

**Планшетный компьютер Приемщика**

Регистрационный номер из 1С ТЗ\_ОТС\_74/24 от 23.09.2024

Срок действия: 1 год

**Функциональные требования:** Электронное мобильное устройство с сенсорным дисплеем позволяющее управлять набором мобильных приложений и дающее возможность взаимодействия с интерактивными компонентами ПО

**Объекты, на которых используется оборудование**

Магазин Магнит	Нет
Магнит Косметик	Нет
Магнит Аптека	Нет
Магнит Семейный	Нет
Магнит Опт	Нет
Распределительный центр	Да
Автотранспортное предприятие	Да
Головная компания, Округа, Филиалы	Нет

**Требования (минимальные)**

1. Операционная система — Android 12 или новее
2. Гарантированное, не менее чем одно, обновление ПО с повышением версии операционной системы Android
3. Дисплей – емкостный, multitouch
4. Диагональ дисплея – 7–8 дюймов
5. Динамик – обязательно
6. Разрешение дисплея – не менее 1280x800 пикселей
7. Процессор производительностью не менее чем Qualcomm Snapdragon 430, MediaTek Helio P20, HiSilicon Kirin 650, Samsung Exynos 7904
8. Оперативная память – не менее 4 Гб
9. Встроенная память – не менее 16 Гб
10. Фотокамер:
10.1. с автофокусом
10.2. Основная – не менее 8 Мп
11. Подключение через Wi-Fi (Подробные требования в Приложении 3)
12. Интерфейсы – micro-USB или USB type C
13. Датчики
13.1. G-сенсор
13.2. освещенности
14. Время автономной работы от аккумуляторной батареи – не менее 10 часов в активном режиме (при нахождении экрана во включённом состоянии с яркостью 50%)

15. Зарядное устройство – обязательное наличие в комплекте, с евровилкой
16. Класс защиты – не ниже IP 64
17. Рабочий диапазон температур – в диапазоне от +4 до +45 С
18. Ударопрочность – должен выдерживать многократные падения на бетонный пол с высоты не менее 1,2 м., в любой плоскости без нарушения функциональности устройства, во всем диапазоне рабочих температур
19. Комплектация ремнем для ношения на плече или запястье - обязательно
20. Поставляемое оборудование должно иметь заводскую сборку, выпускаться серийно и не должно входить в перечень оборудования, объявленного производителем к прекращению серийного производства
21. Гарантия — не менее 2 лет. Наличие на территории РФ развитой сети авторизованных сервисных центров
22. Соблюдение требований, предъявляемых к устройствам по управлению и конфигурированию средствами EMM AirWatch (Требования указаны в приложении 1)
23. ОС устройства должна поддерживать API по управлению со стороны EMM AirWatch
24. Прошивка не должна содержать следов компрометации устройства (отсутствие root, скриптовых «закладок» и т.д.)
25. Соблюдение требований стандартов управления устройствами с ОС Android (Требования указаны в приложении 2)
26. Наличие SDK, не требующего регистрации на серверах вендора и доступа к ним в ходе работы устройства (автономность работы SDK), либо предоставление расширенных системных привилегий для EMM MMobile, посредством подписи вспомогательного приложения EMM подписью вендора
27. При наличии интерфейсов удаленного управления должны обеспечиваться следующие требования ИБ:
27.1. Наличие механизмов авторизации и аутентификации.
27.2. Пароль должен удовлетворять требованиям к длине, сложности и сроку службы (не менее 12 символов и возможность устанавливать срок действия пароля).
27.3. Ролевая модель доступа к интерфейсу удаленного управления (пользователь \ администратор и т.д.).
27.4. Подключение с использованием безопасных протоколов (шифрование: например, HTTP's).
27.5. Поддержка распространенных корпоративных дистрибутивов операционных систем (Windows, Unix).

#### Ответственные за согласование

Подразделение	Пункты для согласования	Ф.И.О.
Отдел учета и тестирования оборудования	Все	Цой В. Ю.
Направление сопровождения логистики	7–11, 17	Беляева И. В.
Команда проекта «Иннополис»	Все	Никулин И. А.
Направление сетевой инфраструктуры	11	Красноперов А. С.
Сектор платформ управления пользовательскими устройствами	1, 12–15, 22-24	Тесленко С. А.
Отдел сопровождения пользователей	1, 12–15, 22-24	Шурбаев А. Е.

Группа противодействия мошенничеству	27	Лалаев О. В.
Управление по ИТ-сопровождению регионов	15, 21	Шаранов Д. С.
Направление входящего потока	1-21	Подлесный Д. Г.
Отдел по складской обработке маркированных товаров	1-21	Магомедова И. В.
Отдел сопровождения категории ИТ оборудование/ПО и персонала	Все	Власюк И. А.

## Приложение 1. Поддержка устройством требований EMM AirWatch.

Все указанные требования являются критичными и устройство должно их поддерживать.

Функции устройства	Управление	Обоснование
Allow Camera	включение/отключение доступа к камере	В рамках проекта может не использовать, и пользователь может использовать камеру для копирования корпоративных данных, а также пользователь может использовать устройства не по назначению (в личных целях)
Allow Factory Reset	включение/отключение доступа к «Сброс к заводским настройкам»	Злоумышленник может украсть устройство и попытаться сбросить корпоративные настройки или обойти установленные ограничения
Allow Airplane Mode	включение/отключение доступа к режиму «Самолет»	Пользователь может отключить каналы связи.
Allow Screen Capture	включение/отключение функции создание скриншотов	Пользователь не должен иметь возможности отключение экрана блокировки, вследствие незаблокированное устройство может привести к компроментации корпоративных данных
Allow Clipboard	включение/отключение работы с буфером обмена	Пользователь не должен иметь возможности копирования корпоративных данных из одного приложения в другое, для исключения компроментации данных
Allow USB Media Player	включение/отключение доступа к MTP	Пользователь не должен иметь возможности использования корпоративного устройства по неназначению
Allow NFC	включение/отключение доступа к NFC	Пользователь не должен иметь возможности передачи данных по NFC
Allow Safe Mode	включение/отключение доступа к «Безопасный режим»	Пользователь не должен иметь возможности загрузки устройства в «безопасном режиме»
Allow USB Debugging	включение/отключение доступа к «режиму разработчика»	Пользователь не должен иметь возможность подключать устройство в режиме разработчика, для исключения фактов управления устройством при помощи ПК
Allow USB Mass Storage	включение/отключение режима «устройство как хранилище (SD карта)»	Пользователь не должен иметь возможность подключать устройство к ПК в режиме внешнего хранилища, для исключения фактов компроментации корпоративных данных
Allow Google Backup	включение/отключение бэкапирования на сервера Google	Корпоративные данные не должны храниться на Google-серверах
Allow SD Card Access	включение/отключение доступа к SD карте	Пользователь не может иметь возможности работы с SD картами, для исключения фактов установки не согласованного ПО или переноса корпоративных данных на внешние хранилища
Allow USB Host Storage	включение/отключение режима «устройство как внешнее хранилище»	Для исключения фактов компроментации данных
Allow Google Play	включение/отключение доступа к Play Market	Пользователь не должен иметь возможности устанавливать на корпоративные устройства не согласованное ПО из Play Market-a
Allow Access to Device Settings	включение/отключение доступа к настройкам устройства	Пользователь не должен иметь возможности изменять настройки устройства под свои личные цели

Allow Developer Options	включение/отключение доступа к настройкам «режима разработчика»	Пользователь не должен иметь возможности изменять настройки устройства под свои личные цели
Allow Non-Market App Installation	включение/отключение установки приложений из неизвестных источников	Может привести к установке несогласованного ПО
Allow Copy & Paste Between Applications	включение/отключение обмена данными между приложениями посредством буфера обмена	Пользователь не должен иметь возможности копирования корпоративных данных из одного приложения в другое, для исключения компроментации данных
Allow Google Account Sync	включение/отключение синхронизации с серверами Google	Корпоративные данные не должны храниться на Google-серверах
Allow Bluetooth	включение/отключение управления Bluetooth	Пользователь может воспользоваться данной функцией для передачи корпоративных данных другое устройство, через Bluetooth
Allow Data Connection	включение/отключение доступа к передаче данных по мобильным сетям/Wi-Fi	Пользователь может воспользоваться данной функцией для передачи корпоративных данных по неразрешенным типам связи
Allow Wi-Fi Profiles	включение/отключение доступа к настройкам wi-fi соединений	Пользователь может попытаться подключить устройство не к корпоративным Wi-fi сетям
Allow Wi-Fi Changes	включение/отключение доступа к настройкам wi-fi соединений	Пользователь может попытаться подключить устройство не к корпоративным Wi-fi сетям + защита настроенных профилей от изменения
Block Wi-Fi Networks by SSID	управление списком запрещенных wi-fi сетей	Должна быть возможность управлять Wi-fi соединениями. Для исключения фактов подключений к запрещенным Wi-Fi сетям
Allow Native VPN	включение/отключение доступа к настройкам VPN соединений	Должна быть возможность управлять VPN соединениями. Для исключения фактов подключений к некорпоративным VPN серверам
Allow Wi-Fi Direct	включение/отключение использование Wi-Fi директ	Пользователь может попытаться подключить устройство не к корпоративным Wi-fi сетям.
Allow Infrared	включение/отключение ИК-порта	Пользователь может воспользоваться данной функцией для передачи корпоративных данных другое устройство, через ИК порт
Set WiFi Sleep Setting	управление настройками «спящего режима» для Wi-Fi модуля	Предотвратить засыпание WiFi модуля
Allow Cellular	включение/отключение передачи данных через мобильные сети	Запрет использования мобильных данных во внутренних проекта
Allow All Tethering	включение/отключение работы устройства в режиме «точка доступа»	Пользователь может воспользоваться данной функцией для открытия доступа к корпоративным Wi-Fi сетям
Allow Wi-Fi Tethering	включение/отключение работы устройства в режиме Wi-Fi «точка доступа»	Пользователь может воспользоваться данной функцией для открытия доступа к корпоративным Wi-Fi сетям
Allow Bluetooth Tethering	включение/отключение работы устройства в режиме Bluetooth-модема	Пользователь может воспользоваться данной функцией для открытия доступа к корпоративным Wi-Fi сетям
Allow USB Tethering	включение/отключение работы устройства в режиме USB-модема	Пользователь может воспользоваться данной функцией для открытия доступа к корпоративным Wi-Fi сетям
Allow Task Manager	включение/отключение доступа к Диспетчеру задач	Пользователь может воспользоваться данной функцией для попытки управления устройством

Allow Email Forwarding	включение/отключение автопересылки писем на почтовые ящики	Запрет настройки автопересылки почты на другой email
Disable Non-Enterprise Email Account Addition	включение/отключение регистрации некорпоративной почты	Запрет регистрации личных п/я на корпоративных устройствах
Prevent Installation of Blacklisted Apps	включение/отключение блокирования установки/запуска приложений из черного списка	Должна быть возможность управлять «Черным списком» приложения, для исключения фактов установки несогласованного ПО
Prevent Un-Installation of Required Apps	включение/отключение блокирования удаления приложений из списка «Обязательных приложений»	Должна быть возможность управлять списком обязательных приложения, для исключения фактов удаления ПО пользователем
Allow Only Whitelisted Apps	включение/отключение блокирования установки приложений не входящих в «Белый» список	Должна быть возможность управлять «Белым списком» приложения, для установки/использования только разрешенного ПО
Silent Application Install	установка приложений без запросов у пользователя	Должна быть возможность установки ПО без привлечения к этому пользователя, т. к. пользователь может отказаться от установки
Allow Activation Lock	включение/отключение доступа к активации устройства на серверах Google	Пользователь не должен иметь возможности активировать устройство на свою УЗ с целью дальнейшего его управления из Google аккаунта
Allow Developer Mode	включение/отключение доступа к «режиму разработчика»	Запрет использования режима отладки и разработки на пользовательских устройствах
Allow Firmware Recovery	включение/отключение доступа к режиму «Восстановления»	Пользователь может воспользоваться данным режимом для несогласованного обновления прошивки или сброса к заводским настройкам
Remote Control	Удаленное управление устройством и доступ файлам устройствам	Для упрощения процесса техподдержки должна быть возможность удаленного управления экраном устройства, а также получения файлов с устройств
Certificate Management	удаленная установка/удаление сертификатов с устройства	Для корректной работы с корпоративными ресурсами требуется возможность устанавливать и удалять сертификаты на устройствах компании
Silent Certificate Install	тихая установка сертификатов	Для корректной работы с корпоративными ресурсами требуется устанавливать на устройства сертификаты компании без привлечения к этой процедуре пользователя
Allow Lock Screen Settings	включение/отключение/изменение корпоративных настроек экрана блокировки	Для настройки экрана блокировки согласно требованиям ИБ

## Приложение 2. Поддержка устройством требований EMM mMobile.

1. На устройстве не должно быть предустановленного приложения, являющегося DeviceOwner
2. На устройстве не должно быть скриптов, сервисов или других механизмов, автоматически изменяющих состав администраторов или DeviceOwner'ов устройства (например, устройство автоматически ставит администратором какое-то приложение вендора)
3. На устройстве должна корректно работать отладка по USB или не должно быть препятствий для её включения
4. Устройство не должно при своём запуске запускать приложения вендора, перекрывающие экран
5. Реализация подсистемы Android Enterprise должна быть стандартной
6. Устройство не должно автоматически изменять состав заблокированных/отключённых приложений
7. Операционная система при наличии Google-сервисов должна поддерживать стандартный мастер настроек Google, при отсутствии, аналогичное решение вендора, которое бы позволяло установить DeviceOwner с помощью QR-кодов на сброшенное до заводских настроек устройство.

## Приложение 3. Требования, предъявляемые к устройствам для работы в среде Wi-Fi.

1. Все устройства должны соответствовать российским требованиям и нормам. Технические характеристики радио модуля устройства должны соответствовать требованиям решения ГКРЧ от 07.07.2007 №07-20-03-001, приложения к решению ГКРЧ от 16.06.2021г. №21–58-05.
2. Устройство должно поддерживать частотные каналы шириной 20MHz и 40MHz.
3. Устройство должно поддерживать работу в сетях с открытым и скрытым SSID
4. Должен быть предусмотрен режим отключения одного из модулей.
5. Должен быть предусмотрен выбор приоритета одного из модулей.
6. Устройство должно поддерживать работу в следующих стандартах сети Wi-Fi:

	ММ/МК/МА	ГМ	РЦ	Ф	ГК	СП/ТК
Сети 802.11b/g/n (2.4 ГГц)	+	+	+	+	+	+
Сети 802.11a/n (5 ГГц)	+	+	+	+	+	+
Сети 802.11ac	*	*	+	+	+	+
Сети 802.11ac wave 2	-	-	+	*	+	*
Сети 802.11ax	-	-	*	*	*	-

7. Устройство должно поддерживать протоколы роуминга в сети Wi-Fi:

	ММ/МК/МА	ГМ	РЦ	Ф	ГК	СП/ТК
Протокол 802.11v	-	+	+	+	+	+
Протокол 802.11k	-	+	+	+	+	+
Протокол 802.11r	-	-	+	+	+	+

8. Устройство должно поддерживать протоколы авторизации в сети Wi-Fi:

	ММ/МК/МА	ГМ	РЦ	Ф	ГК	СП/ТК
Авторизация по протоколу WEP	+	+	+	+	+	-
Авторизация по протоколу WPA/WPA2-PSK	+	+	+	+	+	+
Авторизация по протоколу WPA2-Enterprise (EAP-PEAP), логин + пароль	+	+	+	+	+	+
Авторизация по протоколу WPA2-Enterprise (EAP-TLS), логин + сертификат	+	+	+	+	+	+

9. Устройство должно поддерживать настройку для работы в сети по протоколу DHCP
10. Должен быть предусмотрен режим ручной настройки IP-протокола.

Пояснения к таблицам: '+' – обязательно требуется, '-' – не требуется, '\*' – рекомендовано.