



УДК 004.7

*А.В. Самочадин, Т.Н. Самочадина, Д.А. Тимофеев, С.О. Попов***БАЗОВАЯ ФУНКЦИОНАЛЬНОСТЬ СИСТЕМ ЦЕНТРАЛИЗОВАННОГО
УПРАВЛЕНИЯ МОБИЛЬНЫМИ УСТРОЙСТВАМИ***A.V. Samochadin, T.N. Samochadina, D.A. Timofeev, S.O. Popov***BASE FEATURES OF MOBILE DEVICE MANAGEMENT SYSTEMS**

Проведен анализ функциональности систем централизованного управления мобильными устройствами, которая реализуется ведущими производителями в этой области. Результатом анализа является выделение базового набора функций, необходимого для реализации конкурентного решения по управлению мобильными устройствами, а также идентификация функций, реализация которых может дать преимущество перед конкурентами.

УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ; ФУНКЦИОНАЛЬНОСТЬ; ТРЕБОВАНИЯ.

We survey feature sets of main mobile device management systems on the market. All features are split into 7 categories: mobile platform support, hosting mode, policy management, inventory management, device state management, security management, software distribution. For each category, we identify the features that are implemented in most MDM systems. These features must be implemented in any new mobile device management system that is supposed to compete with current market leaders' software. The analysis also showed that there is a set of features (namely, device location discovery, and remote access to equipment) that are desired, yet underrepresented in mobile device management software, so implementation of these features may become an advantage.

MOBILE DEVICE MANAGEMENT; FEATURES; REQUIREMENTS.

Мобильные технологии активно внедряются в различные отрасли бизнеса. Компании видят в мобильных технологиях средства повышения производительности сотрудников и, как следствие, приобретения конкурентных преимуществ на рынке. Наиболее перспективными отраслями для внедрения мобильных технологий являются те, бизнес в которых предполагает мобильность сотрудников или связан с массовым обслуживанием клиентов: торговые, страховые компании, образовательные учреждения, дистрибьюторы. Аналитики прогнозируют во всем мире 30–35-процентный рост числа сотрудников, использующих мобильные технологии в своей производственной деятельности. Количество пользователей современных интеллектуальных мобильных устройств в России очень велико, и это позволяет ожидать высокую динамику внедре-

ния мобильных технологий в ближайшее время. Основным подходом к внедрению мобильных технологий сегодня является использование централизованного управления мобильными устройствами (MDM).

Исследования, проведенные 451 Research (The 451 Group) [1], показали, что технологии централизованного управления мобильными устройствами входят в число трех наиболее востребованных и быстро растущих информационных технологий. Исследовательская и консалтинговая компания Gartner [2] также относит управление мобильными устройствами к числу десяти наиболее перспективных технологий. Объем рынка MDM-решений в 2010 г. составил 150 млн [3], в 2011 – 444,6 млн долларов США [4, 5]. Согласно данным Gartner [6], объем рынка оценивался в 784 млн в 2012 и более чем в один млрд долларов США в

2013 г. В целом, рынок MDM-решений показал очень высокий рост в 2011 г., увеличившись почти в три раза, после чего стабильно рос более чем на 50 % в год. Число компаний, использующих MDM-решения, растет пропорционально объему рынка [7].

Чрезвычайно благоприятны для рынка MDM-решений и прогнозы на ближайшие годы, которые выполнялись ведущими консалтинговыми компаниями Gartner, IDC, The Radicati Group, Mind Commerce. Все они прогнозируют в 2014–2016 гг. рост рынка на 20–35 % в год. Ожидается и соответственный рост числа пользователей MDM. Согласно данным Mind Commerce [8], в начале 2014 г. их число составляет 180 млн, а к 2015 г. должно увеличиться до 390 млн человек.

В Российской Федерации отсутствуют собственные полнофункциональные решения в области управления мобильными устройствами, поэтому актуально создание конкурентоспособного программного продукта отечественного производства. Конкурентоспособность разрабатываемого программного обеспечения по сравнению с зарубежными аналогами должна быть обеспечена улучшенными функциональными, потребительскими и стоимостными показателями продукции.

Рынок MDM в современном состоянии классифицируется как незрелый [2], с быстро растущим количеством поставщиков и появлением новых вариантов технологических решений. Функциональность представленных на рынке систем пока не устоялась и отличается большим разнообразием. Лидирующая группа производителей старается включать в свои продукты функциональность, которая имеется у конкурентов, поэтому функциональные возможности решений лидеров рынка отличаются друг от друга меньше, чем у производителей второго эшелона.

Задачей настоящей работы было выделение основных функций управления мобильными устройствами, которые должны быть реализованы в системе MDM, чтобы она могла составить конкуренцию лучшим из представленных на рынке MDM решений. При этом мы опирались на два кри-

терия. Первым из них является доля коммерческих решений, в которых реализована каждая из функций. Отсутствие возможностей, предоставляемых большей частью других реализаций, снижает конкурентоспособность системы. Вторым критерием является степень заинтересованности конечных пользователей в сервисах, которые строятся на основе базовых функций системы MDM. В первую очередь необходимо реализовывать те функции, которые нужны для разработки наиболее востребованных сервисов. Оценки степени заинтересованности пользователей, использованные в данной статье, были получены в результате опроса [9].

Основные производители менеджеров мобильных устройств. На рынке менеджеров мобильных устройств активно работают более 100 поставщиков, поставляющих различные варианты решений [10], из которых 39 выделены в обзорах ведущих консалтинговых компаний (Gartner [10], Solutions Review [11], Forester [12]) как лидеры рынка. Для подробного рассмотрения мы отобрали следующие 20 производителей, которые упоминаются не менее чем в двух обзорах ведущих консалтинговых компаний: Absolute Software (<https://www.absolute.com>), AirWatch (<http://www.air-watch.com>), AmTel (<http://www.amtelnet.com>), Boxtone (<http://boxtone.com>), Citrix (<http://www.citrix.com>), Excitor (<http://www.excitor.com>), Fiberlink (MaaS360) (<http://www.maas360.com>), Good Technology (<http://www1.good.com>), IBM (<http://www-03.ibm.com>), Kaseya (<http://www.kaseya.com>), LANDesk (<http://www.landesk.com>), McAfee (<http://www.mcafee.com>), MobileIron (<http://www.mobileiron.com>), Notify Technology (Globo) (<http://www.globopl.com>), Sophos (<http://www.sophos.com>), SOTI (<http://www.soti.net>), Sybase (<http://www.sybase.ru>), Symantec (<http://www.symantec.com>), Tangoe (<http://www.tangoe.com>), Trend Micro (<http://www.trendmicro.com.ru>). Источниками информации о предлагаемых ими решениях являются обзоры рынков [10–14] и сведения, опубликованные на сайтах производителей.

Функциональность решений MDM. Со-

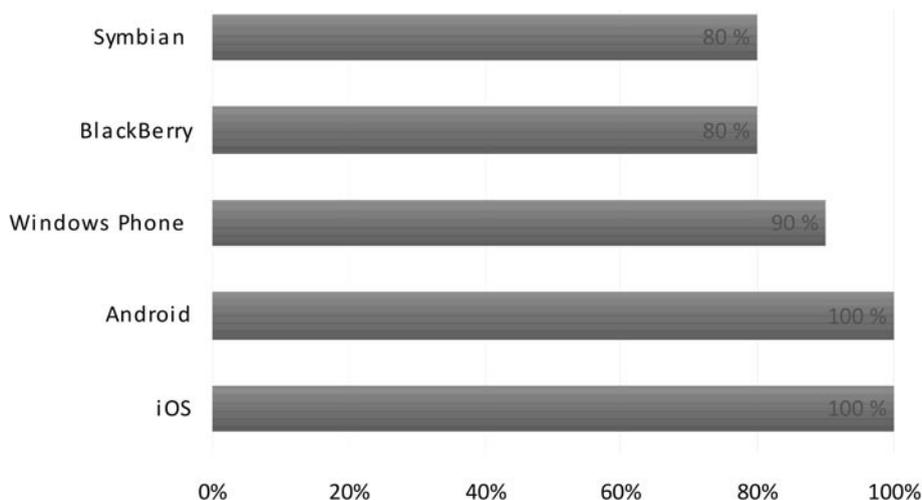


Рис. 1. Поддерживаемые мобильные платформы

гласно Gartner [12], MDM определяется как спектр продуктов и услуг, которые предоставляют организациям возможность развертывать и поддерживать различные корпоративные приложения на мобильных устройствах.

На основе обзоров консалтинговых компаний [11, 13] и анализа различных решений были выделены семь категорий (направлений функциональности), каждая из которых разбивается на подкатегории. На основании этой классификации проводится анализ решений, предоставляемых основными производителями.

Ключевыми категориями, на базе которых проводится оценка представленных на рынке решений, являются поддерживаемые мобильные платформы, способы поставки, применение политик, управление инвентаризацией, управление состоянием мобиль-

ных устройств, управление безопасностью и управление распространением приложений.

Поддерживаемые мобильные платформы. Все производители поддерживают лидирующие на рынке мобильных платформ системы iOS и Android (рис. 1). Большинство производителей поддерживают Windows Phone, при этом за 2013 г. доля поддерживающих эту платформу решений резко выросла. Следует также отметить снижение доли поддержки BlackBerry и Symbian, связанное с быстрым падением популярности этих платформ на рынках смартфонов и планшетов. Согласно прогнозам аналитических компаний, в ближайшие три-четыре года распределение выпускаемых мобильных устройств по операционным системам будет выглядеть следующим образом: Android – первое место с большим отрывом,

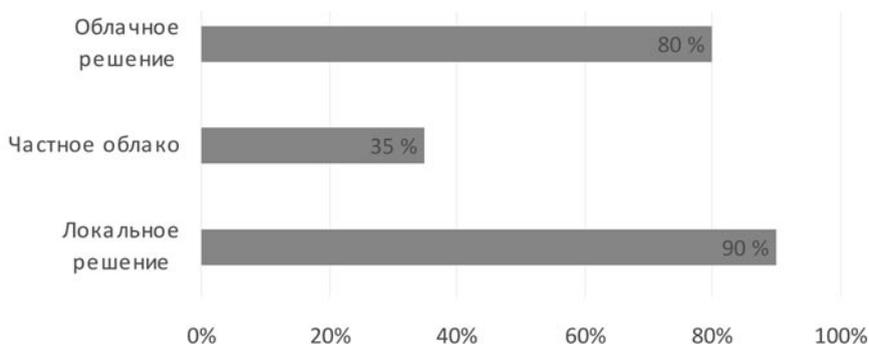


Рис. 2. Способы поставки

iOS и Windows Phone – второе и третье место с очень небольшой разницей. Суммарная доля рынка трех указанных мобильных платформ составит более 90 %. Операционные системы Symbian, Asha, BlackBerry, Bada будут занимать очень небольшую долю мирового и российского рынка (1–3 %), поэтому поддержка этих мобильных платформ в разрабатываемых решениях MDM не является необходимой.

Используемые способы поставки. Производители предлагают следующие способы поставки решений MDM (рис. 2):

- Локальное решение. В этом случае поставляется локальное программное обеспечение, которое разворачивается с использованием инфраструктуры организации покупателя.

- Облачное решение. Программное обеспечение MDM размещается в облачной среде поставщика, а заказчику предоставляется удаленный доступ к системе MDM.

- Частное облако – облачное решение, которое передается заказчику и размещается в «частном облаке» под его контролем.

Локальное решение является традиционным способом поставки и поддерживается всеми производителями. Среди других способов поставки наиболее востребованы облачные решения, поскольку они позволяют организациям получить возможности MDM без начальных инвестиций в инфраструктуру.

Применение политик. Чтобы мобильное устройство было доступно для удаленного управления, оно должно пройти процедуру инициализации устройства на сервере MDM. В процессе инициализации на устройство устанавливается MDM-профиль, содержащий настройки политик безопасности и другую конфигурационную информацию (рис. 3).

Производители предлагают следующие способы установки настроек и ограничений мобильного устройства:

- инициализация с помощью средств управления конфигурацией;

- инициализация через портал самообслуживания.

Оба способа являются востребованными

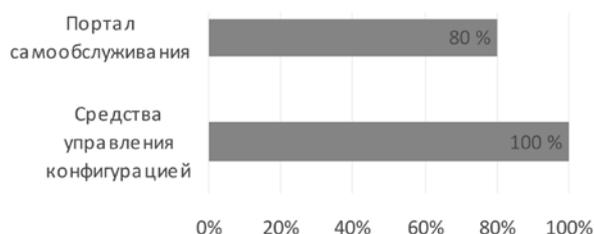


Рис. 3. Применение политик

ми и поддерживаются практически всеми реализациями MDM.

Управление инвентаризацией. Инвентаризация подключенных к корпоративной сети мобильных устройств является одной из основных функций MDM (рис. 4). Процесс инвентаризации мобильных устройств включает периодическое получение от мобильных устройств информации об их программно-технических характеристиках (ПТХ) и местоположении, и накопление этой информации в едином реестре.

Инвентаризация устройств должна предоставлять данные для решения следующих задач:

- мониторинг ПТХ, включая отслеживание ПТХ мобильных устройств и обнаружение устройств, нарушающих требования назначенных групповых политик;

- отслеживание местоположения мобильного устройства;

- применение групповых политик управления мобильными устройствами, зависящих от физического местоположения мобильного устройства;

- мониторинг памяти и срока службы батареи путем отслеживания использования соответствующих ресурсов мобильных устройств;

- построение инвентаризационных отчетов;

- администрирование и формирование административных отчетов.

Следует отметить, что представленные на рынке решения в наименьшей степени поддерживают функции, связанные с местоположением пользователей.

Управление состоянием устройств. Под управлением состоянием устройств по-

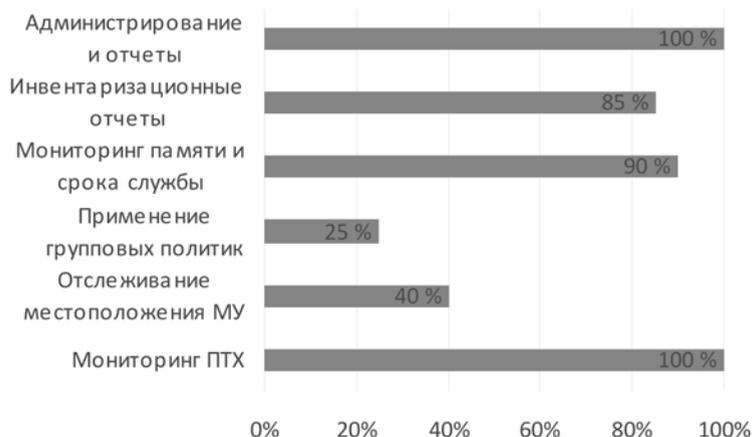


Рис. 4. Инвентаризация мобильных устройств

нимаются действия, приводящие к блокировке, разблокировке и восстановлению заводских настроек мобильных устройств. Эти действия могут выполняться как администраторами MDM, так и пользователями устройств самостоятельно. Производители систем MDM предлагают следующие способы управления состоянием мобильных устройств (рис. 5).

- Дистанционная блокировка /разблокировка мобильных устройств. При необходимости (например, при краже или потере устройства) мобильное устройство можно удаленно заблокировать. Связь с устройством возможна даже в случае замены SIM-карты. Функция отслеживания

SIM-карты обнаруживает смену SIM-карты в устройстве, сообщает MDM новый номер телефона и позволяет применить все меры защиты на случай кражи.

- Дистанционная блокировка и разблокировка сенсоров мобильных устройств (микрофон, видекамера).

- Обнаружение мобильных устройств, которые в течение длительного времени не выходили на связь с системой MDM.

- Восстановление данных утерянного устройства.

- Блокировка аппаратных возможностей.

Все функции управления состоянием устройства (за исключением восстановле-

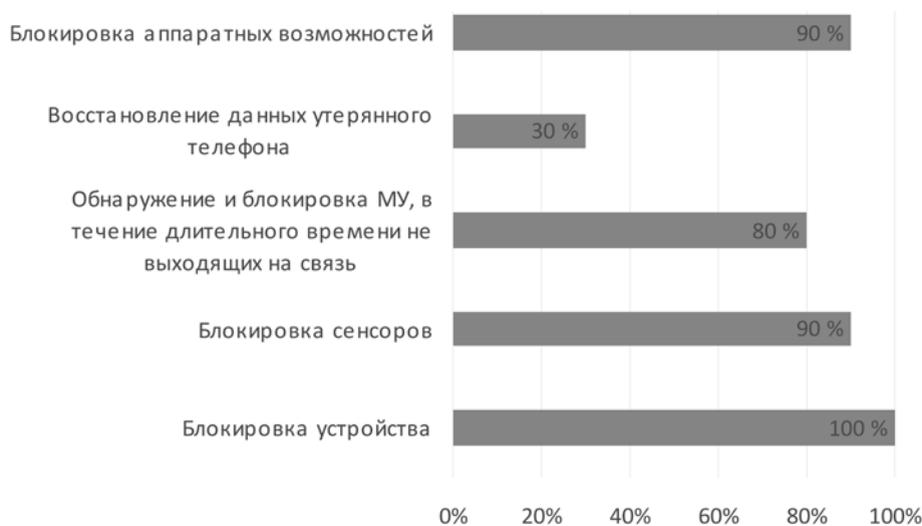


Рис. 5. Управление состоянием устройств

ния данных утерянного телефона) включаются в функциональность практически всех систем MDM.

Управление безопасностью. К основным угрозам безопасности [15] относятся вредоносное программное обеспечение, взлом мобильных устройств, хищение или потеря мобильных устройств, случайная утечка данных, преднамеренное распространение данных сотрудниками организации. Основными мерами защиты являются [15] использование средств защиты от вредоносного программного обеспечения, регулярная установка обновлений, разграничение уровней доступа к ИТ-системам, политика послеаварийного восстановления и шифрование конфиденциальных данных.

Необходимый уровень защиты обеспечивается в системах MDM с помощью следующего набора функций управления безопасностью (рис. 6), которые являются практически обязательными для MDM.

- Политика применения паролей, которая включает следующие возможности:

- контроль доступа пользователей к данным, устройствам и приложениям, контроль сетевых подключений;

- возможность удаленно включать использование пароля на устройствах пользователей, устанавливать сертификаты безопасности;

- возможность настройки различных аспектов политики применения паролей, таких как ограничения на использование приложений и ресурсов, применение их к определенным группам, пользователям, устройствам.

- Выборочное удаленное стирание: возможность стереть с устройства корпоративные данные, оставив личные данные пользователя нетронутыми.

- Полное удаление всех данных: возможность при необходимости удалить корпоративные данные с устройства и вернуть его заводские настройки.

- Обнаружение взломанных или модифицированных устройств.

- Контроль соблюдения требований: возможность разрешать использование только тех устройств, которые отвечают заданным требованиям к состоянию устройства (отсутствие взлома и наличие шифрования), состоянию пользователя (его членство в группе) или состоянию приложений (наличие обязательных приложений

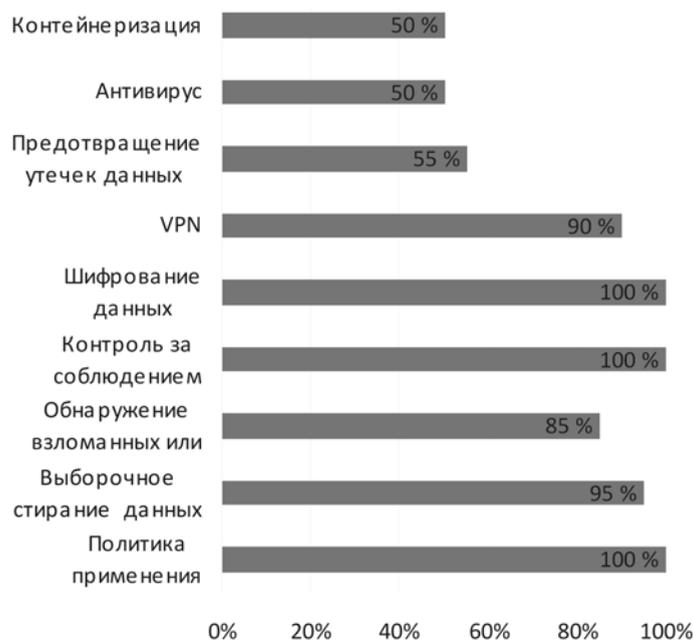


Рис. 6. Управление безопасностью

и отсутствие запрещенных приложений). Если устройство не соответствует требованиям, пользователю обычно предоставляются инструкции по настройке устройства.

- Шифрование данных: шифрование всех или некоторых данных на устройстве и, возможно, сменных носителях.

- Организация подключения VPN для защищенного удаленного доступа к корпоративным ресурсам.

Следующие функции применяются существенно реже и не являются обязательными функциями MDM.

- Предотвращение утечек данных. В то время как меры защиты данных в первую очередь направлены на предотвращение несанкционированного доступа к данным, средства обнаружения утечек предназначены для сокращения ущерба от умышленных действий авторизированных пользователей.

- Антивирусная защита: установка и обновление программного обеспечения для защиты от вредоносных приложений.

Новым, перспективным подходом к обеспечению безопасности является контейнеризация, представляющая собой набор механизмов для разделения корпоративных и личных данных и приложений на устройствах. Эта технология позволяет осуществлять контроль и защиту данных в контейнере, ограничивать операции перемещения данных в незащищенные области и предотвращать их извлечение из контей-

нера. Например, можно гарантировать, что защищенные данные не будут отправлены с устройства с помощью сторонних программ электронной почты или SMS. К контейнеру могут применяться такие правила, как локальное шифрование данных, выборочное удаленное стирание, предотвращение утечки данных. Невысокий процент включения этой функции в MDM-решения связан с относительно недавним ее появлением.

Управление распространением приложений. Управление распространением приложений позволяет решить две основные задачи: автоматизировать установку и обновление приложений, необходимых для выполнения должностных обязанностей сотрудника, и обеспечение безопасности путем оперативного распространения обновлений и ограничения на установку сторонних приложений.

Производители предлагают следующие возможности распространения программного обеспечения (рис. 7).

- Дистанционное автоматическое распространение и обновление программного обеспечения.

- Белый и черный списки приложений. Белый список приложений дает возможность установки на устройство только одобренных приложений. Черный список ограничивает доступ к нежелательным или потенциально вредным приложениям.

- Ограничение доступа к общедоступным магазинам приложений. В целях обе-

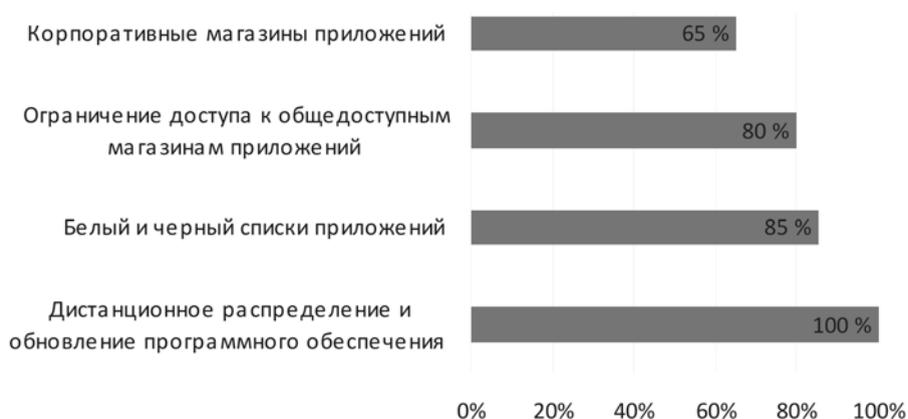


Рис. 7. Управление распространением приложений

спечения безопасности и повышения производительности труда предоставляется возможность ограничения доступа к приложениям в общедоступных магазинах. Доступ при этом возможен только к разрешенным приложениям.

- Корпоративные магазины приложений. Магазины позволяют пользователям получить доступ ко всем мобильным инструментам, необходимым для выполнения их работы.

Наиболее распространенными являются функции дистанционного распространения и обновления программного обеспечения и поддержка белого и черного списков приложений. Поддержка корпоративных магазинов приложений для платформ iOS и Windows Phone реализована производителями самих этих мобильных платформ.

Минимальная функциональность MDM. Функциональность решений, предлагаемых производителями MDM, отличается большим разнообразием, однако можно выделить следующий набор функций, который поддерживается всеми ведущими производителями.

- Поддерживаемые мобильные платформы: Android, iOS, Windows Phone.

- Способы поставки: локальное решение, облачное решение.

- Применение политик: средства управления конфигурацией, портал самообслуживания.

- Управление инвентаризацией: мониторинг ПТХ, отслеживание местоположения мобильных устройств и применение групповых политик на основе местоположения, инвентаризационные административные отчеты.

- Управление состоянием мобильных устройств: блокировка устройств, блокировка сенсоров.

- Управление безопасностью: политика применения паролей, выборочное стирание данных, обнаружение взломанных или модифицированных устройств, шифрование данных, VPN, предотвращение утечек данных, контейнеризация.

- Управление распространением при-

ложений: дистанционное распределение и обновление ПО, белый и черный списки приложений.

Отсутствие функций из приведенного списка ухудшит конкурентоспособность решения, поэтому они должны быть реализованы и в разрабатываемой системе MDM.

Реализация востребованных пользовательских сервисов. Реализация функций, соответствующих минимальному набору, будучи необходимой, тем не менее не обеспечивает сама по себе конкурентных преимуществ. Чтобы сделать разрабатываемую систему привлекательной для клиентов, необходимо предложить решение для определенного класса задач, который представлял бы значительный интерес для пользователей мобильных устройств, но в то же время не имел бы широкой поддержки в продуктах ведущих производителей систем MDM.

Для анализа востребованности мобильных сервисов, которые могут быть реализованы на основе системы MDM, в 2014 г. в Санкт-Петербургском государственном политехническом университете было проведено анкетирование [9], в котором приняли участие студенты, преподаватели и представители администрации Университета. Выбор аудитории был обусловлен тем, что, в соответствии с целями проекта, сфера образования должна стать одной из основных областей применения разрабатываемой системы.

Большая часть сервисов, которые по результатам опроса были сочтены востребованными, может быть реализована на основе существующих систем MDM. Тем не менее были выделены два класса сервисов, которые представляют существенный интерес для пользователей мобильных устройств, но недостаточно поддерживаются системами MDM ведущих производителей.

К первому классу относятся сервисы, использующие данные о местоположении пользователя (в частности, навигационные сервисы и сервисы, предоставляющие информацию о состоянии транспортной сети). Как показано на рис. 4, среди рас-



смотренных систем MDM только 40 % предоставляют функцию определения местоположения устройства, и еще меньшее количество систем поддерживает возможность управления устройством на основе его местоположения. Таким образом, реализация функции определения местоположения мобильных устройств может дать разрабатываемой системе MDM конкурентное преимущество перед системами, не имеющими этой функции.

Одной из возможных причин ограниченной поддержки функции определения местоположения системами MDM может быть трудность локализации устройств в помещениях. Для современных мобильных устройств, оснащенных приемниками GPS или ГЛОНАСС, задача определения координат устройства на открытой местности не представляет сложности. В то же время определение положения устройства в помещении оказывается существенно более трудной задачей, что обусловлено в первую очередь более высокими требованиями к точности локализации. В частности, серьезную проблему представляет определение того, в каком из соседних помещений находится устройство, особенно если задачу локализации нужно решать для многоэтажных зданий.

Исходя из этого, дополнительное конкурентное преимущество можно получить, если удастся повысить точность локализации мобильных устройств в помещениях.

Второй класс сервисов, который вызывает высокий интерес у пользователей, связан с управлением внешними устройствами с помощью мобильных устройств пользователей. Сценарии использования таких сервисов могут включать, к примеру, демонстрацию видеозаписей, фотографий или презентаций с помощью телевизоров или проекторов, создание лабораторных стендов с дистанционным управлением.

Ряд современных устройств (в частности, телевизоров) уже поддерживает дистанционное управление с мобильных устройств, но поддержка обычно ограничивается только одной мобильной платфор-

мой и фиксированным набором сервисов. Значительная часть устройств поддерживает подключение к компьютеру, но не взаимодействует с мобильными устройствами. Для того чтобы такими устройствами можно было дистанционно управлять с помощью мобильных устройств, необходимо решить ряд задач, в число которых входят аутентификация пользователей, разграничение прав доступа (возможно, с учетом местоположения устройства), предоставление пользователю перечня доступных устройств, установка и запуск на мобильных устройствах специализированных приложений для взаимодействия с оборудованием. Эти задачи могут быть решены с помощью системы MDM. В таком случае для поддержки нового класса устройств достаточно будет реализовать сервис взаимодействия с конкретным устройством, используя общий интерфейс управления устройствами MDM. В случае особых требований к интерфейсу управления требуется разработать мобильные приложения для основных мобильных платформ, однако и эта задача может быть упрощена путем реализации интерфейса управления как web-приложения.

Анализ возможностей существующих систем MDM показывает, что ни один из производителей не заявляет возможность управления внешними устройствами в качестве поддерживаемой функции. С учетом востребованности соответствующих сервисов среди пользователей, реализация такой функциональности в системе MDM позволит ей конкурировать с лидирующими на рынке системами управления мобильными устройствами.

В статье приведены данные о наборе базовых функций управления мобильными устройствами, которые реализуются лидирующими производителями решений MDM. В результате анализа выделено подмножество функций, которые должны быть реализованы в любой системе MDM, чтобы она была способна конкурировать с альтернативными решениями на мировом рынке систем управления мобильными

ми устройствами. Кроме того, определены две функции (локализация мобильных устройств и организация интерфейса дистанционного управления внешними устройствами), реализация которых в системе MDM может дать ей конкурентные преимущества, в т. ч. по сравнению с лидерами рынка.

Разработка программного обеспечения для систем централизованного управления мобильными устройствами проводится в рамках совместного проекта компании IBS (Москва) и Санкт-Петербургского государственного политехнического университета.

Работа выполняется при финансовой поддержке Министерства образования и науки РФ, госконтракт № 02.G25.31.0024 от 12.02.2013 г.

СПИСОК ЛИТЕРАТУРЫ

1. **Kennedy D.** *Information security: Wave 16. 2013 451 Research, LLC* [электронный ресурс] / URL: <http://www.451research> (дата обращения 2013).
2. **Gartner, Inc.** *Top 10 Mobile Technologies for 2012 and 2013* [электронный ресурс] / URL: <http://my.gartner.com/portal/server.pt?open=512&objID=270&mode=2&PageID=3862698&resId=1923514> (дата обращения 2013).
3. **Meidata.** *Mobile Device Management Global Market Analysis* [электронный ресурс] / URL: <http://meidata.com/> (дата обращения 2014).
4. **Hoffman B.** *Worldwide Mobile Enterprise Management Software 2012 – 2016 Forecast and Analysis and 2011 Vendor Share.* IDC 2012.
5. **Adamson M.** *MDM: A Top Trend to Follow for the Enterprise and Solution Providers Alike.* MDM Solutions News [электронный ресурс] / URL: <http://solutions-review.com/mobile-device-management/mdm-a-top-trend-to-follow-for-the-enterprise-and-solution-providers-alike/> (дата обращения 2013).
6. **Donovan F.** *Gartner: AirWatch, Citrix, MobileIron among MDM leaders* [электронный ресурс] / URL: <http://www.fiercemobileit.com/story/gartner-airwatch-citrix-mobileiron-among-mdm-leaders/2013-06-05> (дата обращения 2013).
7. **Обзор: Мобильные приложения для бизнеса 2013** [электронный ресурс] / URL: http://www.cnews.ru/reviews/new/mobilnye_prilozheniya_dlya_biznesa_2013/ (дата обращения 2013).
8. **Mind Commerce.** *The Future of Mobile Device Management (MDM)* [электронный ресурс] / URL: <http://blogs.skillsoft.com/learning-re-imagined/2014/03/the-future-of-mobile-device-management-mdm.html> (дата обращения 2013).
9. **Samochadin A., Raychuk D., Voinov N., Ivanchenko D., Khmelkov I.** *MDM based Mobile Services in Universities // International Journal of Information Technology & Computer Science.* 2014. Vol. 13. No. 2. Pp. 35–41.
10. **Gartner, Inc.** *Magic Quadrant for Mobile Device Management Software* [электронный ресурс] / URL: <http://www.gartner.com/technology/reprints.do?id=1-1FRG59X&ct=130523&st=sb> (дата обращения 2013).
11. **Solution Review.** *Mobile Device Management Buyers Guide.* 2014.
12. **Gray B., Kane C.** *Market Overview: On-Premises Mobile Device Management Solutions, Q3 2011.* 2012.
13. **Basso M., Redman P.** *Critical Capabilities for Mobile Device Management.* Gartner, Inc. 2012.
14. **Majdi E.B.** *Evaluation of Mobile Device Management tools and analyzing integration models for mobility enterprise.* Umee University, 2013.
15. **Унчин Р., Чебышев В.** *Мобильные угрозы – 2013.* ЗАО «Лаборатория Касперского» [электронный ресурс] / URL: https://www.securelist.com/ru/analysis/208050833/Mobilnye_ugrozy_2013 (дата обращения 2013).

REFERENCES

1. **Kennedy D.** *Information security: Wave 16. 2013 451 Research, LLC.* Available: <http://www.451research>
2. **Gartner, Inc.** *Top 10 Mobile Technologies for 2012 and 2013.* Available: <http://my.gartner.com/portal/server.pt?open=512&objID=270&mode=2&PageID=3862698&resId=1923514>
3. **Meidata.** *Mobile Device Management Global Market Analysis.* Available: <http://meidata.com/>
4. **Hoffman B.** *Worldwide Mobile Enterprise Management Software 2012 – 2016 Forecast and Analysis and 2011 Vendor Share.* IDC 2012.
5. **Adamson M.** *MDM: A Top Trend to Follow for the Enterprise and Solution Providers Alike.* MDM



Solutions News. Available: <http://solutions-review.com/mobile-device-management/mdm-a-top-trend-to-follow-for-the-enterprise-and-solution-providers-alike/>

6. **Donovan F.** *Gartner: AirWatch, Citrix, MobileIron among MDM leaders*. Available: <http://www.fiercemobileit.com/story/gartner-airwatch-citrix-mobileiron-among-mdm-leaders/2013-06-05>

7. *Obzor: Mobilnyye prilozheniya dlya biznesa 2013*. Available: http://www.cnews.ru/reviews/new/mobilnye_prilozheniya_dlya_biznesa_2013/

8. *Mind Commerce. The Future of Mobile Device Management (MDM)*. Available: <http://blogs.skillssoft.com/learning-re-imagined/2014/03/the-future-of-mobile-device-management-mdm.html>

9. **Samochadin A., Raychuk D., Voinov N., Ivanchenko D., Khmelkov I.** MDM based Mobile Services in Universities, *International Journal of Information Technology & Computer Science*, 2014,

Vol. 13. No. 2, Pp. 35–41.

10. **Gartner, Inc.** *Magic Quadrant for Mobile Device Management Software*. Available: <http://www.gartner.com/technology/reprints.do?id=1-1FRG59X&ct=130523&st=sb>

11. *Solution Review. Mobile Device Management Buyers Guide*. 2014.

12. **Gray B., Kane C.** *Market Overview: On-Premises Mobile Device Management Solutions, Q3 2011*. 2012.

13. **Basso M., Redman P.** *Critical Capabilities for Mobile Device Management*. Gartner, Inc. 2012.

14. **Majdi E.B.** *Evaluation of Mobile Device Management tools and analyzing integration models for mobility enterprise*. Umee University, 2013.

15. **Unuchin R., Chebyshev V.** *Mobilnyye ugrozy – 2013*. ZAO «Laboratoriya Kasperskogo». Available: https://www.securelist.com/ru/analysis/208050833/Mobilnye_ugrozy_2013

САМОЧАДИН Александр Викторович – профессор кафедры распределенных вычислений и компьютерных сетей Института информационных технологий и управления Санкт-Петербургского государственного политехнического университета.

195251, Россия, Санкт-Петербург, ул. Политехническая, д. 29.

E-mail: samochadin@gmail.com

SAMOCHADIN, Alexander V. *St. Petersburg State Polytechnical University.*

195251, Politekhnicheskaya Str. 29, St. Petersburg, Russia.

E-mail: samochadin@gmail.com

САМОЧАДИНА Татьяна Николаевна – старший преподаватель кафедры распределенных вычислений и компьютерных сетей Института информационных технологий и управления Санкт-Петербургского государственного политехнического университета.

195251, Россия, Санкт-Петербург, ул. Политехническая, д. 29.

E-mail: samochadina@dcn.icc.spbstu.ru

SAMOCHADINA, Tatiana N. *St. Petersburg State Polytechnical University.*

195251, Politekhnicheskaya Str. 29, St. Petersburg, Russia.

E-mail: samochadina@dcn.icc.spbstu.ru

ТИМОФЕЕВ Дмитрий Андреевич – старший преподаватель кафедры распределенных вычислений и компьютерных сетей Института информационных технологий и управления Санкт-Петербургского государственного политехнического университета.

195251, Россия, Санкт-Петербург, ул. Политехническая, д. 29.

E-mail: dtim@dcn.icc.spbstu.ru

TIMOFEEV, Dmitry A. *St. Petersburg State Polytechnical University.*

195251, Politekhnicheskaya Str. 29, St. Petersburg, Russia.

E-mail: dtim@dcn.icc.spbstu.ru

ПОПОВ Сергей Олегович – *IBS, руководитель проектов.*
127434, Россия, Москва, Дмитровское ш., д. 9Б.
E-mail: spopov@ibs.ru

ПОПОВ, Sergey O. *IBS Group Holding Ltd.*
127434, Dmitrovskoye Sh. 9B, Moscow, Russia.
E-mail: spopov@ibs.ru