

Краткое описание системы «ТАЛИСМАН В-FORCE»

Система «ТАЛИСМАН В-FORCE» предназначена для организации защищенной IP телефонной связи, между абонентами «Интернет» или ведомственной цифровой сети связи. Представляет собой набор технических средств и программного обеспечения, используемых в целях нейтрализации всех видов атак на информационные ресурсы абонента, при проведении сеансов связи, со стороны любого потенциального противника. Несмотря на некоторую схожесть «ТАЛИСМАН В-FORCE» с системой «Skype» она использует собственные алгоритмы и является отдельной инновационной разработкой. Использование в качестве транспортной среды «ИНТЕРНЕТ», которая, обладает более высоким уровнем разведдоступности по отношению к сетям связи PSTN потребовало применения целого комплекса мер, помимо шифрования, гарантирующих безопасность информации. Реализация проекта основывалась на специально построенной модели потенциального противника, с учетом предполагаемых возможностей по негласному получению защищаемой информации, что позволило во многом нейтрализовать его действия.

Процессы работы системы состоят из нескольких этапов:

1 этап регистрация абонента в сети, происходит автоматически при включении компьютера без участия абонента;

шаг 1 установление соединения;



шаг 2 формирование зашифрованного виртуального тоннеля между сервером и абонентом;



После установления соединения начинается процесс формирования ключевой информации, а по его окончании организуется зашифрованный VPN канал связи между сервером и абонентом. В дальнейшем все процессы происходят под защитой первого контура шифрования, который обеспечивает:

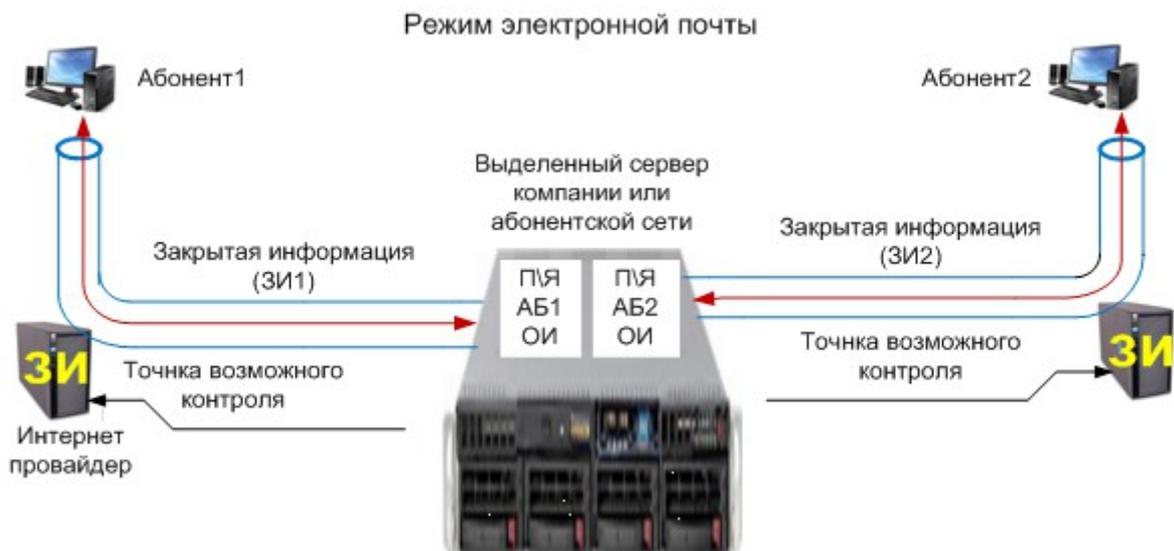
- шифрование идентификационных данных абонентов;
- шифрование адресной информации, т. е. определить кто, когда и кому звонил не возможно;
- защиту информационного (речевого) сигнала от идентификации с ликвидацией всех демаскирующих признаков сеансов связи. В канале связи постоянно идет цифровой трафик «криптогамма». Установить сам факт соединения абонентов не возможно так как не занятый (пустой) канал связи по сигналу ни чем не отличается от используемого при сеансе связи;
- шифрование информации при работе в режиме «электронной почты»;
- шифрование информации на участке «абонент – сервер» при выходе на открытые сети связи PSTN и GSM;

шаг 3 обмен идентификационными данными и регистрация абонента в сети;



Все необходимые регистрационные данные абонентов хранятся на сервере в зашифрованном виде. Системы защиты не позволяют получить их даже при попадании оборудования в руки противника. Сервер работает под управлением специально разработанной операционной системы DNLinux.

2 этап использование системы для передачи файлов и коротких сообщений в режиме электронной почты.



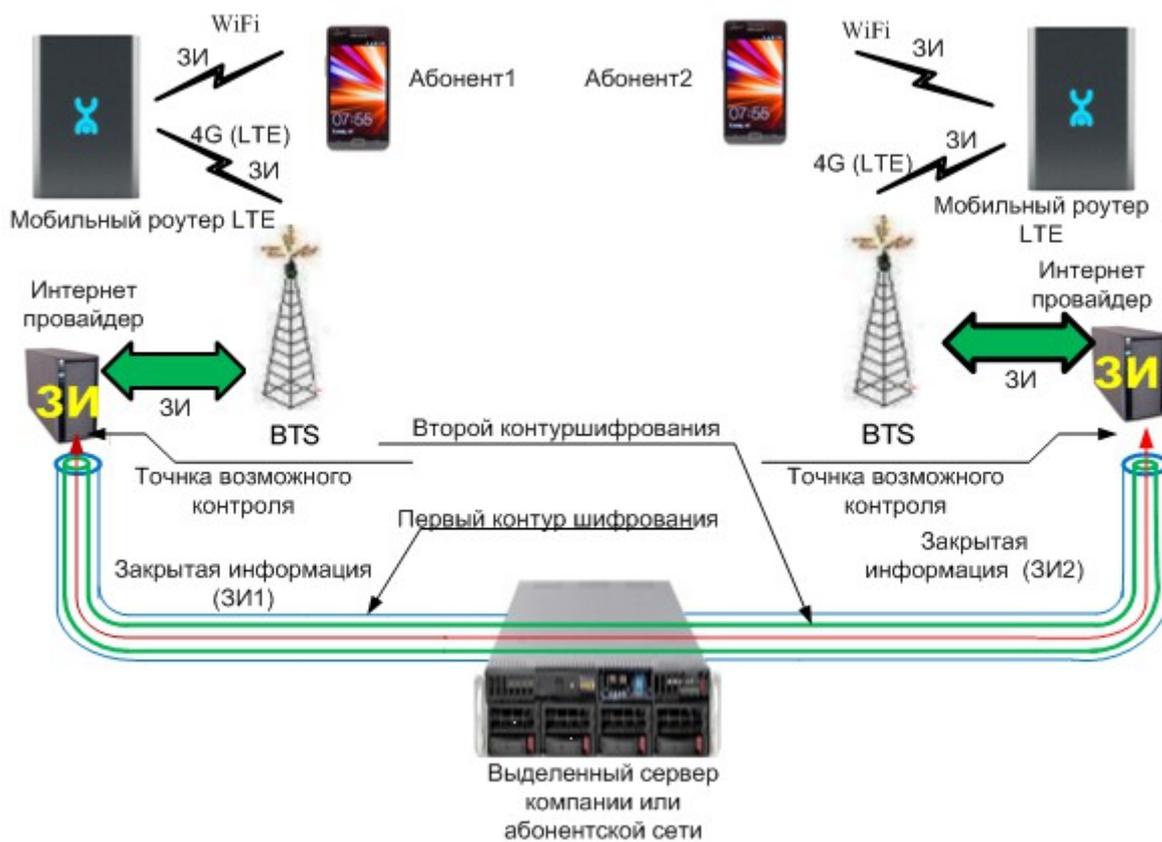
Этот режим используется для передачи файлов и коротких сообщений при отсутствии адресата в сети связи. Сообщение передается по зашифрованному каналу связи на сервер, где хранится в открытом виде до появления адресата в сети. После этого оно шифруется и передается абоненту автоматически.

3 этап формирование второго контура шифрования, использование системы для телефонных переговоров, передачи файлов и коротких сообщений с гарантированной доставкой и защитой,

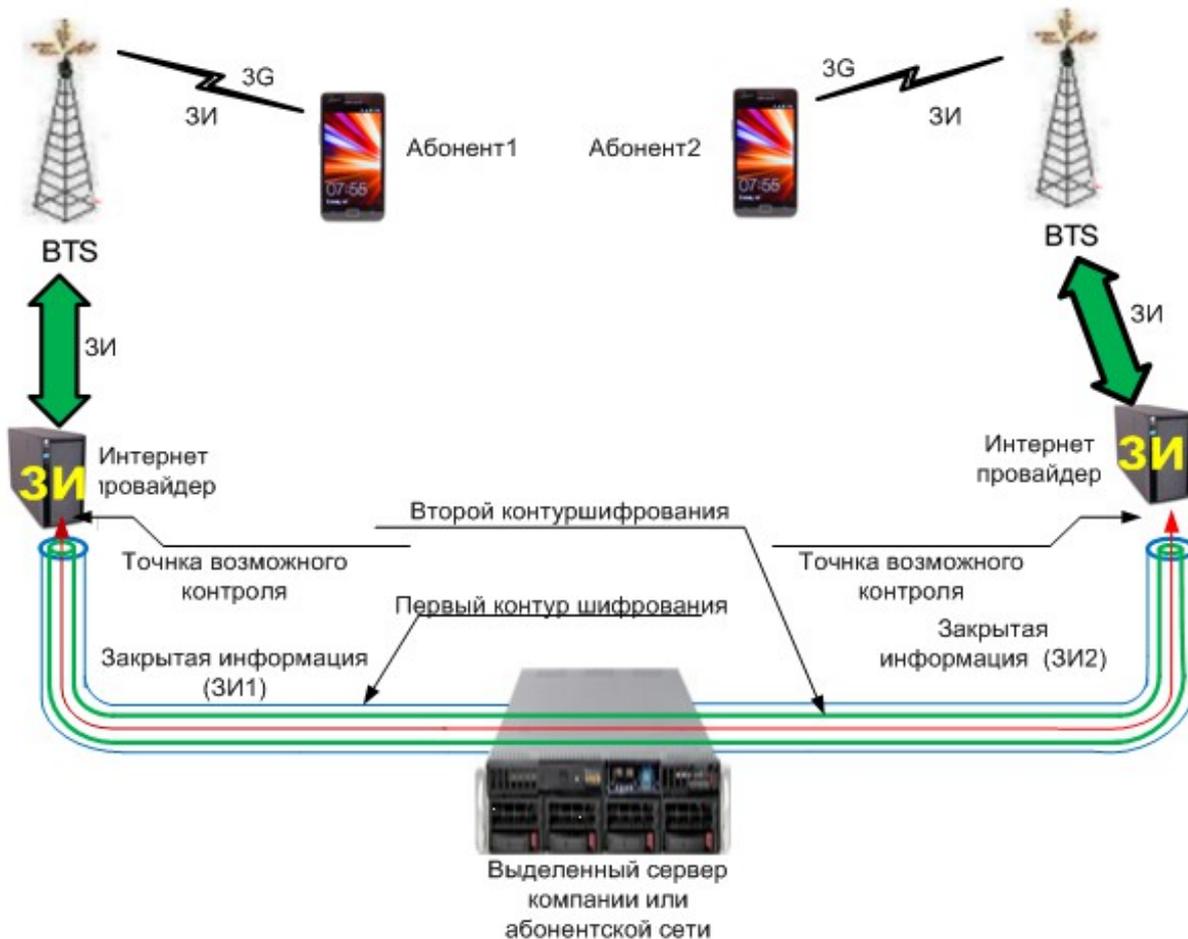


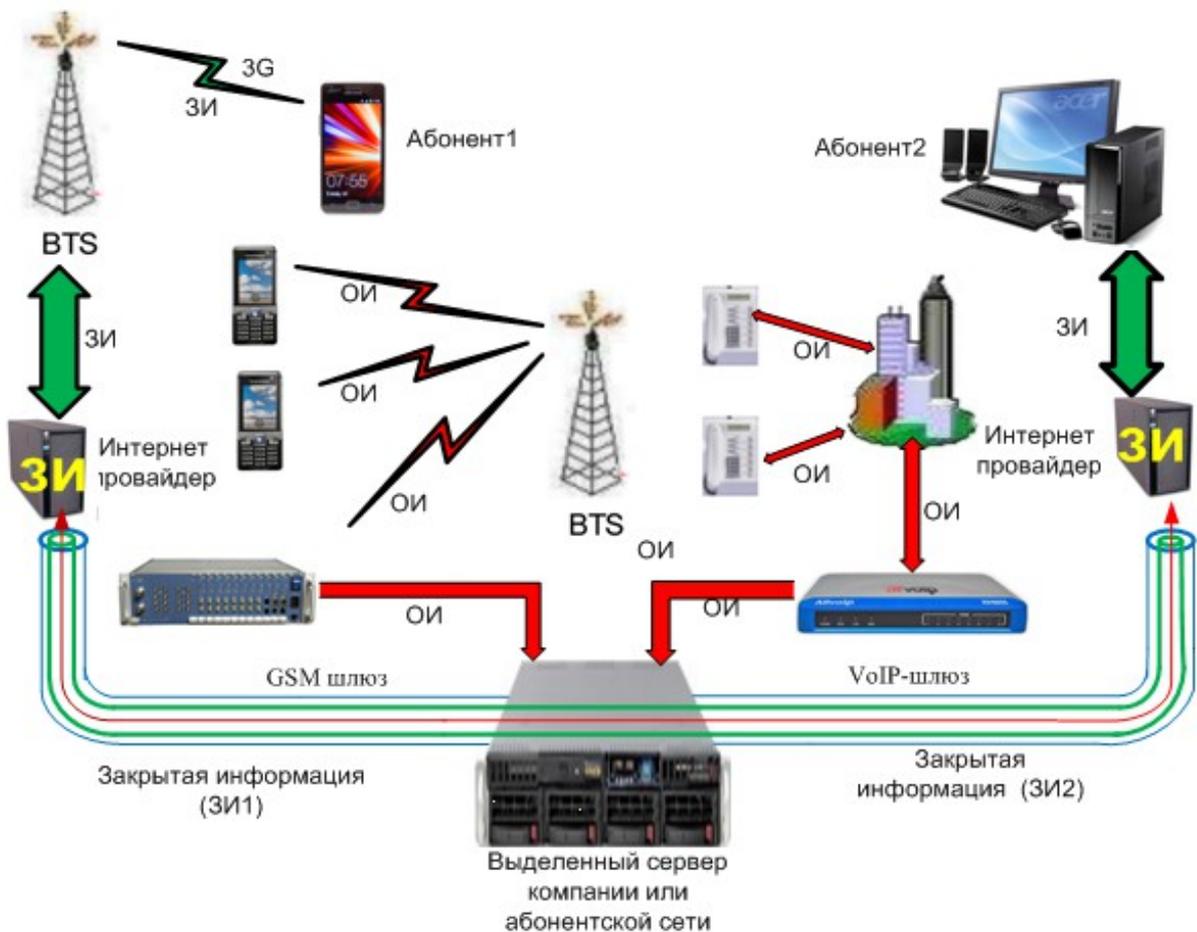
Этот режим обеспечивает самый высокий уровень защищенности информации. При соединении (абонент-абонент) внутри первого контура шифрования формируется второй, в работе которого сервер уже не участвует. Информация шифруется дважды разными алгоритмами. Процесс формирования сеансовых ключей второго контура шифрования проходит под защитой первого и противник его не видит.

В этом случае перед противником встает целый ряд практически неразрешимых задач. Попытки получения защищаемой информации техническими средствами



Работа по каналам 3G сети GSM





Дополнительный режим работы позволяющий абоненту, оставаясь скрытым, выходить на открытые сети связи. По желанию абонента система может осуществлять автоматический поиск нужного абонента на открытых сетях связи по заранее предустановленным номерам, отправлять SMS сообщения и осуществлять сеансы связи с ними. Однако связь на участке «сервер - сети общего пользования» будет открытой.

В состав «ТАЛИСМАН В-FORCE» входит система интеллектуальной адаптации к пропускной способности канала связи, которая после оценки качества сформированного «тоннеля» использует для данного сеанса связи наиболее приемлемый речевой кодек. Высочайшее качество речевого сигнала, отсутствие «эхо», минимальные временные задержки, а также высокий уровень защищенности информации в сочетании с минимальными затратами на установку и эксплуатацию ставят систему «ТАЛИСМАН В-FORCE» в ряд лучших инновационных разработок сегодняшнего дня.

Применение «ТАЛИСМАН В-FORCE» для ведения телефонных переговоров с использованием интернет трафика снижает затраты даже по сравнению с обычной IP телефонией не говоря уже о сетях междугородней и международной связи. Это связано с тем что объемы трафика необходимые для работы «ТАЛИСМАН В-FORCE» значительно ниже чем требуемые для обычной IP-телефонии.

Таким образом со временем все затраты на «ТАЛИСМАН В-FORCE» полностью окупятся.

Технические характеристики системы приведены в отдельных приложениях.