УДК: 004.056 DOI: 10.53816/23061456_2021_7–8_107

МЕТОДИКА СИНТЕЗА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ, ИСКЛЮЧАЮЩАЯ РЕАЛИЗАЦИЮ DDOS-АТАК НА ЭЛЕМЕНТЫ КОРПОРАТИВНОЙ СИСТЕМЫ УПРАВЛЕНИЯ

THE METHOD OF INFORMATION AND TELECOMMUNICATIONS SYSTEM SYNTHESIS, EXCLUDING THE IMPLEMENTATION OF DDOS ATTACKS ON THE ELEMENTS OF THE CORPORATE MANAGEMENT SYSTEM

Д-р воен. наук Ю.И. Стародубцев, А.А. Кузьмич

D.Sc. Yu.I. Starodubtsev, A.A. Kuzmich

ВАС им. С.М. Буденного

Для защиты от DDoS-атак разработано значительное количество решений. При совокупности этих способов, их реализации или готовности к использованию, остается вероятность того, что с любого места информационно-телекоммуникационной системы возможна реализация DDoS-атаки на элементы корпоративной системы управления.

В статье представлена методика синтеза информационно-телекоммуникационной системы, исключающей реализацию DDoS-атак на элементы корпоративной системы управления в течении их эксплуатации.

С помощью разработанной методики можно получить данные о параметрах транспортной сети и сети доступа, при применении которых исключается возможность реализации DDoS-атак на элементы корпоративной системы управления. Методика предназначена для должностных лиц, обеспечивающих процесс планирования, развертывания и функционирования корпоративной системы управления.

Ключевые слова: инфомационо-телекомуникационная система, корпоративная система управления, DDoS-атака, деструктивные программные воздействия, метод редукции, теория графов, транспортная сеть.

A significant number of solutions have been developed to protect against DDoS attacks. With the combination of these methods, their implementation or readiness for use, it remains likely that from any place of the information and telecommunications system, it is possible to implement a DDoS attack on the elements of the corporate management system.

The article presents a method for the synthesis of an information and telecommunications system that excludes the implementation of DDoS attacks on elements of a corporate management system during their operation.

With the help of the developed methodology, it is possible to obtain data on the parameters of the transport network and access network, when using which the possibility of implementing DDoS attacks on elements of the corporate management system is excluded.

The methodology is intended for officials who ensure the process of planning, deploying and functioning of the corporate management system.

Keywords: information and telecommunications system, corporate management system, DDoS attack, destructive software effects, reduction method, graph theory, transport network.

В условиях нарастающей интеграции информационно-телекоммуникационной системы (ИТКС) с сетью связи общего пользования (ССОП), резко возросла роль вопросов защищённости процесса функционирования корпоративных систем управления (КСУ) от деструктивных программных воздействий (ДПВ) [1–3].

Анализ известных работ показал, что задача синтеза информационно-телекоммуникационной системы, исключающей реализацию DDoS-атак на элементы корпоративной системы управления, не ставилась и не решалась, а разрабатывались только отдельные способы, снижающие степень ущерба [4–6].

Суть DDoS-атаки заключается в следующем. Введем пограничные узлы на фрагменте ССОП, к которым подключен источник деструктивного воздействия, который генерирует трафик q. Зададим пропускную способность линий связи C_j, а также производительность оборудования μ_i, используемого на узлах фрагмента ССОП. Введем I-ое количество узлов с неким вычислительным ресурсом, в котором какие-то узлы защищены, а какие-то не защищены и имеют уязвимость в виде избыточного вычислительного ресурса. Фактически избыточный деструктивный трафик может генерироваться с одного элемента ССОП, а может одновременно с нескольких элементов ССОП, в зависимости от степени защищенности этих элементов и степени использования вычислительного ресурса. Таким образом, атака возможна, если пропускная способность суммы линий связи, входящих в элемент интегрированной ИТКС КСУ, больше производительности оборудования этого элемента, который является обслуживающим прибором:

$$\sum_{j=1}^{N}\lambda_j > \mu_i,$$

где μ_i — производительность оборудования элемента ССОП; λ_j — пропускная способность j-ой линии связи.

Постановка задачи

Задача заключается в синтезе ИТКС, в которой для каждого элемента, используемого КСУ должно выполняться условие

$$\sum_{j=1}^{N}\lambda_j \le \mu_i, \text{ при } C_c \ge C_{\text{КСУ}}^{\text{Треб}}, \qquad (1)$$

где μ_i — производительность оборудования элемента КСУ; λ_j — пропускная способность j-ой линии связи; C_c — пропускная способность сети; $C_{\text{КСУ}}^{\text{Треб}}$ — требуемая пропускная способность КСУ для обеспечения услуг связи.

Приведенное выше условие (1) должно обеспечивать заданное количество и качество услуг связи.

Исходя из постановки задачи для решения применяются метод редукции, теория графов и теория массового обслуживания.

Исходные данные:

– количество узлов связи N ССОП;

– количество информационных направлений между элементами КСУ R_{ij};

– требуемая пропускная способность КСУ для обеспечения услуг связи $C_{\text{КСУ}}^{\text{Треб}}$;

– индекс центральности $\delta_{\text{ц}} \in [1,6]$ для каждого i-го узла из N.

Ограничения и допущения:

1. Структура и размерность анализируемой ССОП в территориальном смысле соответствует нормативам территориального размещения КСУ;

2. Анализируемые элементы ССОП относятся к одному провайдеру связи;

3. Оператор связи ССОП реализует маршрутизацию на основе принципа минимизации транзитных узлов связи на каждом информационном направлении, или на основании другого, но известного принципа;

4. Предполагаем, что вычислительные средства задействуют свой ресурс только на генерацию и передачу трафика.

Характеристика исходной ситуации

Заданы структура КСУ и требования к услугам связи, а также ССОП с данными о точках привязки узлов связи (УС) органов (элементов) КСУ к ССОП, пограничный узел, как исходный источник деструктивного воздействия, который генерирует трафик q, процентное соотношение I-ых узлов с неким вычислительным ресурсом и различным уровнем защищенности на имеющих избыточный вычислительный ресурс (рис. 1).

В рассматриваемом фрагменте ССОП используется коммутационное оборудование,

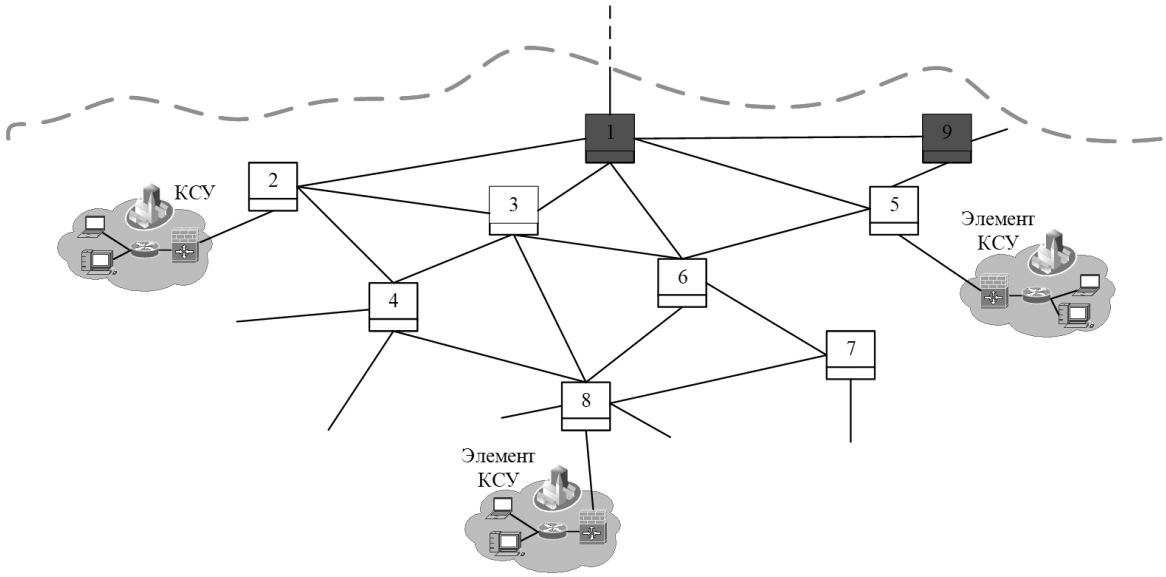

Рис. 1. Вариант графического представления фрагмента структуры ССОП с привязкой узлов КСУ

предназначенное для разделения/объединения потоков и их передачи от одного элемента сети к другому.

Пропускная способность линий связи обуславливается выбранной физической средой передачи данных. В качестве физической среды передачи данных используются различные виды кабелей: коаксиальный кабель, неэкранированная витая пара, экранированная витая пара, оптический кабель.

В исходной ситуации предположим, что пропускная способность линий связи в теории имеет бесконечную пропускную способность, а на практике эти значения достаточно велики, и предопределяются имеющимся набором средств связи.

Современные транспортные сети основаны на коммутации каналов и пакетов. Для создания линий связи (каналов) коммутаторы транспортных сетей поддерживают один из методов статистического мультиплексирования [7].

К настоящему времени сформировалось два поколения цифровых сетей:

– плезиохронная цифровая иерархия (ПЦИ);

– синхронная цифровая иерархия (СЦИ).

В табл. 1 приводятся значения уровней скоростей ПЦИ и СЦИ [8].

Методика синтеза информационно-телекоммуникационной системы, исключающей реализацию DDoS-атак на элементы корпоративной системы управления в течении заданного времени реализована в виде обобщенного алгоритма, представленного на рис. 2.

В блоке 1 задаем исходные данные:

– количество узлов связи N ССОП;

– количество информационных направлений между элементами КСУ R_{ij};

Таблица 1

Значение уровней скоростей ПЦИ и СЦИ

Плезиохронная цифровая иерархия			Синхронная цифровая иерархия		
уровень иерархии	количество каналов предыдущего уровня	скорость, Мбит/с	уровень иерархии	STN-N	скорость, Мбит/с
0	1	0,064	0	-	51,840
1	30	2,048	1	STM-1	155,520
2	4	8,448	2	STM-4	622,080
3	4	34,368	3	STM-16	2488,320
4	4	139,264	4	STM-64	9953,280

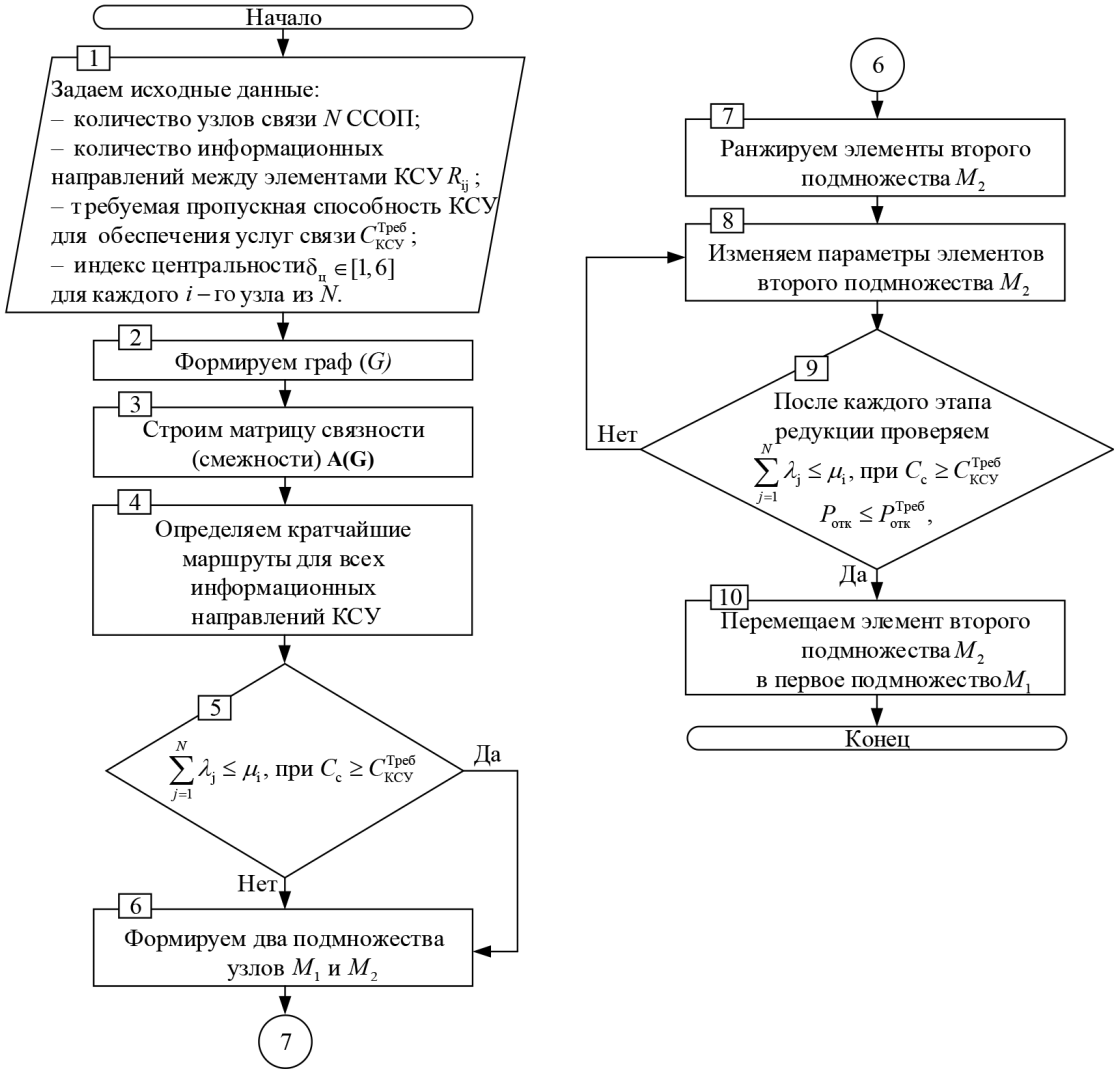

Рис. 2. Обобщенный алгоритм методики

– требуемая пропускная способность КСУ для обеспечения услуг связи $C_{КСУ}^{Треб}$;

– индекс центральности $\delta_ц \in [1,6]$ для каждого *i*-го узла из *N*.

В блоке 2 формируем граф $G = \{V_i, E_j\}$, с парой непустых множеств V_i вершин графа (узлов связи) и E_j ребер графа (линий связи), который отражает топологию и структуру ССОП.

В блоке 3 для графа $G = \{V_i, E_j\}$ строим матрицу связности (смежности) $\mathbf{A(G)} = \|\mathbf{a_{ij}}\|$, в которой

$$a_{ij} = \begin{cases} 1, \text{ если } G \text{ существует ребро } (V_i, V_j) \\ 0, \text{ если } G \text{ отсутствует ребро } (V_i, V_j) \end{cases}.$$

Следовательно, матрица связности (смежности) **A(G)**:

$$\mathbf{A(G)} = \begin{vmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{vmatrix}.$$

В блоке 4 определяем кратчайшие маршруты для всех информационных направлений КСУ.

Маршрут информационного направления — это путь, организованный между двумя или более конечными узлами сети в процессе организации каналов связи различного вида в целях взаимодействия пунктов управлений и обмена информацией в КСУ.

В теории графов задача определения кратчайших маршрутов является одной из составных и классических.

Наиболее известными алгоритмами определения кратчайших маршрутов в графах являются:

– алгоритм Дейкстры;

– алгоритм Беллмана-Форда;

– алгоритм поиска A*;

– алгоритм Флойда-Уоршелла;

– алгоритм Джонсона.

Осуществив анализ каждого из указанных алгоритмов [9], целесообразно использовать алгоритм Дейкстры — один из самых простых вариантов определения кратчайших маршрутов в графах.

Определение кратчайших путей каждого информационного направления осуществляется при помощи фиксации пути прохождения каждого *i*-го ИН через узлы фрагмента ССОП (рис. 3), путём запоминания всех узлов ССОП по нумерации в таблицу маршрутов информационных направлений КСУ (табл. 2).

В блоке 5 проверяем выполнение условия (1) для всех узлов, входящих в маршруты информационных направлений КСУ.

В блоке 6 по результатам проверки формируем два подмножества узлов $M_1 = \{2;8\}$ и $M_2 = \{3;6;5\}$. Для элементов первого подмножества M_1 условие (1) выполняется, а для элементов второго подмножества M_2 не выполняется.

В блоке 7 элементы второго подмножества M_2 ранжируем по степени невыполнения условия (1).

В блоке 8 последовательно для всех узлов сформированного вариационного ряда элементов второго подмножества M_2 дискретно, на заданную величину Δ снижаем исходные параметры пропускной способности линий связи этого узла, а при необходимости и степень его связ-

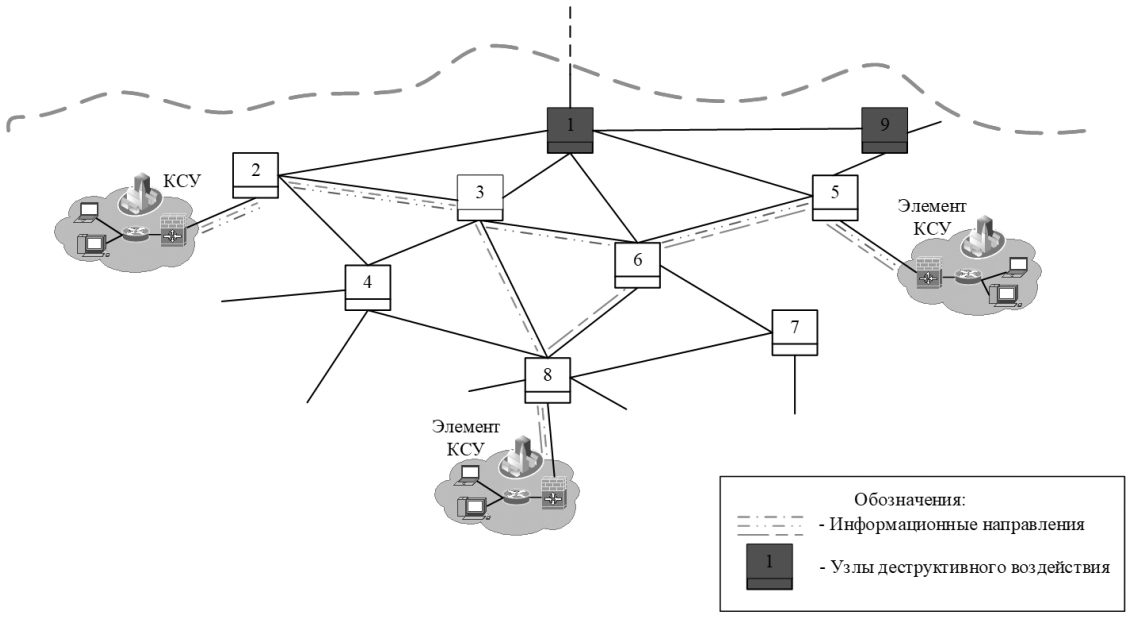

Рис. 3. Вариант формирования информационных направлений КСУ

Таблица 2

Маршруты ИН КСУ

Номер ИН КСУ	Маршрут ИН КСУ	Общие узлы ССОП
1	2, 3, 8	2, 3, 5, 6, 8
2	2, 3, 6, 5	
3	8, 6, 5	

ности с другими узлами, за исключением линий входящих в маршрут ИН КСУ.

В блоке 9 на каждом этапе редукции проверяем выполнение условий путем оценки. Каждое из ребер графа в теории массового обслуживания характеризуется интенсивностью потока λ_{ij}.

1. Поток заявок в сетях передачи данных классически описывают при помощи простейшего потока [10].

Простейший поток заявок представляет собой временную последовательность независимых случайных событий. Под событием понимается поступление вызова. Этот поток имеет три свойства:

– стационарность;

– ординарность;

– отсутствие последействия.

Стационарность потока — вероятность поступления k заявок за интервал времени τ зависит только от величины этого интервала и не зависит от того, где на оси времени он выбран.

Ординарность потока — вероятность поступления двух и более заявок за интервал времени, стремящийся к нулю, тоже стремится к нулю.

Отсутствие последействия — независимость настоящего от прошлого, т.е. процесс поступления заявок не зависит ни от процесса поступления до настоящего момента, ни от состояния системы обслуживания.

Для простейшего потока вероятность поступления k заявок за интервал времени t является случайной величиной, имеющей распределение Пуассона:

$$P_k = \frac{(\lambda t)^k}{k!} e^{-\lambda t},$$

где λ — интенсивность потока (заявок/ед. времени).

Интервалы времени между заявками в таком потоке также случайны и имеют экспоненциальное распределение вероятности:

$$F(x) = 1 - e^{-\lambda t}.$$

2. Процесс обслуживания. Обслуживающее устройство занимается заявкой в случайное время, которое имеет экспоненциальное распределение вероятности:

$$F(x) = 1 - e^{-\mu t},$$

где μ — интенсивность обслуживания (заявок/ед. времени).

Следовательно интенсивность нагрузки ρ:

$$\rho = \frac{\lambda}{\mu}.$$

Вероятность отказов в обслуживании определяем по формуле Эрланга:

$$P_{\text{отк}} = \frac{\frac{\rho^n}{n!}}{\sum_{n=0}^{n} \frac{\rho^n}{n!}}.$$

Сравниваем вероятность отказов с допустимой вероятностью отказов:

$$P_{\text{отк}} \le P_{\text{отк}}^{\text{Треб}}. \qquad (2)$$

При выполнении условий (1) и (2) перемещаем элемент второго подмножества M_2 в первое подмножество M_1 (блок 10). Если условия (1) и (2) не выполняются, то повторяем действия в блоке 8.

Процедура редукции завершается при исключении всех элементов из второго подмножества M_2.

Финальные параметры пропускной способности линий связи, степени связности на момент завершения процедуры редукции характеризуют сеть КСУ, на которой невозможно развить DDoS-атаки.

Выводы

В рамках статьи сформулирована и решена актуальная задача синтеза информационно-телекоммуникационной системы, в которой с помощью разработанной методики можно получить данные о параметрах сети корпоративной системы управления, обеспечивающих исключение возможности реализации DDoS-атак.

Литература

1. О связи. Федеральный закон РФ от 07.07.2003 № 126-ФЗ // Собрание законодательства Российской Федерации от 14 июля 2003 года ст. 18.

2. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирую-

щих воздействий и ведения разведки. — СПб: Наукоемкие технологии. 2020. 130 с.

3. Об информации, информационных технологиях и о защите информации. Федеральный закон РФ от 27.07.2006 № 149-ФЗ // Принят Государственной Думой от 08 июля 2006 г. Ст. 16.

4. Стародубцев Ю.И., Гречишников Е.В., Закалкин П.В., Добрышин М.М., Петухова Ю.А. Способ снижения ущерба, наносимого сетевыми атаками серверу виртуальной частной сети // Патент на изобретение RU 2685989, опубл. 23.04.2019. 15 с.

5. Гречишников Е.В., Добрышин М.М., Горелик С.П. Способ защиты элементов виртуальных частных сетей связи от DDOS-атак // Патент на изобретение RU 2636640, опубл. 27.11.2017. 16 с.

6. Гречишников Е.В., Белов А.С., Кузьмич А.А., Добрышин М.М., Исаченко В.Г. Способ оценки эффективности информационно-технических воздействий на сети связи // Патент на изобретение RU 2541205, опубл. 10.02.2015. 21 с.

7. Кутузов О.И. Инфокоммуникационные системы и сети. — СПб: Лань. 2020. 126 с.

8. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. — СПб: Питер. 2016. С. 265–269.

9. Изотова Т.Ю. Обзор алгоритмов поиска кратчайшего пути в графе // Академия ФСО России. Новые информационные технологии в автоматизированных системах. 2016. С. 341–344.

10. Давыдов А.Е., Смирнов П.И., Парамонов А.И. Проектирование телекоммуникационных систем и сетей. Раздел Коммутируемые сети связи. Расчет параметров сетей связи и анализ трафика. — СПб: Университет ИТМО. 2016. С. 14–15.

References

1. About communication. Federal Law of the Russian Federation of 07.07.2003 № 126-FZ // Sobranie zakonodatelstva Rossiyskoy Federatsii of July 14, 2003. Article 18.

2. Makarenko S.I. Models of the communication system in the conditions of deliberate destabilizing influences and conducting intelligence. — St. Petersburg: Science-intensive technologies. 2020. 130 p.

3. About information, information technologies and information protection. Federal Law of the Russian Federation № 149-FZ of 27.07.2006 // Adopted by the State Duma on July 08, 2006. Article 16.

4. Starodubtsev Yu.I., Grechishnikov E.V., Zakalkin P.V., Dobryshin M.M., Petukhova Yu.A. A method for reducing the damage caused by network attacks to a virtual private network server // Patent for the invention RU 2685989, publ. 23.04.2019. 15 p.

5. Grechishnikov E.V., Dobryshin M.M., Gorelik S.P. A method for protecting elements of virtual private communication networks from DDOS attacks // Patent for invention RU 2636640, publ. 27.11.2017. 16 p.

6. Grechishnikov E.V., Belov A.S., Kuzmich A.A., Dobryshin M.M., Isachenko V.G. A method for evaluating the effectiveness of information and technical impacts on communication networks // Patent for invention RU 2541205, publ. 10.02.2015. 21 p.

7. Kutuzov O.I. Infocommunication systems and networks. — St. Petersburg: Lan. 2020. 126 p.

8. Olifer V.G. Computer networks. Principles, technologies, protocols: Textbook for universities. 5th ed. — St. Petersburg: Piter. 2016. P. 265–269.

9. Izotova T.Yu. Review of algorithms for finding the shortest path in a graph // The Academy of the Federal security service of Russia. New information technologies in automated systems. 2016. P. 341–344.

10. Davydov A.E., Smirnov P.I., Paramonov A.I. Design of telecommunications systems and networks. The section Switched communication networks. Calculation of communication network parameters and traffic analysis. — St. Petersburg: ITMO University. 2016. P. 14–15.