Method of optimum channel switching in equipment of infocommunication network in conditions of cyber attacks to their telecommunication infrastructure.

S S Kochedykov, A N Noev, A V Dushkin, I A Gubin

FKOU the Voronezh institute FSIN of Russia, 1a, Irkutskaya St., Voronezh, 396072, Russia

E-mail: Infosec36@mail.ru

Abstract. On the basis of the mathematical graph theory, the method of optimum switching of infocommunication networks in the conditions of cyber attacks is developed. The idea of representation of a set of possible ways on the graph in the form of the multilevel tree ordered by rules of algebra of a logic theory is the cornerstone of a method. As a criterion of optimization, the maximum of network transmission capacity to which assessment Ford-Falkerson’s theorem is applied is used. The method is realized in the form of a numerical algorithm, which can be used not only for design, but also for operational management of infocommunication networks in conditions of violation of the functioning of their switching centers.

1. Introduction. In the modern world, cybercrime has become widely spread. No week passes without sensational messages about cyber attacks on public authorities, cracking computer systems of banks and corporations, violation of operation of logistic centers and even supermarkets. Cybercrime begins to envelop wide and local infocommunication area networks, turning them into the tool of the organization, carrying out and coordinating terrorist operations worldwide. Hackers increase the number of cyber attacks on military infrastructures of nuclear powers, at the same time inventing new and more perfect methods of attacks. In these conditions, protection against cyber attacks and in general the problem of fighting against cybercrimes in the infocommunication sphere come to the fore [1], acquiring a pronounced anti-terrorist painting. At the same time, it is easy to note that the overwhelming number of publications on this subject is devoted to purely technical or program and technological issues of protection of infocommunication systems against the attacks from hackers, insiders, phreaks and other subjects of computer crime. The system questions, related to development of methods of switching an optimum channel in the equipment of infocommunication networks in the conditions of cyber attacks to their telecommunication infrastructure, has not gained due development yet.

2. Formulation of a task.
Let there be some infocommunication network including program and hardware components of telecommunication infrastructure, which are subjected to the attacks from cybercriminals. Let us present this network in count’s form \( G^{(\text{com})}(I,U) \), in which a set of tops \( I = \{i_1,i_2,\ldots,i_N\} \) consists of
switching centers, and the set of arcs is interpreted as $U = \{(i_k, i_l)\}$, $k, l = 1 \div N$ – a set of direct lines of communication between switching centers [2]. For each arch of count $(i_k, i_l) \in U$, let us put size in compliance with $\alpha(i_k, i_l) \geq 0$, equal to forming secondary quantity (switched) communication links. Let us characterize an effect of cyber attacks on such network by sizes $\beta(i_k, i_l) \geq 0$, measured by the quantity of secondary communication channels, put out of operation from number $\alpha(i_k, i_l)$ due to violation of the operation of program complexes of switching centers. Then sizes $q(i_k, i_l) = \alpha(i_k, i_l) - \beta(i_k, i_l)$ will characterize real throughput of direct lines of communication of switching in the conditions of impact on telecommunication infrastructure from cybercriminals between centers. Let us allocate two subsets $P$ and $Q$ on set $I$, such that $p \in P$ corresponds to sources of messages, and $q \in Q$ – to their recipients. One should recognize that the purpose of cyber attacks is the greatest possible capacity reduction of a network by implementation of malicious applications in the software of switching centers. The task will consist in development of an algorithm capable in the conditions of cyber attacks to realize the channel switching on network $G^{(com)}$, that at the set effect experiences influence from cyber attacks $G^{(attack)}(P, Q)$; graph $G^{(part \ com)}(P, Q)$ is formed by secondary communication channels with the maximum capacity between elements of sets $P$ and $Q$.

3. Solution of a task.
Let us consider, first, a special case of a bipolar network, that is when $|P| = |Q| = 1$, and then specify how it is possible to modify a method for the general case. For the solution of the formulated task, let us use Ford-Falkerson’s theorem (in its interpretation stated in [3]), according to which the maximum capacity of the network between any pair of tops $p$ and $q$ is defined by the section, minimum by capacity $S\{p, q\}$, dividing tops $p$ and $q$, graph $G^{(part \ com)}$, removal of which from set $U$ breaks off all ways between them:

$$S\{p, q\} = \left\{ (i, j) \in U \right\} \left\{ \begin{array}{l} \{G^{(com)} = G_p^{(part \ com)} \cup G_q^{(part \ com)} \cup S\{p, q\}, \\
p \in G_p^{(part \ com)}, q \in G_q^{(part \ com)}, \\
G_p^{(part \ com)} \cup G_q^{(part \ com)} = \emptyset \end{array} \right\} \right..$$

At the same time, minimum section $S_{\min}\{p, q\}$, on which it is reached, is called:

$$S_{\min}\{p, q\} \rightarrow \min_{S(i,j)} \sum_{i,j} q_{i,j}.$$

It is possible to construct any section $S\{p, q\}$, knowing a set of all ways which exist between $p$ and $q$. Let us present such set in the form of a tree of ways $D_{G^{(com)}}(p)$, which will be built, being conformed with the following rules:

a) let us consider that top $p \in I$ forms tree root $D_{G^{(com)}}(p)$ or its zero tier:

$$J_0(p) = p;$$

b) all tops $i \in I$, such that $(p, i) \in U$ forms the first tier of tree $D_{G^{(com)}}(p)$, that is:
\( J_j(p) = \left\{ i \in I \left| (p, i) \in U \right. \right\}; \)

c) for formation \( r \), tier \( J_r(p) \), let us choose any top \( j \in J_{r-1} \), different from \( q \), also let us consider all tops \( l \in I \), that is \( (j, l) \in U \); let us exclude tops which have already reached tiers with smaller numbers from the received list and are ancestors of top \( j \); having done these operations for all \( j \in J_{r-1} \), one will receive:

\[
J_p(p) = \left\{ l \in I \left| \forall j \in J_{r-1} (j \neq q) \right. \wedge \left[ (j, l) \in U \right] \wedge \left[ I \notin W(j) \right] \right\},
\]

where \( W(j) \) – great number of ancestors of top \( j \).

Creation of tree \( D_{G_{\text{new}}} (p) \) comes to an end when the next tier is empty.

Let us note that the considered set of operations of the course on everyone \( r \) ‘s step follows from (1); there is a truncation of a set of the considered tops. Besides, it is obvious that all ways \( \mu(p, q) \) form set \( W(q) \), ordered according to numbers of tiers, and the quantity of all ways is equal to the number of copies of tops \( q \) in all tiers \( D_{G_{\text{new}}} (p) \).

Let us renumber all ways on tree \( D_{G_{\text{new}}} (p) \) arbitrarily:

\[
M_{(p, q)} = \left\{ \mu_r(p, q) \right\}_{r=1}^R.
\]

Then, for obtaining some section \( S(p, q) \), it is sufficient for every way \( \mu_r(p, q) \) to be removed exactly on one arch. It means that if to designate the event through \( B(S(p, q)) \), consisting in obtaining some section, and through \( \beta_r(i, j) \) – removal of arch \( (i, j) \) from way \( \mu_r(p, q) \), then:

\[
B(S(p, q)) = \left[ \exists_{(i, j) \in \mu_r(p, q)} \beta_1(i, j) \right] \wedge \left[ \exists_{(i, j) \in \mu_r(p, q)} \beta_2(i, j) \right] \wedge \ldots \wedge \left[ \exists_{(i, j) \in \mu_r(p, q)} \beta_r(i, j) \right].
\]

Using distributivity of the equation:

\[
(\beta_a \vee \beta_c) \wedge (\beta_b) = (\beta_a \wedge \beta_b) \vee (\beta_c \wedge \beta_b),
\]

let us get:

\[
B(S(p, q)) = \exists_{(i, j, k) \in \mu_r(p, q)} \left[ \beta_k(i_1, j_1) \wedge \beta_2(i_2, j_2) \wedge \ldots \wedge \beta_k(i_R, j_R) \right].
\]

Let us simplify (4), using the following rules of absorption:

\[
\beta_a \wedge \beta_c = \beta_a; \quad (5)
\]

\[
(\beta_a \wedge \beta_c) \vee (\beta_a \wedge \beta_c) = (\beta_a \wedge \beta_c); \quad (6)
\]

\[
(\beta_a \wedge \beta_c) \vee (\beta_a \wedge \beta_c) = (\beta_a \wedge \beta_c). \quad (7)
\]

After transformation of expression (4) by rules (5)-(7), disjunctive representation \( B(S(p, q)) \) will define the minimum set of sections.

For development of a numerical algorithm of optimum switching of a network in the conditions of cyber attacks to its switching centers, let us designate conversions (5)-(7) by parameter \( F_{(p, q)} \) and use the following specifying definitions [3]:

- two sections \( S_1(p, q) \) and \( S_2(p, q) \) will be called independent if any of them is not a part of another;
- the maximum set of the independent sections dividing tops \( p \) and \( q \) will be called the fundamental system of sections and designated by symbol \( FS\{p,q\} \);
- let us say that section \( S_1\{p,q\} \) absorbs section \( S_2\{p,q\} \), if \( S_1\{p,q\} \subseteq S_2\{p,q\} \);
- graph \( G^{(\text{com1})} \) will be called thinned out and designated by symbol \( G^{(\text{remove})} \), if some set of arches is removed from it.

Using these definitions and Ford-Falkerson's theorem, let us formulate two lemmas.

Lemma 1. Transformations \( F_{(p,q)} \) are brought to \( FS\{p,q\} \), and, at the same time, for any section dividing \( p \) and \( q \), there will be a section from a fundamental system which absorbs it or in formal expression \( \forall S^\ast\{p,q\} = (\exists S\{p,q\} \in FS\{p,q\}) \land (S\{p,q\} \subseteq S^\ast\{p,q\}) \).

Lemma 2. Each element of the fundamental system of the sections dividing \( p \) and \( q \) is thinned out by column \( G^{(\text{remove})} \) and absorbs some set of elements \( FS\{p,q\} \).

Following directly from the first lemma that required minimum section \( S_{\text{min}}\{p,q\} \) contained in the fundamental system, there is: \( S_{\text{min}}\{p,q\} = \min_{S\{p,q\} \in FS\{p,q\}} \left[ \sum_{(i,j) \in S\{p,q\}} q_{i,j} \right] \).

When switching an optimum channel in a telecommunication network in the conditions of cyber attacks to its centers, such switching comes down to determination of a set of ways \( \mu\{p,q\} \) from tree \( D^{(\text{com1})}_G\{p\} \), each of which including arch \((i,j) \in S_{\text{min}}\{p,q\}\). Let us designate the count's subgraph \( G^{(\text{com2})} \) formed by the specified set of ways through \( G^{(\text{com2})}_G \). It is obvious that \( G^{(\text{com2})}_G \) corresponds to the required optimum switching.

Taking into account the algorithm of the optimum switching of a network in the conditions of cyber attacks, its switching centers look as follows:

\[
\text{Step 1. } G^{(\text{com1})}_G \xrightarrow{F_{(p,q)}} FS\{p,q\};
\]

\[
\text{Step 2. } S_{\text{min}}\{p,q\} = \min_{S\{p,q\} \in FS\{p,q\}} \left[ \sum_{(i,j) \in S\{p,q\}} q_{i,j} \right];
\]

\[
\text{Step 3. } S_{\text{min}}\{p,q\} \xrightarrow{F_{(p,q)}^{-1}} G^{(\text{com2})}_G.
\]

Here, symbol \( F_{(p,q)}^{-1} \) is the transformation defining a set of the ways containing arches designated as \( S_{\text{min}}\{p,q\} \).

It follows from lemma 2 that the fundamental system of sections \( FS\{p,q\} \) transformation is an invariant of the primary network, and \( F_{(p,q)} \) for rarefied column \( G^{(\text{remove})} \) comes down to exclusion from elements \( FS\{p,q\} \) of remote arches and to application of transformations (5)-(7) to the changed elements. It means that transformation \( F_{(p,q)} \) in full has to be used only once, and at each subsequent definition (caused, for example, by change of objects and intensity of cyber attacks) it is replaced with simpler operations. The last circumstance increases significantly the speed of an algorithm that allows using it not only for design, but also for diagnosing operability of the system [4] and operational management of infocommunication networks in conditions of violation of their functioning by cybercriminals.
Let us generalize transformation $F_{(p,q)}$ in case $K$-polar network. For this case, 
$\{P,Q\} = \{p_s, q_s\}_{s=1}^K$. Then, it is obvious that:

$$FS\{p,q\} = \min \left( \bigcap_{s=1}^K FS\{p_s,q_s\} \right),$$

(11)

where the «min» symbol has designated a procedure of minimization for rules of absorption (5)-(7).

Taking into account (11), application of algorithm (8)-(10) gives minimum section $S_{min}\{p,q\}$ for a case of the multi-polar network.

4. Analysis of experiment results.

On the basis of results of modeling, let us carry out the analysis of the functioning of the centers of switching for the purpose of definition of the best strategy of counteraction to cyber threats.

Thus, it has been established that a complex use in the equipment of systems switching of information security of different types (program and hardware) intended for counteraction to cyber threats, based on methods of optimum switching, allows one to increase efficiency of counteraction to cyber threats from 60% to 75% in comparison with use of only means of the given (program) type. Besides, it allows one to increase efficiency of protection against 15% to 30% in comparison with use of only means and the systems of protection against cyber threats of built-in (hardware) type. As a result of a computing experiment defining an optimum method of switching, it has been established that the lack of using means of counteraction to cyber threats reduces timeliness of realizing problems of switching from 60% to 80%. Use of means and the systems of counteraction to cyber threats of the given (program) type increases timeliness of circuit switching from 25% to 50%. Use of means of built-in (hardware) type increases timeliness of realizing problems of switching from 45% to 60%. Complex use of means and the systems of counteraction to cyber threats of different types (hardware-software) within the offered method increases timeliness of realization of problems of optimum switching from 35% to 65%. A graphic interpretation of made calculations is shown in figure 1.

5. Conclusion.

The task of switching an optimum channel in telecommunication equipment of infocommunication networks in conditions of cyber attacks on switching centers is reduced to simulation of a subject of attacks using mathematical count of type $G^{\text{com}(1)}(I,U)$. In it, $I = \{i_1, i_2, \ldots, i_N\}$ – set of the centers of

![Figure 1. A graphic interpretation of made experiments according to an efficiency indicator of counteraction to cyber threats of protection means](image-url)
switching, and \( U = \{(i_k, i_l)\} \), \( k, l = 1 \div N \) – set of direct lines of communication between switching centers with the subsequent search for its critical section. It allowed one to develop a new method of switching the optimum channel of telecommunication equipment and to offer a numerical algorithm of optimum switching in the conditions of cyber attacks by the criterion of a throughput maximum. The algorithm has that advantage of being used not only for design, but also for operational management of information security of infocommunication networks in the conditions of violation of functioning of their switching centers and elimination of consequences of a cyber attack.

References

[1] Novoseltsev V I, Kochedykov S S, Noev A N 2017 Influence of cyber attacks to the result of competition Current problems of applied mathematics, informatics and mechanics: collection of works of the International scientific and technical conference (Voronezh: Research Publications publishing house) ISBN 978-5-9500319-1-5

[2] Kristofides N 1978 Theory of counts: algorithmic approach The translation with English (M.: World)

[3] Novoseltsev V I, Kochedykov S S Orlova D E 2017, Tensor analysis Krone and his applications (Voronezh: Publishing and printing center "Scientific Book")

[4] Kochedykov S S, Dushkin A V, Novoseltsev V I 2017, Tool and algorithmic diagnostic devices of operability of actuation mechanisms of automated control systems 2017 2nd International Ural Conference on Measurements (UralCon) p 193 – 198. IEEE Conference Publications ISBN 978-1-5386-0521-9 IEEE Catalog Number: CFP17URL-ART DOI: 10.1109/URALCON.2017.8120709