ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.85

DOI: 10.21822/2073-6185-2026-53-1-157-169 Обзорная статья/ Review article

Технологии искусственного интеллекта в решении задач информационной безопасности

Д.А. Потиенко, Д.С. Чмыхало, О.Л. Легонько
Донской государственный технический университет,
344003, г. Ростов-на-Дону, пл. Гагарина 1, Россия

Резюме. Цель. Целью исследования является анализ возможностей применения технологий искусственного интеллекта для решения задач информационной безопасности. **Метод.** Исследование основано на проактивном подходе, направленном на снижение негативного воздействия внутренних и внешних угроз; на принципах решения задач информационной безопасности, особенностях и возможностях интеллектуальных методов. **Результат.** Разработанный алгоритм внедрения технологий искусственного интеллекта в структуру системы информационной безопасности предприятия описывает основные этапы, которые необходимо пройти при построении интеллектуальных подсистем защиты информации. **Вывод.** Внедрение технологий искусственного интеллекта в сферу информационной безопасности позволит строить адаптивные интеллектуальные системы защиты информации, обеспечивающие оперативность реагирования на изменяющиеся угрозы, атаки и возникающие инциденты. Разработчикам и специалистам служб безопасности необходимо управление рисками, формирование принципов ответственности и прозрачности процессов функционирования интеллектуальных подсистем защиты информации.

Ключевые слова: информационная безопасность, защита информации, интеллектуальные технологии, искусственный интеллект, интеллектуальная система

Для цитирования: Д.А. Потиенко, Д.С. Чмыхало, О.Л. Легонько. Технологии искусственного интеллекта в решении задач информационной безопасности. Вестник Дагестанского государственного технического университета. Технические науки. 2026;53(1):157-169. DOI:10.21822/2073-6185-2026-53-1-157-169.

Artificial Intelligence Technologies in Solving Information Security Problems

D.A. Potienko, D.S. Chmykhalo, O.L. Legonko
Don State Technical University,
1Gagarin Square, Rostov-on-Don 344003, Russia

Abstract. Objective. The purpose of this study is to analyze the potential of artificial intelligence technologies for solving information security problems. **Method**. The study is based on a proactive approach aimed at reducing the negative impact of internal and external threats; on the principles of solving information security problems; and on the features and capabilities of intelligent methods. **Result.** The developed algorithm for implementing artificial intelligence technologies describes the key steps required to build intelligent information security subsystems. **Conclusion**. The implementation of artificial intelligence technologies will enable the development of adaptive, intelligent security systems that quickly respond to threats, attacks, and incidents. Security professionals must manage risks and establish principles of accountability and transparency in the operation of intelligent information security subsystems.

Keywords: information security, information protection, intelligent technologies, artificial intelligence, intelligent system.

For citation:D.A.Potienko, D.S.Chmykhalo, O.L.Legonko. Artificial Intelligence Technologies in Solving Information Security Problems. Herald of Daghestan State Technical University. Technical Sciences. 2026;53(1):157-169. (In Russ) DOI:10.21822/2073-6185-2026-53-1-157-169.

Введение. В условиях стремительного развития информационных технологий и цифровизации общества, вопросы обеспечения информационной безопасности становятся все более актуальными для руководителей различных предприятий и организаций вне зависимости от их области деятельности. Атаки на информационные инфраструктуры, утечки персональных данных и другой конфиденциальной информации представляют серьезные риски для предприятий и частных лиц [1]. Указ Президента РФ «О развитии искусственного интеллекта в Российской Федерации» устанавливает основные направления и цели государственной политики в области искусственного интеллекта, указывает на необходимость внедрения технологий искусственного интеллекта в различные сферы, в том числе в защиту информации [2]. Искусственный интеллект предлагает новые подходы к решению проблем защиты информации, позволяя автоматизировать процессы обнаружения и реагирования на угрозы. Изучение технологий искусственного интеллекта в контексте информационной безопасности имеет большое значение для повышения эффективности защиты информации, минимизации рисков, и, как следствие, уменьшения финансовых и других потерь для предприятий.

Постановка задачи. Цель исследования заключается в анализе возможностей применения технологий искусственного интеллекта для решения задач информационной безопасности. Для достижения цели изучены существующие технологии искусственного интеллекта, определены области информационной безопасности, которые нуждаются в разработке эффективных способов решения задач, сформулированы рекомендации по внедрению технологий искусственного интеллекта в практику защиты информации. Важным представляется выполнение анализа потенциальных проблем, связанных с использованием интеллектуальных систем. Ключевыми вопросами информационной безопасности являются предотвращение утечки информации и несанкционированных воздействий на защищенную информацию, что определено в соответствии с ГОСТ Р 50922-2006 [3].

Информационная безопасность включает методы и действия, направленные на защиту конфиденциальной информации, например, такой как персональные данные, коммерческая тайна, интеллектуальная собственность. Основными задачами являются обеспечение целостности данных и доступность информации для пользователей с установленными правами доступа [4]. Для минимизации затрат руководство предприятия должно реализовать процессы управления инцидентами информационной безопасности [5]. Регулярное обновление программного обеспечения и мониторинг сетевого трафика позволяют выявлять уязвимости и предотвращать атаки [6]. Очень важным представляется этап обучения сотрудников основам информационной безопасности, принципам работы с конфиденциальной информацией и техническими средствами защиты информации. Это позволяет сократить количество инцидентов информационной безопасности, которые могут привести к утечке или модификации данных, уменьшить влияние человеческого фактора на уровень защищенности информационных ресурсов. Организационные меры защиты, включая разработку политики безопасности, соблюдение законодательных норм и стандартов, касающихся защиты предприятий от юридических рисков [7]. Постоянное совершенствование методов несанкционированного получения информации (вирусное программное обеспечение, фишинговые атаки), сложность современных информационных систем, которая делает их более уязвимыми к атакам, развитие таких технологий, как облачные вычисления и интернет-вещей, приводят к тому, что добиться требуемого уровня защищенности информационных ресурсов возможно только при условии создания комплексной системы защиты и своевременной модификации методов и средств защиты.

Эффективная защита требует проактивного подхода, направленного на снижение негативного воздействия внутренних и внешних угроз. Однако для многих предприятий является актуальной проблема финансирования для внедрения мер безопасности остается. Инвестиции в безопасность могут показаться высокими, но они необходимы для защиты информации и предотвращения серьезных последствий. Предприятия должны рассматривать информационную безопасность как приоритетную задачу, решение которой позволит

минимизировать риски и возможные потери. Решение проблем защиты информации требует комплексного подхода и стратегического планирования.

Методы исследования. Одним из перспективных направлений является внедрение технологий искусственного интеллекта в практику защиты информации [8]. Потенциально это позволит реализовать анализ больших объемов данных в реальном времени, с целью выявления аномалий и подозрительного поведения пользователей, обеспечит значительное сокращение времени реагирования на инциденты. Алгоритмы машинного обучения способны обучаться на исторических данных, что позволит им лучше распознавать потенциальные угрозы, и повысит точность обнаружения атак. Искусственный интеллект обладает способностью адаптироваться к новым данным, посредством дообучения в процессе выполнения пользователями обновления моделей и реализации процедур обучения.

Термин «искусственный интеллект» появился в начале 60-х годов XX в. [9]. Искусственный интеллект фокусируется на создании машин, способных выполнять задачи, требующие человеческого интеллекта [10]. Это включает обработку естественного языка, распознавание образов и принятие решений.

Интеллектуальная система - это информационно-вычислительная система, обладающая способностью к накоплению, анализу больших массивов информации, модификации знаний на основе полученной информации, принятию решений в условиях неопределенности, адаптации, самообучения, самоорганизации [11]. Интеллектуальная система способна действовать целенаправленно, используя логические выводы и алгоритмы. Как правило, интеллектуальные системы рассматриваются в контексте управления и оптимизации процессов и могут интегрироваться в различные сферы деятельности человека, от медицины до промышленности.

Технологии искусственного интеллекта - это множество методов, позволяющих машинам выполнять задачи, требующие интеллекта, аналогичного человеческому. Эти методы, применяются для решения широкого спектра задач, включая автоматизацию процессов, анализ данных и взаимодействие с пользователями. Согласно Указа Президента РФ, технологии искусственного интеллекта представляют собой совокупность технологий, включающую компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта [2].

Компьютерное зрение - это область, занимающаяся анализом и интерпретацией визуальной информации с помощью алгоритмов искусственного интеллекта [12]. Технологии компьютерного зрения применяются для распознавания объектов и лиц на изображениях и видео, что особенно необходимо в таких сферах как информационная и национальная безопасность, медицина и автомобильная промышленность.

Обработка естественного языка представляет собой технологию искусственного интеллекта, реализация которой позволяет компьютерной системе понимать и генерировать тексты на естественных языках [13]. Обработка естественного языка применяется в таких областях, как чат-боты, системы перевода и голосовые помощники. Распознавание и синтез речи - это технология искусственного интеллекта, позволяющая преобразовать речевые сигналы в текстовую информацию - распознавание речи, и, наоборот, создать речевой сигнал из текстовых данных - синтез речи [14], широко применяются в голосовых помощниках, системах автоматического перевода и интерфейсах для слабовидящих.

Интеллектуальная поддержка принятия решений использует методы искусственного интеллекта для анализа исходных данных, выявления закономерностей и формирования рекомендаций для пользователя [15]. Такие системы помогают специалистам принимать более обоснованные и быстрые решения в сложных ситуациях, минимизируя человеческий фактор. Понятие перспективных методов искусственного интеллекта приводится в Указе Президента РФ: это методы, направленные на создание принципиально новой научно-технической продукции, в том числе в целях разработки универсального (сильного) искусственного интеллекта [2]. Исследователи, занимающиеся развитием теории искусственного

интеллекта и внедрением его в различные области деятельности, используют классификацию, в соответствии с которой выделяется три вида искусственного интеллекта, в зависимости от его функциональных возможностей: узкий (слабый) (Artificial Narrow Intelligence, ANI), общий (сильный) (Artificial General Intelligence, AGI) и суперсильный (Artificial Super Intelligence, ASI) [16, 17]. Слабый искусственный интеллект ориентирован на интеллектуальное выполнение конкретных задач, и функционирует в рамках заранее сформированного набора правил. Сильный искусственный интеллект обладает способностью к самостоятельному обучению и решению различных задач, а также имеет самосознание. Суперсильный искусственный интеллект представляет собой теоретически возможный искусственный интеллект, который превосходит человеческий, способен к решению сложных проблем, мышлению, эмоциям. В настоящее время реализован только слабый искусственный интеллект, который, как правило, разделяют на два вида: традиционный и генеративный. Разделение, в большей степени, связано с появлением генеративных моделей искусственного интеллекта. В одной из первых работ, посвященных этой тематике, авторы предлагают новый алгоритм машинного обучения без учителя, основанный на использовании двух искусственных нейронных сетей, между которыми происходит состязательный процесс, заключающийся в том, что одна сеть генерирует образы, а другая - отделяет правильные образы от неправильных [18]. Такая модель получила название генеративно-состязательная сеть (Generative Adversarial Network, GAN). Примером генеративного искусственного интеллекта является ChatGPT. Отличительной чертой генеративного искусственного интеллекта от традиционного является его возможность создавать новые тексты, изображения, аудио- и видеоинформацию. Интеллектуальные системы, построенные на основе традиционного искусственного интеллекта, эффективно используются для анализа данных и составления прогнозов - это голосовые помощники, рекомендательные и поисковые системы. Они обучены следовать заданным правилам и выполнять определенную работу, но они не создают ничего нового. Технологии искусственного интеллекта внедряются во многие сферы деятельности, в том числе, и в область защиты информации.

В ходе исследования составлен список задач информационной безопасности, которые представляют основные направления в обеспечении комплексной защиты информационных систем и ресурсов [19]; охватывают широкий спектр проблем безопасности - от выявления и предотвращения атак до анализа поведения пользователей и управления инцидентами. Сосредоточенность на этих задачах обусловлена их критической важностью для минимизации рисков, своевременного реагирования на угрозы и обеспечения непрерывности бизнес-процессов. Своевременное и надежное решение подобных задач особенно актуально для предприятий, работающих в сфере IT, финансовом и государственном секторах, здравоохранении, энергетике и транспорте. Список стратегически важных задач обеспечения информационной безопасности предприятий, с описанием возможных функций искусственного интеллекта в их решении:

1. Обнаружение и предотвращение вторжений. Функция искусственного интеллекта - анализ сетевого трафика с минимизацией времени выявления подозрительных событий. Позволит сократить время реагирования на потенциальные угрозы от злоумышленников.

2. Анализ угроз. Функция искусственного интеллекта - обработка относительно больших объемов данных об атаках и уязвимостях с целью выявления закономерностей. Позволит предприятиям выполнять прогнозирование изменения списков актуальных угрозы информационной безопасности.

3. Обнаружение вирусного программного обеспечения. Функция искусственного интеллекта - распознавание вирусных программ не по известным сигнатурам, а на основе особенностей их поведения.

4. Управление доступом. Функция искусственного интеллекта - реализация интеллектуальных систем аутентификации, которые наблюдают за поведением пользователей и обеспечивают доступ к соответствующим ресурсам, а также дополнительно могут выполнять отслеживание действий пользователей в реальном времени для выявления

подозрительных или аномальных действий. Это позволит уменьшить вероятности успешной реализации внутренних угроз информационной безопасности.

5. Анализ рисков. Функция искусственного интеллекта - оценка вероятностей угроз, размеров потенциального ущерба и рисков информационной безопасности.

6. Управление инцидентами. Функция искусственного интеллекта - анализ событий информационной безопасности, выявление инцидентов с минимизацией времени и с учетом правил реагирования на инциденты (оповещение ответственных лиц, сохранение доказательств для последующего проведения расследования и нахождения виновных).

Решению задачи разработки и внедрения интеллектуальных систем защиты информации посвящено множество научно-исследовательских проектов, научных статей и диссертационных исследований. Так, в работе [20] выполнен анализ возможностей методов машинного обучения для обеспечения информационной безопасности. Авторы предлагают варианты применения искусственного интеллекта для решения таких задач информационной безопасности, например, как анализ логов, построение систем обнаружения вторжений, защита от фишинга, анализ поведения пользователей.

В статье [21] авторы предложили использовать искусственные нейронные сети для автоматического выявления аномалий в сетевом трафике, что стало основой для систем обнаружения вторжений (Intrusion Detection System, IDS) на базе технологии искусственного интеллекта. Идея заключалась в обучении искусственных нейронных сетей распознавать нормальное поведение сети и выявлять отклонения, указывающие на возможные атаки. Авторы работы [22] описывают платформу MADAM ID, которая использует методы интеллектуального анализа данных и машинного обучения для автоматического извлечения признаков из данных аудита системы и построения моделей обнаружения вторжений на основе этих признаков. Идеи статьи активно реализуются в современных системах обнаружения (IDS) и предупреждения вторжений (Intrusion Prevention System, IPS), облачных платформах, промышленных системах и инструментах кибербезопасности для автоматического обнаружения сложных угроз с помощью машинного обучения.

В работе [23] представлена гибридная структура искусственного интеллекта на основе биологических технологий для кибербезопасности, которая основана на методах машинного обучения, и подходящая для защиты критически важных сетевых приложений в военных информационных системах. В статье [24] авторы предлагают интегрированную структуру inTIME на основе машинного обучения, которая позволяет специалистам по безопасности работать с данными по угрозам информационной безопасности, собирать, используя различные источники информации, проводить анализ, обмениваться. Эта платформа не требует администрирования, имеет открытый исходный код. В исследовании [25] представлена методология TTPXHunter для автоматизированного получения информации об угрозах в виде тактик, техник и процедур (Tactics, Techniques, and Procedures, TTP) из отчетов о реализованных угрозах. Методология основана на модели обработки естественного языка, которая обучена для нахождения и выделения данных об угрозах в текстах отчетов. Авторы указывают, что на тестовых данных система достигает высокой точности (f1-score около 92-97%), что показывает ее эффективность по сравнению с существующими методами. В исследовании [26] авторы описывают практический опыт применения машинного обучения для преобразования неструктурированных текстов об отчетах по угрозам безопасности в структурированные данные, которые содержат техники атак. Авторы сформулировали выводы о том, какие модели работают эффективнее, и какие еще задачи в этой области предстоит решить. Работа [27] представляет собой обширный обзор современных методов глубокого обучения, применяемых для обнаружения вредоносного программного обеспечения. Информация, представленная в этой статье, является полезным источником для теоретических и практических специалистов в области информационной безопасности. Также в статье рассматриваются имеющиеся проблемы и задачи требующие решения в области глубокого обучения в контексте обнаружения вредоносного кода. В работе [28] разрабатывается система обнаружения вредоносных программ, использующая

методологии глубокого обучения и отбора признаков. В исследовании использованы два набора данных о сетевом трафике, содержащие вредоносный и нормальный трафик. Использован метод корреляционного отбора признаков, чтобы уменьшить размерность данных, а затем выполнено обучение с использованием моделей глубокого обучения. Результаты, которые предоставляют авторы, показывают, что в некоторых сценариях уменьшение числа признаков почти не влияет на качество обнаружения вредоносного программного обеспечения. В статье [29] авторы разработали модификацию искусственной нейронной сети для обнаружения и классификации вредоносного программного обеспечения с использованием механизмов внимания на базе модели ResNeXt. Модель, которую назвали ResNeXt+, обучается фокусироваться на признаках вредоносного кода. Эксперименты показали, что ResNeXt+ превосходит существующие методы по точности обнаружения и классификации вредоносного кода при тестировании на различных наборах данных.

Статья [30] посвящена разработке механизма принятия решений по управлению доступом с использованием методов машинного обучения. Авторы предлагают схему под названием EPDE-ML (Efficient Permission Decision Engine based on Machine Learning), которая преобразует запросы на управление доступом, основанные на атрибутах, в вектор решений о разрешении или отказе, превращая задачу управления доступом в задачу бинарной классификации (разрешить или запретить доступ. В качестве алгоритма классификации используется случайный лес (Random Forest, RF). Авторы утверждают, что эксперименты показали относительно высокую точность (около 92,6%) разработанного механизма, и высокую производительность при увеличении масштаба политики доступа.

В работе [31] авторы предлагают новую модель Attribute/Behavior-Based Access Control, которая использует не только атрибуты пользователей и ресурсов, но и их поведенческие характеристики, извлеченные из лог-файлов. В статье описывается метод построения признаков поведения пользователя и применение алгоритмов машинного обучения для обучения и тестирования модели на базе данных из репозитория машинного обучения UCI. Результаты экспериментов показывают, что предложенная модель обладает высокой точностью и эффективностью в выявлении пользователей с аномальным поведением. Исследование [32] посвящено разработке комплексного подхода к оценке рисков информационной безопасности с использованием методов многокритериального принятия решений (Multi-Criteria Decision Making, MCDM) и машинного обучения. Используется техника, которая позволяет экспертам учитывать различные критерии и выражать свои оценки на естественном языке. Также в этом исследовании, дополнительно к MCDM-методам, применяются алгоритмы машинного обучения для предсказания типов атак.

В работе [33] авторы разработали новую гибкую модель оценки рисков информационной безопасности, которая объединяет стандарты, экспертные знания, машинное обучение и онтологическое моделирование. Модель использует кластерный анализ (метод k-means) для выявления скрытых паттернов в данных о рисках, и создает иерархическую структуру рисков с помощью онтологий для их более точной классификации. Для визуализации результатов и выполнения анализа рисков авторы предлагают использовать тепловые карты, что позволяет специалистам выявить взаимосвязи и приоритеты угроз.

В работе [34] разработана система управления инцидентами для критической инфраструктуры, основанная на искусственном интеллекте и дополненной реальности. Система использует несколько модулей и видеопотоки от камер видеонаблюдения для обнаружения угроз и передачи информации на место происшествия и в центр управления. Внедрение этой системы и тестирование в реальных условиях позволило пересмотреть стандартные процедуры безопасности. В работе [35] авторы описывают агентную систему искусственного интеллекта LLexus, которая предназначена для автоматизации процесса реализации инструкций по устранению неисправностей в облачных сервисах. Как правило, инженеры выполняют сложные трудоемкие инструкции. Разработанная система должна понимать необходимую последовательность действий, и позволят укорить восстановление работы сервиса, снизить нагрузку на инженеров.

Обсуждение результатов. Результаты проведенного анализа сформированы в табл. 1, в виде задач информационной безопасности с описанием применяемых для их решения методов искусственного интеллекта и возможными источниками исходных данных.

Таблица 1. Методы искусственного интеллекта в задачах защиты информации
Table 1. Artificial intelligence methods in information security tasks

Задача защиты информации The task of information security	**Методы искусственного интеллекта Methods of artificial intelligence**	**Источник данных Data source**
Обнаружение и предотвращение вторжений Intrusion detection and prevention	Долгая краткосрочная память (Long Short-Term Memory, LSTM): анализ временных последовательностей сетевого трафика для выявления аномалий и атак [36]. Автоэнкодеры (Autoencoders, AE): выявление аномалий в сетевых данных [37]. Градиентный бустинг (Gradient Boosting Machines, GBM): классификация событий на нормальные и подозрительные [38]. Изоляционный лес (Isolation Forest, IF): обнаружение аномалий [39]. Кластеризация HDBSCAN: выявление аномальных групп трафика [40]. Трансформеры (Transformers): обработка последовательностей логов для выявления сложных паттернов [41]	Исторические данные о сетевом трафике - логи сетевого трафика, системы мониторинга
Анализ угроз Threat Analysis	LSTM: анализ последовательностей событий и текстов отчетов, выявление временных зависимостей и паттернов в данных [42]. Сверточные нейронные сети (Convolutional Neural Networks, CNN): извлечение признаков из структурированных данных и текстов, представленных в виде числовых массивов (тензоров) [43]. GBM: классификация типов угроз на основе извлеченных признаков [44] Обработка естественного языка (Natural Language Processing, NLP): анализ текстов отчетов и описаний угроз [45]	Данные о предыдущих атаках и уязвимостях — базы данных о кибератаках, отчеты о безопасности
Обнаружение вирусного программного обеспечения Detection of virus software	LSTM и CNN: анализатор журналов, API-мониторинг [46]. AE: выявление аномалий в поведении программного обучения [47]. GBM: классификация вредоносных и нормальных программ [48] .IF: выявление аномалий [49]	Данные о вредоносном программном обеспечении, поведение программ — антивирусные базы данных, данные о поведении приложений
Управление доступом Access control	Случайный лес (Random Forest, RF): классификация событий доступа [30]. LSTM: анализ последовательностей действий пользователей (User Behavior Analytics, UBA) [50]. Биометрические модели на основе глубокого обучения (Deep Learning based Biometrics, DL Biometrics): распознавание и аутентификация по биометрическим данным [51, 52]	Данные о поведении пользователей — логи доступа, системы аутентификации
Анализ рисков Risk analysis	Байесовские сети (Bayesian Networks, BN): моделирование вероятностей возникновения рисков [53]. GBM: прогнозирование вероятности рисков [54]	Данные о прошлых инцидентах, уязвимостях, отчеты об инцидентах, базы данных уязвимостей
Управление инцидентами Incident Management	LSTM, RF: анализ последовательностей инцидентов, классификация инцидентов [55]. кластерный анализ (метод k-means): кластеризация инцидентов для выявления групп [56]. AE: обнаружение аномалий [57]. Обучение с подкреплением (Reinforcement Learning, RL): автоматизация реагирования на инциденты [58]. NLP: анализ текстовых описаний и отчетов по инцидентам [59]	Данные о событиях информационной безопасности логи инцидентов, системы уведомлений

Процесс разработки и введения в эксплуатацию интеллектуальной системы защиты информации состоит из следующих основных этапов:

- оценка текущего уровня защищенности информации предприятия:выполняется аудит систем безопасности и выявление уязвимостей в механизмах защиты;
- определение целей использования искусственного интеллекта и формулирование задач, для решения которых предназначена интеллектуальная система;
- выбор интеллектуального метода и инструментов построения системы;
- разработка интеллектуальной системы, ее адаптация и интеграция в информационную инфраструктуру предприятия;
- обучение и тестирование интеллектуальной системы;
- введение интеллектуальной системы в эксплуатацию: выполняется запуск системы в рабочем режиме, проводится мониторинг работы, и оптимизация параметров системы на основе полученных данных;
- обучение персонала принципам работы с новой системой;
- регулярный аудит системы, учет замечаний, требований пользователей и сотрудников службы безопасности.

Описанный обобщенный алгоритм внедрения технологий искусственного интеллекта в структуру системы информационной безопасности представлен на рис. 1.

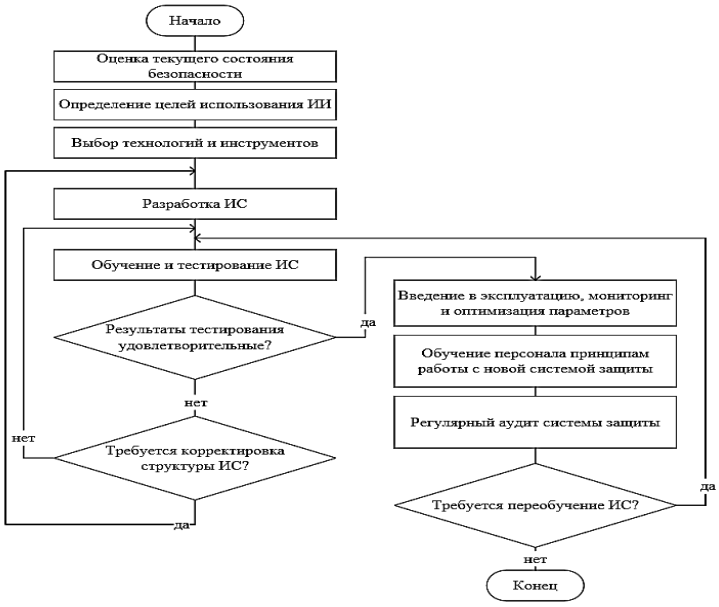

Рис. 1 – Обобщенный алгоритм внедрения технологий искусственного интеллекта в структуру системы информационной безопасности предприятия
Fig. 1 – Generalized algorithm for the implementation of artificial intelligence technologies into the structure of an enterprise's information security system

Необходимо принимать во внимание, что рассмотренные задачи информационной безопасности имеют свои отличительные особенности, которые необходимо учитывать при разработке и внедрении интеллектуальной системы защиты, и соответственно, включить дополнительные этапы в предлагаемый алгоритм:

- для решения задачи обнаружения и предотвращения вторжений необходимо выполнить специальную настройку системы для обеспечения минимизации ложных срабатываний;
- решение задачи анализа угроз требует разработки алгоритмов для анализа и выявления закономерностей;
- для решения задачи обнаружения вирусного программного обеспечения необходимо обеспечить минимизацию ложных срабатываний при выявлении вредоносных программ; потребуется обеспечить сбор и обработку обучающих данных, и разработать процедуры по обновлению моделей в реальном времени;
- в случае применения интеллектуальных методов для решения задачи управления доступом необходимо разработать систему аутентификации, которая должна учитывать особенности поведения пользователей, или физиологические признаки (в случае использования биометрической системы аутентификации). Также при анализе поведения пользователей необходимо разработать процедуры определения нормального поведения, и обеспечения конфиденциальности данных;
- решение задачи анализа рисков требует использования аналитических методов оценки потенциального ущерба от успешной реализации угроз безопасности;
- решение задачи управления инцидентами требует интеграции с системами оповещения о подозрительных событиях.

Вывод. Можно выделить перспективные подходы к развитию искусственного интеллекта для каждой из рассматриваемых задач защиты информации. В настоящее время подходы находятся на стадии активных исследований или пилотных проектов.

1. В области обнаружения и предотвращения вторжений дальнейшее развитие предположительно будет связано с реализацией интеллектуальных систем, способных автоматически адаптировать тактику защиты под новые типы угроз. Теоретически это возможно осуществить с помощью генеративного искусственного интеллекта на основе моделей типа GAN для моделирования новых типов атак, и автоматической генерации сценариев защиты или вариационных автоэнкодеров (Variational Autoencoder, VAE) для выявления аномалий

в сетевом трафике, и глубоких нейронных сетей (Deep Learning) для адаптивного анализа поведения систем.

2. Перспективы в решении задачи анализа угроз связаны с построением интеллектуальных систем, предназначенных для прогнозирования возникновения новых угроз, уязвимостей и атак на компьютерные системы и сети. При этом необходимо использовать глубокое обучение, например, LSTM или трансформеры для анализа исторических данных об уязвимостях и предсказания новых угроз и модели машинного обучения для выявления закономерностей в данных об атаках.

3. Перспективное направление в решении задачи обнаружения вирусного программного обеспечения связано с построением самообучающихся систем, анализирующих поведение программ на основе обучающих данных, посредством глубокого обучения (например, CNN или RNN).

4. В области управления доступом перспективным является построение самообучающихся систем биометрической аутентификации (например, на базе глубокого обучения) и самообучающиеся биометрических систем, анализирующих поведение пользователей в реальном времени.

5. В области анализа рисков информационной безопасности перспективным направлением является построение генеративных моделей сценариев кризисных ситуаций с помощью моделей типа GAN или VAE и предсказания появления редких значимых событий (концепция «черный лебедь», The Black Swan) с помощью моделей предсказания на основе временных рядов (например, LSTM, Transformer).

6. Дальнейшее развитие методов решения задачи управление инцидентами может быть достигнуто путем внедрения систем, способных автоматически разрабатывать стратегии реагирования на атаки злоумышленников, а также самообучающихся аналитических систем для расследования инцидентов на базе обучения с подкреплением.

Одной из основных проблем, возникающих при внедрении технологий искусственного интеллекта в сферу информационной безопасности является задача назначения ответственных лиц в случае возникновения ошибок в работе интеллектуальных систем. Виновниками могут быть разработчики, организация, применяющая интеллектуальные средства или сама система. Поэтому необходимы четкие указания для формирования принципов определения ответственности, прописанные на законодательном уровне.

Другая проблема связана со специфическими особенностями интеллектуальных систем, основанных на процессах обучения. Такие системы, по сути, представляют собой «черный ящик», что затрудняет понимание того, каким образом они принимают решения. Это может вызвать недоверие к работе интеллектуальных систем защиты информации со стороны пользователей и государственных органов, курирующих вопросы обеспечения информационной безопасности в соответствии с действующим законодательством.

Еще одна проблема заключается в том, что интеллектуальные системы обучающиеся на данных уязвимы к атакам, направленным на манипулирование данными. В этом случае интеллектуальная система может принимать неверные решения, пройдя обучение на искаженных примерах. Рассмотренные специфические особенности технологий искусственного интеллекта и задач обеспечения защиты информации позволяют определить ряд рекомендаций, следование которым позволит снизить инвестиционные (экономические), кадровые и технические риски при развертывании интеллектуальных систем в целях информационной безопасности. В первую очередь необходимо разработать стратегию внедрения искусственного интеллекта, учитывающую потребности конкретного предприятия в области информационной безопасности. Проводить работы по внедрению поэтапно, начиная с пилотных проектов, чтобы оценить эффективность и выявить потенциальные проблемы.

Далее следует провести обучение сотрудников навыкам работы с интеллектуальной системой, разъяснить им назначение и принципы ее функционирования. Обязательно необходимо установить границы ответственности за действия интеллектуальных систем, включая юридические аспекты и внутренние регламенты. Руководство предприятия

и сотрудники службы безопасности должны обеспечить проведение регулярного аудита и обновления интеллектуальной системы с целью выявления уязвимостей, своевременного реагирования на изменения списка актуальных угроз информационной безопасности.

Важным является процесс сотрудничества с экспертами в областях информационной безопасности и технологий искусственного интеллекта для того, чтобы наполнить интеллектуальную систему соответствующими знаниями, и обеспечить прозрачность работы системы для понимания пользователями процессов принятия решений.

Внедрение технологий искусственного интеллекта в сферу информационной безопасности обеспечивает построение эффективных систем защиты, которые позволяют автоматизировать процессы мониторинга и реагирования на инциденты, такие системы могут адаптироваться к новым видам угроз посредством обучения, и реализуют проактивную защиту информационных ресурсов и систем. При этом необходимо обеспечить прозрачность работы систем и разработать процедуры определения ответственных лиц при принятии решений на основе результатов работы систем.

Библиографический список:

1. Шинкарецкая Г.Г., Берман А.М. Кибератаки – Противоправное использование цифровых технологий // Международное право. 2022. № 1. С. 40-50. DOI: 10.25136/2644-5514.2022.1.37271 URL: https://nbpublish.com/library_read_article.php?id=37271
2. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» [Электронный ресурс] // ГАРАНТ. URL: https://base.garant.ru/72838946/ (дата обращения: 21.03.2025)
3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.:Стандартинформ, 2008. 12 с.
4. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. – М.: Стандартинформ, 2006. – 20 с.
5. ГОСТ Р 59710-2022. Защита информации. Управление компьютерными инцидентами. Общие положения. – М.: Российский институт стандартизации, 2022. – 16 с.
6. Миланович Е.А., Селезнёв И.Л. Система анализа сетевого трафика для обеспечения безопасности сети // Молодой ученый. – 2020. – № 15 (305). – С. 86-89. – URL: https://moluch.ru/archive/305/68701/ (дата обращения: 21.03.2025).
7. ГОСТ Р ИСО/МЭК 27002-2021. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности– М.: Стандартинформ, 2021. – 74 с.
8. Мещеряков Р.В., Мельников С.Ю., Пересыпкин В.А., Хорев А.А. Перспективные направления применения технологий искусственного интеллекта при защите информации//Вопросы кибербезопасности. 2024. № 4(62). DOI:10.21681/2311-3456-2024-4-02-12
9. Дартмутская конференция по искусственному интеллекту [Электронный ресурс]//Психология. – URL: https://psixologiya.org/blog/2504-dartmutskaya-konferenciya-po-iskusstvennomu-intellektu.html (дата обращения: 21.03.2025).
10. Что такое искусственный интеллект и его виды [Электронный ресурс] aisimple.ru.:https://aisimple.ru/22-chto-takoe-ii.html (дата обращения: 21.03.2025).
11. Усамов И.Р. Роль интеллектуальных информационных систем в современном мире / И.Р. Усамов, А.А. Албакова, А.А. Мустиев // Актуальные вопросы современной науки: теория, технология, методология и практика: Материалы Международной научно-практической онлайн-конференции, приуроченной к 60-ти летию член-корреспондента Академии наук ЧР, доктора технических наук, профессора Сайд-Альви Юсуповича Муртазаева, Грозный, 28 апреля 2021 года. – Грозный: Грозненский государственный нефтяной технический университет имени академика М.Д. Миллионщикова, 2021. – С. 267-272. – DOI 10.34708/GSTOU.CONF.2021.10.35.053. – EDN PMXCRD.
12. Рейнхард Клетте. Компьютерное зрение. Теория и алгоритмы /пер. с англ. А.А. Слинкин. М.: ДМК Пресс, 2019. – 506 с.: ил.
13. Прошина М.В. Современные методы обработки естественного языка: нейронные сети//Экономика строительства. 2022. № 5. https://cyberleninka.ru/article/n/sovremennye-metody-obrabotki-estestvennogo-yazyka-neyronnye-seti(дата обращения: 21.03.2025).
14. Tjandra, A., Sakti, S., & Nakamura, S. End-to-End Speech Recognition Sequence Training With Reinforcement Learning. IEEE Access,2019;7:79758-79769.
15. Чечнев В.Б. Использование систем поддержки принятия решений в автоматизации процессов принятия решений. *Электронные библиотеки*. 2025;28(1):163-183. DOI 10.26907/1562-5419-2025-28-1-163-183. EDN OGRDVD.
16. Pohl J. Artificial Superintelligence: Extinction or Nirvana? InterSymp-2015. № 27 P. 1–20.
17. Илюшин Л.С., Н.А. Торпашева. Технологии искусственного интеллекта как ресурс трансформации образовательных практик Ярославский педагогический вестник. – 2024. – № 3(138). С. 62-71. DOI 10.20323/1813-145X-2024-3-138-62. EDN ADWMMG.
18. Goodfellow Ian, Pouget-Abadie Jean, Mirza Mehdi, Xu Bing, Warde-Farley David, Ozair Sherjil, Courville Aaron, Bengio Yoshua Generative Adversarial Nets.Proceedings of the International Conference on Neural Information Processing Systems. 2014;2672–2680.
19. Баланов А.Н. Комплексная информационная безопасность: учебное пособие для вузов. – 2-е изд., Санкт-Петербург: Лань, 2025, - 400 с.
20. Доргушаова А.К., Довгаль В.А., Козлова Н.Ш., Козлов Р.С. Обзор использования технологий машинного обучения в обеспечении информационной безопасности данных: настоящее и будущее //Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2024. – №1 (336). https://cyberleninka.ru/article/n/obzor-ispolzovaniya-tehnologiy-mashinnogo-obucheniya-v-obespechenii-informatsionnoy-bezopasnosti-dannyh-nastoyaschee-i-buduschee (дата обращения: 23.03.2025).
21. Mukkamala, S., Janoski, G.I., & Sung, A.HIntrusion detection using neural networks and support vector machines. Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No.02CH37290) 2002;2:1702-1707
22. Lee, W., & Stolfo, S. (2000). A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security (TISSEC), 3, 227 - 261.
23. Demertzis, K., & Iliadis, L.S. (2015). A Bio-Inspired Hybrid Artificial Intelligence Framework for Cyber Security.
24. Koloveas, P., Chantzios, T., Alevizopoulou, S., Skiadopoulos, S., & Tryfonopoulos, C. (2021). inTIME: A Machine Learning-Based Framework for Gathering and Leveraging Web Data to Cyber-Threat Intelligence. Electronics.
25. Rani, N., Saha, B., Maurya, V., & Shukla, S.K. (2024). TTPXHunter: Actionable Threat Intelligence Extraction as TTPs from Finished Cyber Threat Reports. Digital Threats: Research and Practice, 5, 1 - 19.

26. Orbinato, V., Barbaraci, M., Natella, R., & Cotroneo, D. (2022). Automatic Mapping of Unstructured Cyber Threat Intelligence: An Experimental Study: (Practical Experience Report). 2022 IEEE 33rd International Symposium on Software Reliability Engineering (ISSRE), 181-192.
27. Ajvad Haneef K., Madhu Kumar S.D. (2023). Deep Learning Techniques for Malware Detection: A Comprehensive Survey. 2023 International Conference on Computer, Electronics & Electrical Engineering & their Applications (IC2E3), 1-7.
28. Alomari, E., Nuiaa, R.R., Alyasseri, Z.A., Mohammed, H.J., Sani, N.S., Esa, M.I., & Musawi, B.A. (2023). Malware Detection Using Deep Learning and Correlation-Based Feature Selection. Symmetry, 15, 123.
29. He, Y., Kang, X., Yan, Q., & Li, E. (2024). ResNeXt+: Attention Mechanisms Based on ResNeXt for Malware Detection and Classification. IEEE Transactions on Information Forensics and Security, 19, 1142-1155.
30. Liu, A., Du, X., & Wang, N. (2021). Efficient Access Control Permission Decision Engine Based on Machine Learning. Secur. Commun. Networks, 2021, 3970485:1-3970485:11.
31. Afshar, M., Samet, S., & Usefi, H. (2021). Incorporating Behavior in Attribute Based Access Control Model Using Machine Learning. 2021 IEEE International Systems Conference (SysCon), 1-8.
32. Alqazzaz, A. (2024). Integrated Neutrosophic methodology and Machine Learning Models for Cybersecurity Risk Assessment: An exploratory study. International Journal of Neutrosophic Science.
33. Barlybayev, A., Sharipbay, A., Shakhmetova, G., & Zhumadillayeva, A. (2024). Development of a Flexible Information Security Risk Model Using Machine Learning Methods and Ontologies. Applied Sciences.
34. Nastou, P.E., Papataxiarhis, V., Moutsis, S.N., Tsintotas, K.A., Petroudis, G., Papastamatiou, N., Mesaritakis, C., Gasteratos, A., Vouyioukas, D., & Gavathas, P. (2024). An Efficient Highly-Secure AI-Based System for Incident Management in Critical Infrastructures. 2024 IEEE International Conference on Imaging Systems and Techniques (IST), 1-6.
35. Las-Casas, P.H., Kumbhare, A.G., Fonseca, R., & Agarwal, S. (2024). LLexus: an AI agent system for incident management. ACM SIGOPS Operating Systems Review, 58, 23 - 36.
36. Harshitha, T.S. (2024). Intrusion Detection and Prevention Using CNN-LSTM. International Journal of Science, Engineering and Technology.
37. Alhassan, S., Abdul-Salaam, G., Micheal, A., Missah, Y.M., Ganaa, E.D., & Shirazu, A.S. (2024). CFS-AE: Correlation-based Feature Selection and Autoencoder for Improved Intrusion Detection System Performance. J. Internet Serv. Inf. Secur., 14, 104-120.
38. Abualhaj, M.M., Abu-Shareha, A.A., & Rateb, R. (2025). Enhancing intrusion detection systems with hybrid HHO-WOA optimization and gradient boosting machine classifier. International Journal of Reconfigurable and Embedded Systems (IJRES).
39. Maheswaran N., Bose S., Gokulraj G., Anitha T., Shruthi T., Vijayaraj G. (2025). Intrusion Prevention System in SDN Environment for 6G Networks Using Deep Learning. 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), 53-61.
40. Sreenivasa Reddy, G., & Shyama Chandra Prasad, G. (2023). Intrusion detection system using clustering algorithms of neural networks. International Journal of Advanced Research.
41. Sana, L., Nazir, M.M., Yang, J., Hussain, L., Chen, Y., Ku, C.S., Alatiyyah, M.H., Alateyah, S.A., & Por, L.Y. (2024). Securing the IoT Cyber Environment: Enhancing Intrusion Anomaly Detection With Vision Transformers. IEEE Access, 12, 82443-82468.
42. Ravichandra A., Shivakumara T. (2023). Detecting and Real Time Threat Analysis in Smart Grid Networks. Interantional journal of scientific research in engineering and management.
43. Almutairi, L. (2023). Deep Learning based Frameworks for Real-time Cyber Threat Analysis. Journal of Engineering and Applied Sciences.
44. Xie, L., Liao, Z., & Li, H. (2024). Research and Design of an Automated Security Event Analysis and Handling Framework Based on Threat Intelligence. Scalable Comput. Pract. Exp., 25, 1872-1881.
45. Mohammed, S.Y., & Aljanabi, M. (2024). From Text to Threat Detection: The Power of NLP in Cybersecurity. SHIFRA.
46. Karat, G., Kannimoola, J.M., Nair, N., Vazhayil, A., G, S.V., & Poornachandran, P. (2024). CNN-LSTM Hybrid Model for Enhanced Malware Analysis and Detection. Procedia Computer Science.
47. Beg, R., Pateriya, R.K., & Tomar, D.S. (2024). Design of an Iterative Method for Malware Detection Using Autoencoders and Hybrid Machine Learning Models. IEEE Access, 12, 175032-175055.
48. Iqubal, A., & Payal, A. (2024). Malware Detection Technique for Android Devices Using Machine Learning Algorithms. 2024 International Conference on Computing, Sciences and Communications (ICCSC), 1-6.
49. Pawar, J., Avhankar, M.S., Gupta, A., Barve, A., Patil, H., & Maranan, R. (2024). Enhancing Network Security: Leveraging Isolation Forest for Malware Detection. 2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT), 230-234.
50. Zhao, G., Li, X., & Li, H. (2024). A Trusted Authentication Scheme Using Semantic LSTM and Blockchain in IoT Access Control System. International Journal on Semantic Web and Information Systems.
51. Vincent, A., & Anitha, A. (2023). A Survey on Deep Learning Approach for Identity Recognition Using Finger Vein Biometrics. 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT), 971-975.
52. Mounnan, O., Manad, O., Boubchir, L., Mouatasim, A.E., & Daachi, B. (2022). Deep Learning-Based Speech Recognition System using Blockchain for Biometric Access Control. 2022 Ninth International Conference on Software Defined Systems (SDS), 1-2.
53. Sato, R., Kawaguchi, H., & Nakatani, Y. (2025). Malcoda: Practical and Stochastic Security Risk Assessment for Enterprise Networks. IEEE Transactions on Dependable and Secure Computing, 22, 1383-1399.
54. Ngampunprasert, T., & Ketcham, M. (2024). Risk Analysis of Device Within the Organization that are Vulnerable to Cyber Security Attacks with Artificial Intelligence. 2024 IEEE International Conference on Cybernetics and Innovations (ICCI), 1-6.
55. Mohanraj, G., Nadesh, R.K., J, J., S, A., & Sathiyamoorthi, V. (2025). Monitoring Incident Response Using Real-Time Analytics. 2024 International Conference on IT Innovation and Knowledge Discovery (ITIKD), 1-8.
56. Anggraeni, R., Alzami, F., Nurhindarto, A., Budi, S., Megantara, R.A., Rizqa, I., & Muslih, M. (2025). Clustering IT Incidents Using K-Means: Improving Incident Response Time in Service Management. Sinkron.
57. Сафронов Д.А., Кацер Ю.Д., Зайцев К.С. Поиск аномалий с помощью автоэнкодеров.//International Journal of Open Information Technologies. 2022.№8. https://cyberleninka.ru/article/n/poisk-anomaliy-s-pomoschyu-avtoenkoderov (дата обращения: 13.07.2025).
58. Hossain, F., Hasan, K., Amin, A., & Mahmud, S. (2024). Quantum Machine Learning for Enhanced Cybersecurity: Proposing a Hypothetical Framework for Next-Generation Security Solutions. Journal of Technologies Information and Communication.
59. Faheem, M., Awais, M., Iqbal, A., & Zia, H. (2025). Enhancing It incident management with natural language processing and predictive analytics. International Journal of Science and Research Archive.

References:

1. Shinkaretskaya G.G., Berman A.M. Cyberattacks – Criminal Use of Digital Technologies // International Law. 2022. No. 1. P. 40-50. DOI: 10.25136/2644-5514.2022.1.37271. URL: https://nbpublish.com/libraryreadarticle.php?id=37271
2. Decree of the President of the Russian Federation dated October 10, 2019 No. 490 «On the Development of Artificial Intelligence in the Russian Federation» [Electronic resource] // GARANT. https://base.garant.ru/72838946/ (accessed: 21.03.2025)
3. GOST R 50922-2006. Information Protection. Basic Terms and Definitions. – Moscow: Standartinform, 2008. – 12 p.
4. Recommendations for Standardization R 50.1.056-2005. Technical Protection of Information. Basic Terms and Definitions. – Moscow: Standartinform, 2006. – 20 p.

5. GOST R 59710-2022. Information Protection. Management of Computer Incidents. General Provisions. – Moscow: Russian Institute for Standardization, 2022. – 16 p.
6. Milanovich E.A., Seleznev I.L. System for Analyzing Network Traffic to Ensure Network Security // Young Scientist. 2020. No. 15 (305). P. 86-89. URL: https://moluch.ru/archive/305/68701/ (accessed: 21.03.2025)
7. GOST R ISO/IEC 27002-2021. Information Technology. Security Techniques. Code of Practice for Information Security Controls. – Moscow: Standartinform, 2021. – 74 p.
8. Meshcheryakov R.V., Melnikov S.Yu., Peresypkin V.A., Khorev A.A. Promising Areas for the Application of Artificial Intelligence Technologies in Information Protection // *Cybersecurity Issues*. 2024; 4(62). DOI: 10.21681/2311-3456-2024-4-02-12
9. Dartmouth Conference on Artificial Intelligence [Electronic resource] // Psychology. – URL: https://psixologiya.org/blog/2504-dart-mutskaya-konferenciya-po-iskusstvennomu-intellektu.html (accessed: 21.03.2025)
10. What is Artificial Intelligence and Its Types [Electr.resource]aisimple.ru. https://aisimple.ru/22-chto-takoe-ii.html (acces.: 21.03.2025)
11. Usamov I.R. , A.A. Albakova, A.A. Mustiev . The Role of Intelligent Information Systems in the Modern World. Current Issues of Modern Science: Theory, Technology, Methodology, and Practice: Materials of the International Scientific and Practical Online Conference Dedicated to the 60th Anniversary of Corresponding Member of the Academy of Sciences of the Chechen Republic, Dr. of Technical Sciences, Prof. Said-Alvi Yusupovich Murtazayev, Grozny, April 28, 2021. Grozny: Grozny State Oil Technical University named after Academician M.D. Millionshchikov,2021;267-272.DOI:10.34708/GSTOU.CONF..2021.10.35.053. EDN PMXCRD.
12. Reinhard Klette. Computer Vision. Theory and Algorithms.Translated from English by A.A. Slinkin. Moscow: DMK Press, 2019:506.
13. Proshina M.V. Modern Methods of Natural Language Processing: Neural Networks // *Construction Economics*. 2022; 5. URL: https://cyberleninka.ru/article/n/sovremennye-metody-obrabotki-estestvennogo-yazyka-neyronnye-seti (accessed: 21.03.2025)
14. Tjandra, A., Sakti, S., Nakamura,S. End-to-End Speech Recognition Sequence Training With Reinforcement Learning. IEEE Access, 2019;7:79758-79769.
15. Chechnev V.B. Use of Decision Support Systems in Decision-Making Automation. *Electronic Libraries*. 2025; 28(1):163-183. – DOI: 10.26907/1562-5419-2025-28-1-163-183. – EDN OGRDVD.
16. Pohl J. Artificial Superintelligence: Extinction or Nirvana? InterSymp-2015;27:1–20.
17. Ilyushin L.S., Torpashova N.A. Artificial Intelligence Technologies as a Resource for Transforming Educational Practices. *Yaroslavl Pedagogical Bulletin*. 2024; 3(138): 62-71. – DOI: 10.20323/1813-145X-2024-3-138-62. – EDN ADWMMG.
18. Goodfellow Ian, Pouget-Abadie Jean, Mirza Mehdi, Xu Bing, Warde-Farley David, Ozair Sherjil, Courville Aaron, Bengio Yoshua Generative Adversarial Nets. Proceedings of the International Conference on Neural Information Processing Systems (NIPS 2014; 2672–2680.
19. Balanov A.N. Comprehensive Information Security: Textbook for Higher Education Institutions. Saint Petersburg:Lan. 2025;400.
20. Dorgushaeva A.K., Dovgal V.A., Kozlova N.Sh., Kozlov R.S. Review of the Use of Machine Learning Technologies in Ensuring Data Information Security: Present and Future // Bulletin of Adyghe State University. Series 4: Natural-Mathematical and Technical Sciences. 2024. No. 1 (336). URL: https://cyberleninka.ru/article/n/obzor-ispolzovaniya-tehnologiy-mashinnogo-obucheniya-v-obespechenii-informatsionnoy-bezopasnosti-dannyh-nastoyaschee-i-buduschee (accessed: 23.03.2025)
21. Mukkamala, S., Janoski, G.I., & Sung, A.H. (2002). Intrusion detection using neural networks and support vector machines. Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No.02CH37290), 2, 1702-1707 vol.2.
22. Lee, W., & Stolfo, S. (2000). A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security (TISSEC), 3, 227 - 261.
23. Demertzis, K., & Iliadis, L.S. (2015). A Bio-Inspired Hybrid Artificial Intelligence Framework for Cyber Security.
24. Koloveas, P., Chantzios, T., Alevizopoulou, S., Skiadopoulos, S., & Tryfonopoulos, C. (2021). inTIME: A Machine Learning-Based Framework for Gathering and Leveraging Web Data to Cyber-Threat Intelligence. Electronics.
25. Rani, N., Saha, B., Maurya, V., & Shukla, S.K. (2024). TTPXHunter: Actionable Threat Intelligence Extraction as TTPs from Finished Cyber Threat Reports. Digital Threats: Research and Practice, 5, 1 - 19.
26. Orbinato, V., Barbaraci, M., Natella, R., & Cotroneo, D. Automatic Mapping of Unstructured Cyber Threat Intelligence: An Experimental Study: (Practical Experience Report). IEEE 33rd International Symposium on Software Reliability Engineering (ISSRE), 2022; 181-192.
27. Ajvad Haneef K., Madhu Kumar S.D. Deep Learning Techniques for Malware Detection: A Comprehensive Survey. 2023 International Conference on Computer, Electronics & Electrical Engineering & their Applications (IC2E3), 2023; 1-7.
28. Alomari, E., Nuiaa, R.R., Alyasseri, Z.A., Mohammed, H.J., Sani, N.S., Esa, M.I., & Musawi, B.A. Malware Detection Using Deep Learning and Correlation-Based Feature Selection. Symmetry, 2023; 15, 123.
29. He, Y., Kang, X., Yan, Q., & Li, E. (2024). ResNeXt+: Attention Mechanisms Based on ResNeXt for Malware Detection and Classification. IEEE Transactions on Information Forensics and Security, 19, 1142-1155.
30. Liu, A., Du, X., & Wang, N. (2021). Efficient Access Control Permission Decision Engine Based on Machine Learning. Secur. Commun. Networks, 2021, 3970485:1-3970485:11.
31. Afshar, M., Samet, S., & Usefi, H. (2021). Incorporating Behavior in Attribute Based Access Control Model Using Machine Learning. 2021 IEEE International Systems Conference (SysCon), 1-8.
32. Alqazzaz, A. Integrated Neutrosophic methodology and Machine Learning Models for Cybersecurity Risk Assessment: An exploratory study. International Journal of Neutrosophic Science. 2024.
33. Barlybayev, A., Sharipbay, A., Shakhmetova, G., & Zhumadillayeva, A. Development of a Flexible Information Security Risk Model Using Machine Learning Methods and Ontologies. Applied Sciences. 2024.
34. Nastou, P.E., Papataxiarhis, V., Moutsis, S.N., Tsintotas, K.A., Petroudis, G., Papastamatiou, N., Mesaritakis, C., Gasteratos, A., Vouyioukas, D., & Gavathas, P. (2024). An Efficient Highly-Secure AI-Based System for Incident Management in Critical Infrastructures. 2024 IEEE International Conference on Imaging Systems and Techniques (IST), 1-6.
35. Las-Casas, P.H., Kumbhare, A.G., Fonseca, R., & Agarwal, S. LLexus: an AI agent system for incident management. ACM SIGOPS Operating Systems Review, 2024;58: 23 - 36.
36. Harshitha, T.S. Intrusion Detection and Prevention Using CNN-LSTM. International Journal of Science, Engineering and Technology. 2024.
37. Alhassan, S., Abdul-Salaam, G., Micheal, A., Missah, Y.M., Ganaa, E.D., & Shirazu, A.S. (2024). CFS-AE: Correlation-based Feature Selection and Autoencoder for Improved Intrusion Detection System Performance. J. Internet Serv. Inf. Secur., 14, 104-120.
38. Abualhaj, M.M., Abu-Shareha, A.A., & Rateb, R. (2025). Enhancing intrusion detection systems with hybrid HHO-WOA optimization and gradient boosting machine classifier. International Journal of Reconfigurable and Embedded Systems (IJRES).
39. Maheswaran N., Bose S., Gokulraj G., Anitha T., Shruthi T., Vijayaraj G. (2025). Intrusion Prevention System in SDN Environment for 6G Networks Using Deep Learning. 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), 2025; 53-61.
40. Sreenivasa Reddy, G., & Shyama Chandra Prasad, G. (2023). Intrusion detection system using clustering algorithms of neural networks. International Journal of Advanced Research.
41. Sana, L., Nazir, M.M., Yang, J., Hussain, L., Chen, Y., Ku, C.S., Alatiyyah, M.H., Alateyah, S.A., & Por, L.Y. (2024). Securing the IoT Cyber Environment: Enhancing Intrusion Anomaly Detection With Vision Transformers. IEEE Access, 12, 82443-82468.
42. Ravichandra A., Shivakumara T. (2023). Detecting and Real Time Threat Analysis in Smart Grid Networks. Interantional journal of scientific research in engineering and management.
43. Almutairi L Deep Learning based Frameworks for Real-time Cyber Threat Analysis.Journal of Engineering and Applied Sciences. 2023.

44. Xie, L., Liao, Z., & Li, H. (2024). Research and Design of an Automated Security Event Analysis and Handling Framework Based on Threat Intelligence. Scalable Comput. Pract. Exp., 25, 1872-1881.
45. Mohammed, S.Y., & Aljanabi, M. (2024). From Text to Threat Detection: The Power of NLP in Cybersecurity. SHIFRA.
46. Karat, G., Kannimoola, J.M., Nair, N., Vazhayil, A., G, S.V., & Poornachandran, P. (2024). CNN-LSTM Hybrid Model for Enhanced Malware Analysis and Detection. Procedia Computer Science.
47. Beg, R., Pateriya, R.K., & Tomar, D.S. (2024). Design of an Iterative Method for Malware Detection Using Autoencoders and Hybrid Machine Learning Models. IEEE Access, 12, 175032-175055.
48. Iqubal, A., & Payal, A. (2024). Malware Detection Technique for Android Devices Using Machine Learning Algorithms. 2024 International Conference on Computing, Sciences and Communications (ICCSC), 1-6.
49. Pawar, J., Avhankar, M.S., Gupta, A., Barve, A., Patil, H., & Maranan, R. Enhancing Network Security: Leveraging Isolation Forest for Malware Detection. 2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT), 2024;230-234.
50. Zhao, G., Li, X., & Li, H. (2024). A Trusted Authentication Scheme Using Semantic LSTM and Blockchain in IoT Access Control System. International Journal on Semantic Web and Information Systems.
51. Vincent, A., & Anitha, A. (2023). A Survey on Deep Learning Approach for Identity Recognition Using Finger Vein Biometrics. 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT), 971-975.
52. Mounnan, O., Manad, O., Boubchir, L., Mouatasim, A.E., & Daachi, B. (2022). Deep Learning-Based Speech Recognition System using Blockchain for Biometric Access Control. 2022 Ninth International Conference on Software Defined Systems (SDS), 1-2.
53. Sato, R., Kawaguchi, H., & Nakatani, Y. (2025). Malcoda: Practical and Stochastic Security Risk Assessment for Enterprise Networks. IEEE Transactions on Dependable and Secure Computing, 22, 1383-1399.
54. Ngampunprasert, T., & Ketcham, M. (2024). Risk Analysis of Device Within the Organization that are Vulnerable to Cyber Security Attacks with Artificial Intelligence. 2024 IEEE International Conference on Cybernetics and Innovations (ICCI), 1-6.
55. Mohanraj, G., Nadesh, R.K., J, J., S, A., & Sathiyamoorthi, V. (2025). Monitoring Incident Response Using Real-Time Analytics. 2024 International Conference on IT Innovation and Knowledge Discovery (ITIKD), 1-8.
56. Anggraeni, R., Alzami, F., Nurhindarto, A., Budi, S., Megantara, R.A., Rizqa, I., & Muslih, M. (2025). Clustering IT Incidents Using K-Means: Improving Incident Response Time in Service Management. Sinkron.
57. Safronov D.A., Katser Y.D., Zaitsev K.S. Anomaly Detection Using Autoencoders // International Journal of Open Information Technologies. 2022. No. 8. URL: https://cyberleninka.ru/article/n/poisk-anomaliy-s-pomoschyu-avtoenkoderov (accessed: 13.07.2025).
58. Hossain, F., Hasan, K., Amin, A., & Mahmud, S. (2024). Quantum Machine Learning for Enhanced Cybersecurity: Proposing a Hypothetical Framework for Next-Generation Security Solutions. Journal of Technologies Information and Communication.
59. Faheem, M., Awais, M., Iqbal, A., & Zia, H. (2025). Enhancing It incident management with natural language processing and predictive analytics. International Journal of Science and Research Archive.

Сведения об авторах:

Потиенко Даниил Анатольевич, магистрант, кафедра «Вычислительные системы и информационная безопасность»; potienkodaniil@gmail.com

Чмыхало Данил Сергеевич, магистрант, кафедра «Вычислительные системы и информационная безопасность»; chmykhalo3009@gmail.com

Легонько Ольга Леонидовна кандидат технических наук, доцент, кафедра «Вычислительные системы и информационная безопасность», olga_cvetkova@mail.ru; ORCID 0000-0003-4071-6313

Information about authors:

Daniil A. Potienko, Master's student, Department of Computing Systems and Information Security; potienkodaniil@gmail.com

Danil S. Chmykhalo, Master's student, Department of Computing Systems and Information Security; chmykhalo3009@gmail.com

Olga L. Legonko, Cand. Sci. (Eng.), Assoc. Prof., Department of Computing Systems and Information Security, olga_cvetkova@mail.ru; ORCID 0000-0003-4071-6313

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 03.04.2025**.**

Одобрена после рецензирования/Reviced 29.11.2025.

Принята в печать/Accepted for publication 14.01.2026.