Информатика. Экономика. Управление// Informatics. Economics. Management

2025; 4(1)
eISSN: 2782-5280
http://oajiem.com/

УДК: 004.056.53
DOI: https://doi.org/10.47813/2782-5280-2025-4-1-1001-1007

EDN: **DVSBRU**

Современные кибератаки: классификация и способы защиты

А. К. Назарян[1]
И. Н. Карцан[2, 3]

[1]*ФГАОУ ВО «Севастопольский государственный университет», г. Севастополь, Россия*
[2]*ФГБНУ «Аналитический центр», г. Москва, Россия*
[3]*ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», г. Красноярск, Россия*

Аннотация. В статье представлен анализ современных кибератак, их классификации, механизмов реализации и методов защиты. Особое внимание уделено рассмотрению наиболее распространённых видов атак, таких как фишинг, Ransomware, DDoS, атаки через цепочку поставок и вредоносное программное обеспечение. Выявлены ключевые цели атак, включая кражу данных, нарушение доступности, вымогательство и шпионаж. Проанализированы основные методы реализации кибератак, среди которых использование социальных манипуляций, эксплуатация уязвимостей и создание сетей заражённых устройств. На основе рассмотрения примеров реальных атак, включая случаи WannaCry, SolarWinds и Equifax, показаны их последствия для организаций и пользователей. Предложены методы защиты, включающие технические меры (фаерволы, системы обнаружения вторжений, шифрование), организационные меры (политики безопасности, управление доступом) и образовательные инициативы (обучение сотрудников, симуляции атак). Отдельное внимание уделено внедрению современных технологий, таких как искусственный интеллект и машинное обучение, которые позволяют своевременно выявлять и блокировать угрозы. Сделан вывод о важности комплексного подхода к информационной безопасности, сочетающего проактивные меры с обучением и постоянным мониторингом инфраструктуры. Представленные в статье рекомендации направлены на повышение устойчивости цифровых систем к кибератакам и снижение их негативных последствий.

Ключевые слова: кибератаки, информационная безопасность, фишинг, DDoS, методы защиты, шифрование данных, искусственный интеллект.

Для цитирования: Назарян, А. К., & Карцан, И. Н. Современные кибератаки: классификация и способы защиты. Информатика. Экономика. Управление - Informatics. Economics. Management, 4(1), 1001–1007. https://doi.org/10.47813/2782-5280-2025-4-1-1001-1007

Modern cyberattacks: classification and methods of defense

Artur Nazaryan[1]
Igor Kartsan[2, 3]

[1]*Sevastopol State University, Sevastopol, Russia*
[2]*Analytical Center, Moscow, Russia*
[3]*Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russia*

Abstract. The article presents an analysis of modern cyberattacks, their classification, implementation mechanisms and defense methods. Special attention is paid to the most common types of attacks, such as phishing, Ransomware, DDoS, supply chain attacks and malware. Key targets of attacks are identified, including data theft, availability disruption, ransomware and espionage. The main methods of cyberattacks are analyzed, including the use of social manipulation, exploitation of vulnerabilities, and networking of infected devices. Examples of real-world attacks, including WannaCry, SolarWinds, and Equifax, are examined to show the impact on organizations and users. Protection methods including technical measures (firewalls, intrusion detection systems, encryption), organizational measures (security policies, access control), and educational initiatives (employee training, attack simulations) are proposed. Special attention is paid to the introduction of modern technologies, such as artificial intelligence and machine learning, which allow timely detection and blocking of threats. The conclusion is made about the importance of a comprehensive approach to information security, combining proactive measures with training and constant monitoring of infrastructure. The recommendations presented in the article are aimed at increasing the resilience of digital systems to cyberattacks and reducing their negative consequences.

Keywords: cyberattacks, information security, phishing, DDoS, defense methods, data encryption, artificial intelligence.

For citation: Nazaryan, A. K., & Kartsan, I. N. Modern cyberattacks: classification and methods of defense . Informatics. Economics. Management, 4(1), 1001–1007. https://doi.org/10.47813/2782-5280-2025-4-1-1001-1007

© Назарян А. К., Карцан И. Н., 2025

2025; 4(1)
eISSN: 2782-5280
http://oajiem.com/

ВВЕДЕНИЕ

Современное общество неразрывно связано с цифровыми технологиями, что привело к значительному увеличению числа и сложности кибератак [1, 2]. Киберпреступность, как форма угрозы, представляет собой серьезную проблему для государственных, корпоративных и частных пользователей, способных нанести значительный ущерб. В последние годы наблюдается рост частоты и сложности кибератак, что связано с развитием информационных технологий, повсеместным внедрением интернета вещей (IoT), а также усилением угроз в глобальной сети [3]. Актуальность темы киберугроз в значительной мере обусловлена быстро меняющимися технологиями, которыми активно пользуются как преступники, так и те, кто их защищает.

Кибератаки могут быть направлены на различные цели: от кражи конфиденциальной информации и разрушения критической инфраструктуры до политических манипуляций и финансовых махинаций [4, 5]. Их методы становятся все более разнообразными и сложными, включая как традиционные формы атак, такие как фишинг или DDoS, так и более сложные атаки на цепочки поставок или использование уязвимостей в программном обеспечении [6].

Основная проблема заключается в том, что многие организации и пользователи недостаточно защищены от кибератак, что объясняется не только отсутствием знаний о возможных угрозах, но и неспособностью эффективно противодействовать новым типам атак. Традиционные методы защиты, такие как антивирусные программы и фаерволы, хотя и остаются важными, часто оказываются недостаточными для защиты от современных угроз [7, 8]. Это связано с развитием киберпреступности, которая использует все более сложные методы, включая социальную инженерию, уязвимости в цепочках поставок и целенаправленные атаки на слабые места в системах безопасности.

Для эффективной борьбы с кибератаками необходимо выявить и классифицировать основные виды угроз, понять их механизмы реализации и последствия, а также предложить методы защиты, которые позволят минимизировать риски [9, 10]. Важно учитывать, что кибератаки не ограничиваются только техническими уязвимостями, но часто связаны с человеческим фактором, что требует комплексного подхода к безопасности, включающего как технические меры, так и организационные [11].

КЛАССИФИКАЦИЯ КИБЕРАТАК

Кибератаки можно классифицировать по различным признакам (рисунок 1), и одним из самых важных является разделение по целям и методам реализации.

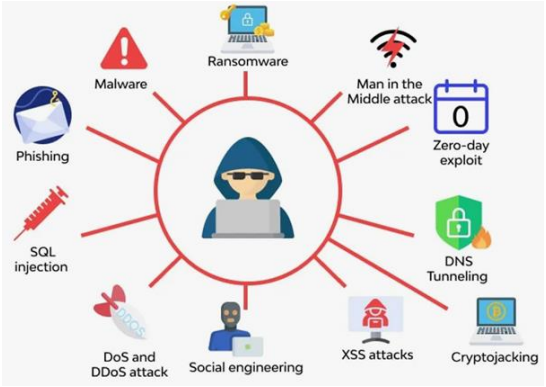


Рисунок 1. Виды кибератак.

Figure 1. Types of cyberattacks.

По целям кибератаки могут преследовать различные намерения, включая кражу данных, нарушение доступности, модификацию данных, вымогательство, шпионаж и нарушение конфиденциальности. Кража данных является одной из самых распространенных целей атак, где злоумышленники пытаются получить доступ к конфиденциальной информации, такой как персональные данные, финансовая информация или интеллектуальная собственность.

Нарушение доступности - это атаки, направленные на блокировку или перегрузку серверов, чтобы легитимные пользователи не могли получить доступ к ресурсам, как это происходит при DDoS-атаках. Модификация данных включает изменения или подмену информации в системах, что может серьезно повлиять на целостность данных и функционирование организаций. Вымогательство связано с попытками получить выкуп за возвращение украденных данных или восстановление работы системы, что часто происходит при использовании Ransomware. Шпионаж предполагает получение конфиденциальной информации для политических, экономических или промышленных целей, а нарушение конфиденциальности касается случаев, когда злоумышленники стремятся получить доступ к

2025; 4(1)
eISSN: 2782-2818
https://www.oajmist.com

личным данным пользователей или организаций, нарушая их права на приватность.

Методы реализации кибератак также разнообразны. Одним из наиболее распространенных методов является социальная инженерия, где злоумышленники используют психологические манипуляции для получения доступа к конфиденциальной информации.

Классическими примерами социальной инженерии являются фишинг, вишинг и смишинг, когда злоумышленники маскируются под доверенные источники и пытаются «выудить» личные данные. Вредоносное программное обеспечение (ПО), или malware, также широко используется для атак, включая вирусы, трояны, черви и шпионские программы, которые могут нанести вред системам, воровать данные или разрушать системы. Атаки на уязвимости (exploits) направлены на использование недостатков в программном обеспечении или операционных системах, что позволяет хакерам получить несанкционированный доступ или управлять системой. DDoS-атаки, при которых злоумышленники используют распределенные сети зараженных устройств для перегрузки серверов, направлены на разрушение нормальной работы системы, часто выводя сайты или сервисы из строя.

Атаки через цепочку поставок включают вмешательство в систему через уязвимости в стороннем ПО или поставках, что может привести к компрометации всей инфраструктуры организации. Атаки типа Man-in-the-Middle (MITM) включают перехват данных между двумя сторонами, что позволяет злоумышленнику изменять или читать передаваемую информацию без ведома пользователей. Наконец, атаки на пароли включают различные способы взлома учетных данных для доступа к системам, например, с использованием brute force или словарных атак, а также фишинг для получения паролей.

Каждый из этих методов имеет свои особенности, и понимание этих различий помогает выработать эффективные стратегии защиты, которые могут значительно снизить риски при возникновении угроз.

Анализ механизмов реализации кибератак позволяет выявить, как именно осуществляются различные типы атак, включая используемые техники и методы.

Фишинг:

- Описание механизма. Поддельные электронные письма, сайты или сообщения, которые имитируют доверенные источники.
- Примеры фишинга. Фишинг в социальных сетях, spear phishing (целевой фишинг), whaling (фишинг для высокопоставленных лиц).
- Последствия. Утечка конфиденциальных данных, компрометация учётных записей.

Вредоносное программное обеспечение (Malware):

- Типы вредоносного ПО. Вирусы, трояны, черви, шпионские программы, клавиатурные шпионы.
- Распространение. Заражённые файлы, вложения в письмах, вредоносные ссылки.
- Воздействие. Шифрование данных (Ransomware), кража информации, нарушение работы систем.

DDoS-атаки:

- Механизм. Массовая отправка запросов для перегрузки серверов или сетей.
- Примеры. Ботнеты, использование IoT-устройств.
- Последствия. Недоступность сервисов, финансовые потери.

Атаки на уязвимости (эксплойты):

- Использование слабостей в программном обеспечении для проникновения в систему.
- Примеры. SQL-инъекции, атаки через XSS (межсайтовый скриптинг).
- Воздействие. Получение несанкционированного доступа, модификация данных.

Атаки Man-in-the-Middle (MITM):

- Описание. Перехват и изменение передаваемых данных между двумя сторонами.
- Примеры. Атаки на незащищённые Wi-Fi сети, подмена DNS.
- Последствия. Кража данных, компрометация сессий.

2025; 4(1)
eISSN: 2782-2818
https://www.oajmist.com

Атаки через цепочку поставок:

- Механизм. Внедрение вредоносного кода или уязвимостей на этапе разработки или поставки ПО.
- Примеры. Атака SolarWinds, вредоносные библиотеки в открытых репозиториях.
- Воздействие. Заражение систем по всей цепочке поставок.

Атаки на пароли:

- Методы. Перебор, фишинг, использование слабых паролей.
- Инструменты. Программы для взлома паролей, атаки через базы утекших данных.
- Последствия. Доступ к критически важным данным и учётным записям.

ЯЗЫКИ ПРОГРАММИРОВАНИЯ ДЛЯ РЕАЛИЗАЦИИ КИБЕРАТАК

Для реализации кибератак используются языки программирования или же готовые инструменты и фреймворки.

Python является одним из наиболее часто используемых языков из-за своей простоты и богатой экосистемы библиотек. Он широко применяется для создания инструментов фишинга, написания скриптов для атак на уязвимости и проведения DDoS-атак. Например, с помощью Python злоумышленники создают программы, которые автоматически рассылают фишинговые письма или сканируют системы на наличие уязвимостей.

C и C++ используются для разработки сложного вредоносного ПО, включая вирусы, трояны и шпионские программы. Эти языки обеспечивают низкоуровневый доступ к системным ресурсам и позволяют злоумышленникам обходить защитные механизмы операционной системы. Кроме того, благодаря своей производительности, C и C++ применяются для написания модулей эксплойтов, которые используют уязвимости в программном обеспечении.

Java нередко используется в атаках на приложения, работающие в среде Java, включая серверы и корпоративные системы. Одним из примеров является написание вредоносного кода для реализации атак на уязвимости Java Virtual Machine (JVM) или создание программ, которые заражают устройства через веб-браузеры.

JavaScript играет ключевую роль в реализации атак, связанных с веб-средой. Этот язык используется для выполнения межсайтового скриптинга (XSS), кражи cookie-файлов, выполнения фишинговых скриптов и создания поддельных форм на веб-страницах. Удобство выполнения JavaScript в браузерах делает его незаменимым инструментом для атак на пользователей веб-приложений.

Для написания вредоносного кода также могут использоваться PowerShell и Bash, особенно в атаках, нацеленных на эксплуатацию серверов или системных процессов. PowerShell активно применяется для обхода антивирусов и выполнения скрытых команд в Windows-системах, тогда как Bash используется для атак на Linux-сервера, включая эксплуатацию командных инъекций.

Таким образом, выбор языка программирования для реализации атаки зависит от ее типа, используемой платформы и желаемого результата. Это подчеркивает важность регулярного обновления программного обеспечения, применения многоуровневых механизмов защиты и повышения осведомлённости пользователей о возможных угрозах.

СТРАТЕГИИ И ТЕХНОЛОГИИ ДЛЯ ПРЕДОТВРАЩЕНИЯ, ОБНАРУЖЕНИЯ И МИНИМИЗАЦИИ ПОСЛЕДСТВИЙ КИБЕРАТАК

В рамках разработки стратегии и технологии для предотвращения, обнаружения и минимизации последствий кибератак основное внимание уделяется техническим, организационным и образовательным аспектам защиты.

Технические меры защиты:

- Фаерволы и системы обнаружения вторжений (IDS/IPS). Фаерволы фильтруют входящий и исходящий трафик, предотвращая несанкционированный доступ, тогда как системы IDS и IPS обнаруживают аномальные действия и автоматически блокируют подозрительные активности.
- Антивирусное и антишпионское программное обеспечение. Используется для обнаружения и устранения вредоносных программ, таких как вирусы, трояны и Ransomware.
- Шифрование данных. Обеспечивает защиту информации в случае её перехвата

2025; 4(1)
eISSN: 2782-2818
https://www.oajmist.com

злоумышленниками. Современные алгоритмы, такие как AES или RSA, делают данные практически недоступными для расшифровки.

- Аутентификация и управление доступом. Использование многофакторной аутентификации (MFA) значительно снижает риск взлома учётных записей. Управление доступом обеспечивает ограничение прав пользователей на основе их ролей.
- Резервное копирование и восстановление. Регулярное создание резервных копий помогает минимизировать потери данных в случае успешной атаки, например, Ransomware.

Для эффективного противостояния кибератакам важно не только применять технические решения, но и выстраивать комплексный подход на уровне организаций. Политики информационной безопасности служат фундаментом, определяющим, как сотрудники должны обращаться с корпоративными системами и данными. Чёткие планы управления инцидентами, включающие мониторинг, анализ и реагирование на кибератаки, позволяют оперативно восстанавливать нормальную работу после инцидентов.

Обучение сотрудников играет важнейшую роль в предотвращении атак, таких как фишинг. Повышение осведомлённости о ключевых угрозах, регулярные тренинги и моделирование реальных атак помогают пользователям распознавать опасные ситуации. Кроме того, развитие культуры безопасности на уровне организации укрепляет общий уровень защиты.

Современные технологии, такие как искусственный интеллект, используются для анализа сетевого трафика и выявления новых угроз в реальном времени. Блокчейн способствует повышению безопасности хранения данных, а сегментация сети минимизирует ущерб, изолируя критически важные системы.

Эти меры дополняют друг друга, создавая многоуровневую защиту. Успешные кейсы, такие как внедрение комплексных мер безопасности в крупных корпорациях или национальных центрах кибербезопасности, демонстрируют, что только скоординированные усилия позволяют эффективно противостоять современным угрозам.

Анализ реальных примеров кибератак помогает лучше понять, как злоумышленники используют уязвимости, и какие последствия могут быть для организаций и пользователей. Один из самых известных инцидентов – атака вируса WannaCry в 2017 году. Это вредоносное ПО, относящееся к категории Ransomware, за считанные дни поразило сотни тысяч устройств по всему миру. WannaCry использовал уязвимость в операционной системе Windows для распространения и шифрования данных на заражённых компьютерах, требуя выкуп за их восстановление. Среди пострадавших оказались крупные корпорации, медицинские центры, и даже государственные учреждения, что подчёркивает масштаб угрозы.

Другим значимым инцидентом стала атака на компанию Equifax в 2017 году. Злоумышленники воспользовались уязвимостью в одном из веб-приложений компании, что привело к утечке персональных данных более 147 миллионов человек, включая их имена, номера социального страхования и кредитную историю. Этот случай продемонстрировал, насколько важна регулярная проверка систем безопасности и своевременное обновление программного обеспечения.

Ещё одним ярким примером стала атака на цепочку поставок SolarWinds в 2020 году. Вредоносный код был внедрён в обновления программного обеспечения Orion, используемого тысячами организаций по всему миру. Эта атака позволила злоумышленникам получить доступ к системам множества компаний и государственных учреждений, подчеркнув опасность атак через цепочку поставок.

Эти примеры показывают, что кибератаки могут наносить не только финансовый, но и репутационный ущерб. Кроме того, они подчеркивают необходимость многоуровневой защиты и проактивного подхода к информационной безопасности.

ЗАКЛЮЧЕНИЕ

Для эффективного снижения рисков кибератак необходимо реализовать комплексный подход, сочетающий технические, организационные и образовательные меры. Прежде всего, важно внедрить регулярное обновление программного обеспечения. Многие атаки становятся возможными из-за использования устаревших систем с известными уязвимостями. Организации должны обеспечить автоматическое обновление программ или внимательно отслеживать выход патчей безопасности.

Другой ключевой аспект – многофакторная аутентификация (MFA). Этот метод значительно усложняет несанкционированный доступ, требуя подтверждения личности пользователя через несколько независимых факторов. Кроме того, важно использовать сильные пароли, избегая их повторного использования для разных аккаунтов.

Организации также должны регулярно проводить обучение сотрудников. Повышение осведомлённости о современных угрозах, таких как фишинг, помогает значительно снизить вероятность успешной атаки. Проведение тестовых сценариев, таких как симуляция фишинговых атак, позволит выявить слабые места и улучшить готовность персонала.

Наконец, важно уделить внимание резервному копированию данных. Наличие актуальных резервных копий снижает последствия атак, таких как Ransomware, и позволяет оперативно восстановить работу системы.

Снижение рисков кибератак требует постоянного мониторинга и адаптации к новым угрозам. Только сочетание технологических решений с осведомлённостью пользователей и строгими организационными политиками позволяет эффективно противостоять современным вызовам кибербезопасности.

СПИСОК ЛИТЕРАТУРЫ

[1] Shchetinin E.Yu., Velieva T.R. Detection of cyber-attacks on the power smart grids using semi-supervised deep learning models. Discrete and Continuous Models and Applied Computational Science. 2022; 3 (30): 258-268. doi: 10.22363/2658-4670-2022-30-3-258-268

[2] Пашаев Ф.Г., Зейналов Д.И., Наджафов Г.Т. Разработка программно-технических средств защиты технологических процессов от киберугроз, Проблемы информационной безопасности. Компьютерные системы. 2024; 2 (59): 104-116. doi: 10.48612/jisp/p79a-z1nu-71vk

[3] Кобец П.Н., Краснова К.А. Современные особенности, причины, условия и совершенствование мер противодействия киберпреступности. Уголовно-исполнительное право. 2024; 1 (19): 103-110. doi: 10.33463/2687-122X.2024.19(1-4).1.103-110

[4] Кривчун Н.А., Солодовников Д.В., Соколов А.К., Шорохов К.Д., Кучук М.И. Кибератаки и методы их предотвращения в информационных системах. Дискуссия. 2024; 7 (128): 120-126. doi: 10.46320/2077-7639-2024-7-128-120-126

[5] Беляева О.Н., Малышева К.М. Значение и роль кибербезопасности в современном мире. Reports Scientific Society. 2024; 2 (46): 5-8.

[6] Намиот Д.Е. О кибератаках с помощью систем искусственного интеллекта. International Journal of Open Information Technologies. 2024; 9 (12): 132-141.

[7] Карцан И.Н., Кобозев Д.С. Аспекты безопасности спутниковой связи. Естественные и технические науки. 2024; 6 (193): 310-312.

[8] Горда М.Д., Чечулин А.А. Модель расследования киберпреступлений. Информатизация и связь. 2023; 3: 92-97. doi: 10.34219/2078-8320-2023-14-3-92-97

[9] Kartsan I.N., Zhukov A.O., Skripachev V.O. Model for calculating the speed of delivery of remotely sensed earth observation information. InterCarto. InterGIS. 2024; 1 (30): 534-544. doi: 10.35595/2414-9179-2024-1-30-534-544

[10] Амшоков А.Х., Гусев А.С. Современные российские меры предупреждения мошенничества. Аграрное и земельное право. 2023; 10 (226): 150-151. doi: 10.47643/1815-1329_2023_10_150

[11] Lapshina I.V., Kravets A.V. Modern cybersecurity from the perspective of cognitive modeling. Ingineering Journal of Don. 2023; 1 (97): 80-95.

REFERENCES

[1] Shchetinin E.Yu., Velieva T.R. Detection of cyber-attacks on the power smart grids using semi-supervised deep learning models. Discrete and Continuous Models and Applied Computational Science. 2022; 3 (30): 258-268. doi: 10.22363/2658-4670-2022-30-3-258-268

[2] Pashaev F.G., Zejnalov D.I., Nadzhafov G.T. Razrabotka programmno-tekhnicheskikh sredstv zashchity tekhnologicheskikh protsessov ot kiberugroz, Problemy informatsionnoj bezopasnosti. Komp'yuternye sistemy. 2024; 2 (59): 104-116. doi: 10.48612/jisp/p79a-z1nu-71vk

[3] Kobets P.N., Krasnova K.A. Sovremennye osobennosti, prichiny, usloviya i sovershenstvovanie mer protivodejstviya kiberprestupnosti. Ugolovno-ispolnitel'noe pravo. 2024; 1 (19): 103-110. doi: 10.33463/2687-122X.2024.19(1-4).1.103-110

[4] Krivchun N.A., Solodovnikov D.V., Sokolov A.K., Shorokhov K.D., Kuchuk M.I. Kiberataki i metody ikh predotvrashcheniya v informatsionnykh sistemakh. Diskussiya. 2024; 7 (128): 120-126. doi: 10.46320/2077-7639-2024-7-128-120-126

2025; 4(1)
eISSN: 2782-2818
https://www.oajmist.com

[5] Belyaeva O.N., Malysheva K.M. Znachenie i rol' kiberbezopasnosti v sovremennom mire. Reports Scientific Society. 2024; 2 (46): 5-8.
[6] Namiot D.E. O kiberatakakh s pomoshch'yu sistem iskusstvennogo intellekta. International Journal of Open Information Technologies. 2024; 9 (12): 132-141.
[7] Kartsan I.N., Kobozev D.S. Aspekty bezopasnosti sputnikovoj svyazi. Estestvennye i tekhnicheskie nauki. 2024; 6 (193): 310-312.
[8] Gorda M.D., Chechulin A.A. Model' rassledovaniya kiberprestuplenij. Informatizatsiya i svyaz'. 2023; 3: 92-97. doi: 10.34219/2078-8320-2023-14-3-92-97
[9] Kartsan I.N., Zhukov A.O., Skripachev V.O. Model for calculating the speed of delivery of remotely sensed earth observation information. InterCarto. InterGIS. 2024; 1 (30): 534-544. doi: 10.35595/2414-9179-2024-1-30-534-544
[10] Amshokov A.Kh., Gusev A.S. Sovremennye rossijskie mery preduprezhdeniya moshennichestva. Agrarnoe i zemel'noe pravo. 2023; 10 (226): 150-151. doi: 10.47643/1815-1329_2023_10_150
[11] Lapshina I.V., Kravets A.V. Modern cybersecurity from the perspective of cognitive modeling. Ingineering Journal of Don. 2023; 1 (97): 80-95.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Назарян Артур Корюнович, студент, ФГАОУ ВО «Севастопольский государственный университет», Севастополь, Россия

Карцан Игорь Николаевич, доктор технических наук, доцент, главный научный сотрудник ФГБНУ «Аналитический центр», Москва, Россия

Artur Nazaryan, Student, Sevastopol State University, Sevastopol, Russia

Igor Kartsan, Dr. Sc., Docent, Chief Researcher of the Analytical Center, Moscow, Russia

Статья поступила в редакцию 10.01.2025; одобрена после рецензирования 03.02.2025; принята к публикации 03.02.2025.

The article was submitted 10.01.2025; approved after reviewing 03.02.2025; accepted for publication 03.02.2025.