Literature Review of Interface for access of the national security service of the Republic of Kazakhstan to the system of legal data interception

**Abstract -** The interface will be implemented for access of national security service of the Republic of Kazakhstan to the system of legal information interception, for the “SHIFT systems” company. At the government expense the remote control of the operator by the authority carrying out operatively-search activity is established. The remote control forms the Interface of access to SOSM.

SOSM (hidden from the **S**ystem of technical means to ensure the functions of **o**peratively-**s**earch **m**easures) - a set of technical means and measures designed for operational and investigative activities in the networks of telephone, mobile and wireless communications and radio communications.

Remote Control provides the necessary number of simultaneous connection of the RM, according to ST RK 2267-2012 (IZM. 2017) paragraph 5.1.4. The implementation of the access interface and its capacity should ensure continuous connection of workstations of administration, processing and supervision, transfer of requests, messages, information in the required amount, without omissions and losses. In this document there is a review of literature about the interface, which allows obtaining access to the system of legal information interception for the national security service of the Republic of Kazakhstan.

***Keywords*** *- Interface; remote control; SORM; legal information interception; national security service of the Republic of Kazakhstan.*

1. INTRODUCTION

The SOSM system was introduced in Russia, later in the Union republics such as Belarus and Kazakhstan. However, the system in these countries is identical to that one in Russia. Besides, not only these countries have this system, but also the countries of Western Europe and the USA. This system have a different name in this countries: CALEA (Communications Assistance for Law Enforcement Act) in the USA and LI (Lawful interception) in the European Union. In addition, in these countries, such equipment is mounted in the ATE, switches, and servers. As well as in China is a global system "Golden Shield", which performs, among other things, the function of the technical resources TR SOSM.

The paper is organized as follow: Section II introduces the “Shift Systems” LLP company we cooperate with. Section III presents SOSM, types of SOSM, why do we need this system, history of the SOSM and describes control in the types of SOSM. Section IV describes the interface for SOSM system for the “Shift Systems” company. Section V consists of the literature review. Section VI compares the different systems and their remote controllers. Section VII concludes the paper, and Section VIII describes the intended application.

1. SHIFT systems company

“Shift Systems” LLP – Kazakh company, which has developed the first domestic certified SOSM product in the Republic of Kazakhstan.

Their hardware and software complex “TOR” © allows to provide:

* Fixed telephony;
* IP-telephony;
* Internet;
* Mobile operators (in developing).

“Shift Systems” LLP performs the entire range of work, from preparing certification documents to implementing and maintaining the SOSM system. All their SOSM complexes have been successfully tested and implemented in the industrial infrastructure of the KNB (National Security Committee) of the Republic of Kazakhstan.

They provide such products as:

* SOSM-1 provides capture of messages from the specified telephone subscribers and collection of statistical information about connections of the specified subscribers;
* SOSM-2 provides capture of messages from the specified Internet subscribers and collection of statistical information about connections of the specified subscribers;
* SOSM-3 provides the collection of service information about all subscribers of both phone and Internet communications.

1. SOSM
2. What is SOSM?

SOSM (System of operatively-search measures) - an abbreviation, the meaning of which has recently been known not only by telecom operators, but also by ordinary users. "Total surveillance", "listening", "invasion of privacy" - all of these things are scary and make you think about the information that we send over the Internet or phone. In fact, for an ordinary citizen it is nothing more than horror stories, but for telecom operators it is an additional expense for a new equipment. The development of the SOSM wiretapping system was started in the late 80s by the State Security Committee (KGB) and has been updated several times up to now. [5]

The major task of the system SOSM is to ensure security of the government and its citizens, which is achieved by selective control of the information being listened to. The National Security Committee (KNB) monitors identified or potential threats and subjects under suspicion. It should be emphasized that they are not interested in a citizen's private life or what he does on the Internet as long as it does not cause threats.

This way, SORM controls:

* Already identified threats;
* Potential threats;
* Subjects under suspicion;
* Subjects of the government secret holders. [8]

For what SOSM is needed?

* In order to ensure the government security;
* In order to ensure the citizens security;
* In order to monitor compliance with the law. [8]

1. Types of SOSM

Nowadays, there are three types of the SOSM system:

* SOSM-1 - Wiretapping of telephone lines (stationary and mobile);
* SOSM-2 - "Wiretapping" the Internet traffic;
* SOSM-3 - Collection of all kinds of communication information, its long-term storage and access to data on subscribers. [5]

The system SOSM-1, which was actively used in telephone communication networks in the period from the end of 1980s to the beginning of 2000s, was the first implementation of the hardware-software complex for ORM (operative research measures) support. Initially, SOSM-1 was aimed only for listening to telephone calls of wire network subscribers (for lack of other communication channels). With the appearance of digital telephony and data transmission networks, technical requirements have been changed, and the functions of SOSM-1 have expanded: wiretapping spread to mobile and VoIP-subscribers. [7]

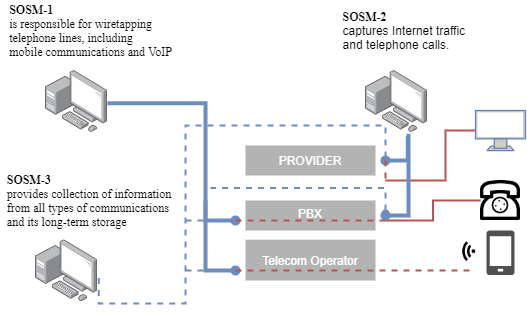


Figure 1. Functions of SOSM-1,2 and 3 (infographic fragment). Source: ria.ru

SOSM-2 allows to capture the Internet traffic. SOSM-2 is a technically more complicated solution than SORM-1 because it is used for capturing all types of traffic that circulates in the operator's network: web, e-mail, video, voice, etc. SOSM-2 is technically a server which connects to the operator's network in order to obtain a copy of all passing traffic. It is controlled by a remote control (RC) on a specific communication channel. The RC is installed in the regional division of the KNB. The area of responsibility in SOSM-2 (as in other SOSMs) is divided between the operator and KNB. The operator ensures deployment, configuration, and maintenance of the automated control subsystem and communication channels, but is not permitted to use its functionality for personal purposes: traffic wiretapping is exclusively the responsibility of the law enforcement agency. In addition to traffic analysis, the intelligence services can obtain other information about the user: connected services, registration data and other statistics. [7]

SOSM-3 is based on the collection of all types of communication information, including its long-term storage and access to data about subscribers. Its contrast to SOSM-1 and SOSM-2 is that SOSM-3 does not intercept user traffic in real-time, it accumulates statistical information about the subscriber. It is possible to obtain a detailed "internet-portrait" of a user by defining all protocols and types of traffic, including messenger traffic, involved in internet-sessions with the help of SOSM-3. The information about billing and authorization of subscribers is received by SOSM-3 from billing service and Radius-server respectively. Data on additional services connected to the subscriber are removed from the telematics server.

The information about the user, according to the requirements for SOSM-3, can be stored for up to 3 years, which requires from the operator additional costs for the installation of capacious data storage systems. Also, the implementation of the SOSM-3 information system may require updating the equipment to ensure the upload of correct data, for example, NAT broadcasts (an example of such a system - SCAT DPI). In the SOSM-3 information system database the decoded traffic must be stored by the operators for 3 years, non-decoded and voice traffic - 6 months.

1. Interface for SOSM system for the “Shift Systems” company

The interface (remote control) will be implemented for access of national security service of the Republic of Kazakhstan to the system of legal information interception, for the “SHIFT systems” company. The remote control forms the Interface of access to SOSM. Interface description:

* + 1. To implement the functions of directing requests to the remote control (system) from the administration workplaces, sending requests to the databases from the processing and supervision workplaces, transmission of the requested messages and information for playback at the processing and supervision workplaces as part of the means of carrying out the ORM and means of collecting and storing the SIS (system information of subcsribers) of telecommunications equipment of the communication network, the formation of access interface(s) shall be provided.
    2. Implementation of the access interface and its capacity shall ensure uninterrupted connection of administration, processing and supervision workplaces, transfer of requests, messages and information in the required volume, without passes and losses.
    3. The access interface shall provide multiuser mode of operation, which provides for the set number of simultaneous connections of administrators, processors and supervisors to the center for conducting the ORM or the center for collecting and storing the SIS in uninterrupted 24-hour mode.
    4. One centralized control center ORM or SIS collection and storage center shall support the number of simultaneous connections in accordance with Table 1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The number of subscribers for one ORM center or SIS collection and storage center | Number of hardware administra-tors | Number of administrator in the building | Number of handler administra-tors | Total number of handlers | Total number of supervi-sors |
| up to 10 000 | 5 | 5 | 5 | 20 | 3 |
| from 10 000 to 100 000 | 10 | 10 | 10 | 100 | 5 |
| from 100 000 to 1 000 000 | 15 | 15 | 15 | 200 | 10 |
| more than 1 000 000 | 30 | 30 | 30 | 500 | 15 |

* + 1. The access interface shall meet the following requirements:
* channel layer protocol - Ethernet;
* transport layer protocol - TCP/IP;
* application layer protocol - HTTP".
  + 1. The access interface shall be formed on the basis of the "WEB-interface" technology, which is a graphical interface "client-server", where the client is the software of administration, processing and supervision workplaces, and the server is the software of the remote control (system), database software.

The server software of the remote control must contain licensed up-to-date anti-virus software as well as the latest software updates of the operating system.

* + 1. Unification of means of carrying out of ORM of the separate switching equipment for formation of the center of carrying out of ORM of a communication network, and also unification of means of gathering and storage of SIS of the separate switching equipment for formation of the center of gathering and storage of SIS of a communication network should be carried out on a physical level according to requirements of point 3.5 on an applied level according to requirements of point 3.6 of the present standard.
    2. The access interface includes the following interfaces:
* administration interface;
* processing interface;
* supervisory interface.
  + 1. The choice of one of the access interfaces shall be provided when the client connects to the server, with the following procedure of authentication and authorization of the administrator, handler and supervisor. One administrator, handler, supervisor should be able to connect only one interface.
    2. A user delimitation mechanism shall be provided:
* the rights of access to the means and functions of ORM and to the means of collecting and storage of SIS;
* on access to information.

Delimitation of users' access rights to the means of carrying out ORM and means of collecting and storage of SIS should be realized by the functions of users: chief administrator, equipment administrators. task administrators, administrators of processors, handlers, supervisors. There shall be one chief administrator in the system, the number of other users shall not be limited.

Removal of the chief administrator shall not be performed.

To differentiate users' access to information, task folders shall be created in the access interface.

1. LITERATURE REVIEW

During the work the following aspects were discussed: features and differences of SOSM-1,2 and 3, foreign analogs of SOSM, communication interface of SOSM, remote control simulator. The general functions of the remote control for SORM were also named.

The development of the SOSM wiretapping system was started in the late 80s by the State Security Committee (KGB) and has been updated several times so far. Now we have three versions:

SORM-1 - wiretapping of telephone lines (fixed and mobile),

SORM-2 - "wiretapping" Internet traffic,

SORM-3 - collection of information of all types of communication, its long-term storage and access to data on subscribers. [5]

While SOSM-1, which was developed in the 80s, is required for listening to telephone calls and has no other function, the differences between SOSM-3 and SOSM-2 require explanation. [4]

SOSM-2 is a system for monitoring Internet users. The system is a device (server), which is connected to the equipment of the provider (telecom operator). The provider only includes it in his network and does not know about the purposes and methods of listening, the management of special services. [4]

How are operational and search measures implemented in the Internet century?

Intelligence agencies begin controlling a person and his traffic if he is suspected of committing or planning illegal activities (theft, break-ins, terrorism, extortion and other criminal and serious administrative offences). A person under surveillance cannot in any way determine that this is happening, just as the provider does not know who the intelligence agency is watching. [4]

Since SOSM equipment must be installed by any Kazakh telecom operator or provider, any user can be monitored. The only way to avoid control is to not use the Internet. Besides traffic analysis, intelligence services may also receive other information about the user: connected services, registration data and other statistics.

By the way, all actions of special services in relation to suspected citizens are regulated by federal laws and orders of ministries of the Republic of Kazakhstan. It is legal to monitor.

The main purpose of SOSM-3 is to obtain the most complete information about the user, not only in real time, but also for a certain period (up to 3 years). If SOSM-1 and SOSM-2 intercept information from a user, then SOSM-3 does not contain such information, but only stores statistics, copies it and creates a profile of the person in the Internet. To accumulate such volumes of data, large storage systems will be used, as well as systems of deep traffic inspection (Deep Packet Inspection) to filter out unnecessary information (movies, music, games) that does not contain useful information for law enforcement agencies.[4]

SOSM-3 has an important function to ensure the safety of citizens and the state, allowing not to disclose the offenses of "accidental criminals", and prevent illegal activities of persons engaged in organized crime on a large scale (terrorism, economic crimes, etc.). [4]

Also, the amendments to the law clearly regulate the requirements for communication channels from the network equipment of the communications operator to SOSM-3. And the functionality of SOSM-3 should ensure that network packets are tied to specific user identifiers, which can then be used to select traffic. Among the key identifiers can be named: logins to mail and messengers, phone numbers, e-mail addresses, user location, ip and url address of the resources visited, and others. [4]

The SOSM system is not unique, as there are analogues in other countries.

In Europe, the requirements for lawful interception (LI) are defined by the European Telecommunications Standards Institute (ETSI), and in the United States, by the Communications Assistance for Law Enforcement Act (CALEA). [7]

Technically, the process of capturing user and statistical information from LI and SOSM is very similar. In terms of functional implementation, LI is fundamentally different from SOSM in that in Europe and the USA, the administrative function to capture and listen to user traffic is formally assigned to operators. Intelligence services, having received a court order, request the necessary information from operators, and only then get access to the subscriber's profile. [7]

In the Kazakh SOSM, the participation of an operator is not required for this purpose. It means that in the case of legal interception the KNB officers have much more authority than their foreign colleagues.

There are several systems operating in China that can be remotely compared to SOSM: the Golden Shield (or Great Chinese Firewall), the Monitoring Bureau and the IJOP system. However, all these solutions are used not so much for listening as for controlling and restricting Chinese access to some or other Internet resources. [7]

India has a Central Monitoring System - the Central Monitoring System - which is close to PRISM by its purpose, but covers only the country's internal networks. [7]

Sweden uses a system similar to SOSM-3 - Titan, which is a database with records of telephone conversations, electronic transactions and Internet traffic. However, Titan is primarily intended for foreign intelligence purposes. [7]

In addition, in these countries, such equipment is mounted in the ATE, switches, and servers.

1. DISCUSSION

Since SOSM analogs differ in foreign countries, so the remote control (interface) and its usage is unique for each country.

Since the 2010s the United Kingdom government has been using a system similar to SOSM-2 and SOSM-3 - The Communications Capabilities Development Program (CCDP), or "Telecommunications Opportunities Development Program". Technically, the system represents capture facilities (servers) and databases, which are designed to store information about all telephone calls, e-mails, discussions in chats and social networks, web browsing and Internet habits of users. Officially, law enforcement agencies may only use CCDP after a court order (under the Regulation of Investigatory Powers Act 2000). [7]

In addition to the CCDP, there is Tempora, a project established by the UK Government Liaison Center in collaboration with the U.S. National Security Agency (NSA). Tempora is also designed for mass listening and traffic interception, but unlike the CCDP it is a more autonomous and technically advanced system. The equipment includes a separate optical communication network, servers and storage for storing Internet content for 3 days and user metadata for a month. Tempora became known in 2013 thanks to Edward Snowden. According to the American, the Government Communications Center ignores the Law of Investigatory Powers Act 2000 and listens to citizens without any restrictions. [7]

There are several programs in the United States that are in one way or another related to traffic interception - official (under CALEA) and unofficial (overseen mainly by the NSA and CIA). [7]

The closest analogue of SOSM is the DCSNet system used by the FBI. The system consists of three software packages, which differ in purpose and technical characteristics:

* DCS3000 (also known as Red Hook) is responsible for intercepting metadata on telephone calls in wired and wireless networks;
* The DCS5000 is a more advanced version of the DCS3000, designed primarily to combat terrorism and espionage;
* DCS6000 (aka Digital Storm) is used to intercept telephone calls, text messages and Internet traffic. [7]

Following the release of classified information provided by Edward Snowden to the Washington Post and The Guardian, systems such as Boundless Informant and PRISM (Program for Robotics, Intelligents Sensing and Mechatronics) became known. Boundless Informant is a global intelligence system designed to process and visualize large amounts of data, in particular data about phone calls. PRISM - complex for in-depth monitoring of Internet traffic. Both systems work in conjunction and are used for wiretapping both inside and outside the U.S.A. [7]

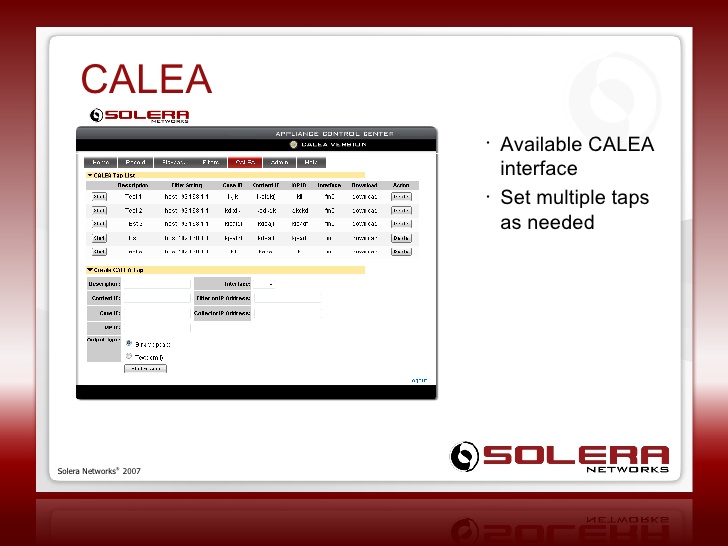


Figure 2. Interface of “Solera networks” company [9]

As we see there is and interface of “Solera Networks” company on the figure 2. “Solera Networks” is the TiVo for the network, They are the foundation for a comprehensive network management and security architecture. [9]

Their interface has such features:

* Record
  + Start and Stop multiple captures
* Playback
  + Playback any period of captured traffic
  + Specify maximum bytes per file
* Filters
  + Filter Inbound/Outbound Traffic
  + Filter for any bit of information
  + Filter at the header or payload level
  + Multiple filters – start and stop at any time, continue to capture
* Administration – Users
  + Assign users
  + Create new users
  + Reset passwords
  + Ability to access CLI from web console
* Administration settings
  + View and change system configurations
  + Change default settings [9]

1. CONCLUSION

To implement the SOSM interface, it is necessary to understand and distinguish the types of SOSM. It is essential to coordinate the functionality and design of the interface with the company "Shift Systems", with which we cooperate.

In this section, the concept of SOSM was reviewed. The types of SOSM system were also explained. Their differences from each other are defined. Analogues of SOSM of other countries were also considered, with an explanation of their differences. The interface and functionality of a foreign company "Solera Networks" for the CALEA system was found and described. Based on the data, some basic functions of the interface were found out.

1. FUTURE WORK

The literature review provides the basis for future work in the development of the SOSM interface. The intention is to explore the functionality more deeply, and in general to development of interfaces of other companies as far as it possible.

REFERENCES

[1] <https://rspectr.com/articles/515/kak-ustroen-sorm>

[2] [https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A1%D0%9E%D0%A0%D0%9C\_(%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0\_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%BE-%D1%80%D0%BE%D0%B7%D1%8B%D1%81%D0%BA%D0%BD%D1%8B%D1%85\_%D0%BC%D0%B5%D1%80%D0%BE%D0%BF%D1%80%D0%B8%D1%8F%D1%82%D0%B8%D0%B9)#:~:text=%D0%A1%D0%9E%D0%A0%D0%9C%20(%D1%81%D0%BE%D0%BA%D1%80.%20%D0%BE%D1%82%20%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%20%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D1%85,%D0%9E%20%D1%81%D0%B2%D1%8F%D0%B7%D0%B8%C2%BB%20%D0%B8%20%D0%BF%D1%80%D0%B8%D0%BA%D0%B0%D0%B7%D1%83%20%D0%9C%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D0%B5%D1%80%D1%81%D1%82%D0%B2%D0%B0](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A1%D0%9E%D0%A0%D0%9C_(%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%BE-%D1%80%D0%BE%D0%B7%D1%8B%D1%81%D0%BA%D0%BD%D1%8B%D1%85_%D0%BC%D0%B5%D1%80%D0%BE%D0%BF%D1%80%D0%B8%D1%8F%D1%82%D0%B8%D0%B9)#:~:text=%D0%A1%D0%9E%D0%A0%D0%9C%20(%D1%81%D0%BE%D0%BA%D1%80.%20%D0%BE%D1%82%20%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%20%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D1%85,%D0%9E%20%D1%81%D0%B2%D1%8F%D0%B7%D0%B8%C2%BB%20%D0%B8%20%D0%BF%)

[3] <https://rspectr.com/articles/515/kak-ustroen-sorm>

[4] <https://vasexperts.ru/blog/osobennosti-i-otlichiya-sorm/>

[5] https://vasexperts.ru/blog/dpi-dlya-sorm-gotovimsya-ekonomit/

[6] <http://1234g.ru/novosti/sorm-ishchet-novye-tekhnologii>

[7] <https://itglobal.com/ru-kz/company/blog/sorm-worldwide-experience/>

[8] <https://www.slideshare.net/TechTalksNSU/ss-61043360>

[9] https://www.slideshare.net/gigamon/solera-networks