Обзорная статья
УДК 004.85:004.056+519.687.1
ББК 16.63+32.972.133
О-14
DOI: 10.53598/2410-3225-2023-4-336-51-59

Обзор использования технологий машинного обучения в обеспечении информационной безопасности данных: настоящее и будущее

(*Рецензирована*)

Асият Капланoвна Доргушаова[1], Виталий Анатольевич Довгаль[2], Наталья Шумафовна Козлова[3], Роман Сергеевич Козлов[4]

[1, 3, 4] *Майкопский государственный технологический университет, Майкоп, Россия*
[2] *Майкопский государственный технологический университет, Адыгейский государственный университет, Майкоп, Россия*
[1] *asdor81@mail.ru*
[2] *urmia@mail.ru*
[3] *natali20052001@bk.ru*
[4] *roma.kozlov.71@mail.ru*

Аннотация. *В данной статье проводится обзор современных технологий машинного обучения в контексте обеспечения информационной безопасности данных. Рассматриваются основные направления использования методов машинного обучения, такие как анализ аномального поведения, прогнозирование угроз, идентификация и аутентификация. Представлены конкретные технические решения, анализ их эффективности, сложности, текущие тренды и перспективы развития технологий машинного обучения в области информационной безопасности данных. Представленные результаты могут быть полезны как специалистам в области информационной безопасности, так и исследователям в области машинного обучения.*

Ключевые слова: *машинное обучение, информационная безопасность, технологии, большие данные, защита, методы машинного обучения, технические решения, угрозы*

Для цитирования: *Обзор использования технологий машинного обучения в обеспечении информационной безопасности данных: настоящее и будущее / А. К. Доргушаова, В. А. Довгаль, Н. Ш. Козлова, Р. С. Козлов // Вестник Адыгейского государственного университета. Сер. : Естественно-математические и технические науки. 2024. Вып. 1* (*336*)*. С. 51–59. DOI: 10.53598/2410-3225-2024-1-336-51-59*

Review Paper

A survey of the use of machine learning technologies in providing information security of data: present and future

Asiyat K. Dorgushaova[1], Vitaliy A. Dovgal[2], Natalya Sh. Kozlova[3], Roman S. Kozlov[4]

[1, 3, 4] *Maikop State Technological University, Maykop, Russia*
[2] *Maikop State Technological University, Adyghe State University, Maykop, Russia*
[1] *asdor81@mail.ru*
[2] *urmia@mail.ru*
[3] *natali20052001@bk.ru*
[4] *roma.kozlov.71@mail.ru*

Abstract. *This article reviews modern machine learning technologies in the context of ensuring information security of data. The main directions of using machine learning methods, such as*

analysis of anomalous behavior, threat prediction, identification and authentication are considered. Specific technical solutions, analysis of their effectiveness, complexity, current trends and prospects for the development of machine learning technologies in the field of information security of data are presented. The presented results can be useful both for information security specialists and researchers in the field of machine learning.

Keywords: *machine learning, information security, technologies, big data, protection, machine learning methods, technical solutions, threats*

For citation*: A survey of the use of machine learning technologies in providing information security of data: present and future / A. K. Dorgushaova, V. A. Dovgal, N. Sh. Kozlova, R. S. Kozlov // The Bulletin of the Adyghe State University. Ser. : Natural-Mathematical and Technical Sciences. 2024. Iss. 1 (336). P. 51–59. DOI: 10.53598/2410-3225-2024-1-336-51-59*

В современном мире информационная безопасность данных играет ключевую роль для организаций и частных лиц. С постоянным увеличением объемов информации и разнообразием угроз, связанных с ее сохранностью, важно применять эффективные защитные инструменты, обеспечивающие конфиденциальность и целостность используемых предприятиями и организациями данных, среди которых в последние десятилетия ярко выделяются технологии машинного обучения, автоматизирующие процессы обнаружения информационных угроз и предотвращения инцидентов ранее неиспользуемыми способами за счет анализа аномального поведения.

Актуальность представленного исследования состоит в анализе существующих технологий машинного обучения (МО) и возможности применения их для обеспечения информационной безопасности. Кроме того, в статье рассмотрены не только основные области применения машинного обучения, но и представлены конкретные технические решения, а также проанализирована их эффективность, показаны сложные аспекты их внедрения в практическую деятельность.

Машинное обучение – один из последних успешных трендов в области искусственного интеллекта, активно внедряемый во многие отрасли, где требуется обработка больших объемов данных, включая обеспечение информационной безопасности массивов данных, часто имеющих конфиденциальный характер [1]. Появление новых возможностей для обеспечения безопасности информации, равно как и построение эффективных инструментов ее защиты, привели к массовому внедрению развивающихся технологий машинного обучения, позволяющих автоматизировать процессы обнаружения и предотвращения угроз безопасности данных, что в конечном итоге делает МО одной из ключевых областей искусственного интеллекта, привлекающей все большее внимание исследователей, инженеров и предпринимателей.

Появление огромных объемов данных, обусловленных законом экспоненциального роста объема знаний и связанного с этим ростом вычислительных мощностей, значительно расширяет возможности машинного обучения, от которых в будущем можно ожидать новых перспективных методов усиления защиты данных. Как пример – использование глубокого обучения как многообещающей технологии машинного обучения позволяет совершенствовать сложные модели информационной безопасности за счет способности эффективно распознавать новые угрозы данным. Кроме того, за счет автоматизации процессов обнаружения и предотвращения информационных угроз машинное обучение улучшит качество технической поддержки сложных алгоритмов обучения, что является важным для специалистов-аналитиков, которые смогут повысить скорость реагирования на изменяющиеся условия внешней среды, позволяя высвободить время для построения масштабных тактических систем безопасности [2].

В целом, существует несколько типов машинного обучения, классификация которых показана на рисунке 1 [3].

Каждый из перечисленных типов машинного обучения выполняет определенные задачи и является актуальным для применения в той или иной сфере бизнеса [4].

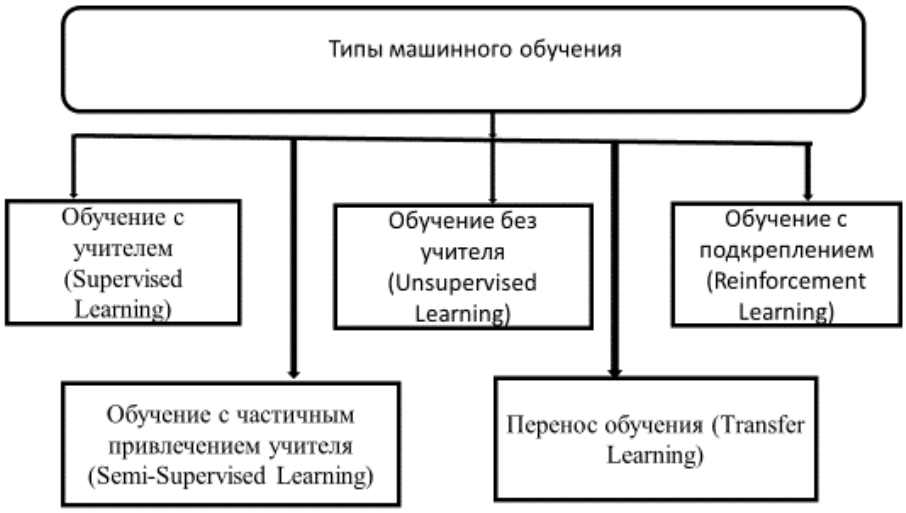

Рис. 1. Классификация типов машинного обучения

Fig. 1. Classification of machine learning types

1. Обучение с учителем (Supervised Learning) – тип машинного обучения, применение алгоритмов которого позволяет решать задачи классификации, регрессии и детекции аномалий информационных процессов, в силу чего считается одним из самых популярных. В целом, обучение с учителем используется для прогнозирования результатов, анализа данных и принятия решений в сфере медицины, финансов, маркетинга и других отраслях, которые так или иначе используют собранные данные.

2. Обучение без учителя (Unsupervised Learning) – тип машинного обучения, традиционно играющий важную роль там, где сложно привлечь эксперта к обработке больших объемов данных, извлечь из данных новую информацию и выявить скрытые взаимосвязи на наборах неразмеченных данных без контроля со стороны пользователя. Такие сферы, как биоинформатика, финансы и Интернет-маркетинг, часто требуют кластеризовать данные, снизить их размерность, установить новые ассоциативные правила, что является хорошим сценарием применения обучения без учителя, помогая выявлять новые тенденции и паттерны.

3. Обучение с подкреплением (Reinforcement Learning) – тип машинного обучения, являющийся актуальным для приложений игровой индустрии, автономных систем и робототехники. Агенты, способные самостоятельно обучаться и принимать оптимальные решения на основе получаемого вознаграждения, находят применение в различных областях – от финансов до транспорта.

4. Обучение с частичным привлечением учителя (Semi-Supervised Learning) – эффективное решение для построения моделей с высокой точностью в условиях недостатка размеченных данных. Применение указанных методов в медицине, анализе текстов и изображений позволяет улучшить результаты классификации и предсказания.

5. Перенос обучения (Transfer Learning) – актуальный вид МО для все более применяемых огромных наборов данных и глубоких нейронных сетей. Перенос обучения из одной задачи в другую позволяет существенно ускорить процесс обучения и повысить точность моделей.

Актуальные типы машинного обучения играют ключевую роль в различных сферах деятельности – от науки до бизнеса [5]. Понимание особенностей каждого типа машинного обучения и их применение в конкретных задачах позволяет создавать инновационные решения и повышать эффективность деятельности в различных отраслях. Дальнейшие исследования в области применения машинного обучения в информационной безопасности могут привести к разработке более эффективных и надежных тех-

нических решений.

Для обеспечения безопасности данных наиболее часто используются следующие методы машинного обучения (рис. 2):

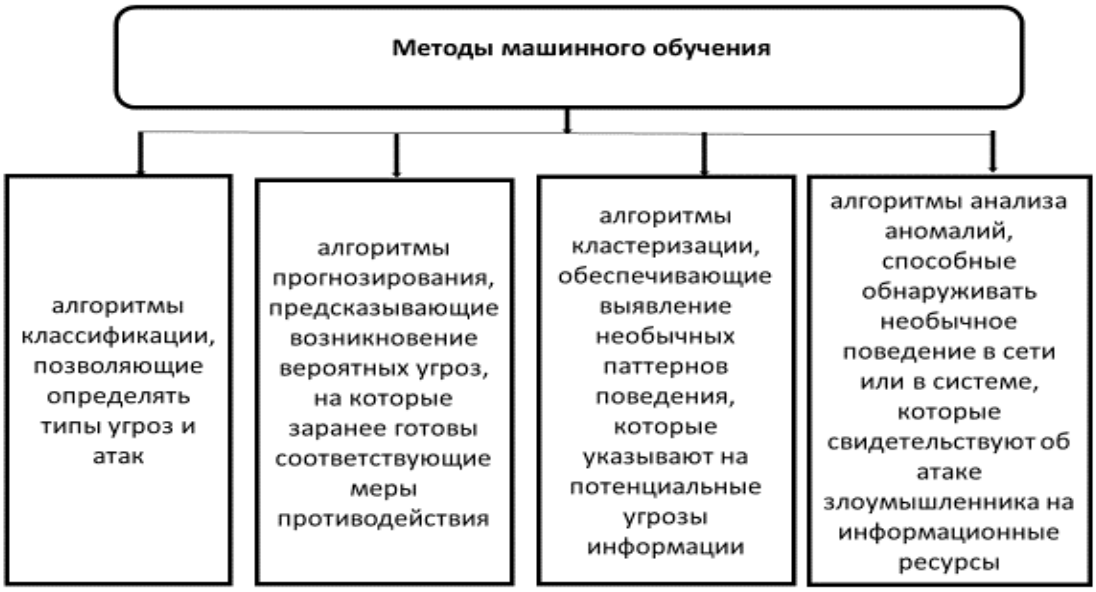

Рис. 2. Методы машинного обучения
Fig. 2. Machine learning methods

Методы машинного обучения занимают ключевое место в обеспечении безопасности данных, позволяя компаниям и организациям оперативно обнаруживать угрозы и реагировать на них. Взаимодействие традиционных методов защиты данных с интеллектуальными алгоритмами машинного обучения обещает создать более надежные и адаптивные системы безопасности в будущем. Опишем основные методы и технические решения, в которых применяется машинное обучение в области информационной безопасности [4].

1. *Анализ логов*. В сфере информационной безопасности машинное обучение широко применяется для анализа журналов регистрации (логов) с целью выявления аномалий и предсказания возможных инцидентов безопасности. Лог-файлы могут содержать данные о работе информационной системы, начиная от действий пользователей до событий в сети, анализ которых помогает выявить потенциальные угрозы и предотвратить возможные атаки.

Автоматизация анализа логов возможна посредством технологии машинного обучения, когда обработка больших объемов данных позволяет выявить скрытые паттерны. Алгоритмы обучения без наблюдения позволяют осуществить кластеризацию регистрационных записей и выявить аномальное поведение системы, что, в свою очередь, может говорить о наличии вредоносных действий или несанкционированного доступа.

Обучаясь на данных о событиях и инцидентах безопасности, полученных из журналов регистрации (логов), машинное обучение дает возможность с определенной вероятностью прогнозировать инциденты информационной безопасности. Для нахождения вероятности возникновения инцидентов модели используют данные, поступающие в хронологическом порядке, и делаются соответствующие выводы. В результате специалисты информационной безопасности могут принимать меры по защите до возникновения реального инцидента.

В пользу глубокого машинного обучения по данным регистрационных журналов говорят примеры. В частности, такой пример приведен в работе [6], где Beeplog анали-

зирует разнородные данные журналов Hadoop или OpenStack в лабораторных условиях, позволяя с вероятностью близкой к 100 % предсказывать опасности после обучения только на 1 % доступных данных.

2. *Системы обнаружения вторжений* (*IDS – Intrusion Detection Systems*). Данные системы анализируют сетевой трафик и поведение пользователей при работе с сетью. При этом выявляются аномальные действия, указывающие на потенциальные угрозы. Примером такой системы является PT Network Attack Discovery поведенческого анализа сетевого трафика (network traffic analysis, NTA) российской компании Positive Technologies. Этот инструмент обнаруживает вредоносную активность злоумышленников на периметре и внутри сети, в том числе в зашифрованном трафике. Кроме этого, «Система мониторинга безопасности СБИС», разработанная там же, представляет собой интегрированное средство, основанное на алгоритмах машинного обучения для обнаружения вторжений и аномалий в сети. Система обладает способностью адаптации к изменяющимся условиям безопасности. Основной недостаток – это возможность ложных срабатываний, которые требуют дополнительной настройки.

3. *Защита от фишинга*. Приведем пример работы этой технологии от Лаборатории Касперского. Она реализуется на базе двух алгоритмов машинного обучения, которые анализируют различные элементы сообщений. При этом автоматически обнаруживается и блокируется фишинг без ложных срабатываний. Первый алгоритм (алгоритм глубокого обучения для обнаружения троянского (спам) программного обеспечения (ПО)) – при нахождении классификатора в облачном сервисе, к которому подключаются при установке на устройство пользователя. Он обрабатывает заголовки электронной почты, используя глубокую нейронную сеть для обнаружения признаков троянского (спаммер) ПО, которое автоматически генерирует и отправляет массовые сообщения. Второй классификатор (алгоритм машинного обучения для обнаружения контекста фишинга) работает на компьютере клиента и определяет фишинговый словарь в теле сообщения. Классификатор основан на глубокой нейронной сети. Он регулярно обучается на основе сотен миллионов записей метаданных – заголовков, полученных из статистики спам-сообщений, обнаруженных продуктами «Лаборатории Касперского». Нейронные сети извлекают из статистики нетривиальные особенности для обнаружения подозрительных заголовков в электронном письме. В период обучения модель анализирует множество примеров фишинговых писем: разбивает их на отдельные фразы и присваивает каждой фразе вес в зависимости от ее потенциальной фишинговой активности или того, насколько она распространена среди фишинговых сообщений. Недостаток таких систем заключается в необходимости постоянного обновления моделей и данных для более точных прогнозов.

4. *Технология анализа поведения пользователей с применением машинного обучения*. Такие системы анализируют обычное поведение пользователей и выявляют аномалии, которые могут указывать на потенциальные угрозы, такие как несанкционированный доступ к данным или утечки информации.

Примером такой системы является разработанная компанией Kaspersky Lab система анализа поведения пользователей [7]. Она применяет методы машинного обучения для выявления аномалий в поведении пользователей и своевременного обнаружения возможных угроз. Преимуществом данной системы является способность раннего обнаружения угроз, основанных на поведении пользователей, что позволяет предотвратить потенциальные инциденты безопасности.

Однако следует отметить, что сложность настройки подобных систем и возможные ложные срабатывания могут быть недостатками данного подхода. Необходимо проводить тщательную настройку алгоритмов машинного обучения, учитывая специфику работы организации и особенности поведения пользователей, чтобы минимизиро-

вать количество ложных срабатываний и обеспечить эффективную работу системы. Тем не менее, системы анализа поведения пользователей с применением машинного обучения остаются важным инструментом в области информационной безопасности, помогая организациям защищать свои данные и ресурсы от различных угроз и атак.

5. *Системы обучения пользователей основам информационной безопасности*. Машинное обучение может быть использовано для персонализации программ обучения пользователей по вопросам кибербезопасности. Анализируя индивидуальные данные о поведении пользователей, такие системы могут предлагать обучающие материалы и рекомендации, способствующие повышению осведомленности и ответственности пользователей в сфере информационной безопасности.

6. *Системы автоматизированного реагирования на угрозы*, использующие машинное обучение для автоматического реагирования на обнаружение угроз безопасности (например, блокирования доступа к определенным ресурсам или запуска процедур восстановления после инцидента). Преимуществом подобных решений является быстрая реакция на угрозы безопасности без необходимости человеческого вмешательства. Недостатком – возможность ошибок в принятии решений.

7. *Системы анализа аутентификации и идентификации*. Методы машинного обучения могут быть использованы для анализа биометрических данных, поведенческих шаблонов пользователей и других параметров аутентификации и идентификации. Применение таких решений позволяет создавать более надежные системы контроля доступа и идентификации пользователей, снижая риск несанкционированного доступа.

8. *Системы мониторинга и анализа активности пользователей*. Машинное обучение может быть применено для анализа активности пользователей в информационных системах, выявления аномальных действий или изменений в обычном поведении пользователей, что помогает оперативно обнаруживать потенциально опасные ситуации и предотвращать угрозы безопасности.

9. *Системы автоматизированного реагирования на обнаруженные угрозы* безопасности – за счет машинного обучения, применяемого для разработки алгоритмов автоматического реагирования, можно быстро и эффективно реагировать на инциденты безопасности (например, блокированием доступа к зараженным ресурсам или изоляцией уязвимых устройств).

10. *Системы прогнозирования угроз*. Методы машинного обучения могут быть использованы для анализа данных о предшествующих угрозах, трендах в кибербезопасности и других факторах, позволяющих прогнозировать будущие угрозы. Указанные системы способствуют выработке проактивных мер по обеспечению безопасности информационных систем.

Перечисленные методы и технические решения демонстрируют разнообразные способы применения машинного обучения в информационной безопасности, позволяют организациям и предприятиям эффективно защищать свои информационные ресурсы от различных угроз. Каждое решение имеет свои достоинства и недостатки, и выбор конкретного подхода зависит от определенных потребностей и целей организации.

Результаты исследований непрерывно проверяются и совершенствуются, чтобы повысить вероятность достижения конечной цели. Сочетание больших данных, систем искусственного интеллекта и машинного обучения способствует повышению уровня обеспечения защиты информации всех заинтересованных организаций за счет более эффективного анализа инцидентов безопасности и реагирования на них, снижения рисков и адаптации усиливающихся киберугроз [8].

Для визуализации различных направлений применения машинного обучения в информационной безопасности можно создать следующую схему (рис. 3) [1].

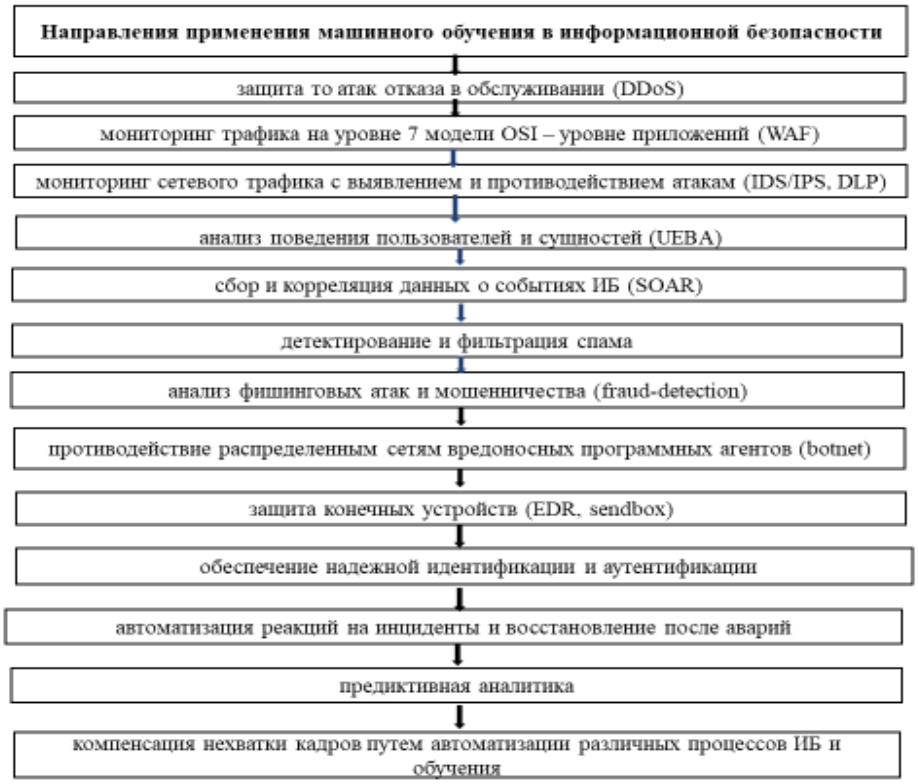

Рис. 3. Направления применения машинного обучения в информационной безопасности

Fig. 3. Directions for the application of machine learning in information security

Технические решения в области информационной безопасности, использующие технологии машинного обучения, играют ключевую роль в обеспечении защиты данных и сетей от угроз. Конкретные технические решения на основе машинного обучения демонстрируют высокую эффективность, однако их внедрение требует значительных усилий и затрат, поэтому применение машинного обучения в информационной безопасности – необходимость, без которой современную систему кибербезопасности представить невозможно [9].

Современные системы машинного обучения позволяют автоматизировать процессы обнаружения угроз, анализа аномального поведения и принятия мер по предотвращению инцидентов, что делает их неотъемлемой частью современных систем безопасности [10]. Применение машинного обучения в области безопасности предлагает многообещающие возможности для обнаружения аномалий и предотвращения угроз.

Существуют вызовы и проблемы, связанные с использованием технологий машинного обучения в области информационной безопасности данных. Например, необходимость постоянного обновления моделей машинного обучения в целях эффективного распознавания новых видов угроз. Также существует проблема интерпретируемости результатов работы алгоритмов машинного обучения, что затрудняет понимание принятых системой решений [3].

Таким образом, можно сделать следующие выводы:

1. Машинное обучение представляет собой мощный инструмент для обеспечения безопасности данных за счет возможности автоматизации процессов обнаружения и предотвращения угроз.

2. Различные методы машинного обучения, такие как нейронные сети, деревья решений и алгоритмы кластеризации, могут быть эффективно применены для анализа больших объемов данных и выявления аномалий.

3. Важно учитывать особенности конкретной среды и типы данных при выборе подходящего метода машинного обучения для обеспечения информационной безопасности.

4. Необходимо постоянно обновлять модели машинного обучения и обучать их на новых данных, чтобы эффективно бороться с появляющимися угрозами.

5. Дальнейшие исследования в области машинного обучения для информационной безопасности могут привести к разработке более точных и надежных систем защиты данных.

Эти выводы подчеркивают важность использования методов машинного обучения в области информационной безопасности и указывают на перспективы развития данной области.

Примечания

1. Клюева И. А. Современные возможности и примеры внедрения машинного обучения // Оригинальные исследования. 2021. Т. 11, № 7. С. 12–32.

2. Галимов Р. Г. Основы алгоритмов машинного обучения – обучение без учителя // Аллея науки. 2017. Т. 1, № 14. С. 807–809.

3. Аюб С. Аспекты интеллектуального анализа данных в бизнесе // Современные технологии в науке и образовании – СТНО-2022 : сб. тр. V Международного науч.-техн. форума, Рязань, 02–04 марта 2022 года : в 10 томах / под общ. ред. О. В. Миловзорова. Рязань : Рязанский государственный радиотехнический университет, 2022. Т. 4. С. 208–211.

4. Довгаль В. А. Анализ актуальных проблем в области кибербезопасности // Дистанционные образовательные технологии : сб. тр. VIII Междунар. науч.-практ. конф., Ялта, 19–21 сентября 2023 года. Симферополь : Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), Общество с ограниченной ответственностью «Издательство Типография "Ариал"», 2023. С. 337–340.

5. Доргушаова А. К., Бирюков И. А. Применение технологий искусственного интеллекта в экономике // Актуальные вопросы устойчивого развития современного общества и экономики : сб. науч. ст. Всерос. науч.-практ. конф., посвящ. Году культурного наследия народов России, Курск, 14–15 апреля 2022 года / Финансовый университет при Правительстве Российской Федерации, Курский филиал. Курск : Университетская книга, 2022. С. 78–81.

6. Deeplog: Anomaly detection and diagnosis from system logs through deep learning / Min Du, Feifei Li, Guineng Zheng, Vivek Srikumar // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017. P. 1285–1298.

7. Защита на основе анализа поведения. URL: https://www.kaspersky.ru/enterprise-security/wiki-section/products/behavior-based-protection (дата обращения: 12.02.2024).

8. Козлова Н. Ш., Довгаль В. А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности // Вестник Адыгейского государственного университета. Сер. : Естественно-математические и технические науки. 2023. Вып. 3 (326). С. 65–72. DOI: 10.53598/2410-3225-2023-3-326-65-72

9. Довгаль В. А., Козлова Н. Ш. Кибербезопасность и информационная безопасность: сходства и отличия // Вестник Адыгейского государственного университета. Сер. : Естественно-математические и технические науки. 2021. Вып. 3 (286). С. 88–97. DOI: 10.53598/2410-3225-2021-3-286-88-97

10. Созыкин А. В. Обзор методов обучения глубоких нейронных сетей // Вестник Южно-Уральского государственного университета. Сер. : Вычислительная математика и информатика. 2017. Т. 6, № 3. С. 28–59. DOI: 10.14529/cmse170303

References

1. Klyueva I. A. Modern opportunities and examples of machine learning implementation // Original research. 2021. Vol. 11, No. 7. P. 12–32.

2. Galimov R. G. The basics of machine learning algorithms – learning without a teacher // Alley of Science. 2017. Vol. 1, No. 14. P. 807–809.

3. Ayub S. Aspects of data mining in business // Modern technologies in science and education – STNO-2022 : collection of proceedings of the 5th International Scientific and Technical Forum, Ryazan, March 02–04, 2022 : in 10 volumes / general ed. by. O. V. Milovzorov. Ryazan : Ryazan

State Radio Engineering University, 2022. Vol. 4. P. 208–211.

4. Dovgal V. A. Analysis of current problems in the field of cybersecurity // Distance educational technologies : collection of proceedings of the 8th International scientific and practical conf., Yalta, September 19–21, 2023. Simferopol : St. Petersburg State Electrotechnical University "LETI" named after V. I. Ulyanov (Lenin), Limited Liability Company "Arial Printing House", 2023. P. 337–340.

5. Dorgushaova A. K., Biryukov I. A. Application of artificial intelligence technologies in economics // Current issues of sustainable development of modern society and economy : collection of scientific articles of All-Russian scientific and practical conf., dedicated to the Year of the Cultural Heritage of the Peoples of Russia, Kursk, April 14–15, 2022 / Financial University under the Government of the Russian Federation, Kursk branch. Kursk: Universitetskaya Kniga, 2022. P. 78–81.

6. Deeplog: Anomaly detection and diagnosis from system logs through deep learning / Min Du, Feifei Li, Guineng Zheng, Vivek Srikumar // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017. P. 1285–1298.

7. Behavior-based protection. URL: https://www.kaspersky.ru/enterprise-security/wiki-section/products/behavior-based-protection (access date: 12/02/2024).

8. Kozlova N. Sh., Dovgal V. A. Analysis of the use of artificial intelligence and machine learning in cybersecurity // The Bulletin of the Adyghe State University. Ser. : Natural-Mathematical and Technical Sciences. 2023. Iss. 3 (326). P. 65–72. DOI: 10.53598/2410-3225-2023-3-326-65-72

9. Dovgal V. A., Kozlova N. Sh. Cybersecurity and information security: similarities and differences // The Bulletin of the Adyghe State University. Ser. : Natural-Mathematical and Technical Sciences. 2021. Iss. 3 (286). P. 88–97. DOI: 10.53598/2410-3225-2021-3-286-88-97

10. Sozykin A. V. An Overview of methods for deep learning in neural networks // Bulletin of the South Ural State University. Ser. : Computational Mathematics and Software Engineering. 2017. Vol. 6, No. 3. P. 28–59. DOI: 10.14529/cmse170303

Авторы заявляют об отсутствии конфликта интересов.

The authors declare no conflicts of interests.

Статья поступила в редакцию 13.02.2024; *одобрена после рецензирования 23.02.2024*; *принята к публикации 24.02.2024*.

The article was submitted 13.02.2024; *approved after reviewing 23.02.2024*; *accepted for publication 24.02.22024*.