



SafePhone PLUS

Комплексное решение для защиты корпоративной мобильной связи

Корпоративные заказчики испытывают потребность в обеспечении конфиденциальности переговоров, как с мобильными, так и с находящимися в пределах корпоративной АТС стационарными абонентами. Если несколько лет назад решения для защиты корпоративной сотовой связи были актуальны только для крупных холдинговых структур, органов власти и режимных государственных предприятий, то в настоящее время готовность использовать такие решения, высказывает все большее количество средних и малых коммерческих компаний.

Компании «НИИ СОКБ» и «ИнфоТеКС» предлагают российским заказчикам решение SafePhone PLUS для защиты корпоративной мобильной связи на основе систем SafePhone и ViPNet, разработанных для обеспечения информационной безопасности в корпоративной мобильной инфраструктуре.



SafePhone
ViPNet & VoIP **PLUS**

Задача защиты корпоративной мобильной связи

Обычно задача защиты корпоративной мобильной связи формулируется следующим образом:

- обеспечить конфиденциальность переговоров, ведущихся с использованием средств мобильной связи;
- блокировать возможный канал прослушивания акустической обстановки вблизи мобильного устройства, когда он не используется.

Угрозы безопасности корпоративной мобильной связи

Основными практически реализуемыми и наиболее используемыми угрозами безопасности корпоративной мобильной связи являются:

- прослушивание акустической обстановки вокруг мобильного устройства;
- адресное прослушивание разговоров конкретного абонента в реальном времени или в отложенном режиме через оператора связи и без него;
- несанкционированный доступ к хранящейся на мобильном устройстве информации, при его утрате;
- несанкционированный доступ в корпоративную сеть, если мобильное устройство используется для доступа к корпоративным ресурсам;
- определение местоположения абонента.

Решения для защиты мобильного голосового трафика разрабатываются как в России, так и за рубежом. Как правило, они имеют специализированную программную и аппаратную часть, обеспечивают закрытую связь только между аналогичными аппаратами, требуют особого технического и сервисного обслуживания, защищают только голосовой трафик, исключая передачу данных, выпускаются ограниченными партиями и достаточно дороги.

Другим перспективным направлением обеспечения конфиденциальности телефонных переговоров является использование не «тяжелых» специализированных телефонов, оснащенных чипами для защищенной беспроводной связи, а «легких» серийных мобильных устройств с развернутым на них программным обеспечением, позволяющим защитить передачу данных и общение через Интернет с использованием технологий VoIP.

Задачи SafePhone PLUS

Комплексное решение SafePhone PLUS для защиты корпоративной системы связи разработано на основе анализа угроз, а также с учетом отечественного и зарубежного опыта. В число задач, решаемых с использованием решения SafePhone PLUS, входят:

- обеспечение безопасности телефонных переговоров;
- защита мобильного устройства и информации, хранящейся на нем;
- обеспечение защищенного доступа к корпоративным ресурсам;
- конфиденциальный обмен данными;
- обеспечение безопасной видеоконференцсвязи на мобильных устройствах;
- реализация возможностей интеграции с корпоративной АТС.

Технологии SafePhone PLUS

Решение построено на базе системы SafePhone для защиты информации на корпоративных мобильных устройствах и защищенной доверенной среды передачи информации ViPNet с использованием публичных и выделенных каналов связи. На мобильном устройстве (смартфон или планшетный компьютер) развертываются клиентские программы SafePhone, ViPNet и SIP-клиент, а на контролируемой территории предприятия — серверные компоненты этих систем: SafePhone Server, ViPNet Coordinator, Server SIP.

Алгоритм функционирования SafePhone PLUS

- При необходимости ведения конфиденциального разговора на мобильном устройстве запускается программа создания виртуального защищенного канала связи.
- Далее запускается приложение SIP, поддерживающее сетевой протокол прикладного уровня, и набирается номер желаемого абонента.
- При поднятии трубки происходит установление сессии и передача голоса в форме зашифрованных пакетов данных.

Задержки, возможные при ведении таких переговоров, измеряются долями секунды, а возможность приема и выполнения звонков по GSM-каналу остается. Кроме того, на мобильном устройстве постоянно работает приложение, обеспечивающее защиту от несанкционированной записи разговора по акустическому каналу и защиту от несанкционированного доступа к информации при его утрате.

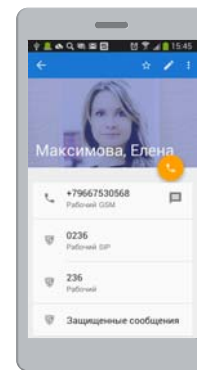
Компоненты, входящие в состав решения SafePhone PLUS



Первый компонент решения, **SafePhone**, представляет собой систему защиты информации на корпоративных мобильных устройствах с централизованным управлением. Функции SafePhone:

- защита от несанкционированного доступа к конфиденциальной информации;
- предотвращение несанкционированной установки стороннего программного обеспечения;
- ведение банка доверенного программного обеспечения;
- контроль использования служебных мобильных устройств;
- применение различных политик безопасности на территории предприятия и за ее пределами;
- мониторинг событий и подготовка отчетов.

Система SafePhone сертифицирована ФСТЭК России и позволяет построить систему защиты информации на корпоративных мобильных устройствах, обеспечивает централизованное управление парком мобильных устройств и защиту от утечки информации, обрабатываемой на данных устройствах.



Второй компонент решения, **Mobile VoIP**, обеспечивает голосовую связь по каналам Интернет или по локальным сетям, доступным с мобильного устройства. Его функциональное назначение:

- конфиденциальные переговоры с мобильными и стационарными абонентами;
- снижение затрат на оплату GSM трафика;
- переадресация звонков;
- единый номер в компании (при интеграции с УПАТС);
- информация о состоянии защищенности звонка и качестве соединения.

Специализированный мобильный клиент VoIP для SafePhone PLUS позволяет выбрать способ осуществления звонка – через защищенный IP канал, или через GSM. При звонке на контакт с несколькими мобильными или стационарными телефонами, Mobile VoIP осуществляет последовательный набор всех номеров. О наличии защиты текущего соединения мобильный клиент информирует пользователя визуально.



Третий компонент решения, **ViPNet**, представляет собой защищенную доверенную среду передачи информации с использованием публичных и выделенных каналов связи (Интернет, телефонные и беспроводные линии связи) путем организации виртуальной частной сети (VPN) с централизованным управлением. Функции ViPNet:

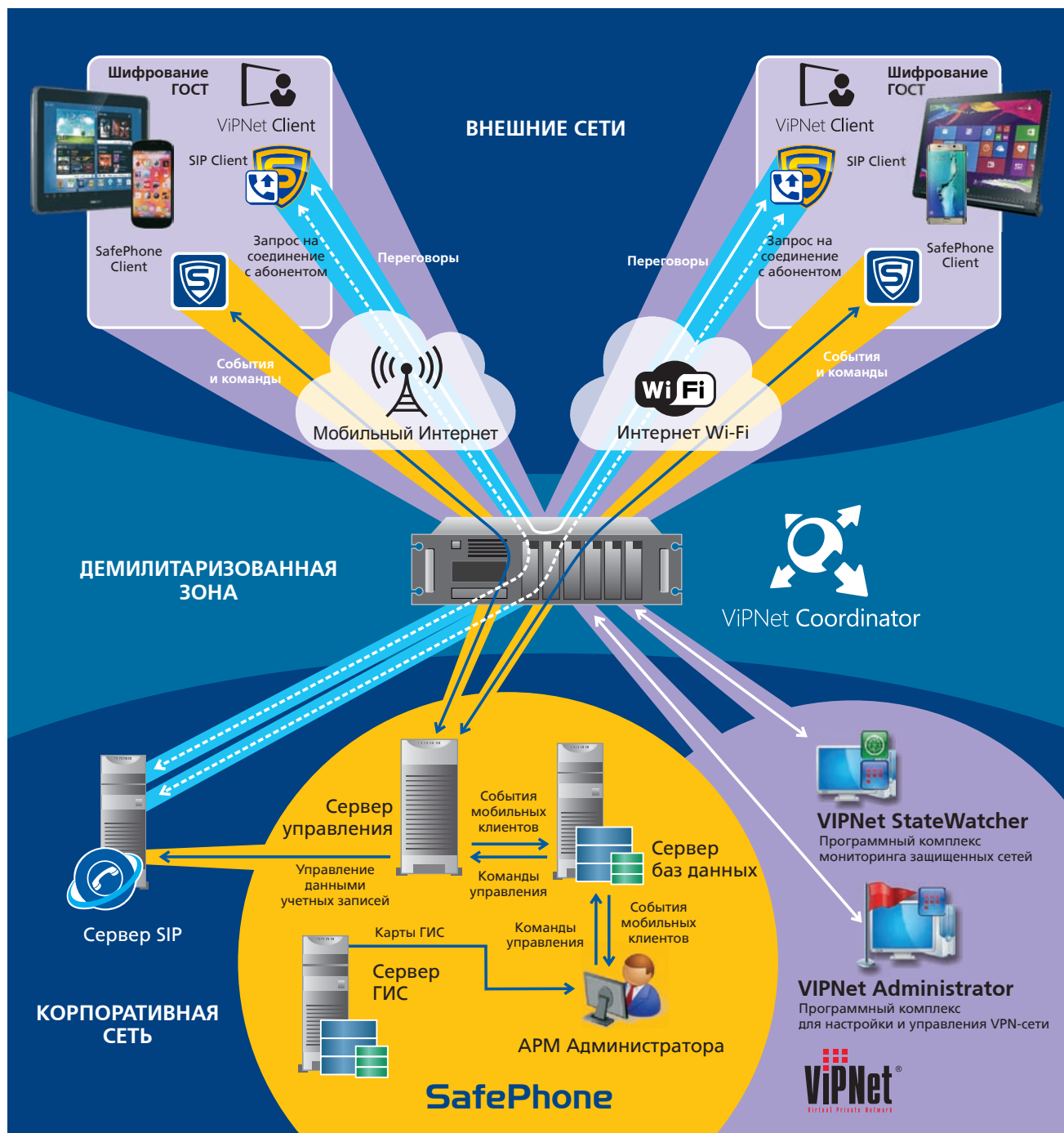
- обеспечение защищенного доступа к корпоративным информационным ресурсам;
- обеспечение доступа к корпоративным терминальным серверам и веб-порталам;
- защита IP-телефонии и других средств коммуникации;
- защита мобильного устройства от сетевых атак.

ViPNet является решением с российской криптографией, сертифицированным ФСБ Российской Федерации.

Особенности SafePhone PLUS

- SafePhone PLUS является российским решением, соответствующим требованиям регулирующих органов;
- сертификация решения по требованиям регуляторов в области ИБ;
- возможность «кастомизации» решения в интересах заказчика, включая предустановку компонентов непосредственно на заводах-изготовителях ведущих мировых производителей мобильных устройств.

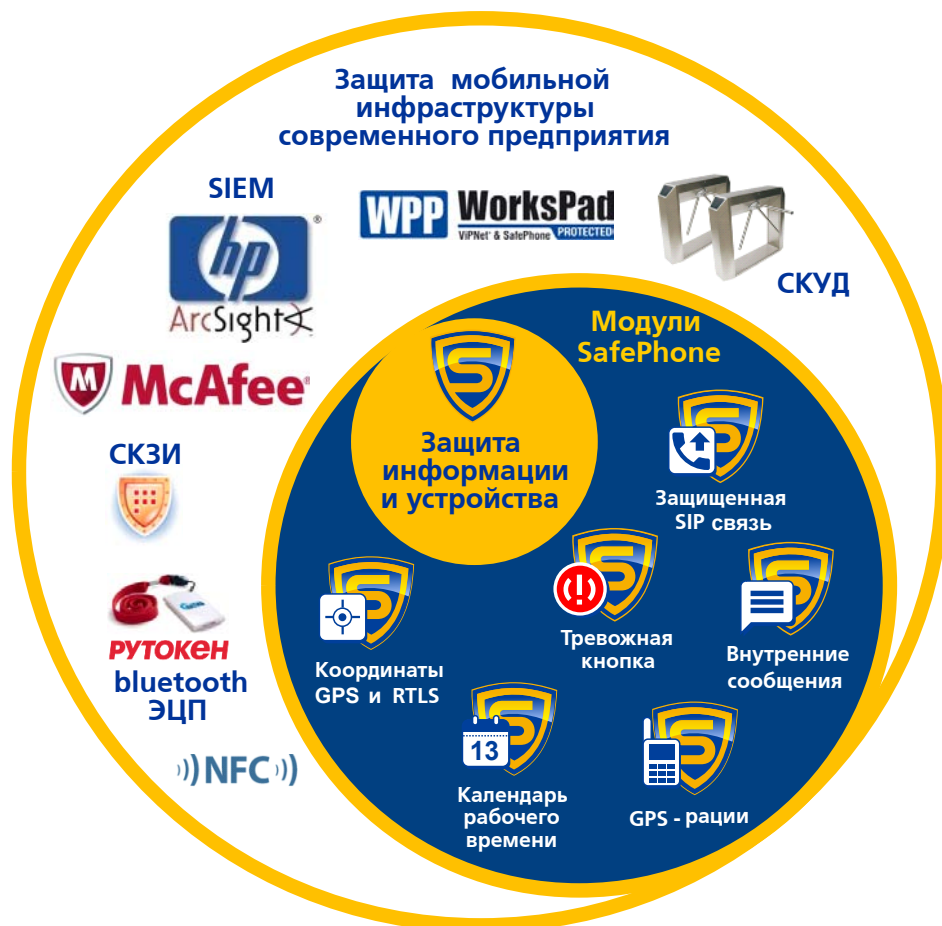
Архитектура решения SafePhone PLUS



SafePhone

ViPNet® & VoIP PLUS

Интеграция SafePhone PLUS с другими продуктами информационной безопасности позволяет создать экосистему защищенной корпоративной мобильности. При этом мобильные устройства по своим функциональным возможностям остаются полноценными инструментами для коммуникаций и для работы с корпоративными данными.



Сертификаты

SafePhone

Сертификат соответствия ФСТЭК России №3005 от 24.10.2013. Срок действия: 24.10.2019

Сертификат соответствия ГАЗПРОМСЕРТ ГО00.RU.1313.H00299 от 08.02.2015. Срок действия: 07.02.2018

ViPNet Client for Android

Сертификат соответствия ФСБ России № СФ/114-3056 от 10.02.2017. Срок действия: 01.06.2018

ViPNet Client for iOS

Сертификат соответствия ФСБ России № СФ/114-3055 от 10.02.2017. Срок действия: 10.08.2018

