Контактная информация

ЗАО “Смарт Лайн Инк”

Москва, Б. Семеновская ул., д. 40, офис 301

Телефон: +7 (495) 967-99-60, +7 (495) 366-21-93 (контактное лицо – Анастасия Дементьева)

Отдел продаж: sales@smartline.ru

Тех. поддержка: support@smartline.ru

