КОД безопасности

Secret MDM

Система управления безопасностью корпоративных мобильных устройств

- Снижение расходов на управление и защиту корпоративных мобильных устройств
- Повышение эффективности рабочих процессов за счет возможности сотрудников подключаться с мобильных устройств
- Соответствие политикам безопасности и нормативным требованиям
- Возможность развертывания в инфраструктуре с десятками тысяч устройств
- Гибкая политика лицензирования по устройствам

Возможности

Управление мобильными устройствами (MDM)

- Управление настройками устройств, звонками, СМС-сообщениями на базе Android с помощью механизма политик.
- Настройка подключений к точкам доступа Wi-Fi.
- Настройка прокси для выхода в Интернет через Wi-Fi.
- Запрет на подключение к недоверенным точкам доступа и ведение «белого» и «черного» списков Wi-Fi.
- Запрет на использование Wi-Fi, Bluetooth, NFC.
- Запрет на использование встроенной фотовидеокамеры и микрофона.
- Управление доступом к серверу корпоративной почты (Exchange).

Поддержка устройств MIG.

Android 9, 10, 11.

Управление приложениями и мониторинг

- Установка приложений из Google Play.
- Распространение приложений из корпоративного магазина приложений или других источников по протоколу https.
- Управление установкой и удалением приложений, в том числе из недоверенных источников.
- Просмотр журналов активностей, переданных с устройства на сервер управления MDM.

Мобильная безопасность

- Удаленная блокировка устройства и управление парольной защитой.
- Удаленный сброс или смена пароля блокировки для восстановления доступа к устройству.
- Дистанционная очистка устройства (затирание всех данных).

Архитектура MDM

Сценарии применения

Органы охраны правопорядка

Задачи

- Патрулирование, идентификация и проверка физических лиц
- Контроль соблюдения правил дорожного движения

Преимущества использования защищенных устройств

- Автоматизация рутинных операций
- Интеграция в ведомственные ИС
- Юридически значимое взаимодействие
- Фиксация местонахождения сотрудника МВД
- Подключаемый сканер для дактилоскопии
- NFC для считывания паспортов нового поколения и электронных карт владельцев оружия

Угрозы

- Потеря устройства
- Перехват передаваемых данных
- Несанкционированный доступ к ведомственным ИС
- Несоответствие требованиям регуляторов

Органы исполнительной власти (Выездная контрольно-надзорная деятельность)

Задачи

- Контроль строек и эксплуатации зданий
- Контроль соблюдения природоохранного законодательства
- Контроль благоустройства территории
- Контроль вывоза мусора и обнаружение несанкционированных свалок

Преимущества использования защищенных устройств

- Отслеживание маршрутов и местоположения
- Фото-видео фиксация нарушений
- Составление уведомлений, актов
- Быстрая актуализация информации
- Юридически значимое взаимодействие

Угрозы

- Потеря устройства
- Перехват передаваемых данных
- Несанкционированный доступ к ведомственным ИС
- Несоответствие требованиям регуляторов

Энергетика и ТЭК (Техническое обслуживание и ремонт)

Задачи

- Поддержание инфраструктуры в исправном состоянии
- Автоматизация работы полевых бригад
- Сбор показаний скважинных замеров
- Технологические обходы, мониторинг и диагностика состояния оборудования и трубопроводов

Преимущества использования защищенных устройств

- Защищенное исполнение устройств
- Отказ от бумажных операций (выдача нарядов-допусков и т.д.)
- Удобный учет расходников и запасных частей
- Применимость во взрывоопасных зонах и местах вероятного воспламенения горючей пыли
- Подключаемые тепловизор и виброметр
- Поддержка NFC и RFID (UHF) для бесконтактного взаимодействия

Угрозы

- Использование устройства не по назначению
- Подмена информации по наряду и необходимым работам на объекте
- Потеря устройства

Техническая поддержка

Техническая поддержка продуктов Secret MDM может осуществляться как напрямую, силами специалистов компании «Код Безопасности», так и через авторизованных партнеров. В случае технической поддержки через партнера, партнер обеспечивает первую линию технической поддержки, а в случае сложных вопросов обращается в службу технической поддержки вендора.

Каталог услуг	Пакет поддержки			
	Базовый	Стандартный	Расширенный	VIP
Способ обращения в ТП	e-mail	веб-портал, e-mail	телефон, веб-портал, e-mail	
Приоритет	Низкий	Средний	Высокий	Наивысший
Консультирование по установке и использованию продукта	●	●	●	●
Доступ к Базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Работа над инцидентами в режиме 8x5 (рабочие дни МСК 10:00–18:00)	●	●	●	●
Регистрация и контроль обращений на веб-портале		●	●	●
Работа над критичными инцидентами в режиме 24x7			●	●
Консультирование по дополнительному функционалу продукта			●	●
Выделенный инженер (для проведения работ)				●
Присутствие инженера на площадке заказчика				●

О компании «Код Безопасности»

Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

+7 (495) 982-30-20 (многоканальный) **info@securitycode.ru** **www.securitycode.ru**