Обзорная статья
УДК 004.85+004.056.5
ББК 32.813.5
К 59
DOI: 10.53598/2410-3225-2023-3-326-65-72

Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности

(*Рецензирована*)

Наталья Шумафовна Козлова[1], Виталий Анатольевич Довгаль[2]

[1] *Майкопский государственный технологический университет, natali20052001@bk.ru*
[2] *Майкопский государственный технологический университет, Адыгейский государственный университет, Майкоп, Россия, urmia@mail.ru*

Аннотация. *Целью данного исследования является обзор и анализ применения влияния искусственного интеллекта и машинного обучения на сферу кибербезопасности, рассматриваются их различные типы, приложения, проблемы и многообещающее будущее, которое их ждет. Используя возможности искусственного интеллекта и машинного обучения, организации могут обеспечить защиту информации в локальных сетях от вредоносных угроз и снижать киберриски. В постоянно развивающемся цифровом мире, наполненном киберугрозами, интеграция искусственного интеллекта (ИИ) и машинного обучения (МО) меняет способы защиты онлайн-доменов. Благодаря способности моделировать интеллектуальное поведение человека и анализировать огромные объемы данных, ИИ и МО играют решающую роль в создании и обработке данных о киберугрозах для борьбы с киберпреступностью.*

Ключевые слова: *кибербезопасность, киберриски, киберугрозы, защита информации, информационная безопасность информационные системы, цифровые технологии, информация, угрозы*

Review Article

Analysis of the use of artificial intelligence and machine learning in cybersecurity

Natalya Sh. Kozlova[1], Vitaliy A. Dovgal[2]

[1] *Maikop State University of Technology, natali20052001@bk.ru*
[2] *Maikop State University of Technology, Adyghe State University, Maikop, Russia, urmia@mail.ru*

Abstract. *The study aims to review and analyze the application of the influence of artificial intelligence and machine learning on cybersecurity, their various types, applications, problems and the promising future they await. Using the capabilities of artificial intelligence and machine learning, organizations can strengthen the ways of protecting their networks from malicious threats and reduce cyber risks. In an ever-evolving digital world filled with constant cyber threats, the integration of artificial intelligence (AI) and machine learning (ML) is changing the way we protect our online domains. Thanks to the ability to model intelligent human behavior and analyze huge amounts of data, AI and ML play a crucial role in creating and processing cyber threat data to fight cybercrime.*

Keywords: *cybersecurity, cyber risks, cyber threats, information protection, information security information systems, digital technologies, information, threats*

I. Введение

История применения искусственного интеллекта и машинного обучения в сфере кибербезопасности насчитывает несколько десятилетий. В то время как первые усилия были сосредоточены на системах обнаружения аномалий на основе правил в середине-

конце 1980-х годов, рост больших данных после 2000 года привел к значительным изменениям в искусственном интеллекте и машинном обучении.

По мере усложнения технологий алгоритмы машинного обучения стали мощным инструментом обнаружения угроз. В конце 2000-х годов применение алгоритмов контролируемого обучения открыло путь к более точному обнаружению и предотвращению угроз. Его примеру последовали алгоритмы неконтролируемого обучения, позволяющие выявлять аномальные закономерности и ранее неизвестные угрозы.

Развитие методов глубокого обучения в прошлом десятилетии произвело революцию в кибербезопасности, благодаря его способности обрабатывать огромные объемы данных и выявлять сложные закономерности. Методы обработки естественного языка (*natural language processing*, *NLP*) [1] также получили известность, позволяя улучшить анализ текстовых данных и обнаружить атаки социальной инженерии.

В настоящее время в области кибербезопасности для борьбы с постоянно развивающимися угрозами и формирования более безопасного цифрового будущего происходит массовое внедрение систем на основе искусственного интеллекта и машинного обучения. Указанные системы работают на основе методов, использующих огромный объем данных, генерируемых цифровыми системами и сетями, для выявления закономерностей, аномалий и потенциальных угроз с большей точностью и эффективностью, обеспечивая упреждающее обнаружение и предотвращение угроз в режиме реального времени. Такое сочетание больших данных, систем искусственного интеллекта и машинного обучения обеспечивает кибербезопасность, предоставив заинтересованным организациям возможность более эффективно анализировать инциденты безопасности и реагировать на них, снижать риски и адаптироваться к развивающимся киберугрозам.

II. Типы искусственного интеллекта и машинного обучения

Кратко рассмотрим несколько фундаментальных типов искусственного интеллекта и машинного обучения, используемых в кибербезопасности ИИ и играющих в ней ключевую роль: обучение с учителем, обучение без учителя, обучение с подкреплением, глубокое обучение и обработка естественного языка. Перечисленные типы включают в себя ряд методов и методологий, которые позволяют системам кибербезопасности обнаруживать, анализировать и реагировать на угрозы с повышенной точностью и эффективностью.

Контролируемое машинное обучение (*обучение с учителем)* [2] включает сбор предварительно классифицированных веб-сайтов (обучающих меток) вместе с соответствующими HTML-кодами и изображениями для этих веб-сайтов (функции обучения). Затем модель «обучается» созданию сопоставления большого количества функций с метками. Обратная связь предоставляется контролируемой модели в виде функции потерь, где модель наказывается за неправильные ответы и вознаграждается за правильные ответы. Таким образом, алгоритм машинного обучения постепенно улучшается по мере того, как в модель поступает все больше и больше размеченных данных.

Неконтролируемое машинное обучение (*обучение без учителя*) [3] предполагает использование только функций обучения БЕЗ меток для определения полезных тенденций и «кластеров» в данных. Этот метод может хорошо сработать в тех случаях, когда имеется много данных, но необходимо с чего-то начать. Недостатком такого типа искусственного интеллекта и машинного обучения будет снижение точности модели и проведение утомительной работы по анализу и маркировке количества веб-сайтов, необходимых для создания современной модели.

Машинное обучение под наблюдением человека (*Machine learning under human supervision*, *HS*/*ML*, *обучение с подкреплением*) [4] – способ, при котором человек гарантирует актуальность модели и ее точность, обнаруживая ошибку алгоритма, с по-

следующим автоматическим включением данных обратно в систему для переобучения модели в целях исключения подобных ошибок в будущем. Постоянный мониторинг, маркировка и процесс переобучения являются ключом к достижению высокой степени точности и минимизации ложных срабатываний, которые могут стать помехой для многих инструментов безопасности.

Глубокое обучение – это подмножество методов машинного обучения, основанное на принципах обработки информации человеческим мозгом [5]. Цель алгоритмов глубокого обучения: получение информации, сопоставимой с человеческой, посредством непрерывного анализа данных с использованием заранее определенной логической структуры. Для этого в глубоком обучении используются сложные алгоритмы, называемые нейронными сетями, которые способны изучать сложные шаблоны и представления на основе данных. Глубокое обучение все чаще применяется в сфере кибербезопасности для улучшения обнаружения угроз, сетевой безопасности и защиты данных.

Обучение с подкреплением (*Reinforcement Learning*, *RL*) – это отдельная парадигма обучения в рамках машинного обучения, которая фокусируется на принятии решений в динамичных средах и черпает вдохновение из того, как люди учатся методом проб и ошибок [6]. Этот подход предполагает обучение системы искусственного интеллекта принимать решения и совершать действия в среде, позволяющей максимизировать вознаграждение или минимизировать наказание. В контексте кибербезопасности обучение с подкреплением может применяться к различным сценариям, таким как адаптивное реагирование на угрозы и динамическое применение политик.

Постоянно взаимодействуя с окружающей средой, система искусственного интеллекта изучает оптимальные стратегии и адаптирует свое поведение на основе наблюдаемых результатов, что позволяет ей эффективно выявлять возникающие угрозы и реагировать на них в режиме реального времени. RL может применяться к кибербезопасности для улучшения мер безопасности и процессов принятия решений. Примеры вариантов использования включают адаптивное обнаружение вторжений, автоматизированные системы реагирования и смягчения последствий, поиск угроз, распределение и оптимизацию ресурсов, а также оценку уязвимостей и исправление.

Обучение с подкреплением с обратной связью от человека (*RLHF*) – это особая форма обучения с подкреплением, которая применяет опыт и знания человека в процессе обучения, что помогает повысить эффективность обучения и добиться более высоких результатов [7]. Помимо взаимодействия с окружающей средой агент также получает указания или обратную связь от человека-эксперта в форме явных сигналов вознаграждения, демонстраций или оценок. Такой подход часто используется в приложениях, где ценен человеческий опыт или предпочтения.

Обработка естественного языка (*NLP*) – это область искусственного интеллекта, специально ориентированная на взаимодействие между машинами и людьми с использованием программного обеспечения, которое может взаимодействовать с человеческим языком для извлечения таких деталей, как настроения, имена людей или мест, намерения, темы и т.д. [6] NLP используется для обнаружения вредоносных программ для анализа больших объемов данных и обнаружения закономерностей, которые можно пропустить с помощью традиционных инструментов безопасности. Алгоритмы NLP анализируют язык, используемый при общении по электронной почте, в содержании веб-сайтов или на платформах социальных сетей, в поисках признаков вредоносной активности (например, ботнетов, спама, фейковых учетных записей и т.д.) и выявления закономерностей и тенденций, которые могут указывать на возникающие угрозы или новые векторы атаки.

Нейронный машинный перевод (*NMT*) – это подраздел NLP, который фокусиру-

ется на использовании искусственных нейронных сетей для перевода текста с одного языка на другой [8]. Поскольку ландшафт угроз не привязан к языку или географическому региону, использование NMT для анализа и перевода больших объемов данных на несколько языков имеет решающее значение для обнаружения вредоносных программ. Аналитики безопасности могут использовать NMT для перевода сообщений между злоумышленниками, содержимого веб-сайтов, сообщений в социальных сетях и другого цифрового контента для выявления шаблонов языка, которые могут указывать на вредоносную деятельность.

III. Применение искусственного интеллекта и машинного обучения в кибербезопасности

Использование искусственного интеллекта и машинного обучения для обеспечения кибербезопасности достаточно разнообразно и позволяет организациям обнаруживать киберугрозы, реагируя на них в режиме реального времени, выявляя закономерности и аномалии в огромных объемах данных, а также улучшая общее управление киберрисками. Ниже приведены некоторые из наиболее распространенных приложений безопасности для искусственного интеллекта и машинного обучения.

Веб-фильтрация и DNS-фильтрация – применение алгоритмов искусственного интеллекта и машинного обучения играет решающую роль при анализе сетевого трафика, URL-адресов и DNS-запросов для выявления и блокировки вредоносных вебсайтов, попыток фишинга, загрузки вредоносного программного обеспечения (ПО) и других киберугроз. Применение искусственного интеллекта и машинного обучения может выполнять автоматизированную категоризацию веб-контента в целях его последующей фильтрации в соответствии с требуемой таксономией организации, что эффективно защищает пользователей от доступа к вредоносным или неподходящим вебсайтам, обеспечивая целостность сети.

Управление уязвимостями: модели машинного обучения могут расставлять приоритеты и оценивать серьезность уязвимостей, анализируя такие факторы, как данные о распространенных уязвимостях и воздействиях (CVE), базы данных эксплойтов и историю исправлений. Алгоритмы машинного обучения могут помочь командам безопасности эффективно распределять ресурсы для внесения исправлений или устранения последствий.

Обнаружение и предотвращение вторжений – применение алгоритмов искусственного интеллекта и машинного обучения – могут анализировать структуру сетевого трафика, системные журналы и поведение пользователей для обнаружения аномалий и выявления потенциальных киберугроз. Модели машинного обучения могут учиться на исторических данных, чтобы распознавать известные шаблоны атак и отмечать подозрительные действия, помогая обнаруживать и предотвращать вторжения.

Обнаружение фишинга – анализ содержимого электронной почты, URL-адресов и выполнение других функций на основе использования модели машинного обучения в целях выявления и блокировки фишинговых писем и спама. Изучая закономерности в больших наборах данных об известных попытках фишинга, алгоритмы машинного обучения могут выявлять подозрительные индикаторы и помогать защищать пользователей от фишинговых атак.

Обнаружение мошенничества – применение модели искусственного интеллекта и машинного обучения для обнаружения мошеннических действий в различных областях, включая финансовые транзакции, онлайн-покупки и кражу личных данных. Алгоритмы машинного обучения могут изучать модели мошеннического поведения на основе исторических данных и применять эти знания для выявления подозрительных транзакций или действий в режиме реального времени.

Обнаружение вредоносного ПО – алгоритмы машинного обучения могут анализировать характеристики файлов, сетевой трафик и модели поведения для выявления и классификации вредоносного ПО. Модели машинного обучения можно обучать на больших наборах данных известных образцов вредоносного ПО для разработки точных систем обнаружения вредоносного ПО.

Аналитика угроз – алгоритмы искусственного интеллекта и машинного обучения извлекают ценную информацию об угрозах, анализируя огромные объемы данных из множества цифровых источников, включая коммерческие каналы угроз, информацию об угрозах из открытых источников, платформ социальных сетей и форумов в даркнете. Методы машинного обучения позволяют автоматизировать обработку, категоризацию и корреляцию данных об угрозах, чтобы предоставить полезную информацию для проактивной защиты.

Охота за угрозами: методы искусственного интеллекта и машинного обучения можно использовать для автоматизации анализа данных с целью выявления закономерностей, аномалий и индикаторов компрометации. Используя эти технологии, группы безопасности могут активно обнаруживать и смягчать потенциальные угрозы, уменьшать количество ложных срабатываний и сосредоточивать свои усилия на расследовании высокоприоритетных рисков, укрепляя общую кибербезопасность.

Сетевая безопасность и анализ трафика – методы искусственного интеллекта и машинного обучения могут анализировать журналы сетевого трафика для обнаружения необычных или вредоносных действий, таких как распределенные атаки типа «отказ в обслуживании» (DDoS) или сетевые вторжения, обнаруживая аномалии, указывающие на потенциальные инциденты безопасности.

Аналитика поведения пользователей и объектов – методы искусственного интеллекта и машинного обучения можно использовать для выявления потенциальных внутренних угроз или аномальных действий путем анализа поведения пользователей, шаблонов доступа и контекстных данных. Изучая типичное поведение и обнаруживая отклонения, указанные системы могут отмечать подозрительные действия пользователя для дальнейшего расследования.

IV. Проблемы и особенности внедрения анализируемых систем

Несмотря на значительные преимущества в области кибербезопасности, предлагаемые искусственным интеллектом и машинным обучением, их внедрение не лишено проблем и особенностей. Решение этих проблем имеет важное значение для обеспечения эффективности, надежности и этичности использования ИИ и машинного обучения в кибербезопасности: начиная состязательными атаками и предвзятостью в системах ИИ и заканчивая проблемами объяснимости и интерпретируемости, а также вопросами конфиденциальности и безопасности данных.

Состязательные атаки

Поскольку системы искусственного интеллекта и машинного обучения становятся неотъемлемыми компонентами кибербезопасности, появление состязательных атак представляет собой серьезную проблему [9]. Состязательные атаки используют уязвимости в моделях машинного обучения, вводя тщательно обработанные входные данные, которые обманывают процесс принятия решений системой. Эти вредоносные входные данные могут привести к неправильной классификации, обходу алгоритмов обнаружения или даже поставить под угрозу целостность всей системы. Понимание природы состязательных атак и разработка надежной защиты от них имеет первостепенное значение для обеспечения устойчивости и надежности систем кибербезопасности на базе искусственного интеллекта.

Предвзятость в системах искусственного интеллекта

Несмотря на огромный потенциал повышения кибербезопасности, наличие предвзятости в процессах принятия решений является серьезной проблемой [10]. Предвзятость может возникать из различных источников, включая предвзятые данные обучения, предвзятые алгоритмы или предвзятую интерпретацию результатов. В сфере кибербезопасности предвзятые системы ИИ могут привести к дискриминационным результатам, неравному обращению или игнорированию определенных типов угроз. Устранение и смягчение предвзятости в системах искусственного интеллекта имеет важное значение для обеспечения справедливости, равенства и беспристрастного принятия решений, гарантируя, что решения по кибербезопасности будут служить всем пользователям и защищать от широкого спектра угроз, не увековечивая существующие предвзятости или неравенство.

Объяснимость и интерпретируемость моделей машинного обучения

Поскольку системы искусственного интеллекта становятся все более сложными и изощренными, понимание обоснования их решений становится все труднее [11]. Отсутствие прозрачности вызывает обеспокоенность по поводу доверия, подотчетности и способности выявлять потенциальные уязвимости или предвзятости в моделях. Обеспечение объяснимости и интерпретируемости моделей машинного обучения имеет решающее значение для специалистов по кибербезопасности, поскольку они позволяют понять обоснование результатов работы системы, проверить ее эффективность и устранить любые непредвиденные последствия или ошибки. Повышая объяснимость и интерпретируемость, организации могут укрепить доверие к системам искусственного интеллекта, улучшить сотрудничество между людьми и машинами и способствовать более эффективному принятию решений в контексте кибербезопасности.

Конфиденциальность и безопасность данных

Использование чувствительных и конфиденциальных данных для обучения и развертывания моделей ИИ может принести значительную пользу, хотя и создает потенциальные риски, включая несанкционированный доступ, утечку данных или неправомерное использование личной информации [12]. Кроме того, необходимо найти баланс между сбором и использованием соответствующих данных для эффективных мер кибербезопасности при соблюдении правил конфиденциальности и этических соображений. Поиск правильного баланса между защитой конфиденциальности данных и обеспечением надежных мер безопасности на протяжении всего жизненного цикла искусственного интеллекта и машинного обучения имеет решающее значение для укрепления доверия и защиты конфиденциальной информации отдельных лиц, но также является серьезной проблемой, которую необходимо преодолеть.

V. Выводы

Искусственный интеллект и машинное обучение продолжают расширять границы кибербезопасности, открывая путь к захватывающим достижениям и возможностям. Будущее обещает автономные системы кибербезопасности, которые развиваются и обучаются, становясь более устойчивыми с каждой атакой. Искусственный интеллект и машинное обучение составят основу сетей «самовосстановления» – систем, способных выявлять, защищать и устранять ущерб от кибератак без вмешательства человека. Более того, искусственный интеллект и машинное обучение будут играть ключевую роль в поиске угроз, помогая специалистам по кибербезопасности в превентивном выявлении угроз. Вместо того, чтобы реагировать на нарушения, системы безопасности будут предвидеть и нейтрализовывать угрозы, формируя проактивную среду кибербезопасности.

Хотя искусственный интеллект и машинное обучение в сфере кибербезопасно-

сти открывают потенциал для обеспечения большей защиты от угроз и устойчивости, их применение наверняка откроет новые проблемы. В частности, пристального внимания требуют этические соображения, опасения по поводу автоматизированных систем, а также угроза вредоносного ПО на базе искусственного интеллекта и все более сложных кибератак. В конце концов, ключевым моментом станет баланс между мощью технологий и мудростью человеческого контроля. Будущее кибербезопасности – это не только создание более мощной защиты; речь идет о создании более умных систем защиты информации.

Примечание

1. Частикова В.А., Козачек К.В., Гуляй В.Г. Методы обработки естественного языка в решении задач обнаружения атак социальной инженерии // Вестник Адыгейского государственного университета. Сер.: Естественно-математические и технические науки. 2021. Вып. 4 (291). С. 95–108. URL: http://vestnik.adygnet.ru

2. Черниговский А.В., Кривов М.В. Нейронные сети как инструмент анализа сетевого трафика // Вестник Ангарского государственного технического университета. 2019. № 13. С. 151-157. DOI: 10.36629/2686-777x-2019-1-13-151-157

3. Берешполов И.С., Кравченко Ю.А., Слепцов А.Г. Алгоритм кластеризации данных для защиты конфиденциальной информации в сети Интернет // Известия ЮФУ. Технические науки. 2023. № 3 (233). С. 74-85. DOI: 10.18522/2311-3103-2023-3-74-85

4. Топольский Н.Г., Вилисов В.Я. Методы, модели и алгоритмы в системах безопасности: машинное обучение, робототехника, страхование, риски, контроль. Москва: ООО «Издательский Центр РИОР», 2021. 475 с. DOI: 10.29039/02072-2

5. Запечников С.В. Модели и алгоритмы конфиденциального машинного обучения // Безопасность информационных технологий. 2020. Т. 27, № 1. С. 51-67. DOI: 10.26583/bit.2020.1.05

6. Менисов А.Б. Технологии искусственного интеллекта и кибербезопасность: монография. Москва: Ай Пи Ар Медиа, 2022. 133 с.

7. Запечников С.В. Информационная безопасность, искусственный интеллект, системы распределенного реестра: достижения, проблемы, перспективы // Вестник современных цифровых технологий. 2023. № 14. С. 20-28.

8. Аветисян А.И. Кибербезопасность в контексте искусственного интеллекта // Вестник Российской академии наук. 2022. Т. 92, № 12. С. 1119-1123. DOI: 10.31857/S0869587322120039

9. Ложников П.С., Сулавко А.Е. Защищенное исполнение нейросетевых алгоритмов искусственного интеллекта: актуальность проблемы и перспективные решения // Региональная информатика и информационная безопасность: сб. тр. XII Санкт-Петербургской межрегион. конф. Санкт-Петербург, 27–29 ноября 2021 года. Санкт-Петербург: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2021. Вып. 10. С. 104-108.

10. Егоров А.А. Стандартизация по Искусственному интеллекту в промышленности (обзор зарубежного состояния). Ч. 2 // Автоматизация и IT в энергетике. 2023. № 1 (162). С. 6–19.

11. Основы цифровой экономики / Е.А. Деркачева, К.А. Карташов, Т.И. Козюбро [и др.]; Кубанский гос. технол. ун-т, Волгодонский инженерно-техн. ин-т (филиал) Национального исслед. ядерного ун-та «МИФИ», АНО «Международная ассоциация ученых, преподавателей и специалистов». Краснодар: Новация, 2021. 422 с.

12. Бижоев Б.М., Иванов С.А., Обаляева Ю.И. Цифровые технологии и сферы их применения. Москва: Изд-во Рос. гос. социального ун-та, 2021. 160 с.

References

1. Chastikova V.A., Kozachek K.V., Gulyay V.G. Methods of natural language processing in solving problems of detecting social engineering attacks // The Bulletin of the Adyghe State University. Ser.: Natural-Mathematical and Technical Sciences. 2021. Iss. 4 (291). P. 95–108. URL: http://vestnik.adygnet.ru

2. Chernigovsky A.V., Krivov M.V. Neural networks as an instrument of analysis of network traffic // Bulletin of Angarsk State Technical University. 2019. No. 13. P. 151–157. DOI: 10.36629/2686-777x-2019-1-13-151-157

3. Bereshpolov I.S., Kravchenko Yu.A., Sleptsov A.G. Data clustering algorithm for protecting confidential information on the Internet // News of the Southern Federal University. Engineering Sciences. 2023. No. 3 (233). P. 74–85. DOI: 10.18522/2311-3103-2023-3-74-85

4. Topolsky N.G., Vilisov V.Ya. Methods, models and algorithms in security systems: machine learning, robotics, insurance, risks, control. Moscow: RIOR Publishing Center LLC, 2021. 475 p. DOI: 10.29039/02072-2

5. Zapechnikov S.V. Models and algorithms for privacy-preserving machine learning // Security of Information Technologies. 2020. Vol. 27, No. 1. P. 51–67. DOI: 10.26583/bit.2020.1.05

6. Menisov A.B. Artificial intelligence technologies and cybersecurity: monograph. Moscow: IPR Media, 2022. 133 p.

7. Zapechnikov S.V. Information security, artificial intelligence, distributed ledgers: achievements, problems, prospects // Bulletin of Modern Digital Technologies. 2023. No. 14. P. 20–28.

8. Avetisyan A.I. Cybersecurity in the context of artificial intelligence // Bulletin of the Russian Academy of Sciences. 2022. Vol. 92, No. 12. P. 1119–1123. DOI: 10.31857/S0869587322120039

9. Lozhnikov P.S., Sulavko A.E. Secure execution of neural network algorithms of artificial intelligence: relevance of the problem and promising solutions // Regional informatics and information security: coll. of proceedings of the 12th St. Petersburg Interregion conf. St. Petersburg, November 27–29, 2021. St. Petersburg: Regional public organization “St. Petersburg Society of Informatics, Computer Science, Communication and Control Systems”, 2021. Vol. 10. P. 104–108.

10. Egorov A.A. Standardization of artificial intelligence in industry (review of the foreign state). Part 2 // Automation and IT in the Energy Sector. 2023. No. 1 (162). P. 6–19.

11. Fundamentals of digital economics / E.A. Derkacheva, K.A. Kartashov, T.I. Kozyubro [et al]; Kuban State Technol. University, Volgodonsk Engineering and Technol. Institute (branch) of the MIFI National Research Nuclear University, ANO International Association of Scientists, Teachers and Specialists. Krasnodar: Novatsiya, 2021. 422 p.

12. Bizhoev B.M., Ivanov S.A., Obalyaeva Yu.I. Digital technologies and areas of their application. Moscow: Publishing House of Russian State Social University, 2021. 160 p.

Авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 01.09.2023; *одобрена после рецензирования 15.09.2023*; *принята к публикации 16.09.2023*.

The authors declare no conflicts of interests.

The article was submitted 01.09.2023; *approved after reviewing 15.09.2023*; *accepted for publication 16.09.2023*.