УДК: 007 DOI: 10.53816/23061456_2021_11–12_116

МЕТОД РЕКОНФИГУРАЦИИ СЕТИ СВЯЗИ С УЧЕТОМ ОЦЕНКИ ИНФОРМИРОВАННОСТИ ИСТОЧНИКА ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ

COMMUNICATION NETWORK RECONFIGURATION METHOD TAKING INTO ACCOUNT INFORMATION AND TECHNICAL IMPACT SOURCE AWARENESS ASSESSMENT

Канд. техн. наук П.В. Закалкин

Ph.D. P.V. Zakalkin

ВАС им. С.М. Буденного

Распределенные корпоративные системы управления для своего функционирования вынуждены использовать ресурсы и услуги, предоставляемые киберпространством. Интеграция в киберпространство делает системы управления целью постоянных атак как одиночных хакеров и кибертеррористов, так и организованных хакерских сообществ. Информационно-технические воздействия на системы управления приводят к снижению качества и количества услуг, предоставляемых элементами корпоративной системы управления, переводит их в нестандартные режимы функционирования, а в крайних случаях приводит к полному отключению. Итоговым результатом воздействий является срыв управления, осуществляемого корпоративной системой управления. В статье рассматривается метод реконфигурации сети связи с учетом оценки информированности источника информационно-технических воздействий, осуществляемых посредством киберпространства. Предлагаемый метод позволяет обеспечить функционирование сети связи в условиях информационно-технических воздействий с учетом оценки информированности источника информационно-технических воздействий о структуре сети связи.

Ключевые слова: сеть связи, оценка информированности, реконфигурация, информационно-технические воздействия.

Distributed corporate management systems are forced to use the resources and services provided by cyberspace for their functioning. Integration into cyberspace makes management systems the target of constant attacks by both single hackers and cyberterrorists, as well as organized hacker communities. Information and technical impacts on management systems lead to a decrease in the quality and quantity of services provided by elements of the corporate management system, transfers them to non-standard modes of operation, and in extreme cases leads to a complete shutdown. The final result of the impacts is the disruption of management carried out by the corporate management system. The article considers the method of reconfiguration of the communication network, taking into account the assessment of the awareness of the source of information and technical impacts carried out through cyberspace. The proposed method makes it possible to ensure the functioning of the communication network in the conditions of information and technical impacts, taking into account the assessment of the awareness of the source of information and technical impacts about the structure of the communication network.

Keywords: communication network, awareness assessment, reconfiguration, information technology impacts.

Являясь сложным, высокотехнологичным, искусственно созданным пространством, киберпространство интегрировало в себя множество технологических процессов. Посредством киберпространства осуществляется управление процессами, реализованными в рамках объектов и субъектов критической инфраструктуры государства, в том числе банковской системой, логистическими процессами, энергетикой, водоснабжением, медициной, образованием и др. [1–3].

Таким образом, множество распределенных корпоративных систем управления (в том числе и антагонистических), включающих в себя множество элементов, вынуждены функционировать посредством использования ресурсов и услуг предоставляемых киберпространством. Интеграция в киберпространство делает эти системы целью постоянных атак как одиночных хакеров и кибертеррористов, так и организованных хакерских сообществ [4–5].

Срыв управления (или увеличения временного интервала, затрачиваемого на цикл управления), осуществляемого корпоративными системами управления (КСУ), возможен посредством осуществления информационно-технических воздействий (ИТВ) на элементы КСУ. Результатом ИТВ является снижение качества и количества предоставляемых элементом услуг, перевод в нестандартные режимы функционирования, а в крайних случаях и к полному его отключению. Соответственно, чем больше элементов КСУ будет подвергнуто ИТВ, тем с большей вероятностью будет нарушено управление всей системой. При этом успех достижения поставленных целей источником ИТВ напрямую зависит от степени его информированности о структуре КСУ, целевом предназначении каждого элемента и их иерархии в КСУ.

В статье под ИТВ понимается целенаправленное, использующее средства и возможности информационных и иных технологий, воздействие противоборствующей стороны на объекты критической информационной инфраструктуры, на автоматизированные системы управления, на образцы вооружения, военной и специальной техники, на процессы их функционирования и применения, нарушающее устойчивость их функционирования и их информационную, технологическую и промышленную безопасность, и приводящее к эскалации военных конфликтов, к возникновению чрезвычайных ситуаций, к нарушению государственного управления национальной обороной, безопасностью и правопорядком, к срыву выполнения военных задач вооруженными силами [6].

Рассмотрение известных подходов [7–11] в области обеспечения защиты КСУ от ИТВ показало, что построение защиты элементов КСУ осуществляется поэлементно. Элементы системы защищаются организационными (организация пропускного режима и т.д.), организационно-техническими мерами, программными и программно-аппаратными средствами (межсетевые экраны, системы обнаружения атак, средства анализа уязвимостей и т.д.). Реализация данных мер на всех элементах КСУ позволяет получить защищенный набор элементов КСУ, и таким образом, КСУ в целом считается защищенной. При этом не учитывается степень информированности источника ИТВ о структуре атакуемой сети связи, что не позволяет обеспечить последовательную и обоснованную реконфигурацию сети связи в случае вскрытия ее структуры противником.

Предлагаемый метод предназначен для сотрудников, обеспечивающих функционирование распределенных КСУ, использующих ресурсы киберпространства.

Исходными данными предлагаемого метода являются:

– $t_{\text{функц}}$ — время, в течение которого осуществляется функционирование сети связи;

– $\overline{t}_{\text{рек}}$ — среднее время, необходимое для реконфигурации сети;

– N_g — набор значений параметров качества предоставляемых услуг связи;

– Δ_g — набор значений допустимого отклонения параметров качества предоставляемых услуг связи;

– $K_{\text{кор}}^{porog}$ — пороговое значение коэффициента корреляции между вариационными рядами K_j^{vazn} и K_{ij}^{vozd};

– K^{uslug} — коэффициент важности предоставляемой услуги связи. Задается в диапазоне от 0 до 1;

– $t_{\text{интервал}}$ — интервал времени, через который рассчитывается весовой коэффициент воздействия K_{ij}^{vozd} для каждого узла сети связи;

– K_j^{vazn} — весовой коэффициент важности элемента сети связи. Весовой коэффициент может находиться в диапазоне значений от «0» до

«1». Нулевое значение принимается при полном отсутствии на узле направлений связи и цифрового потока информации, а значение равное единице отражает максимальное количество направлений связи и цифрового потока информации. Весовой коэффициент задается исходя из количества связей (направлений) элемента сети связи и обрабатываемого им цифрового потока информации;

– площадь реального фрагмента сети связи произвольной формы выбранного региона;

– количество информационно взаимосвязанных абонентов и структуру информационных направлений между ними;

– базу данных для хранения вариантов маршрутизации;

– требуемые значения допустимых интервалов взаимного удаления между информационно взаимосвязанными абонентами;

– характеристики узлов и линий связи сети связи;

– количественный состав и характеристики резерва сил и средств связи.

Обобщенная структурно-логическая последовательность предлагаемого метода представлена на рисунке.

На основе определенных в исходных данных количествах информационно-взаимосвязанных абонентов и структуры информационных направлений между ними осуществляется формирование и ранжирование вариантов маршрутизации.

Сформированные варианты маршрутизации ранжируются согласно значений весового коэффициента важности элементов сети связи, входящих в данный вариант маршрутизации. При ранжировании элементом с наивысшим рангом будет вариант маршрутизации, содержащий наибольшее количество максимально близких друг к другу (на минимальном уровне) значений весового коэффициента важности элементов сети связи.

Под вариантами маршрутизации будем понимать набор маршрутов передачи данных между абонентами, сформированных с учетом структуры информационных направлений между ними.

Каждому варианту маршрутизации (m) в порядке возрастания присваивается номер. Значения диапазона номеров лежат в пределе от 1 до M, где M — общее количество отранжированных вариантов маршрутизации.

На следующем этапе выбирают первый вариант маршрутизации из набора отранжированных вариантов и осуществляют формирование множества маршрутов между информационно взаимосвязанными абонентами в соответствии с выбранным вариантом маршрутизации. После чего в маршрутно-адресную таблицу заносят данные о сформированных маршрутах для каждого информационного направления, а в базу данных заносят остальные варианты маршрутизации.

Выбранный вариант маршрутизации является основой для построения вариационного ряда элементов сети связи согласно весового коэффициента важности ее элементов. После чего все члены построенного вариационного ряда нормируются относительно старшего члена (максимального K^{vazn}).

Параллельно с этим, в процессе функционирования сети осуществляется постоянный мониторинг информационно-технических воздействий на сеть и измерение параметров качества предоставления услуг.

Обнаружение ИТВ осуществляется с помощью системы обнаружения вторжений. Контроль качества предоставляемых услуг связи описан в [12]. Помимо этого, оценку качества услуг связи возможно осуществлять с помощью универсальных измерительных зондов [13].

В процессе функционирования сети через заданный интервал времени $t_{\text{интервал}}$ для каждого узла сети связи рассчитывают весовой коэффициент воздействия K^{vozd}.

Осуществляемые на узел связи ИТВ оказывают влияние на количество и показатели качества услуг связи, предоставляемых узлом. Если набор значений параметров качества предоставляемой услуги связи (N_g) выходит за заданные пределы допустимого отклонения параметров качества (Δ_g), то данная услуга считается не предоставленной и при расчете весового коэффициента воздействия ИТВ K^{vozd} не учитывается. Также не учитываются услуги, предоставление которых в результате ИТВ было остановлено.

Весовой коэффициент воздействия ИТВ K^{vozd} рассчитывают следующим образом:

$$K_{ij}^{vozd} = 1 - \frac{\sum_{x=1}^{X} f_x \cdot K_x^{uslug}}{\sum_{i=1}^{I} f_i \cdot K_i^{uslug}},$$

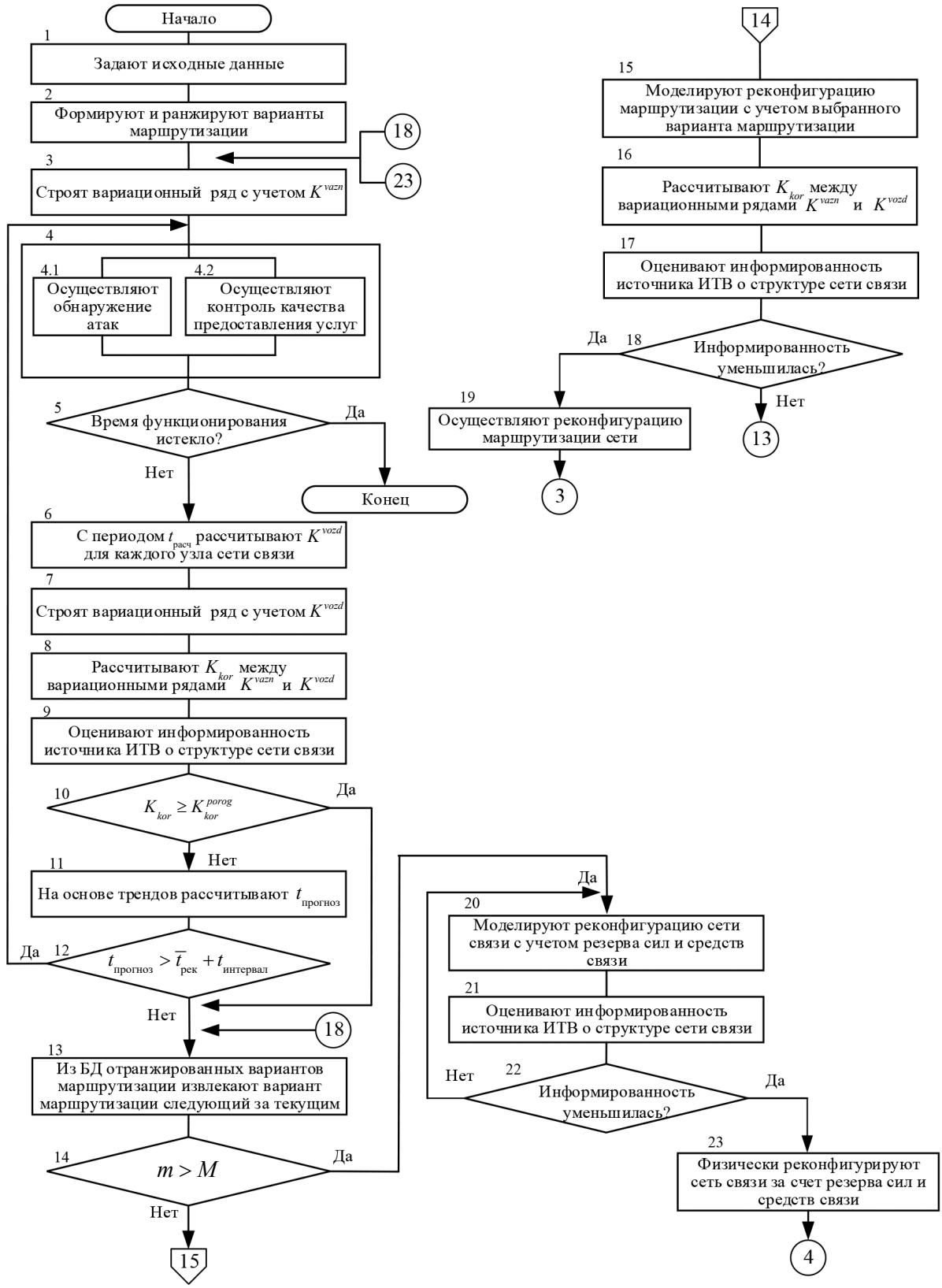

Рис. Обобщенная структурно-логическая последовательность метода предварительной целенаправленной реконфигурации сети связи с учетом оценки информированности источника информационно-технических воздействий о структуре сети связи

где K^{uslug} — весовой коэффициент *i*-го ИТВ на *j*-ый узел сети связи;

f — услуга, предоставляемая узлом сети связи;

X — количество услуг, предоставляемых узлом связи после осуществления в отношении него информационно-технического воздействия;

I — общее количество услуг, предоставляемых узлом связи;

K^{uslug} — коэффициент важности предоставляемой услуги связи. Задается в исходных данных в диапазоне от 0 до 1.

На основе рассчитанных данных строят и запоминают вариационный ряд элементов сети связи по весовому коэффициенту ИТВ на узел сети связи. После построения вариационного ряда нормируют все его члены относительно старшего члена (максимального K_j^{vozd}).

После чего извлекают из памяти вариационный ряд элементов сети связи по весовому коэффициенту ИТВ на узел сети связи и рассчитывают коэффициент корреляции (K_{kor}) между вариационными рядами K^{vazn} и K^{vozd}. Рассчитанные значения позволяют оценить информированность источника ИТВ о структуре системы связи.

Оценка информированности (блок 9) осуществляется по шкале от 0 до 1, т.к. значение K_{kor} находится в диапазоне от 0 до 1, и данный коэффициент показывает фактическую информированность источника ИТВ о структуре системы связи. При этом значение «0» показывает, что источник ИТВ не имеет данных о структуре системы связи; значение «1» соответствует полному совпадению распределения ИТВ по узлам сети связи, согласно весового коэффициента информационно-технического воздействия K^{vozd} и весового коэффициента важности элементов сети связи K^{vazn}. Таким образом, источник ИТВ имеет полные данные о структуре системы связи.

Если полученный коэффициент корреляции больше или равен пороговому значению, то увеличивают значение счетчика *m* на «1», в противном случае на основе трендов прогнозируют время ($t_{\text{прогноз}}$) через которое значение $K_{kor} \geq K_{kor}^{porog}$.

Спрогнозированное значение $t_{\text{прогноз}}$ должно превышать сумму среднего времени, затрачиваемого на реконфигурацию сети, и интервала времени, через который осуществляется расчет весового коэффициента воздействия для каждого узла сети связи. Выполнение данного условия необходимо для того, чтобы на следующем цикле хватило времени на расчет осуществление реконфигурации. В случае выполнения условия $t_{\text{прогноз}} > \overline{t}_{\text{рек}} + t_{\text{интервал}}$ из базы данных отранжированных вариантов маршрутизации извлекают вариант маршрутизации, следующий за текущим. Выбор следующего варианта маршрутизации осуществляется путем увеличения значения текущего варианта маршрутизации *m* на «1».

В случае невыполнения условия $t_{\text{прогноз}} > \overline{t}_{\text{рек}} + t_{\text{интервал}}$ продолжается обычное функционирование сети с осуществлением постоянного мониторинга ИТВ на сеть и измерением параметров качества предоставления услуг.

В следующем блоке осуществляют проверку выполнения условия $m > M$. Данное условие осуществляет проверку рассмотрения всех вариантов маршрутизации, отранжированных в блоке 2. Если все варианты маршрутизации уже рассмотрены, то переходят к блоку 20, в противном случае моделируют реконфигурацию маршрутизации с учетом выбранного варианта маршрутизации.

Моделирование реконфигурации маршрутизации заключается в моделировании изменения маршрутов потоков данных в сети.

После чего рассчитывают коэффициент корреляции (K_{kor}) между вариационными рядами K^{vazn} и K^{vozd} и оценивают информированность источника информационно-технических воздействий о структуре системы связи. Оценка информированности источника информационно-технических воздействий осуществляется по аналогии описанной в блоке 9. Затем осуществляют сравнение фактической информированности источника ИТВ и информированности источника ИТВ, полученной в результате моделирования.

Если информированность, полученная в результате моделирования, меньше фактической, то переходят к блоку 13 и из базы данных отранжированных вариантов маршрутизации извлекают (выбирают) вариант маршрутизации, следующий за текущим.

Если информированность, полученная в результате моделирования больше фактической, то осуществляют реконфигурацию маршрутизации

сети. Реконфигурация маршрутизации заключается в изменении маршрутов потоков данных в сети.

Затем моделируют физическую реконфигурацию сети связи с учетом резерва сил и средств связи. Моделирование осуществляется с учетом количества и качества предоставляемых услуг связи, изменения географических координат абонентов и узлов их привязки к сети связи, изменении режимов работы сети связи (введении резервных каналов (линий) и средств связи.

Основываясь на результатах моделирования, оценивают информированность источника информационно-технических воздействий о структуре системы связи. Оценка информированности источника информационно-технических воздействий осуществляется по аналогии, описанной в блоке 9.

После чего осуществляют сравнение фактической информированности источника информационно-технических воздействий и информированности источника информационно-технических воздействий, полученной в результате моделирования.

Если информированность, полученная в результате моделирования, больше фактической, то переходят к блоку 20, в противном случае, с учетом топологического размещения абонентов, физически реконфигурируют сеть связи за счет резерва сил и средств связи.

Реконфигурация системы связи заключается в изменении режимов работы сети связи, введении резервных каналов (линий) и средств связи, изменении географических координат абонентов и узлов их привязки к сети связи за счет резерва сил и средств связи.

Вывод

Предлагаемый метод реконфигурации сети связи с учетом оценки информированности источника информационно-технических воздействий о структуре сети связи обеспечивает функционирование сети связи в условиях информационно-технических воздействий, за счет последовательной и обоснованной реконфигурации сети связи и оценки информированности источника информационно-технических воздействий о структуре сети связи.

Литература

1. Стародубцев Ю.И., Закалкин П.В., Иванов С.А., Добрышин М.М. Способ защиты серверов услуг сети связи от компьютерных атак // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2020. № 9–10 (147–148). С. 63–67.

2. Стародубцев Ю.И., Закалкин П.В., Иванов С.А., Вершенник Е.В. Способ создания резервной копии объекта // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2021. № 5–6 (155–156). С. 28–35.

3. Коцыняк М.А., Лаута О.С., Иванов Д.А., Лукина О.М. Модель воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2019. № 3–4 (129–130). С. 58–65.

4. Топ угроз ИБ в корпоративных сетях. Результаты мониторинга сетевого трафика в 2020 году // Positive Technologies. 2021. 9 с.

5. Кибербезопасность 2020–2021. Тренды и прогнозы // Positive Technologies. 2021. 25 с.

6. Забегалин Е.В. К вопросу об определении термина «информационно техническое воздействие» // Системы управления, связи и безопасности. 2018. С. 121–149

7. Анисимов В.В., Бегаев А.Н., Стародубцев Ю.И. Модель функционирования сети связи с неизвестным уровнем доверия и оценки ее возможностей по предоставлению услуги VPN с заданным качеством // Вопросы кибербезопасности. 2017. № 1 (19). С. 6–15.

8. Добрышин М.М. Предложение по совершенствованию систем противодействия DDoS-атакам // Телекоммуникации. 2018. № 10. С. 32–38.

9. Grechishnikov E.V., Dobryshin M.M., Kochedykov S.S., Novoselcev V.I. Algorithmic model of functioning of the system to detect and counter cyber attacks on virtual private network // Journal of Physics: Conference Series. International Conference «Applied Mathematics, Computational Science and Mechanics: Current Problems». AMCSM 2018. 2019. P. 012064.

10. Сидоренко Е.Н., Стародубцев Ю.И., Сухорукова Е.В., Фёдоров В.Г. Способ защиты информационно-телекоммуникационных сетей специального назначения от сетевых компьютерных

атак // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей: в 3-х томах. 2016. С. 333–337.

11. Патент № 2690213 Российская Федерация, G06N 5/00, H04W 16/22. Способ моделирования оптимального варианта топологического размещения множества информационно взаимосвязанных абонентов на заданном фрагменте сети связи общего пользования / Вершенник А.В., Вершенник Е.В., Латушко Н.А., Стародубцев Ю.И.; заявитель и патентообладатель Латушко Н.А., Стародубцев Ю.И. – 2018118104; заявл. 16.05.2018; опубл 31.05.2019. бюлл. № 16. 17 с.

12. Ваняшин С.В. Контроль качества предоставления услуг (SLA) в сетях IP/MPLS // Федеральное агентство связи. ФГБОУВПО «Поволжский государственный университет телекоммуникаций и информатики». — Самара. 2017.

13. Добрышин М.М., Закалкин П.В., Кузмич А.А. Система определения причин отказа в обслуживании в условиях эксплуатационных отказов и информационно-технических воздействий // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2020. № 7–8 (145–146). С. 38–43.

References

1. Starodubtsev Yu.I., Zakalkin P.V., Ivanov S.A., Dobryshin M.M. Method of protecting communication network services servers from computer attacks // Voprosy oboronnoi tekhniki. Seriia 16. Tekhnicheskie sredstva protivodestviia terrorizmu. 2020. № 9–10 (147–148). P. 63–67.

2. Starodubtsev Yu.I., Zakalkin P.V., Ivanov S.A., Vershennik E.V. Method of creating a backup copy of the object // Voprosy oboronnoi tekhniki. Seriia 16. Tekhnicheskie sredstva protivodestviia terrorizmu. 2021. № 5–6 (155–156). P. 28–35.

3. Kotsynyak M.A., Lauta O.S., Ivanov D.A., Lukina O.M. Model of impact of targeted cyber attack on information and telecommunication network // Voprosy oboronnoi tekhniki. Seriia 16. Tekhnicheskie sredstva protivodestviia terrorizmu. 2019. № 3–4 (129–130). P. 58–65.

4. Top IB threats in corporate networks. Results of network traffic monitoring in 2020 // Positive Technologies. 2021. 9 p.

5. Cybersecurity 2020–2021. Trends and forecasts // Positive Technologies. 2021. 25 p.

6. Zabegalin E.V. On the definition of the term «information technology impact» // Management, communication and security systems. 2018. P. 121–149.

7. Anisimov V.V., Begaev A.N., Starodubtsev Yu.I. Model of communication network functioning with unknown level of trust and assessment of its capabilities to provide VPN service with specified quality // Cybersecurity issues. 2017. № 1 (19). P. 6–15.

8. Dobryshin M.M. Proposal for improvement of DDoS attack control systems // Telecommunications. 2018. № 10. P. 32–38.

9. Grechishnikov E.V., Dobryshin M.M., Kochedykov S.S., Novoselcev V.I. Algorithmic model of functioning of the system to detect and counter cyber attacks on virtual private network // В сборнике: Journal of Physics: Conference Series. International Conference «Applied Mathematics, Computational Science and Mechanics: Current Problems». AMCSM 2018. 2019. P. 012064.

10. Sidorenko E.N., Starodubtsev Yu.I., Sukhorukova E.V., Fedorov V.G. A way to protect special-purpose information and telecommunications networks from network computer attacks // In the collection: Current problems of information and telecommunications communications in science and education. Collection of scientific articles: in 3 volumes. 2016. P. 333–337.

11. Patent № 2690213 Russian Federation, G06N 5/00, H04W 16/22. A method of modeling an optimal version of topological placement of a plurality of information-related subscribers on a given fragment of a public communication network // Vershennik A.V., Vershennik E.V., Latushko N.A., Starodubtsev Yu.I.; applicant and patent holder Latushko N.A., Starodubtsev Yu.I. – 2018118104; declared. 16.05.2018; publ 31.05.2019. Bull. № 16. 17 p.

12. S.V. Vanyashin. Training manual. Quality of Service Quality Control (SLA) in IP/MPLS // Federal Communications Agency. FSBUVPO «Volga State University of Telecommunications and Informatics». — Samara. 2017.

13. Dobryshin M.M., Zakalkin P.V., Kuzmich A.A. System for determining the causes of denial of service in conditions of operational failures and information and technical impacts // Voprosy oboronnoi tekhniki. Seriia 16. Tekhnicheskie sredstva protivodestviia terrorizmu. 2020. № 7–8 (145–146). P. 38–43.