**К вопросу об информационной безопасности мобильных устройств**

**Шавель А.Н.**
Белорусский национальный технический университет

«Консьюмеризация» — использование сотрудниками компаний собственных мобильных устройств для работы с корпоративной информацией ставит перед ИТ-отделами компаний новые проблемы, связанные с обеспечением безопасности конфиденциальных данных.

Все больше организаций открывают своим сотрудникам доступ к корпоративной сети и приложениям для работы через личные мобильные устройства (смартфоны, планшетные компьютеры, ноутбуки и т. п.), купленные и обслуживаемые самими сотрудниками. Это представляет определенную угрозу информационной безопасности, и, если к защите ноутбуков уже выработаны общие подходы, то потребность в современных методах защиты потребительских мобильных устройств компании только начинают осознавать.

Для компаний предоставление доступа к корпоративным данным и приложениям может быть выгодно по нескольким причинам: повышение продуктивности, оперативности доступа к информации, а также повышение лояльности сотрудников. Однако консьюмеризация ИТ привносит множество новых вопросов, связанных с управлением устройствами и обеспечением конфиденциальности корпоративных данных, которые теперь обрабатываются и хранятся на разнообразных устройствах, не контролируемых ИТ-отделами. По мнению аналитиков Gartner, попытки запретить или контролировать использование мобильных устройств показали свою несостоятельность — первыми нарушителями корпоративных политик становятся сами руководители компании, желающие использовать новейшие устройства, одновременно требуя от ИТ-отделов их поддержки.

Консьюмеризация и риски информационной безопасности

Основные риски связаны с тем, что корпоративные данные хранятся и обрабатываются на устройствах, изначально не приспособленных для защиты со стороны корпоративных ИТ-служб. В случае утери или кражи устройства данные могут стать доступными злоумышленникам, а утерянный смартфон или планшет может открыть доступ к корпоративным приложениям или позволить подключиться к внутренней сети предприятия. Поэтому очень важно вовремя узнать о пропаже устройства, заблокировать его, очистить данные и проверить, не были ли скомпрометированы учетные записи халатного сотрудника.

Корпоративные данные могут «утечь» не только в результате кражи или потери устройства, но и при подключении устройства к сторонним

компьютерам, а поскольку невозможно запретить сотрудникам подключать собственные устройства к другим компьютерам, то важно обеспечить шифрование корпоративных данных, хранящихся в памяти устройства или на карте памяти.

Помимо рисков, связанных с неправомерным доступом к корпоративным данным в результате утери или кражи устройств, есть и риски, связанные с заражением устройств вредоносным кодом, например через каталоги мобильных приложений под видом игр или полезных программ, и здесь очень уязвима платформа Android и устройства, использующие Android Market.

### Защита мобильных устройств

Современные операционные системы мобильных устройств имеют в своем арсенале возможности для централизованного управления, но часто их недостаточно — они фрагментированно защищают данные или требуют вмешательства пользователей, поэтому такие задачи решаются системами управления Mobile Device Management (MDM) и системами обеспечения безопасности данных в мобильных устройствах. Функционал этих систем можно проиллюстрировать на примере решения типовых проблем защиты мобильных устройств в корпоративной среде средствами Trend Micro Mobile Security 7.0.

Хаотичное подключение устройств к корпоративным ресурсам. Одной из первоочередных задач системы MDM является инвентаризация самих мобильных устройств: учет и отслеживание их основных параметров (IMEI, тип и версия операционных систем). Важно также организовать слежение за устройством со «взломанной» ОС, открывающим потенциально вредоносному коду возможности обхода инструментов защиты ОС и собственно систем MDM. В Trend Micro Mobile Security 7.0 можно отслеживать подключенные устройства и группировать их в домены управления для выполнения типовых настроек и упрощения администрирования. Администратору доступен поиск устройств по ОС и номеру телефона или быстрый поиск устройств с устаревшими настройками безопасности.

**Распределение устройств и привязка к пользователям**. Кроме отслеживания того, за какими сотрудниками закреплены устройства, необходимо также реализовывать рабочие процессы по выдаче и изъятию корпоративных устройств или их подключению к корпоративной системе защиты, например, система может предоставлять веб-интерфейс создания и согласования заявок на подключение новых устройств.

**Обеспечение единообразия корпоративного ПО**. Важная задача MDM — управление приложениями: доставка, установка, обновление, удаление и

блокировка нежелательных приложений. Этот функционал необходим как для распространения корпоративных приложений, которые могут быть недоступны пользователям через стандартные магазины приложений, встроенные в ОС, так и для запрета использования сторонних приложений, потенциально влияющих на безопасность корпоративных данных. Кроме того, система должна иметь возможность аудита установленных приложений, а также выдавать отчетность по установленным приложениям.

**Распространение корпоративных настроек и политик на устройства**. Здесь речь идет о распространении настроек, таких как параметры корпоративного почтового сервера, календаря или VPN-сервера для доступа к корпоративным сервисам. Например, Trend Micro Mobile Security позволяет централизованно устанавливать на устройствах настройки сетей Wi-Fi, VPN-подключений и электронной почты.

**Защита данных в случае кражи**. К мерам защиты относятся удаленная очистка устройства от всех данных, шифрование и усиление аутентификации пользователя при доступе к устройству. Например, политиками системы может быть задана минимальная длина и сложность кода разблокировки устройства с целью предотвращения несанкционированного использования. Некоторыми производителями предлагается отслеживание физического местоположения устройств с помощью GPS или мобильных сетей, что облегчает поиск украденных или утерянных устройств. Например, средствами Trend Micro Mobile Security 7.0 можно удаленно заблокировать устройство, удалить все данные и отследить его местоположение на картах Google, пройдя по ссылке на последнее актуальное местоположение устройства, а также задать сложность PIN-кода для разблокировки устройства.

**Контроль утечки данных**. Контроль и избирательное разрешение или блокировка некоторых функций устройства также призваны ограничить возможности утечек данных с устройства – например, запрет использования устройства в качестве USB-накопителя. Trend Micro Mobile Security 7.0 предлагает политики защиты устройств и ограничения функционала, привязанные к определенному местоположению. Например, при нахождении устройства в офисе компании сотруднику могут быть недоступны функции фото- и видеосъемки или обмена файлами по Bluetooth, а вне офиса можно будет продолжать пользоваться устройством в обычном режиме.

**Защита от вредоносных программ**. Важной мерой является реализация поиска вредоносных программ в памяти устройства и на съемных картах памяти, а также обнаружение в момент установки нового ПО. В Trend Micro Mobile Security 7.0 администратор может на основе политик задать параметры сканирования устройства и карты памяти в реальном времени,

по расписанию указать типы файлов для сканирования и действия с обнаруженным потенциально вредоносным кодом.

**Защита от фишинга**. Системы защиты мобильных устройств должны нейтрализовывать направленные на пользователей угрозы, такие как фишинг-сайты, маскирующиеся под легитимные и выманивающие персональные данные или любую другую информацию. Например, фишинговые рассылки могут быть частью спланированного нападения на корпоративную сеть и служить отправной точкой для дальнейшего развития атаки. Браузеры мобильных устройств часто не имеют таких развитых инструментов обнаружения фишинговых и других вредоносных сайтов и средств оповещения о них пользователей, какими оснащены браузеры для «настольных» ОС. Именно поэтому функция веб-фильтрации может быть важным защитным механизмом системы контроля и безопасности мобильных устройств в корпоративной среде. В Trend Micro Mobile Security 7.0 используется защита веб-ресурсов на основе инфраструктуры Trend Micro Smart Protection Network, объединяющей данные от миллионов клиентских устройств и автоматизированных механизмов обнаружения вредоносной и подозрительной активности в сети, а также рекомендации аналитиков Trendlabs

**Защита от телефонного спама**. Фильтрация нежелательных звонков и SMS является дополнительной мерой, востребованной в продуктах для защиты смартфонов пользователей, и может применяться в корпоративной среде, централизованно управляясь на основе политик. Например, можно построить защиту по принципу белого или черного списка.

Единый инструментарий для разных платформ. Важным фактором при выборе системы управления и безопасности мобильных устройств является возможность работы со всеми современными мобильными операционными системами (iOS, Android, Symbian, Windows Mobile, BlackBerry, Windows Phone) и их защиты с помощью одной системы.