НИИ СОКБ
ЦЕНТР РАЗРАБОТКИ

КОМПЛЕКСНАЯ ЦИФРОВАЯ МУЛЬТИПЛАТФОРМА УПРАВЛЕНИЯ МОБИЛЬНЫМИ СРЕДСТВАМИ КОММУНИКАЦИЙ

РЕАЛИЗАЦИЯ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ПЛАТЁЖНЫХ ТЕРМИНАЛОВ

SAFEMOBILE

Москва

2024

ФТ-5 Контроль установки программных решений по удаленному управлению устройствами

Есть несколько способов реализации данного требования, которые можно использовать по отдельности или совместно.

Вариант 1. Запрет самостоятельной установки приложений пользователем с помощью политик ограничений. В этом случае на устройстве будут установлены только те приложения, которые явно разрешил администратор.

Для этого нужно создать и назначить на устройство Android профиль типа «Политики ограничений Android», указав в нём политики, как показано на рисунке ниже:

- Запретить установку приложений – Да;
- Запретить установку приложений из неизвестных источников – Да;
- Запретить установку приложений из неизвестных источников в рабочем профиле и на устройстве – Да;
- Заблокировать сторонние магазины приложений – Да.

Также с помощью политики «Запретить захват экрана и дистанционную трансляцию экрана монитора» можно ограничить на устройстве работу любых приложений для удалённого управления экраном устройства. При включенном запрете ни одно приложение не сможет получить доступ к отображаемой на экране устройства информации.

Подробнее о создании и назначении профилей см. п. 2.6.8 Раздел «Профили» в руководстве администратора UEM SafeMobile.

Вариант 2. Режим киоска, в котором пользователю разрешён доступ только к тем приложениям, которые явно разрешил администратор. Настроить этот режим можно с помощью профиля типа «Режим киоска Android».

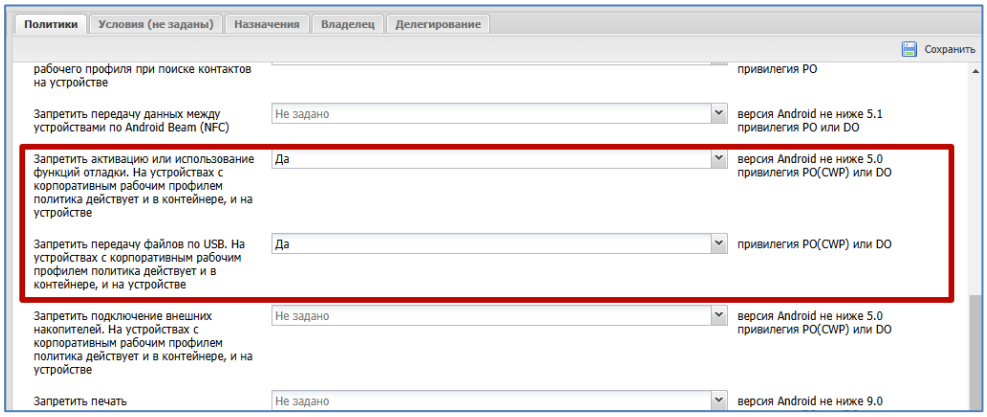
Вариант 3. Можно настроить выполнение автоматических действий в случае установки на устройство приложений из определённого администратором списка. Например, заблокировать устройство, стереть с него корпоративные данные или применить к нему дополнительные ограничения. Настроить это поведение можно с помощью правил несоответствия. Подробнее о создании и настройке таких правил см. п. 2.6.9 Раздел «Правила несоответствия» руководства администратора UEM SafeMobile.

АТ-22 Ограничение использования определенных типов устройств по USB

Уточнение требования. Например, с возможностью подключить устройство с правами администратора.

Штатные механизмы ОС Android позволяют управлять доступом к функциям отладки и передаче данных по USB. Чтобы ограничить пользователя в этих возможностях следует создать и назначить на устройство профиль типа «Политики ограничений Android», указав в нём политики, как показано на рисунке ниже:

- Запретить активацию или использование функций отладки – Да.
- Запретить передачу файлов по USB – Да.



Подробнее о создании и назначении профилей см. п. 2.6.8 Раздел «Профили» в руководстве администратора UEM SafeMobile.

Возможности ОС Android не позволяют раздельно управлять доступом к разным типам USB устройств. Например, запретить USB-накопители, но разрешить подключать внешнюю клавиатуру с помощью OTG-кабеля. Специализированный API

такого рода может быть предоставлен только производителем оборудования. Если он будет предоставлен, мы сможем интегрировать его в UEM SafeMobile.

АТ-23 Ограничение возможности установки приложений без подписи производителя/вендора

Запрет самостоятельной установки приложений пользователем с помощью политик ограничений согласно варианту 1 реализации требования ФТ-5. Проверка подписи приложений реализована на уровне прошивки платёжных терминалов и не может быть настроена с помощью внешних СЗИ, таких как UEM SafeMobile.

АТ-24 Ограничение возможности установки приложений, кроме явно разрешенных администратором

Запрет самостоятельной установки приложений пользователем с помощью политик ограничений согласно варианту 1 реализации требования ФТ-5.

АТ-28 Ограничение использования беспроводных сетей и интерфейсов доступа (NFC, Bluetooth)

Для ограничения доступа к NFC и Bluetooth рекомендуется применить на устройстве следующие политики из состава профиля типа «Политики ограничений Android»:

- Запретить Bluetooth на устройстве;
- Запретить передачу данных по Bluetooth с устройства;
- Запретить изменение настроек Bluetooth;
- Запретить передачу данных между устройствами по Android Beam (NFC).

Подробнее о создании и назначении профилей см. п. 2.6.8 Раздел «Профили» в руководстве администратора UEM SafeMobile.

АТ-29 Запрет режима отладки в ОС

Запрет реализуется с помощью применения к устройству политики ограничений «Запретить активацию или использование функций отладки», как это предложено в способе реализации требования АТ-22.