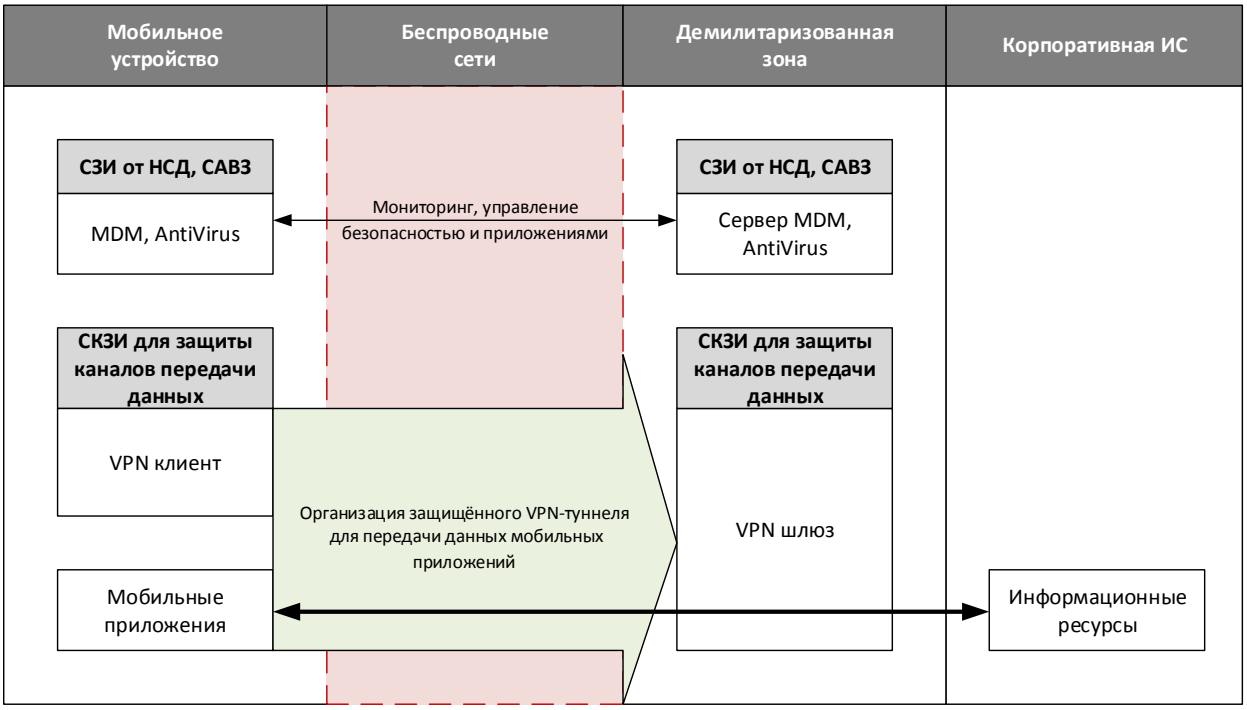
Концепция защищённого удалённого доступа к корпоративной информационной системе с мобильных устройств

Сокращения

1. ИС- информационная система
2. ЛВС – локальная вычислительная сеть.
3. МУ – мобильное устройство.
4. МЭ – межсетевой экран.
5. НСД – несанкционированный доступ.
6. ОС – операционная система.
7. ПО – программное обеспечение.
8. САВЗ – средство антивирусной защиты.
9. СЗИ – средство защиты информации.
10. СКЗИ – средство криптографической защиты информации.

Типовая схема защищённого удалённого доступа



Приведённая схема организации защищённого удалённого доступа может применяться, как в государственных, так и корпоративных ИС любого уровня защищенности.

Описание компонентов

СЗИ от НСД, САВЗ

В качестве СЗИ от НСД возможно использовать EMM SafePhone (сертификат ФСТЭК России № 4157 до 03.09.2024), включено в Единый реестр российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (рег.№ 4435 от 12.04.2018).

ПО SafePhone успешно внедрено в ГИС здравоохранения города Москвы, Московской и Калужской областей. ПО SafePhone является единственной мультиплатформой управления МУ, включая МУ на базе ОС Android, iOS, Sailfish (Аврора), Tizen, Windows и macOS, сертифицированной ФСТЭК России.

Завершены работы по интеграции ПО SafePhone с антивирусными библиотеками Лаборатории Касперского. Подана заявка на сертификацию совместного решения на соответствие требованиям ТУ, требованиям доверия и требованиям профиля защиты САВЗ типа «В» четвёртого класса защиты.

Ключевые функциональные возможности продукта:

1. Мониторинг местоположения МУ, включая контроль соблюдения МУ регламентных маршрутов и контроль посещения МУ определённых администратором геозон.
2. Контроль признаков наличия программного взлома МУ (root) с автоматическим удалением корпоративных приложений и их данных в случае обнаружения.
3. Управление политиками безопасности мобильных устройств:
   3.1. Настройка требований к паролям – наличие, сложность, срок действия, число смен пароля до возможности его повтора, число ошибок ввода пароля, приводящих к сбросу МУ к заводским настройкам.
   3.2. Управление доступом к интерфейсам записи и передачи данных – камера, микрофон, NFC, USB, Wi-Fi, мобильный интернет, режим мобильной точки доступа (tethering), внешние SD-карты памяти, совершение звонков и отправка сообщений.
   3.3. Ограничение возможности установки и удаления приложений пользователем МУ.
   3.4. Ограничение доступа к функциям и режимам работы МУ, способным нарушить работу СЗИ и СКЗИ – включение авиарежима или режима разработчика, возможность изменения даты и времени пользователем МУ, загрузка МУ в безопасном режиме.
4. Управление мобильными приложениями:
   4.1. Установка, и обновление приложений, нужных для работы. При этом с помощью SafePhone возможно при необходимости вернуть предыдущую версию приложения, если новая версия содержит ошибки или менее удобна.
   4.2. Централизованная настройка мобильных приложений[1] – распространение параметров подключения и параметров, специфичных для отдельных регионов или пользователей.
   4.3. Блокировка и удаление приложений, мешающих работе – мессенджеры, социальные сети, предустановленные игры и развлекательные сервисы.
5. Удалённая блокировка МУ или сброс МУ к заводским настройкам в случае потери или кражи МУ или подготовки МУ для нового сотрудника.
6. Инвентаризация параметров МУ – марка, модель, версия ОС, серийный номер, идентификатор GSM модуля (IMEI), данные о SIM-карте (идентификатор ICCID, номер телефона), уровень заряда батареи, данные о пользователе МУ (ФИО, должность, место работы).
7. Поиск и устранение вредоносного ПО на МУ.

СКЗИ для защиты каналов передачи данных

СКЗИ предназначены для организации защищённого VPN туннеля с ГОСТ шифрованием между МУ и корпоративной ЛВС. Наличие общего VPN туннеля для мобильных приложений на МУ позволяет им получать защищённый удалённый доступ к корпоративным информационным ресурсам без необходимости использования библиотек СКЗИ в мобильных приложениях и проведения тематических исследований, связанных с использованием библиотек СКЗИ.

В России представлены два производителя, предоставляющих решения для построения VPN на МУ – это решения компаний ИнфоТеКС (ViPNet) и КриптоПро (NGate). Решения обоих производителей

[1] Для обеспечения возможности удалённой настройки мобильные приложения должны поддерживать соответствующие механизмы производителя ОС МУ

полностью совместимы с SafePhone. Если в корпоративной инфраструктуре уже представлено одно из этих решений, его можно распространить на МУ, что позволит сократить затраты на внедрение и последующее сопровождение СКЗИ. Далее кратко о преимуществах каждого из решений.

Преимущества ViPNet от ИнфоТеКС – наличие действующего сертификата ФСБ России на VPN клиент для Android и iOS.

Преимущества КриптоПро NGate[2]:

1. Возможность удалённого конфигурирования VPN клиента с помощью SafePhone.
2. Отсутствие необходимости предварительной загрузки на МУ ключей шифрования вручную администратором СКЗИ.
3. Возможность аутентификации доступа пользователя к VPN с помощью корпоративных учётных записей в каталоге LDAP.

Преимущества использования МУ Samsung

1. Возможность организации эффективной защиты от несанкционированного доступа (НСД) к информации МУ путём установки неоригинальных образов восстановления (recovery), которые загружаются вместо Android и предоставляют злоумышленнику доступ к данным МУ. На МУ других производителей технических мер защиты от этой атаки нет.
2. Наличие механизмов автоматической установки СЗИ в процессе первичной инициализации МУ, исключающих компрометацию МУ до установки СЗИ. Аналогичные механизмы для МУ других производителей в России недоступны.
3. Возможность управления обновлениями ОС МУ – запрет обновления ОС МУ или установка на МУ предварительно одобренных администратором обновлений ОС. Аналогичных функций на МУ других производителей нет.

[2] Сертификация СКЗИ для Android и iOS планируется в 2021 году