Abstract: In this paper, the analysis shows that construction of systems of information security, transmitted by radio satellite communication channels, it is widely used: first of all cryptographic methods of information security, which ensure the integrity of the authentication and the confidentiality of transmitted information. The used techniques in satellite communication systems radio channels dependent on the limitations, impose an information system, first of all in terms of the interaction protocols, ways and means of transmitting information commands.

Keywords: Communication systems, Authentication radio channels, Encryption method, Protocols, Implementation.

Introduction:

It is currently becoming more common communication system, operating by satellite communication channels.

In connection with a small satellite communication channels protectiveness great importance is the task of ensuring the confidentiality transmitted through this information channel.

Threat model analysis, acting on satellite radio communication system, possible to identify the following authentication problem:

1. Command and other information authentication radio channels transmitted in satellite communication systems [1, 2].
2. Users, have to establish the authenticity of the correspondent, which establishes a control channel.

3. Authentication program, files, stored in database, while simultaneously checking the integrity of the object of protection, perhaps the solution to these problems based on the method of block symmetric encryption, asymmetric encryption block, stream encryption methods.

**The problem and solution:**

Used of the techniques in satellite communication systems radio channels dependent on the limitations, impose an information system, first of all in terms of the interaction protocols, ways and means of transmitting information commands.

To date, the solution of authenticity problems associated with the development and implementation of a variety of block encryption algorithms.

To them, first of all, you must include standard DES (USA), and algorithms, based on asymmetrical transformation with public keys.

The main advantage of modular algorithms is their adaptability and ease of use in communication networks.

When you use strong data each unit received is encrypted using one and the same key. This allows you to organize as virtual, and data gram transmission, and when the block encryption is necessary provide synchronization to within the boundaries of the package.

Depending on the possible cargo is used a symmetrical, and asymmetric encryption algorithm. In the case of the using of symmetric cryptographic algorithms sources (transmitter) and the receiver must fully trust each other. In asymmetric systems transmitter and receiver many by parties, don’t trust each other [3, 4].

Regarding encryption speed (decryption) it is more preferred symmetric cryptosystem. In a hardware implementation, they provide a speed of several tens Mgb/s, and when the program – units Mgb/s.
In the class of asymmetric encryption algorithms to use of a foreign element base can be achieved within a speed of tens or hundreds Kbit/s.

In a stream cipher system, direct conversion is carried out using the ration:

\[ C_i = M_i \oplus r_i \]  

(1)

Where: \( M_i \) – Element information sequence open a message.

\( r_i \) - The element encoding sequence.

The inverse transformation is performed on the receiving side according to the rule

\[ M_i^* = (C_i^* - r_i)(mod p) \]  

(2)

Where: \( * - i \) - indicates possible presence in the resulting distorted message, effect of transfer over the communication channel or storage in characters carriers.

\( P \) – Conversion module.

The founded application system produced binary conversion information \( p=2 \).

In this case the expressions (1) and (2) have the form:

\[ C_i = M_i \oplus r_i \]  

(3)

\[ M_i = C_i \oplus r_i \]  

(4)

The analysis showed, what and to provide theoretical or practical non decrypted Gamma-line conversion \( r_i \) it must meet the following requirements:

- Period \( L \) sequence \( r_i \) to realize theoretical non decrypted should be infinity, but to implement practical non decrypted \( L > L_{pr} \) where \( L_{pr} \) – limit the period \( L \);
- The type implementation sequence \( r_i \) it should clearly defined key \( K_i \) chosen from a full set of keys \( \{K\} \);
- According to its structural properties of sequence \( r_i \) should in limit the limit of approach to sequence, formed randomly sensor;
- The possibility of formation of one and the same implement \( r_i \) at various sets of equipment for in-line conversion under certain keys \( K_i \);
The main advantage of the method are in –line conversion [5, 6, 7]:

a) The possibility of construction a theoretical and practical non cryptic system;

b) The possibility of implementing fast conversion speed (up 10 mb/s) and, as consequence, working in real time,

c) The ability of automatic rejection of false information by error propagation.

The next table summarizes the data transferred each of the above methods.

<table>
<thead>
<tr>
<th>The method of appointment</th>
<th>Resistance method</th>
<th>Conversion speed</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetric block transform method</td>
<td>Computationally fortitude</td>
<td>To 10 mb/s</td>
<td>Software hardware</td>
</tr>
<tr>
<td>Asymmetric block transform method</td>
<td>Computationally fortitude</td>
<td>100 kb/ s</td>
<td>software</td>
</tr>
<tr>
<td>Stream encryption method</td>
<td>Practically non – cryptic</td>
<td>Up 10 mb/ s</td>
<td>Software hardware</td>
</tr>
</tbody>
</table>

Analysis of the table shows, that give the nature and functioning of the satellite communication systems.

(The need of work in real time with the start – stop serial transmission methods and processing of nouns and restriction of the length of transmitted information block). The most suitable method, which can be used to convert the special information, it is the method of in –line conversion.

Application only by flow conversion team on the radio channel satellite communication systems, as studies have shown, make it infective because most of the information block long.

The most commonly used system with information packet, it is a method based on the formation of a secure message authentication code.
The essence of the message authentication code formation method is that for information unit joins an additional unit (authentication code) formed participation and information bit of the previous blocks, as well as time varying system parameters.

The results:
In this way, optimal terms of maximum security transmitted by satellite radio channels information, as well as the speed is a method of block line conversion with the subsequence an additional of authentication code.
Finally the analysis shows that construction of systems of information security, transmitted by radio satellite communication channels, it is widely used: first of all cryptographic methods of information security, which ensure the integrity of the authentication and the confidentiality of transmitted information.
The used techniques in satellite communication systems radio channels dependent.

References:

