УДК 004.056.2

Программа визуализации результатов оценки и анализа качества функционирования IP-сети в условиях воздействия кибератак

А. А. Привалов[3], Д. Д. Титов[1,2], А. И. Толстихин[2]

[1] Петербургский государственный университет путей сообщения Императора Александра I, Россия, 190031, Санкт-Петербург, Московский пр., 9

[2] ОАО «Супертел», Россия, 197101, Санкт-Петербург, Петроградская наб., 38А

[3] Академия войск национальной гвардии, Россия, 198206, Санкт-Петербург, ул. Летчика Пилютова, 1

Для цитирования: *Привалов А. А.*, *Титов Д. Д., Толстихин А. И.* Программа визуализации результатов оценки и анализа качества функционирования IP-сети в условиях воздействия кибератак // Известия Петербургского университета путей сообщения. СПб.: ПГУПС, 2024. Т. 21, вып. 4. С. 973–980. DOI: 10.20295/1815-588X-2024-04-973-980

Аннотация

Цель: разработка программного обеспечения, которое способно визуализировать работу телефонной IP-сети в условиях кибератак, используя предложенную в научной статье математическую модель. Программа должна обеспечивать глубокий анализ воздействия атак на производительность сети, а также предоставлять результаты в удобной для интерпретации графической форме. **Методы:** для достижения целей использовались методы математического анализа. Основные математические модели включают уравнения для расчета распределения воздействия, времени восстановления и других параметров сети. Программа применяет численное интегрирование и дифференцирование для расчета распределения времени обслуживания. Программа использует гамма-распределение для расчета функции доведения пакетов с данными с заданным качеством. В качестве функций распределения случайных параметров потоков данных использовались распределения Пуассона, Вейбулла и Парето. **Результаты:** программа позволяет моделировать различные сценарии кибератак и их воздействие на основные показатели сети, анализировать такие характеристики, как время доведения, вероятность потери пакетов и устойчивость сети. Результаты анализа показывают, как различные виды воздействий и параметры восстановления влияют на функционирование сети, что позволяет оператору оценить эффективность различных методов защиты и повреждений. **Практическая инновационность:** результаты, полученные в ходе технологического моделирования, могут быть использованы для повышения устойчивости и надежности телекоммуникационных систем, особенно тех, которые работают на оборудовании ОАО «Супертел». Программа предоставляет операторам инструмент для анализа состояния сети, разработки превентивных мер и оптимизации стратегий восстановления после удара. Она также может быть интегрирована в систему поддержки принятия решений и использоваться для выявления случаев несанкционированного доступа.

Ключевые слова: кибератака, IP-сеть, математическое моделирование, функции распределения, счетное интегрирование устойчивости сети, оборудование ОАО «Супертел»

Введение

В современном мире к системам цифровой связи предъявляются высокие требования по таким параметрам, как скорость передачи данных, надежность доведения информации и устойчивость к кибератакам. Телефонные IP-сети, используемые для передачи голосовых,

видео и текстовых данных, особенно подвержены угрозам, таким как DDoS-атаки на доступность сервисов и другие виды кибератак. Эффективная защита и восстановление таких сетей требуют использования сложных математических моделей и инструментов для анализа и визуализации киберугроз [1, 2, 3].

Разработанная часть программного обеспечения предоставляет возможность сымитировать работу телефонной IP-сети, функционирующей на оборудовании компании ОАО «Супертел», в условиях кибератак. Оборудование компании ОАО «Супертел» является основой многих телекоммуникационных систем, и его широкое использование делает критически важными понимание и оценку последствий кибератак на такие сети [4, 6, 8].

Модель, предложенная в статье Evaluating the Functioning Quality of Data Transmission Networks in the Context of Cyberattacks, представляет собой мощный инструмент для оценки качества функционирования сетей передачи данных в условиях внешних угроз. Используя основные параметры модели, такие как среднее время восстановления сети после атаки (t_AvRes), интенсивность атак (Y_attack1, Y_attack2) и дисперсия времени реализации атак (DD_r1, DD_r2), можно построить точную картину воздействия атак на IP-сети. Однако для практического использования этих данных необходимо создать удобные и понятные инструменты для визуализации, которые позволят операторам сетей и аналитикам быстро и эффективно принимать решения по повышению устойчивости сети [5, 7, 8, 11, 13].

В данной статье описывается фрагмент программного обеспечения АРМ должностного лица дирекции связи, который имитирует процесс функционирования IP-сети в условиях кибератак. Этот фрагмент позволяет оценить устойчивость сети, проанализировать влияние различных типов атак и разработать стратегии по их предотвращению и устранению. Использование этого инструмента также полезно для исследования и анализа качества функционирования IP-сетей, построенных на оборудовании ОАО «Супертел», что позволяет более эффективно проводить тестирование и повышать общую надежность сети.

Актуальность и значимость исследования

С увеличением объема передаваемых данных и числа подключенных устройств телефонные IP-сети становятся все более сложными и уязвимыми для различных угроз. В связи с этим возрастает необходимость использования современных инструментов для анализа и защиты таких сетей от кибератак. Телефонные IP-сети, построенные на оборудовании ОАО «Супертел», широко распространены в России, обеспечивая связь для различных организаций, включая государственные структуры и крупные предприятия.

Исследования, подобные работе Evaluating the Functioning Quality of Data Transmission Networks in the Context of Cyberattacks, показывают важность глубокого анализа параметров сети в условиях атак. Модель, предложенная в этой статье, позволяет оценивать, как различные виды атак влияют на задержки в сети, потери данных, восстановление после сбоев и другие важные параметры. Однако для эффективного применения этих знаний на практике требуется удобный инструмент для анализа и визуализации данных, который сможет учитывать все особенности конкретной сети и предоставлять результаты в удобной форме.

Разработка такого инструмента и его интеграция в системы мониторинга и управления сетью позволяют значительно повысить устойчивость и надежность IP-сетей. Это особенно важно для сетей, работающих на оборудовании

ОАО «Супертел», которое используется для обеспечения связи в критически важных инфраструктурах. Таким образом, предложенное программное обеспечение может стать ключевым элементом в стратегии защиты и восстановления сетей от кибератак.

Математическая модель и основные расчеты

Математическая модель, используемая в разработанном программном обеспечении, основана на анализе вероятностных характеристик работы сети в условиях кибератак. Основные параметры, которые учитываются в модели, включают [8, 9, 10, 11, 12, 13, 14]:

• **Среднее время восстановления после кибератаки (t_AvRes).** Этот параметр показывает, как быстро сеть способна вернуться к нормальному состоянию после того, как была подвергнута атаке.

• **Вероятность успешной реализации атак (P_r1 и P_r2).** Эти параметры определяют, какова вероятность того, что атака определенного типа будет успешно проведена и нанесет ущерб сети.

• **Дисперсия времени реализации атак (DD_r1 и DD_r2).** Эти параметры важны для понимания того, насколько варьируется время, необходимое для реализации атаки, что может влиять на стратегию защиты сети.

Описание разработанного программного обеспечения

Программное обеспечение, разработанное на основе данной модели, предназначено для проведения анализа и визуализации работы телефонной IP-сети в условиях кибератак. Оно было создано с использованием языка программирования Python, что обеспечивает гибкость и широкие возможности для его расширения и модификации в будущем.

Программа включает следующие основные модули:

1. *Модуль ввода данных.* Пользователь вводит основные параметры сети, такие как средняя скорость передачи данных (U), количество узлов на маршруте (N), общий объем памяти (K_total), а также параметры, связанные с атаками и восстановлением сети: интенсивность атак (Y_attack1, Y_attack2) и коэффициент восстановления сети (k).

2. *Модуль расчетов.* На основе введенных данных программа производит расчеты основных характеристик сети, используя предложенные в модели формулы. Программа рассчитывает такие параметры, как вероятность потери данных на маршруте, время доведения, интенсивность поступления, интенсивность обслуживания и другие.

3. *Модуль визуализации.* Программа строит графики и диаграммы, показывающие влияние кибератак на работу сети. Например, на графике может быть отображено изменение вероятности успешной атаки в зависимости от времени или количество потерянных пакетов данных в сети.

Пример использования программы можно рассмотреть на типичном сценарии атаки на сеть. Пусть, например, сеть подвергается атаке первого типа с вероятностью успешной реализации P_r1 = 0,5, а также атаке второго типа с вероятностью P_r2 = 0,5. При этом среднее время восстановления после атаки t_AvRes = 5,6 с, а среднее время реализации атак t_R1 = 300 с и t_R2 = 400 с соответственно. Вводя эти данные в программу, оператор может получить графическое отображение того, как изменяются ключевые параметры сети во времени, что позволяет понять, насколько критично воздействие каждой из атак и какие меры по восстановлению необходимо предпринять в первую очередь (рис. 1).

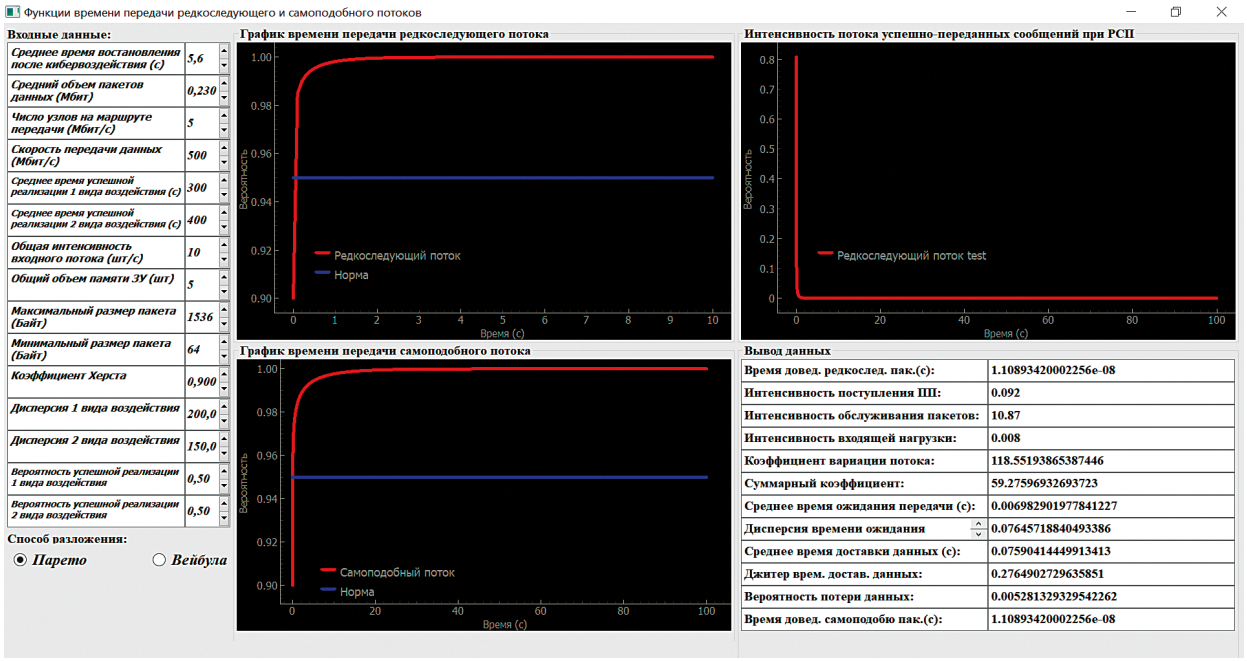

Рис. 1. Окно приложения, отображающее ключевые параметры телефонной IP-сети при воздействии на нее

Применение разработанного ПО

Программное обеспечение, описанное в данной статье, предназначено для применения в различных сценариях мониторинга и управления телефонными IP-сетями. Одним из ключевых его применений является тестирование устойчивости сетей в условиях имитации различных кибератак.

Сценарий 1. Тестирование сети в условиях DDoS-атаки

Представим, что сеть, работающая на оборудовании ОАО «Супертел», подвергается DDoS-атаке. В этом сценарии атака направлена на истощение ресурсов сети путем отправки большого объема трафика. Используя разработанное ПО, оператор может ввести параметры атаки, такие как интенсивность трафика и вероятность успешной реализации атаки, и увидеть, как изменяются ключевые показатели сети — задержка, потери пакетов и вероятность восстановления.

Программа позволяет визуализировать изменение этих параметров во времени, что дает оператору возможность оценить, насколько критично воздействие атаки и каковы возможности сети по восстановлению.

Сценарий 2. Анализ устойчивости сети к комплексным атакам

В данном сценарии сеть подвергается одновременно нескольким видам атак — DDoS и атаке на доступность сервисов. Программа позволяет учитывать влияние каждой атаки отдельно, а также анализировать их совокупное воздействие на сеть. Это особенно важно для сетей, которые обслуживают критически важные объекты, где даже небольшие сбои могут привести к серьезным последствиям.

Оператор может использовать ПО для определения слабых мест в сети и разработки стратегии защиты, включая установку дополнительных узлов или изменение маршрутизации трафика.

Сценарий 3. Оптимизация восстановления сети

В этом сценарии программа используется для анализа эффективности различных стратегий восстановления сети после атаки. Например, можно сравнить, как изменяется время восстановления в зависимости от увеличения ресурсов на восстановление или применения различных методов защиты.

Программа предоставляет визуализацию этих изменений, что позволяет операторам принимать обоснованные решения и выбирать наиболее эффективные стратегии восстановления.

Влияние на телекоммуникационные системы и оборудование

Программное обеспечение, описанное в данной статье, имеет большое значение для телекоммуникационных систем, работающих на оборудовании ОАО «Супертел». Использование этой программы позволяет операторам таких систем не только оценивать текущее состояние сети, но и прогнозировать возможные проблемы, что особенно важно в условиях увеличивающегося числа кибератак.

Например, в системах, обслуживающих крупные предприятия или государственные организации, использование этого ПО позволит значительно снизить риски, связанные с потерей данных или отказом системы в результате атаки. Визуализация работы сети в условиях атак дает возможность не только оперативно реагировать на инциденты, но и разрабатывать превентивные меры, повышающие общую устойчивость сети.

Заключение

Разработка программного обеспечения для визуализации работы телефонной IP-сети в условиях кибератак представляет собой важный шаг в обеспечении устойчивости и надежности современных телекоммуникационных систем. Используя математическую модель, описанную в статье Evaluating the Functioning Quality of Data Transmission Networks in the Context of Cyberattacks, данное ПО позволяет наглядно представить последствия различных видов атак и принять меры по их предотвращению.

Для сетей, построенных на оборудовании ОАО «Супертел», использование этого ПО особенно актуально, так как оно позволяет повысить надежность и устойчивость сети, минимизировать риски и обеспечить бесперебойную работу в условиях увеличивающегося числа киберугроз.

Дальнейшее развитие данной программы может включать в себя расширение функционала для учета новых типов атак, интеграцию с системами автоматического мониторинга и управления сетью, а также разработку методов прогнозирования атак на основе машинного обучения.

Библиографический список

1. Шелухин О. И. Причины самоподобия телетрафика и методы оценки показателя Херста // Электротехнические и информационные комплексы и системы. 2007. Т. 3. № 1. С. 5–14.

2. Математическая GERT-модель технологии передачи метаданных в облачные антивирусные системы / В. В. Босько [и др.] // Системи обробки інформації: збірник наукових праць. Харьков: ХУПС, 2014. Вып. 1(117). С. 137–141.

3. Привалов А. А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ. СПб.: ВМА, 2000. 166 с.

4. Привалов А. А., Куделя В. Н. Методы математического моделирования систем и процессов связи. СПб.: Изд-во Политехн. ун-та, 2009. 368 с.

5. Назаров А. Н., Сычев К. И. Модели и методы расчета показателей качества функционирования

узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. 2-е изд., доп. и перераб. Красноярск: Поликом, 2011. 491 с.

6. Кучерявый А. Е., Цуприков А. Л. Сети связи следующего поколения. М.: ФГУП ЦНИИС, 2006. 278 с.

7. Назаров А. Н., Сычев К. И. Модели и методы исследования процессов функционирования узлов коммутации сетей связи следующего поколения при произвольных распределениях поступления и обслуживания заявок различных классов качества // Телекоммуникации и транспорт. 2012. № 7. С. 135–140.

8. Структура транспортной сети связи ОАО «РЖД» и возникновение фазового перехода / А. О. Кравцов [и др.] // ELTRANS 10.0 (Элтранс-2019): материалы X Международного симпозиума «Элтранс-2019» (Eltrans-2019), посвященного 210-летию со дня основания первого транспортного вуза России — Петербургского государственного университета путей сообщения Императора Александра I (Санкт-Петербург, 9–11 октября 2019 года). СПб.: ИПК «НП-Принт», 2023. С. 190–196. EDN VYEFGL

9. Привалов А. А., Титов Д. Д. Метод оценки качества функционирования IP-сетей при передачи приоритетного многопродуктового потока данных в условиях кибератак // Материалы межвузовской научно-практической конференции «Современное состояние безопасности на транспорте и перспективы ее совершенствования» (Санкт-Петербург, Петергоф, 20 апреля 2022 года). СПб.: Военный институт (инженерно-технический), 2022. С. 72–86. EDN GNPBCV

10. Привалов А. А., Титов Д. Д. Модель процесса работы узла коммутации технологической IP-сети при обслуживании приоритетного многопродуктового потока в условиях DDOS-атак нарушителя // Фундаментальные и прикладные научные исследования: сборник трудов по материалам X Международного конкурса научно-исследовательских работ (Уфа, 5 декабря 2022 года). Уфа: Вестник науки, 2022. С. 92–104. EDN JUCSGZ

11. Привалов А. А., Титов Д. Д. Модель процесса передачи приоритетного многопродуктового потока по каналу телефонной IP-сети в условиях компьютерных атак нарушителя // Инновационные научные исследования в современном мире: сборник трудов по материалам X Всероссийского конкурса научно-исследовательских работ (Уфа, 28 ноября 2022 года). Ч. 1. Уфа: Вестник науки, 2022. С. 63–73. EDN DYCEIY

12. Привалов А. А., Лукичева В. Л., Титов Д. Д. Модель процесса функционирования узла коммутации технологической сети передачи данных в условиях DDOS атак нарушителя // Информация и космос. 2021. № 2. С. 66–75. EDN FQPOKK

13. Привалов А. А., Лукичева В. Л., Титов Д. Д. Модель процесса доставки пакетов по каналу передачи данных в условиях компьютерных атак нарушителя // Известия Петербургского университета путей сообщения. 2021. Т. 18, № 2. С. 229–241. DOI 10.20295/1815-588X-2021-2-229-241. EDN UAZOYV

14. Evaluating the functioning quality of data transmission networks in the context of cyberattacks / A. Privalov [et al.] // Energies. 2021. Vol. 14. No. 16. DOI 10.3390/en14164755. EDN FKDDCC

Дата поступления: 13.09.2024
Решение о публикации: 21.11.2024

Контактная информация:
ПРИВАЛОВ Андрей Андреевич — докт. воен. наук, профессор; aprivalov@inbox.ru
ТИТОВ Даниил Дмитриевич — аспирант; titovdd178@gmail.com
ТОЛСТИХИН Александр Игоревич — al.tolstikhin@gmail.com

Program of visualisation of results of evaluation and analysis of IP-network functioning quality under the influence of cyber-attacks

A. A. Privalov[3], D. D. Titov[1,2], A. I. Tolstikhin[2]

[1] Emperor Alexander I St. Petersburg State Transport University, 9, Moskovsky pr., Saint Petersburg, 190031, Russia

[2] Supertel OJSC, 38A, Petrogradskaya Naberezhnaya, Saint Petersburg, 197101, Russia

[3] Academy of National Guard Troops, 1, Letchika Pilyutova st., Saint Petersburg, 198206, Russia

For citation: *Privalov A. A., Titov D. D., Tolstikhin A. I.* Program of visualisation of the results of evaluation and analysis of the IP-network functioning quality under the influence of cyberattacks. // Proceedings of Petersburg Transport University. 2024. Vol. 21, iss. 4. P. 973–980. (In Russian) DOI: 10.20295/1815-588X-2024-04-973-980

Abstract

Purpose: the purpose of this paper is to develop software that is able to visualise the operation of an IP telephone network under cyberattacks using the mathematical model proposed in the research paper. The software should provide an in-depth analysis of the impact of attacks on network performance, as well as provide results in an easy to interpret graphical form. **Methods:** mathematical analysis and counting analysis methods were used to achieve the objectives. The basic mathematical models include equations to calculate impact distribution, restoration time and other network parameters. The programme applies numerical integration and differentiation to calculate the service time distribution. The distribution models include exponential, impulse and gamma distributions. Poisson, Weibull and Pareto distributions were used as distribution functions for random data flow parameters. **Results:** the software is able to simulate different cyberattack scenarios and their impact on key network metrics, analysing characteristics such as delivery time, packet loss probability and network resilience. The results of the analysis show how different types of impacts and recovery parameters affect network performance, allowing the operator to evaluate the effectiveness of different protection and damage techniques. **Practical innovativeness:** the results obtained in the course of technological modelling can be used to improve the stability and reliability of telecommunication systems, especially those operating on Supertel equipment. The software provides operators with a tool to analyse network conditions, develop preventive measures and optimise post-impact recovery strategies. It can also be integrated into a decision support system and used to identify cases of unauthorised access.

Keywords: cyberattack, IP-network, mathematical modelling, distribution functions, counting integration of network resilience, Supertel equipment

References

1. Sheluhin O. I. Prichiny samopodobiya teletrafika i metody ocenki pokazatelya Hersta // Elektrotekhnicheskie i informacionnye kompleksy i sistemy. 2007. T. 3. No. 1. S. 5–14. (In Russian)

2. Matematicheskaya GERT-model' tekhnologii peredachi metadannyh v oblachnye antivirusnye sistemy / V. V. Bos'ko [i dr.] // Sistemi obrobki informaciï: zbirnik naukovih prac'. Har'kov: HUPS, 2014. Vyp. 1(117). S. 137–141. (In Russian)

3. Privalov A. A. Metod topologicheskogo preobrazovaniya stohasticheskih setej i ego ispol'zovanie dlya analiza sistem svyazi VMF. SPb.: VMA, 2000. 166 s. (In Russian)

4. Privalov A.A., Kudelya V.N. Metody matematicheskogo modelirovaniya sistem i processov svyazi. SPb.: Izd-vo Politekhn. un-ta, 2009. 368 s. (In Russian)

5. Nazarov A.N., Sychev K.I. Modeli i metody rascheta pokazatelej kachestva funkcionirovaniya uzlovogo oborudovaniya i strukturno-setevyh

parametrov setej svyazi sleduyushchego pokoleniya. 2-e izd., dop. i pererab. Krasnoyarsk: Polikom, 2011. 491 s. (In Russian)

6. Kucheryavyj A.E., Cuprikov A.L. Seti svyazi sleduyushchego pokoleniya. M.: FGUP CNIIS, 2006. 278 s. (In Russian)

7. Nazarov A.N., Sychev K.I. Modeli i metody issledovaniya processov funkcionirovaniya uzlov kommutacii setej svyazi sleduyushchego pokoleniya pri proizvol'nyh raspredeleniyah postupleniya i obsluzhivaniya zayavok razlichnyh klassov kachestva // Telekommunikacii i transport. 2012. No. 7. S. 135–140. (In Russian)

8. Struktura transportnoj seti svyazi OAO "RZHD" i vozniknovenie fazovogo perekhoda / A.O. Kravcov [i dr.] // ELTRANS 10.0 (Eltrans-2019): materialy X Mezhdunarodnogo simpoziuma "Eltrans-2019" (Eltrans-2019), posvyashchennogo 210-letiyu so dnya osnovaniya pervogo transportnogo vuza Rossii — Peterburgskogo gosudarstvennogo universiteta putej soobshcheniya Imperatora Aleksandra I (Sankt-Peterburg, 9–11 oktyabrya 2019 goda). SPb.: IPK "NP-Print", 2023. S. 190–196. EDN VYEFGL (In Russian)

9. Privalov A.A., Titov D.D. Metod ocenki kachestva funkcionirovaniya IP-setej pri peredachi prioritetnogo mnogoproduktovogo potoka dannyh v usloviyah kiberatak // Materialy mezhvuzovskoj nauchno-prakticheskoj konferencii "Sovremennoe sostoyanie bezopasnosti na transporte i perspektivy ee sovershenstvovaniya" (Sankt-Peterburg, Petergof, 20 aprelya 2022 goda). SPb.: Voennyj institut (inzhenerno-tekhnicheskij), 2022. S. 72–86. EDN GNPBCV (In Russian)

10. Privalov A.A., Titov D.D. Model' processa raboty uzla kommutacii tekhnologicheskoj IP-seti pri obsluzhivanii prioritetnogo mnogoproduktovogo potoka v usloviyah DDOS-atak narushitelya // Fundamental'nye i prikladnye nauchnye issledovaniya: sbornik trudov po materialam X Mezhdunarodnogo konkursa nauchno-issledovatel'skih rabot (Ufa, 5 dekabrya 2022 goda). Ufa: Vestnik nauki, 2022. S. 92–104. EDN JUCSGZ (In Russian)

11. Privalov A.A., Titov D.D. Model' processa peredachi prioritetnogo mnogoproduktovogo potoka po kanalu telefonnoj IP-seti v usloviyah komp'yuternyh atak narushitelya // Innovacionnye nauchnye issledovaniya v sovremennom mire: sbornik trudov po materialam X Vserossijskogo konkursa nauchno-issledovatel'skih rabot (Ufa, 28 noyabrya 2022 goda). Ch. 1. Ufa: Vestnik nauki, 2022. S. 63–73. EDN DYCEIY (In Russian)

12. Privalov A.A., Lukicheva V.L., Titov D.D. Model' processa funkcionirovaniya uzla kommutacii tekhnologicheskoj seti peredachi dannyh v usloviyah DDOS atak narushitelya // Informaciya i kosmos. 2021. No. 2. S. 66–75. EDN FQPOKK (In Russian)

13. Privalov A.A., Lukicheva V.L., Titov D.D. Model' processa dostavki paketov po kanalu peredachi dannyh v usloviyah komp'yuternyh atak narushitelya // Izvestiya Peterburgskogo universiteta putej soobshcheniya. 2021. T. 18, no. 2. S. 229–241. DOI 10.20295/1815-588X-2021-2-229-241. EDN UAZOYV (In Russian)

14. Evaluating the functioning quality of data transmission networks in the context of cyberattacks / A. Privalov [et al.] // Energies. 2021. Vol. 14. No. 16. DOI 10.3390/en14164755. EDN FKDDCC

Received: 13.09.2024
Accepted: 21.11.2024

Author's information:
Andrey A. PRIVALOV — Dr. Sci. in Military; Professor; aprivalov@inbox.ru
Daniil D. TITOV — Postgraduate Student; titovdd178@gmail.com
Alexander I. TOLSTIKHIN — al.tolstikhin@gmail.com