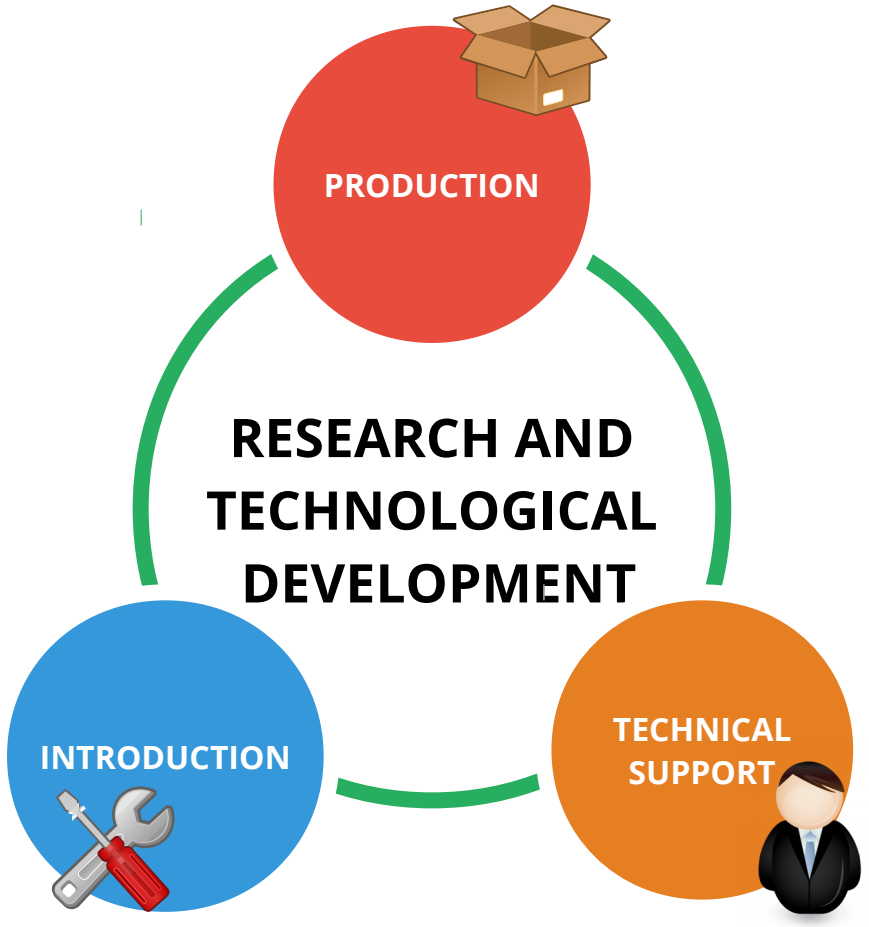
TECHNOLOGICAL MEASURES FOR **INFORMATION PROTECTION**

in telecommunication networks

«BazIS»

- Professional developer of technical solutions for information protection in telecommunication networks;
- Established in 2002;
- Office in Moscow;
- Own scientific and production base;
- Specialization – creation of national protected software for equipment and communication networks;
- Wide network of partners on the territory of the Russian Federation;

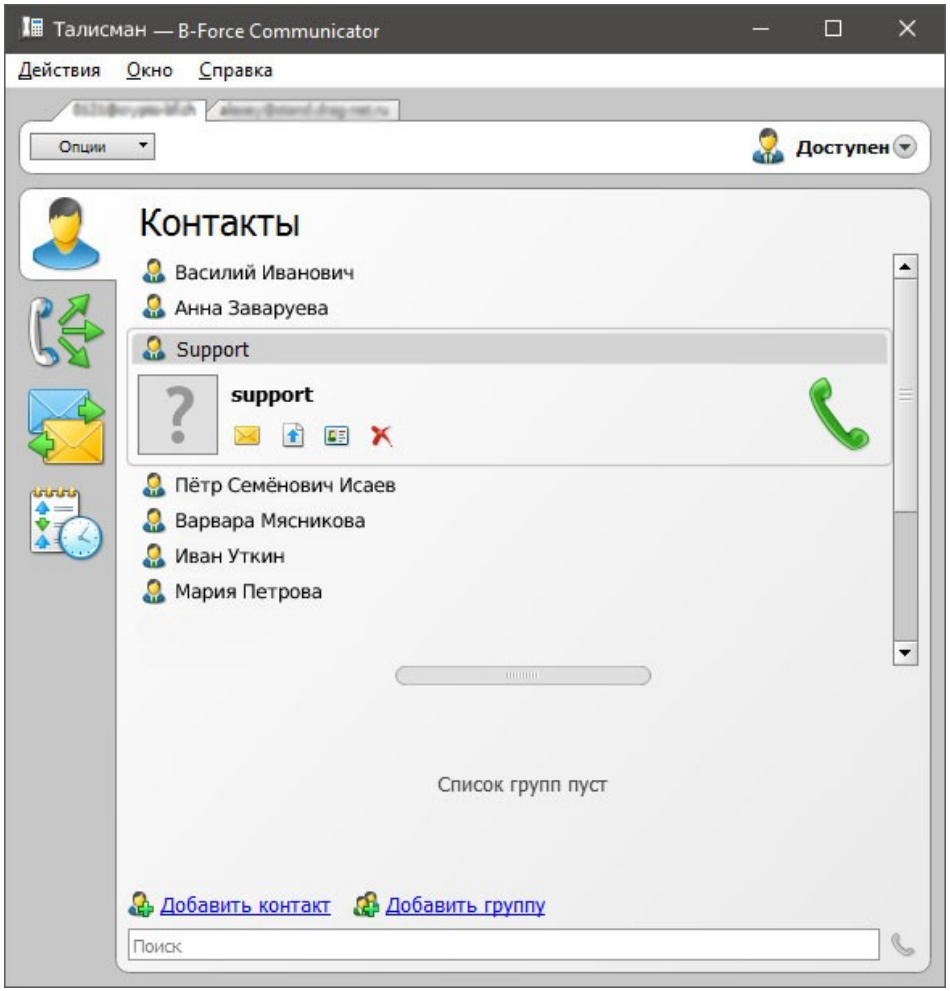


«B-Force»

«**B-Force**» system is not a coverage, it is a guarantee of information safety during communication sessions. It allows to neutralize any attacks to information resources of the subscriber on the part of any potential enemy.

«**B-Force**» system uses its own algorithms and is a separate innovative solution. The complex of software and hardware allows to implement the most extensive range of service functions of the subscriber along with high quality and safety of communication.

«B-Force»



Easy and user-friendly interface able to fulfill any task of the subscriber.

«B-Force» Telephone communication

Protected IP telephony meets all demands in communication. You may enjoy safe calls “phone-to-phone”, “computer-to-phone” or “computer-to-computer”. The use of a wide range of voice codecs depending on the communication channel capacity ensures high quality of reconstructed speech.

«B-Force» Video calls

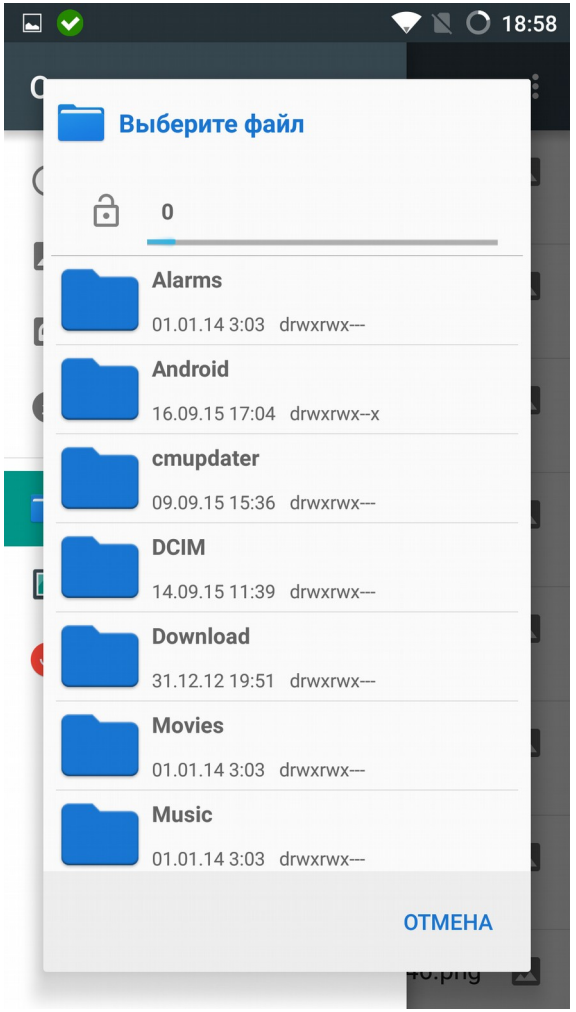
Video calls, as well as regular calls, due to excellent quality of audio and image change the level of communication between the subscribers.

«B-Force» Exchange of messages

Organization of a system of transfer of short information messages in the mode (point-to-point), i.e. in the process of communication with another subscriber without disrupting the connection.

«B-Force» Transfer of files

Organization of protected document workflow in “point-to-point” mode by using electronic digital signature (EDS) under GOST R 34.10-2001 based on the value of hash function under GOST R 34.11-94 or SHA256, SHA384 (at the subscriber’s choice).



«B-Force» e-mail

A letter in e-mail mode will be stored on the server until the subscribers connects to the network. Then, it will be automatically transferred to the subscriber. Herewith, if the subscriber's phone is switched off or out of coverage the warning system notifies the subscriber via SMS to connect to its mail box.

«B-Force» Protection system

Ensures:

I. **organization** of two-circuit encryption system;

- first circuit – «subscriber-to-server»;
- second circuit – «subscriber-to-subscriber»;

II. **protection** of information (speech) signal against identification with liquidation of all give-away characteristics of communication sessions (digital traffic “cryptogram” is constantly running through the communication channel, and the fact of subscribers connection itself cannot be determined);

«B-Force» Protection system

III.protection against the enemy connection to the communication channel (visual indication of the subscriber authentication line in this session - 4 digits);

IV.protection against receiving of information from previous communication sessions by the enemy in case of device discredit (theft);(parameters of current session key settings automatically destroyed immediately after the answer of the other subscriber);

«B-Force» Protection system

V.protection from arising of additional channels for information leakage when operating the device (blocking of all not declared functions of a smart phone based on software analysis and processing);

VI.protection of address information of subscribers (it is impossible to determine who made the call, when the call was made, and whom the call was made to);

«B-Force» Protection system

VII.protection against the use of the device by the enemy in case of its discredit (theft) (distance blocking of discredited device);

VIII.protection against all methods of control over the subscriber on the part of GSM operators (operation without a SIM card with turned off radio through GSM means via common Wi-Fi access points);

«B-Force» Service functions

I. organization of a subscriber notification system on the necessity to connect to the Internet via SMS if the subscriber's device is switched off or out of coverage;

II. organization of a subscriber search system under the predetermined numbers on open communication networks PSTN and GSM;

«B-Force» Service functions

III. a possibility of remote adding (deleting) the group subscribers;

IV. instant connection without dialing;

V. keeping all main service functions of the device basic model;

«B-Force» Terms and definitions

RTP *(Real-time Transport Protocol)* — operates on the transport level and is used during real-time traffic transfer.

TLS *(Transport Layer Security)* — is a cryptographic protocol ensuring protected transfer of data between the nodes in the Internet.

SRTP *(Secure Real-time Transport Protocol)* — is a safe real time data transfer protocol and is designed for encryption, exchange of keys under Diffie–Hellman algorithm, message authentication and integration, protection against data replacement RTP in one-way and multicast transmission of media and in applications.

«B-Force» Terms and definitions

DMZ *(Multi-Service Access Node)* — is a technology ensuring safety of the servers crossing the perimeter.

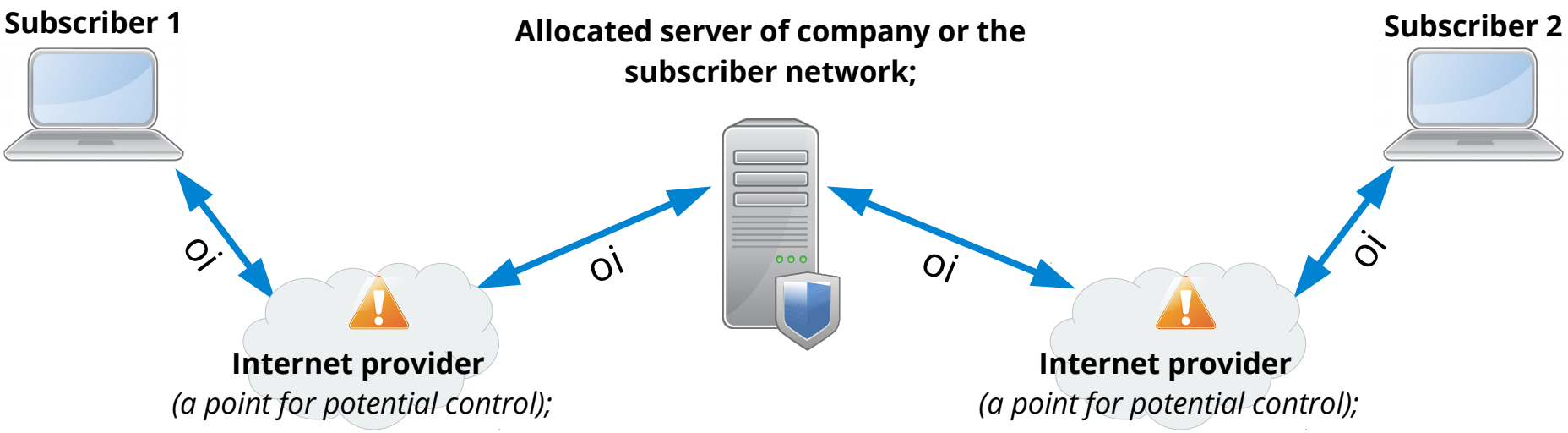
SIP *(Session Initiation Protocol)* — is a standard method for establishing and completion of user Internet session including exchange of multimedia content (video and audio conference, instant messages).

SIP proxy server (*from proxy meaning representative*) represents the interests of the user in the network. It receives the requests and processes them.

CLI *(Call Level Interface)* — is a programming standard envisaged in ISO /IEC 9075-3:2003 document.

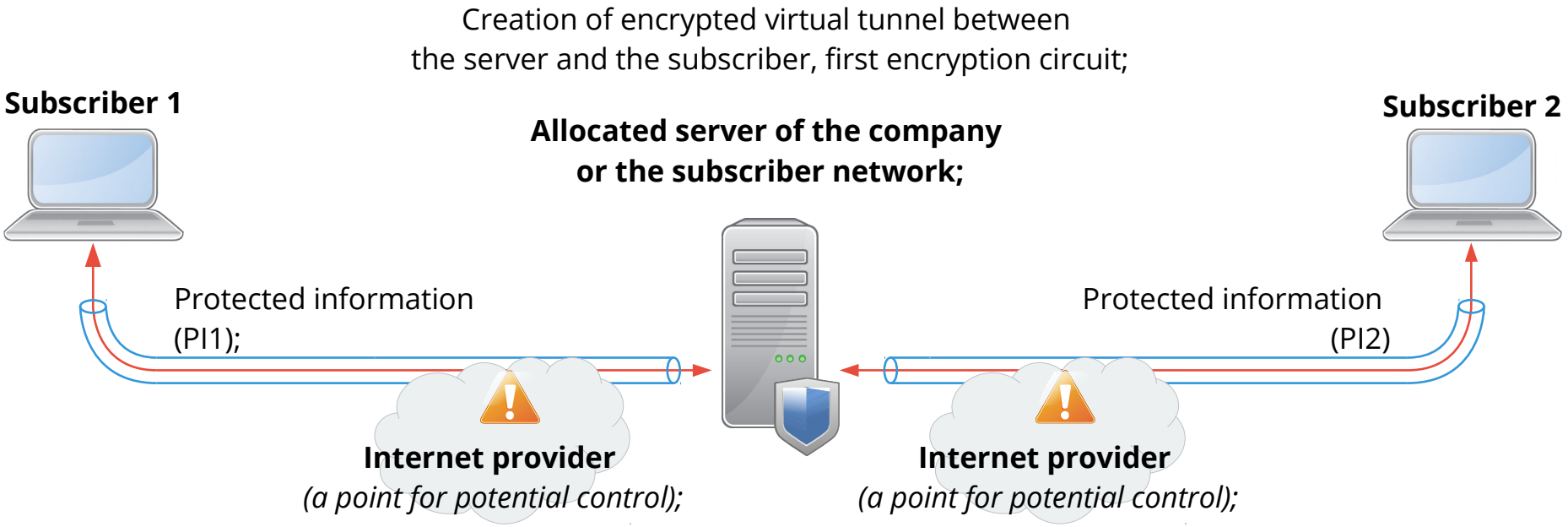
«B-Force» Operation mode

Passing open information signals in the mode
“establishing connection with the allocated server”;



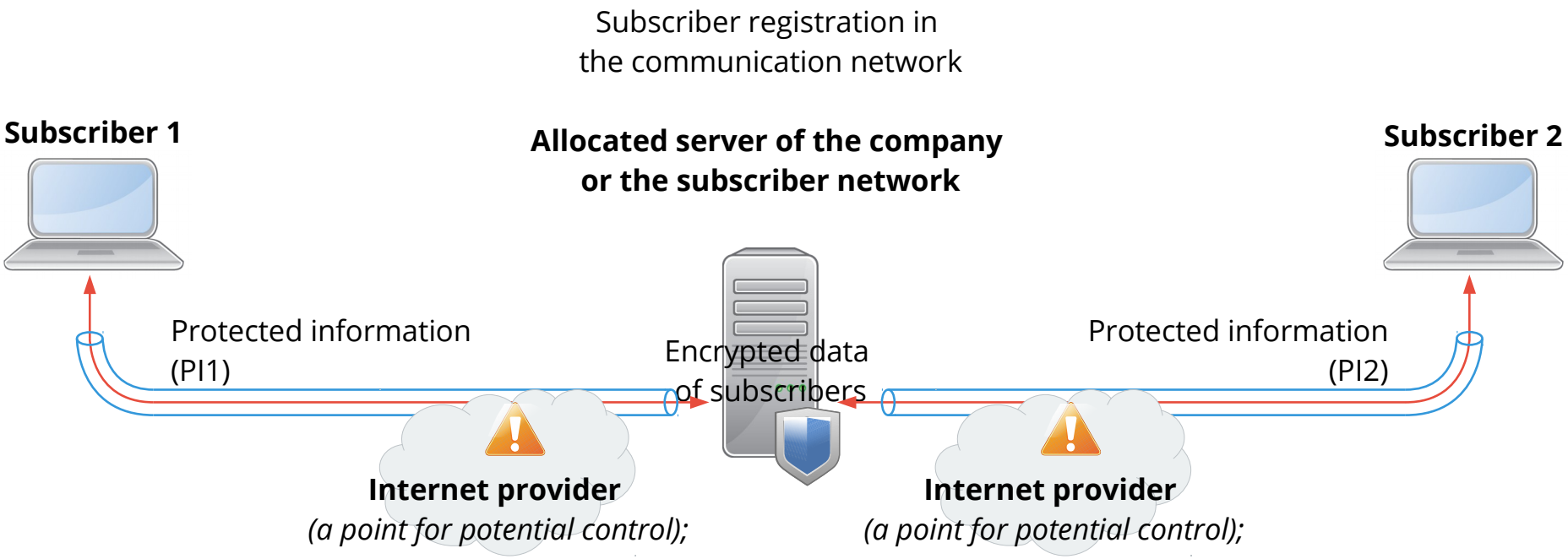
- The subscriber is automatically registered in the network when the computer is switched on without the subscriber participation;
- Establishing the connection;
- Creation of encrypted virtual tunnel between the server and the subscriber;

«B-Force» Operation mode



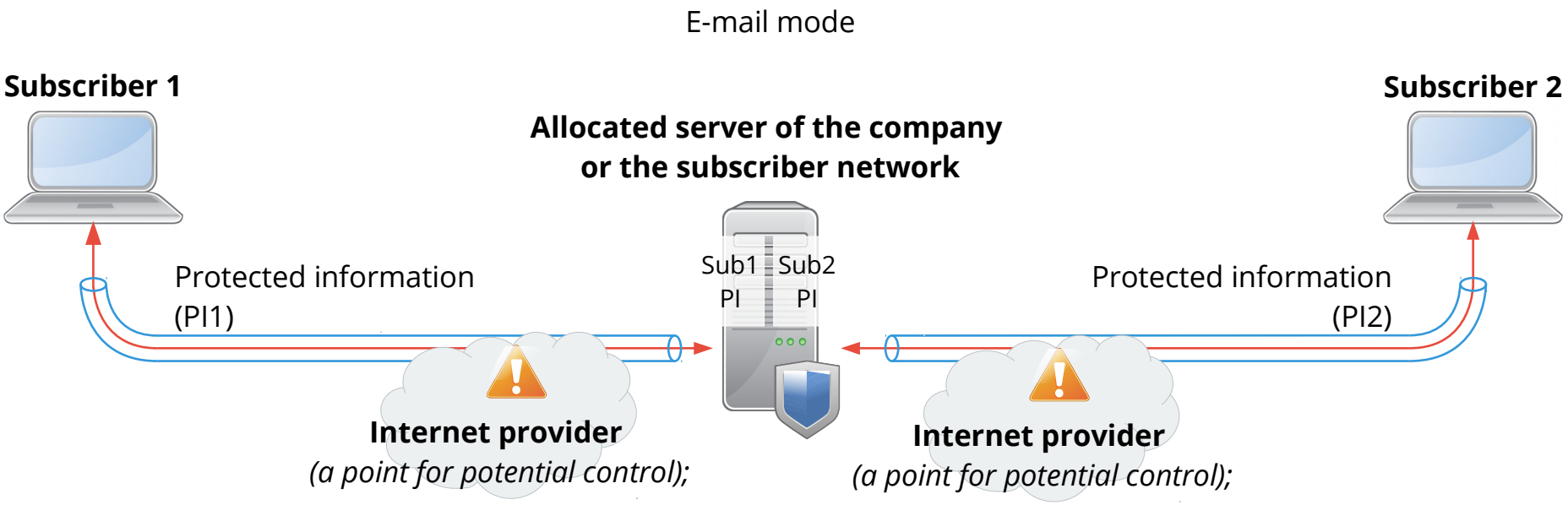
- Encryption of identification data of subscribers;
- Encryption of address information, i.e. it is impossible to determine who made the call, when the call was made and whom the call was made to;
- Encryption of information during operation in the mode “e-mail”;

«B-Force» Operation mode



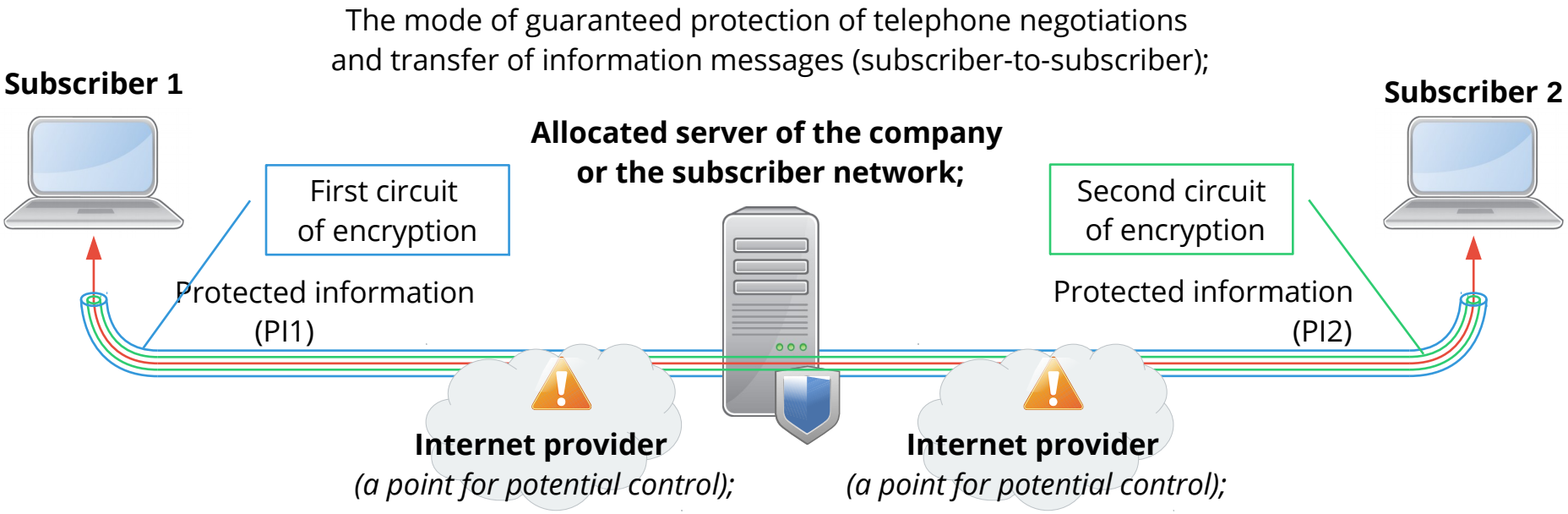
- All required registration data of subscribers are stored on the server in the encrypted form. Protection systems do not allow to get them even if the equipment is taken by the enemy. The server is controlled by specially developed operation system DNLinux.

«B-Force» Operation mode



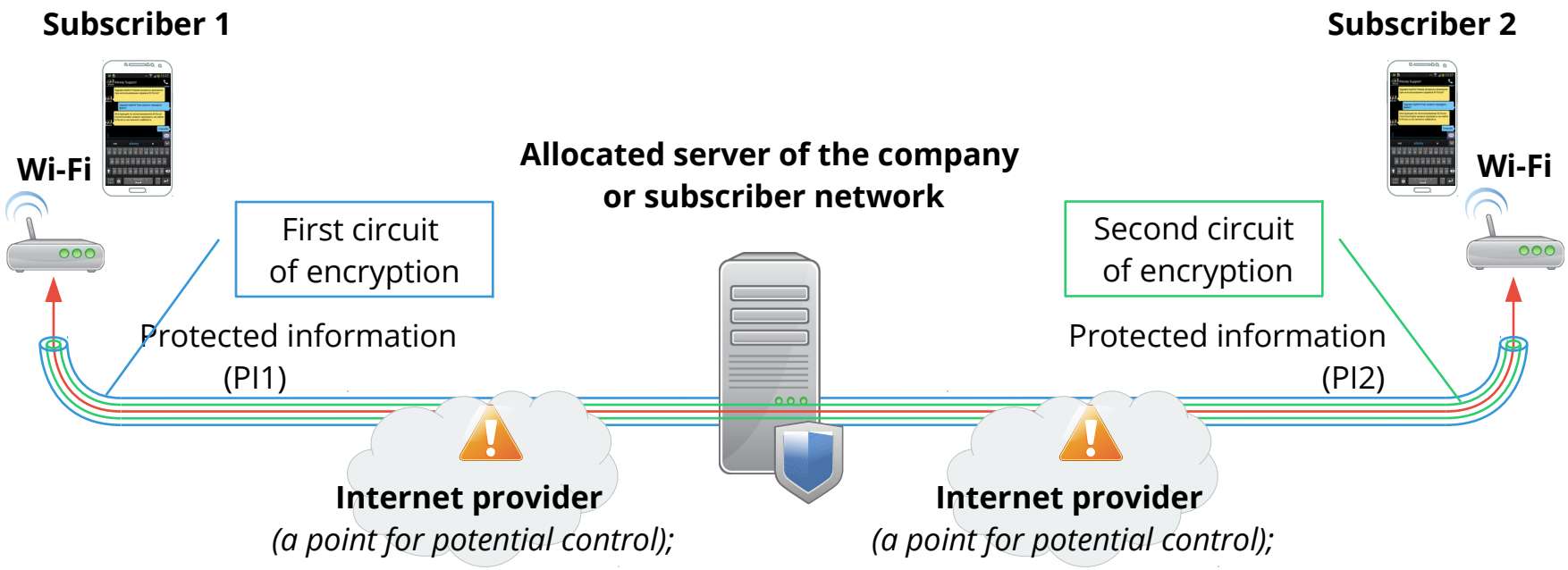
- This mode is used for transfer of files and short messages provided the addressee is not connected. The message is transferred through the encrypted communication channel to the server where it is stored in an open form until the addressee is connected to the network. Then it is encrypted and transferred to the subscriber automatically.

«B-Force» Operation mode



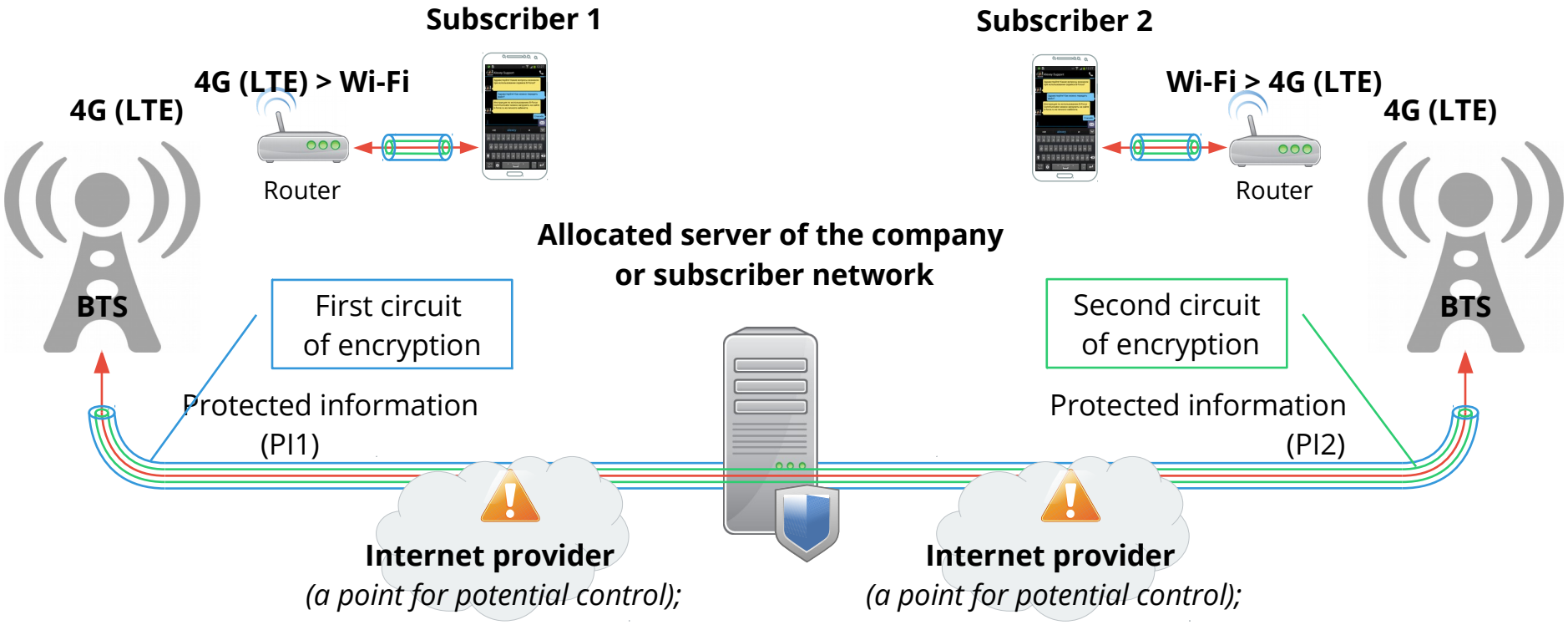
- This mode ensures the highest level of information protection. When connection (subscriber-to-subscriber) is established, the second circuit is created within the first one, and the server does not participate in its operation. The information is encrypted twice via different algorithms. The process of session keys formation of the second encryption circuit is protected by the first circuit, and the enemy does not see it.

«B-Force» Operation mode



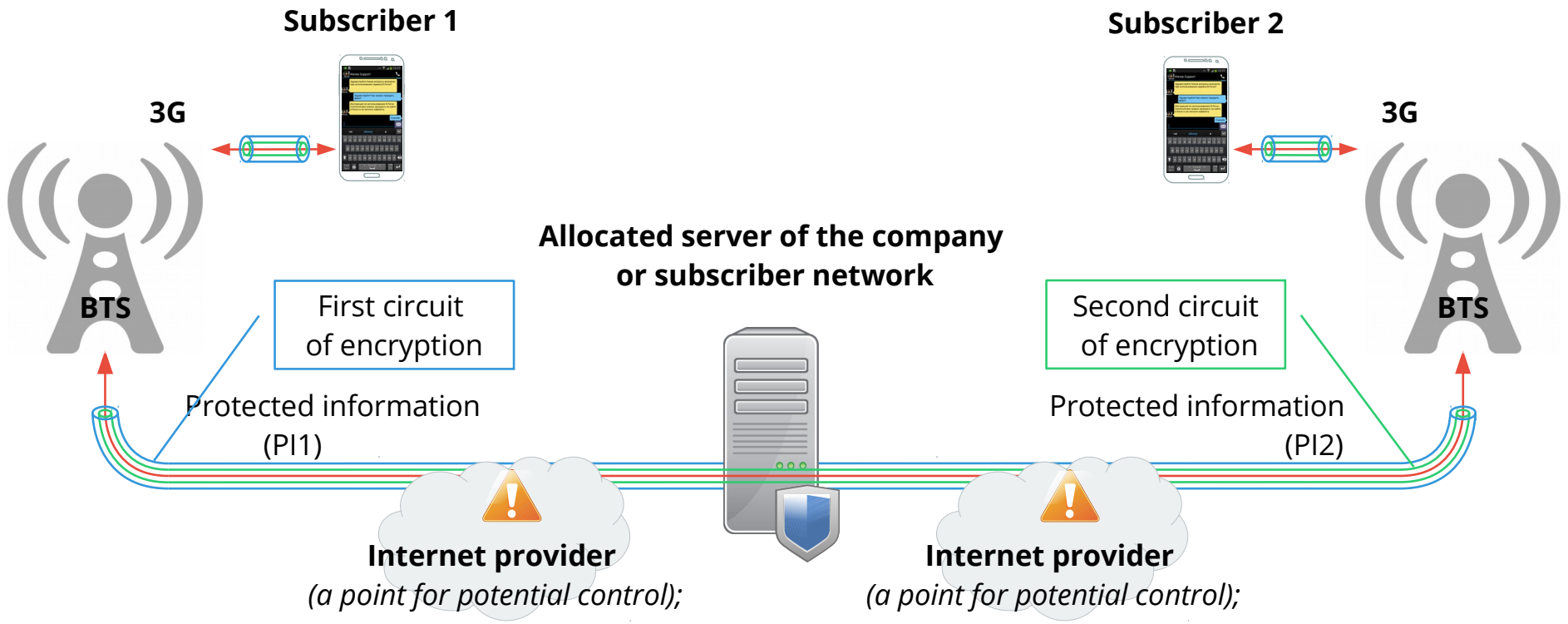
- When using this system option, the enemy cannot even define the location of the subscribers as access points may be any. The communication session is organized without a SIM card with switched off GSM radio means.

«B-Force» Operation mode



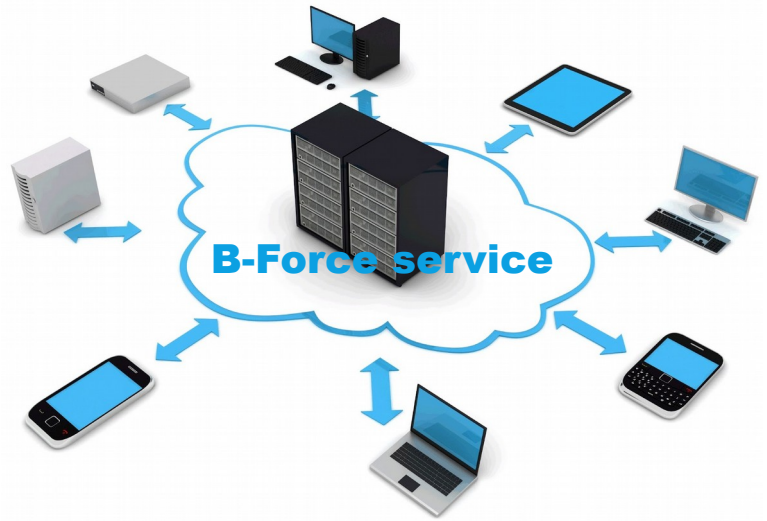
- A system option created with the use of a 4G mobile router (LTE).

«B-Force» Operation mode



- Operation on 3G channels.

«B-Force» Network architecture



- B-Force system uses standard open protocols: SIP, TLS, SRTP, ZRTP.
- TLS provides an encrypted authenticated channel for signaling transfer, SRTP ensures encryption and authentication of media traffic, ZRTP implements exchange of keys for “point-to-point” connection. SIPS scheme support provides for establishment of TLS encrypted connection on all segments of network of a call data transfer. These protocols used together allow to ensure safety of the transferred information.

«B-Force» Requirements to communication channel

The system requires continuous Internet connection. Various connection types have various minimum requirement to the communication channel. The Table below shows the efficiency of a particular connection type provided by the application depending on the available Internet access channel.

Connection type	LTE / Wi-Fi	3G	GPRS / EDGE
Video calls	+	-	-
File transfer	+	+	-
Voice communication	+	+	-
Message	+	+	+
Subscriber status	+	+	+