ТЕХНИЧЕСКИЕ СРЕДСТВА
ЗАЩИТЫ ИНФОРМАЦИИ

в телекоммуникационных сетях связи

«БазИС»

• Профессиональный разработчик технических решений защиты информации в телекоммуникационных сетях связи;

• Основан в 2002году;

• Офис в Москве;

• Собственная научно-производственная база;

• Специализация – создание национального защищенного ПО для оборудования и сетей связи;

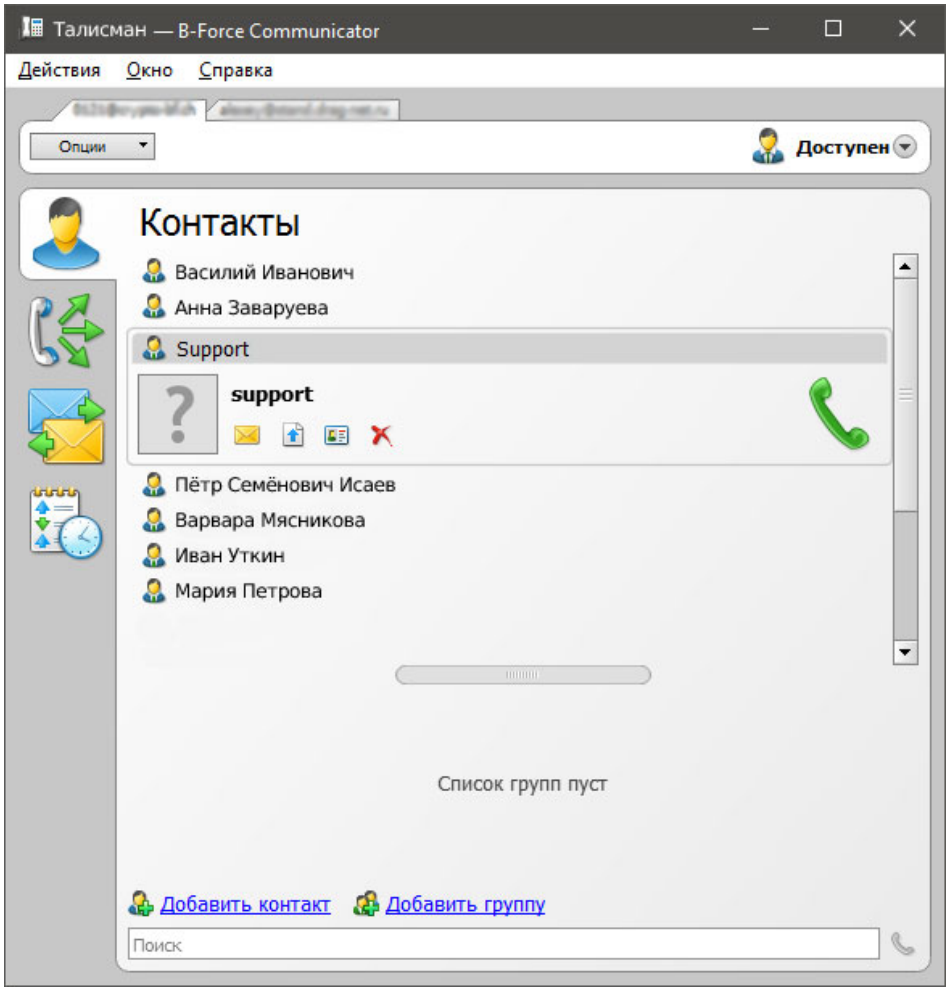
• Широкая сеть партнеров на территории РФ;

«B-Force»

Система «B-Force» это не страховка, это **гарантия безопасности** информации ,при проведении сеансов связи. Это нейтрализация всех видов атак на информационные ресурсы абонента со стороны любого потенциального противника.

Система «B-Force» использует собственные алгоритмы и является отдельной инновационной разработкой. Набор технических средств и программного обеспечения, реализует широчайший набор сервисных функций абонента в сочетании с высоким качеством и безопасностью связи.

«B-Force»



Простой и понятный интерфейс, способный реализовывать любые задания абонента.

«B-Force» телефонный разговор

Защищенная IP-телефония полностью обеспечивает потребности в коммуникации. Вы можете осуществлять безопасные звонки «телефон-телефон», «компьютер-телефон» или «компьютер-компьютер». Использование широкого набора речевых кодеков в зависимости от пропускной способности канала связи, обеспечивает высокое качество восстановленного речевого сигнала;

«B-Force» видеосвязь

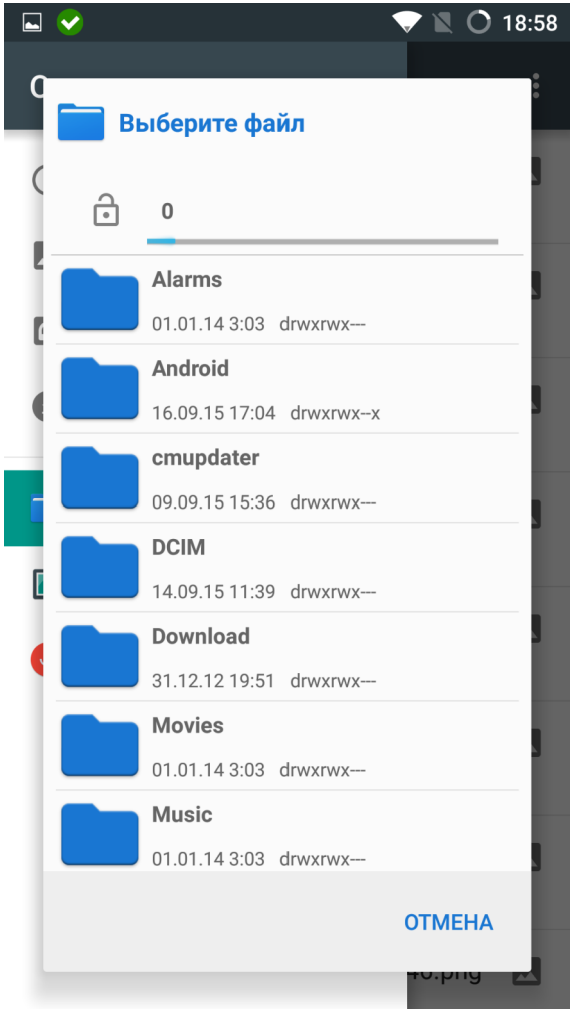
Видеосвязь, как и простые звонки, благодаря отличному качеству звука и изображения изменяет уровень общения между абонентами.

«B-Force» обмен сообщениями

Организация системы передачи коротких информационных сообщений в режиме (точка-точка) т.е. в процессе разговора с противоположным абонентом без разрушения соединения.

«B-Force» передача файлов

Организация защищенного документооборота в режиме «точка-точка» использованием **электронно цифровой подписи (ЭЦП)** по ГОСТ Р 34.10-2001 на основе значения хэш-функции по ГОСТ Р 34.11-94 или SHA256, SHA384 (по выбору абонента)



«B-Force» электронная почта

Письмо в режиме электронной почты будет храниться на сервере до появления абонента в сети. После этого оно будет передано абоненту автоматически. При этом если аппарат абонента выключен или находится вне зоны действия сети система оповещения через SMS сообщение проинформирует его о необходимости подключения к почте.

«B-Force» системы защиты

Обеспечивает:

I. **организацию** двухконтурной системы шифрования;

- первый контур- «абонент-сервер»
- второй контур-«абонент-абонент»

II.защиту информационного (речевого) сигнала от идентификации с ликвидацией всех демаскирующих признаков сеансов связи; (в канале связи постоянно идет цифровой трафик «криптограмма» и установить сам факт соединения абонентов не возможно)

«B-Force» системы защиты

III.защиту от подключения противника к каналу связи; (визуальная индикация строки аутентификации абонента в данном сеансе связи 4 знака).

IV.защиту от получения противником информации предыдущих сеансов связи в случае компрометации (хищения) устройства; (параметры текущих сеансовых ключевых установок автоматически уничтожаются сразу после ответа противоположного абонента)

«B-Force» системы защиты

V.защиту от появления дополнительных каналов утечки информации при работе устройства; (блокировка всех не декларируемых функций смартфона на основе анализа и переработки ПО)

VI.защиту адресной информации абонентов (определить кто, когда и кому звонил не возможно)

«B-Force» системы защиты

VII.защиту от использования противником аппарата в случае его компрометации (утери);(дистанционная блокировка скомпрометированного устройства)

VIII.защиту от всех методов контроля за абонентом со стороны операторов связи GSM. (работа без SIM карты с выключенными радио средствами GSM через точки доступа Wi-Fi общего пользования)

«B-Force» сервисные функции

I.организацию системы оповещения абонента о необходимости подключения к сети Интернет через SMS сообщения, в случае если аппарат абонента выключен или находится вне зоны действия сети;

II.организацию системы поиска абонента по заранее предустановленным номерам на открытых сетях связи PSTN и GSM;

«B-Force» сервисные функции

III.возможность дистанционного пополнения (удаления) абонентов группы

IV.мгновенное соединение без набора номера;

V. сохранение всех основных сервисных функций базовой модели аппарата;

«B-Force» термины и определения

RTP *(Real-time Transport Protocol)* — работает на транспортном уровне и используется при передаче трафика реального времени.

TLS *(Transport Layer Security)* — криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети Интернет

SRTP *(Secure Real-time Transport Protocol)* — безопасный протокол передачи данных в реальном времени и предназначен для шифрования ,обмена ключей по алгоритму Диффи — Хелмана, установления подлинности сообщения, целостности, защиту от замены данных RTP в однонаправленных и multicast передачах медиа и приложениях.

«B-Force» термины и определения

DMZ *(Multi-Service Access Node)* — технология обеспечения защиты серверов, пересекающих периметр.

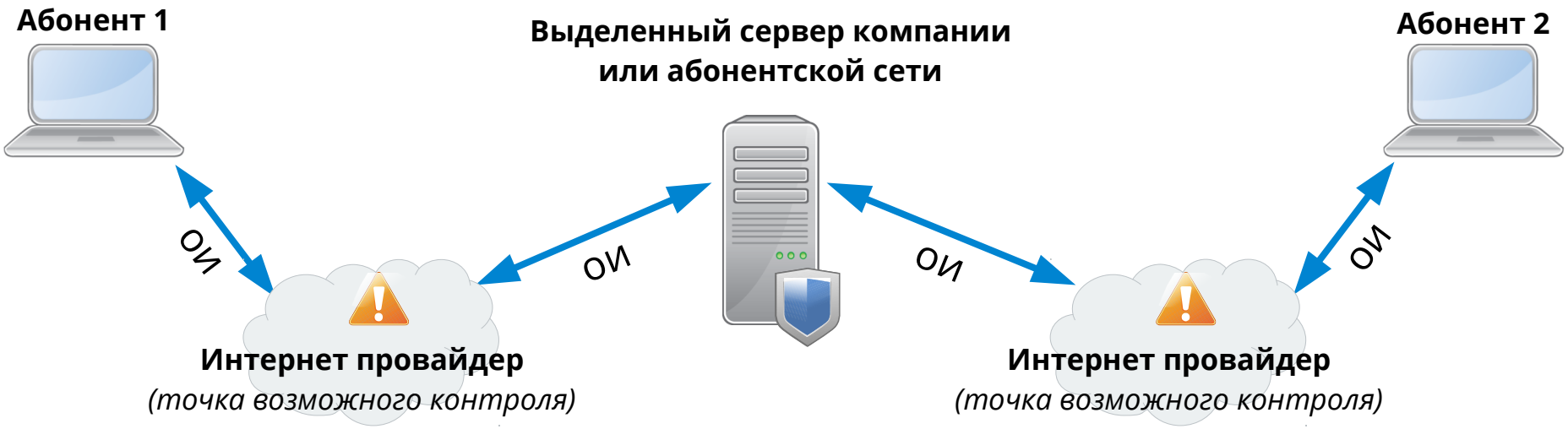
SIP *(Session Initiation Protocol — протокол установления сеанса)* — стандарт на способ установления и завершения пользовательского интернет-сеанса, включающего обмен мультимедийным содержимым (видео- и аудиоконференция, мгновенные сообщения,).

SIP прокси-сервер *(от proxy — «представитель»)* представляет интересы пользователя в сети. Он принимает запросы и обрабатывает их.

CLI *(Call Level Interface)* — Интерфейс уровня вызовов. программный стандарт, закрепленный в документе ISO /IEC 9075-3:2003

«B-Force» режимы работы

Прохождение открытых информационных сигналов в режиме «установления соединения с выделенным сервером»



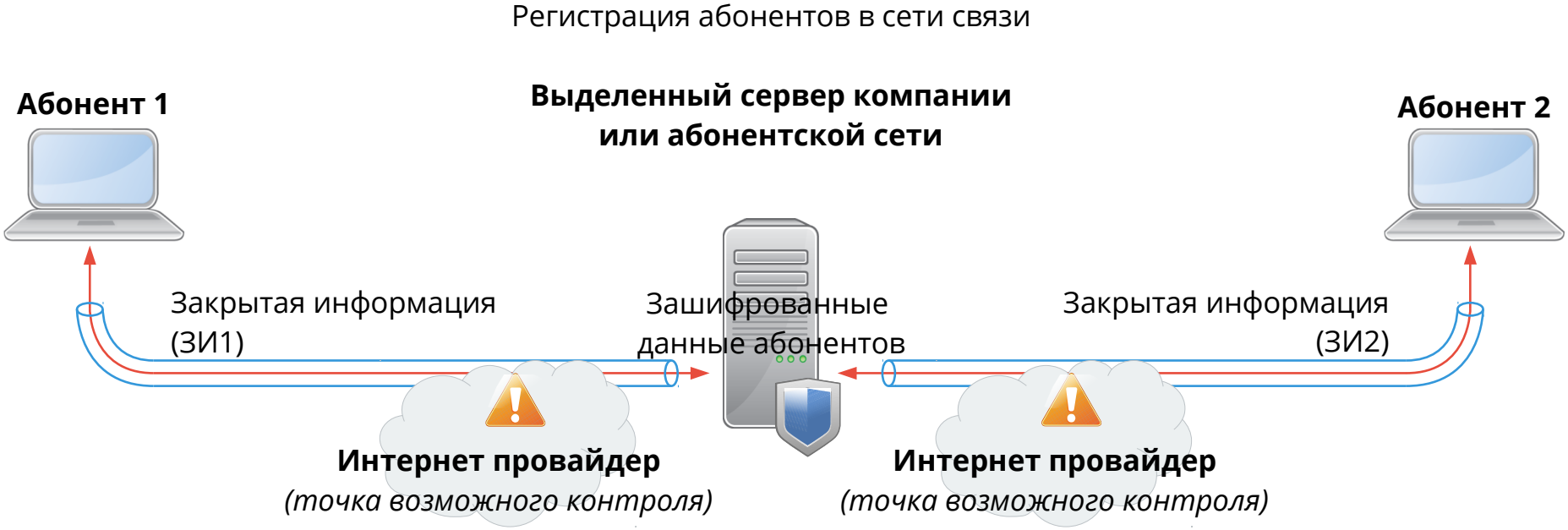
- Регистрация абонента в сети, происходит автоматически при включении компьютера без участия абонента;
- Установление соединения;
- Формирование зашифрованного виртуального тоннеля между сервером и абонентом;

«B-Force» режимы работы

Формирование зашифрованного виртуального тоннеля между сервером и абонентом, первый контур шифрования

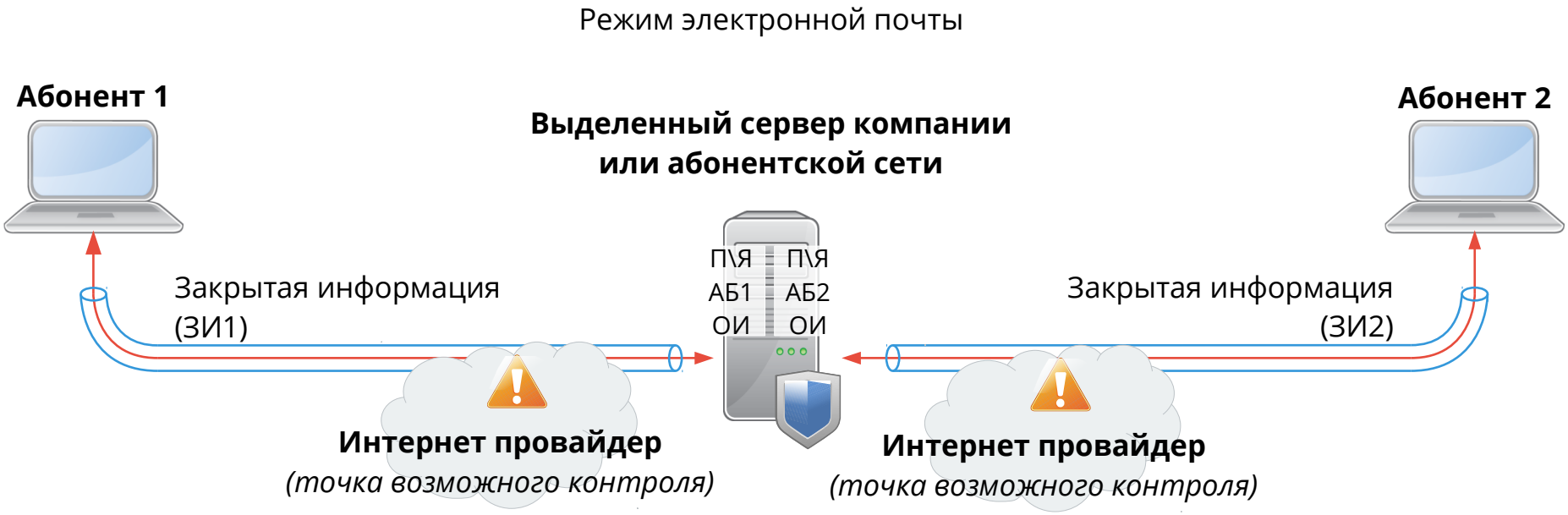
- Шифрование идентификационных данных абонентов;
- Шифрование адресной информации, т. е. определить кто, когда и кому звонил не возможно;
- Шифрование информации при работе в режиме «электронной почты»;

«B-Force» режимы работы



- 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.

«B-Force» режимы работы

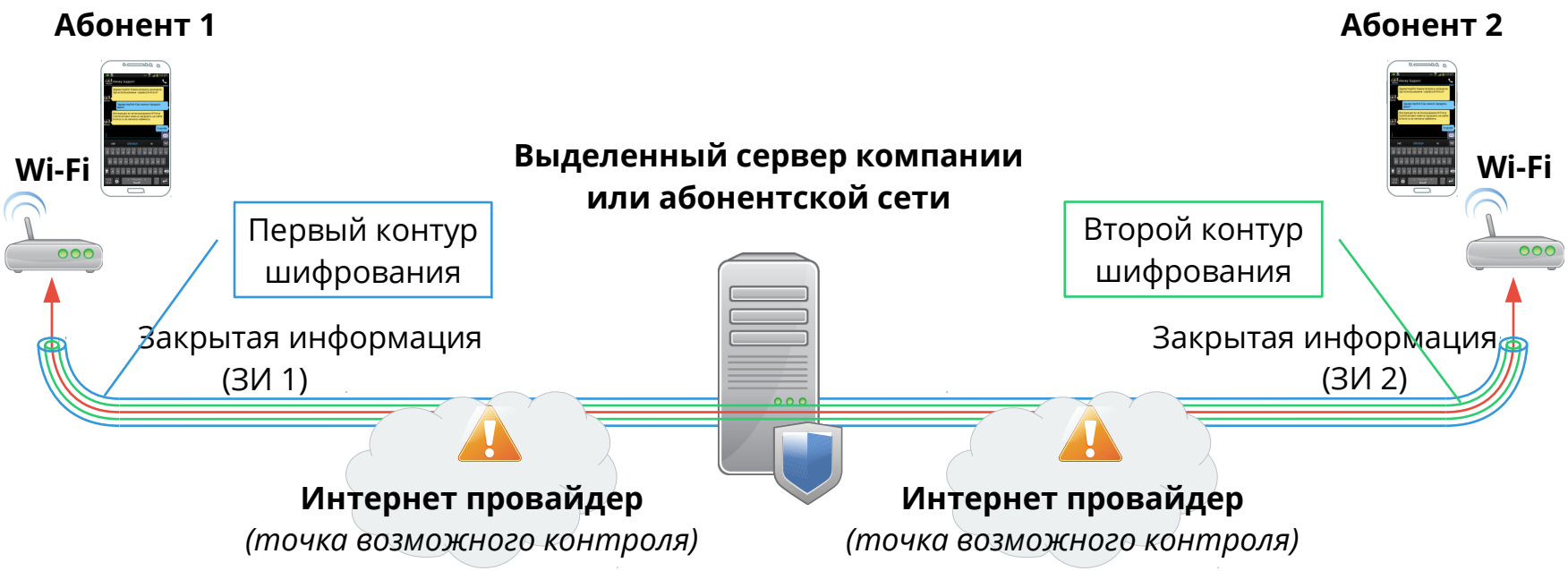


- Этот режим используется для передачи файлов и коротких сообщений при отсутствии адресата в сети связи. Сообщение передается по зашифрованному каналу связи на сервер ,где хранится в открытом виде до появления адресата в сети. После этого оно шифруется и передается абоненту автоматически.

«B-Force» режимы работы

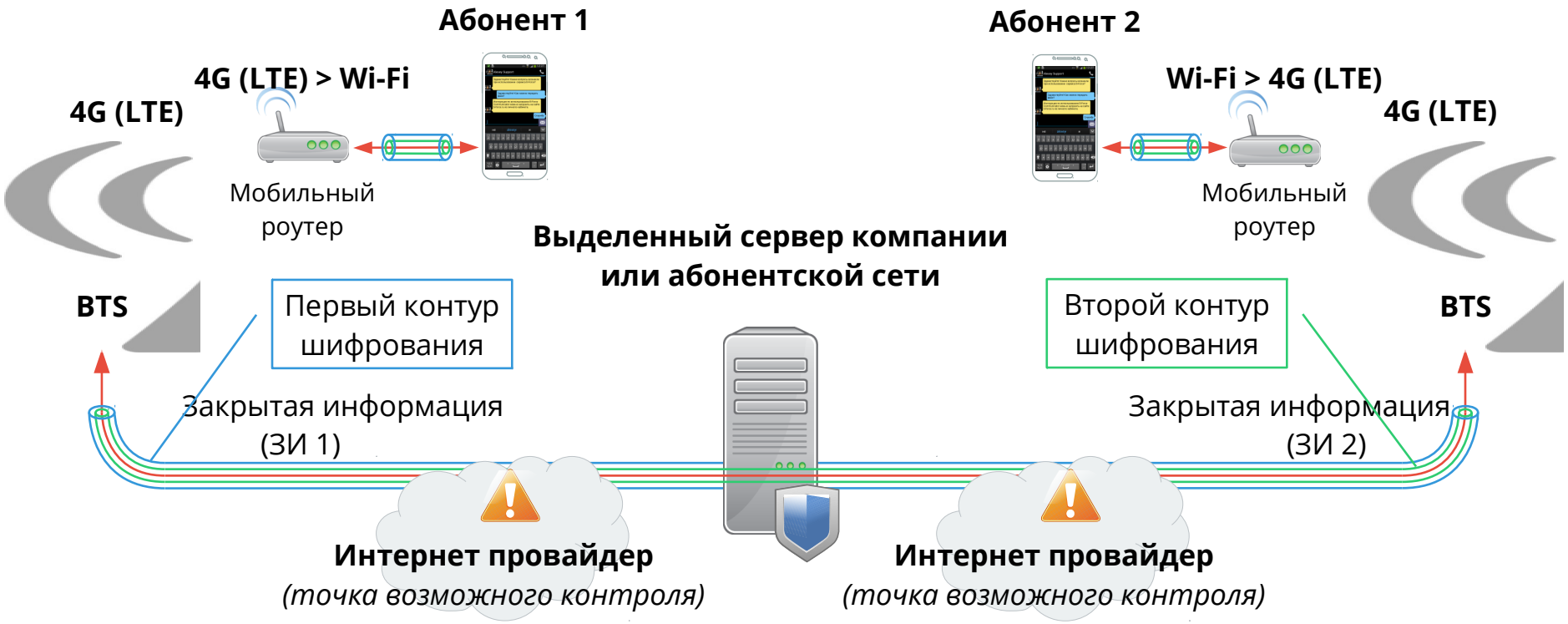
- Этот режим обеспечивает самый высокий уровень защищенности информации. При соединении (абонент-абонент) внутри первого контура шифрования формируется второй, в работе которого сервер уже не участвует. Информация шифруется дважды разными алгоритмами. Процесс формирования сеансовых ключей второго контура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

«B-Force» режимы работы



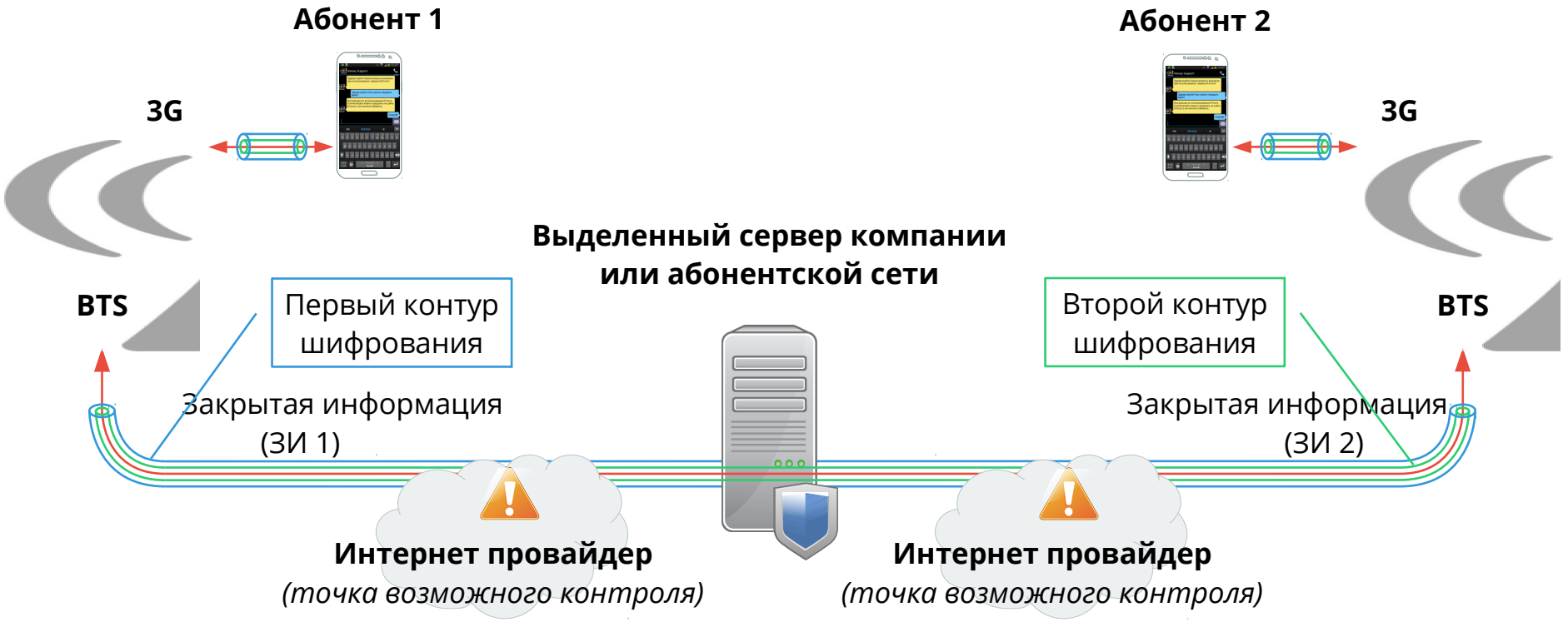
- При использовании этого варианта системы противник не сможет даже определить местоположение абонентов, поскольку точки доступа могут быть любыми. Сеанс связи организуется без SIM карты с выключенными радио средствами GSM.

«B-Force» режимы работы



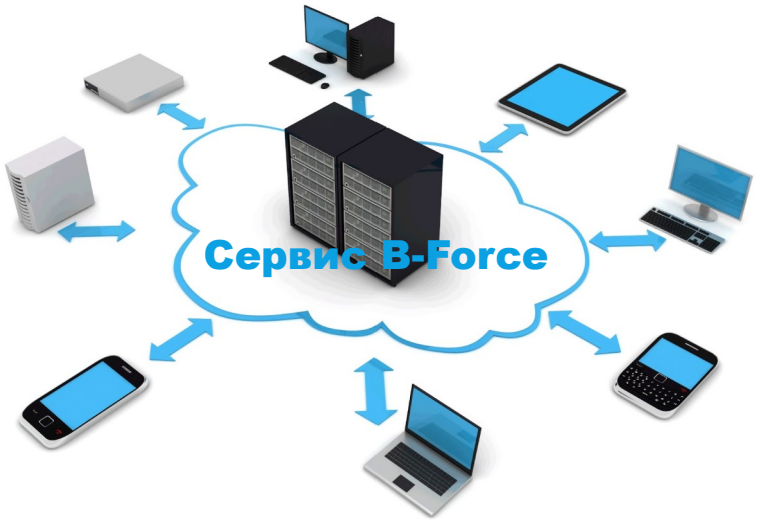
- Вариант построения системы с использованием мобильного роутера 4G (LTE)

«B-Force» режимы работы



- Работа по каналам 3G

«B-Force» архитектура сети



- Система «B-Force» использует стандартные открытые протоколы: SIP, TLS, SRTP, ZRTP.
- TLS предоставляет зашифрованный аутентифицированный канал для передачи сигнализации, SRTP обеспечивает шифрование и аутентификацию медиа-трафика, ZRTP реализует обмен ключами для обеспечения связи «точка-точка». Поддержка схемы SIPS предусматривает установку шифрованного соединения TLS на всех сегментах сети передачи данных звонка. Совокупность применения этих протоколов позволяет говорить о гарантиях безопасности передаваемой информации.

«B-Force» требования к каналу связи

Система требует постоянного подключения к Интернету. Различные типы связи имеют различные минимальные требования к каналу связи. Таблица ниже отображает работоспособность тех или иных типов связи, предоставляемых приложением, в зависимости от доступного канала доступа в сеть Интернет.

Тип связи	LTE / Wi-Fi	3G	GPRS / EDGE
Видеозвонки	+	-	-
Передача файла	+	+	-
Голосовая связь	+	+	-
Сообщение	+	+	+
Статус абонента	+	+	+