

Безопасность распределенных систем и телекоммуникаций

Научная статья

DOI 10.66424/2071-8217-2026-3-13

УДК 004.056.5, 004.896, 629.5.067

АНАЛИЗ УГРОЗ ПРИКЛАДНОГО УРОВНЯ IOT-СИСТЕМ И ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ ИХ БЕЗОПАСНОСТИ

А. М. Арбузов^{1*}, А. П. Нырков¹, Д. В. Гаскаров¹, И. В. Ли²

¹ Государственный университет морского и речного флота имени адмирала С. О. Макарова, Санкт-Петербург, Россия

² Санкт-Петербургский государственный морской технический университет, Санкт-Петербург, Россия

✉ *artarbuzv@gmail.com

ДЛЯ ЦИТИРОВАНИЯ

Арбузов А. М., Нырков А. П., Гаскаров Д. В., Ли И. В. Анализ угроз прикладного уровня IoT-систем и применение методов машинного обучения для обеспечения их безопасности // Проблемы информационной безопасности. Компьютерные системы. 2026. № 3. С. 179–189.
DOI: 10.66424/2071-8217-2026-3-13

ПОСТУПИЛА 27.04.2026

ПРИНЯТА 05.08.2026

ОПУБЛИКОВАНА 13.10.2026

© Арбузов А. М., Нырков А. П., Гаскаров Д. В., Ли И. В.

Издатель: Санкт-Петербургский политехнический университет Петра Великого

АННОТАЦИЯ

Проведен анализ угроз, характерных для прикладного уровня современных IoT-систем, а также возможностей применения алгоритмов машинного обучения для обеспечения его безопасности. Исследование сфокусировано на анализе данного уровня, поскольку приложения управления IoT имеют разнородную поверхность для реализации атак. Проводится обзор работ, в которых предлагаются решения на основе алгоритмов машинного обучения для обнаружения и предотвращения угроз, которым подвержены современные IoT приложения, поскольку данные приложения в том числе являются точкой взаимодействия человека с IoT-системой. Также поднимаются вопросы использования машинного обучения для противодействия методам социальной инженерии, которые могут быть направлены на пользователей IoT.

КЛЮЧЕВЫЕ СЛОВА

Интернет вещей, водный транспорт, архитектура IoT-систем, уровень приложений, социальная инженерия, фишинг, большие языковые модели, машинное обучение, кибербезопасность

Original article

DOI 10.66424/2071-8217-2026-3-13

ANALYSIS OF THREATS OF APPLICATION LEVEL OF IOT-SYSTEMS AND APPLICATION OF MACHINE LEARNING METHODS TO ENSURE THEIR SAFETY

A. M. Arbuzov^{1*}, A. P. Nyrkov¹, D. V. Gaskarov¹, I. V. Li²

¹Admiral Makarov State University of Maritime and Inland Shipping, St. Petersburg, Russia

²State Maritime Technical University, St. Petersburg, Russia

✉ *artarbuzv@gmail.com

FOR CITATION

Arbuzov A. M., Nyrkov A. P., Gaskarov D. V., Li I. V. Analysis of threats of application level of IoT-systems and application of machine learning methods to ensure their safety. *Problems of information security. Computer systems*. 2026. No. 3, pp. 179–189. DOI: 10.66424/2071-8217-2026-3-13 (In Russian)

RECEIVED 27.04.2026

ACCEPTED 05.08.2026

PUBLICATION 13.10.2026

ABSTRACT

This paper analyzes threats characteristic of the application layer of modern IoT systems, as well as the potential of machine learning algorithms for ensuring its security. The study focuses on the analysis of this layer, since IoT management applications have a highly diverse attack surface. The paper reviews studies proposing machine-learning-based solutions for detecting and preventing threats affecting modern IoT applications. Since these applications also serve as a point of interaction between humans and IoT systems, the paper also addresses the use of machine learning to counter social engineering techniques targeting IoT users.

KEYWORDS

Internet of Things, water transportation, IoT systems architecture, application layer, social engineering, phishing, large language models, machine learning, cybersecurity

1. ВВЕДЕНИЕ

Технологии интернета вещей являются одними из наиболее быстроразвивающихся технологий текущего века. Особенно тесно они связаны с другим технологическим направлением – искусственным интеллектом. Предлагается огромное количество концепций, основанных на совместном применении технологий IoT и алгоритмов машинного обучения (Machine Learning – ML), где IoT-системы обеспечивают сбор данных об окружающей среде, которые могут использоваться интеллектуальными алгоритмами. В сфере водного транспорта IoT-системы нашли свое применение в такой концепции, как «Умный порт», направленной на автоматизацию технологических процессов порта, а также надводный автономный транспорт, где системы IoT используются в качестве коннектора взаимодействия между алгоритмами ML и окружающей средой. Данные концепции позволяют значительно разгрузить человека, увеличить эффективность систем и как итог сократить экономические расходы [1].

Однако IoT-системы имеют свои уязвимости, которые могут быть эксплуатированы злоумышленником, что в свою очередь может не просто нанести материальный ущерб, а поставить под угрозу жизни людей.

Данная работа является продолжением научного труда [2] в рамках которого,

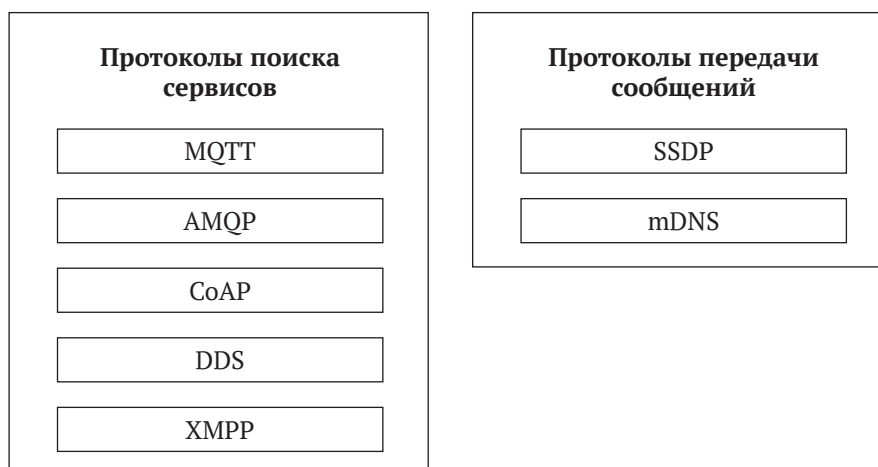
авторы провели обзор работ по использованию алгоритмов ML в противодействии кибератакам физического и сетевого уровней. Здесь будет рассмотрен верхний уровень архитектуры IoT – уровень приложений, его уязвимости и возможности использования подходов ML для обеспечения защищенности данных систем. Отдельно будут рассмотрены атаки социальной инженерии, в том числе с использованием больших языковых моделей, а также методы противодействия им с помощью алгоритмов ML.

2. АРХИТЕКТУРА ПРИКЛАДНОГО УРОВНЯ

Прикладной уровень, или уровень приложений – самый высокий уровень в архитектуре IoT. Здесь находятся пользовательские приложения, позволяющие управлять IoT-системой. Хорошим примером взаимодействия человека и системы IoT является «Умный дом» от Apple. Все новые модели iPhone, MacBook, iPad поставляются с уже встроенным приложением управления IoT под названием Home. Это приложение позволяет управлять аксессуарами HomeKit с любого устройства от Apple [3].

На данном уровне в основном используются два вида протоколов (см. рисунок). Одни нацелены на передачу сообщений

Уровень приложений



Протоколы прикладного уровня

Application-layer protocols

(например, MQTT, DDS, CoAP и т.д.), задачей других является обнаружение служб (например, SSDP и mDNS).

Прикладной уровень не менее важен, чем физический и сетевой, поскольку именно от него во многом зависит, будет ли потребитель пользоваться системой IoT. Здесь первично удобство, поэтому пользовательские интерфейсы с течением времени все больше упрощаются и чаще обычного становятся целью кибератак.

Уязвимости и атаки прикладного уровня. На прикладном уровне IoT-систем самыми распространенными являются семь протоколов: MQTT, CoAP, AMQP, DDS, XMPP, mDNS, SSDP. Данные протоколы используются с целью передачи информации и для обнаружения служб. Выбор протоколов зависит от того, какие функции должна выполнять IoT-система. Например, протоколы CoAP и MQTT отлично подходят для сбора данных, а mDNS и SSDP являются более предпочтительными в IoT-системах для функции поиска услуг.

Данные протоколы являются отличным решением по транспортировке данных, но в плане безопасности они не так совершенны. Часть протоколов имеет слабые механизмы защиты, в остальных протоколах подобные механизмы все

отсутствуют. Рассмотрим безопасность каждого протокола отдельно.

MQTT легковесный протокол прикладного уровня, который широко используется в IoT благодаря своей оптимизации. Данный протокол используется как в системах умных домов, так и в областях промышленности и здравоохранения, что делает его критически важным сегментом систем [4]. В качестве меры безопасности в MQTT используются протоколы шифрования TLS/SSL, которые сказываются на энергопотреблении, но при этом значительно повышают безопасность [5]. Однако данный протокол имеет ряд рисков, первым из которых является неправильно настроенное шифрование [6]. Также протокол уязвим к DoS-атакам, поскольку его архитектура строится на модели «публикация – подписка». Центральным компонентом этой модели является брокер, который в результате может быть перегружен чрезмерным количеством запросов [6–8].

Протокол DDS также использует механику «публикация – подписка», однако, в отличие от MQTT, ему не нужен центральный брокер, что делает его крайне гибким и легко масштабируемым [9], также протокол имеет большие возможности интеграции благодаря поддержке

плагинов. Учитывая, что в некоторых реализациях протокол может передавать данные об участниках системы в открытом виде, что в свою очередь позволяет провести атаку «человек посередине» [10]. Также стоит учитывать, что опасность могут представлять сами плагины, поскольку они могут нести в себе уязвимости, допущенные в рамках разработки, что также может расширять поверхность атак.

AMQP – открытый протокол уровня приложений, используемый для обмена сообщений между разнородными системами. Данный протокол использует модель очередей сообщений, и поддерживает асинхронную передачу данных между сервисами и клиентами [11]. Основные уязвимости протокола связаны с неправильным конфигурированием и пользовательскими интерфейсами. Открытые команды выключения этого протокола могут быть использованы для отказа в обслуживании.

Протокол CoAP является связующим звеном между конечными IoT-устройствами (сенсорами). Его основой является REST-подобная модель «запрос – ответ» [12]. В данном протоколе необходимо найти некий баланс между производительностью протокола и его защищенностью. Чем выше уровень безопасности, тем больше нагрузка на вычислительные ресурсы. Поэтому пренебрежение некоторыми службами защиты в угоду производительности может сделать данный протокол уязвимым для атак. В протоколе используется DTLS – реализация TLS на базе протокола UDP, который открывает возможности реализации атаки типа «отказ в обслуживании».

Протокол XMPP поддерживает большое количество разнообразных механизмов защиты, таких как шифрование (TLS), цифровая подпись на основе расширения XEP-0027, SSO. В некоторых реализациях данного протокола имеются проблемы, связанные с аутентификацией. Например, реализация Mellium подвержена уязвимости CVE-2024-46957 [13], которая позволяет атакующему обойти механизмы аутентификации с помощью подделки

ответа, что приводит к подмене пользователей и утечке данных.

Протоколы SSDP и mDNS ориентированы на поиск сервисов в сети IoT. Протокол SSDP нацелен на обнаружение устройств и последующую их настройку. Протокол mDNS выполняет аналогичную функцию поиска служб, а также занимается разрешением имен хостов на локальных каналах без использования централизованного DNS-сервера, т.е. протокол позволяет устройству выбрать имя в зоне .local (псевдодомена верхнего уровня), которая используется для идентификации хостов (упомянутая экосистема HomeKit от Apple как раз использует данный протокол для разрешения имен) [14]. Данные протоколы не имеют никаких встроенных механизмов защиты [15], что делает их полностью безоружными перед злоумышленником. Основная часть атак на данные протоколы из-за отсутствия механизмов защиты – атака «человек посередине» и отказ в обслуживании (DoS и DDoS).

Стоит учесть, что приложения, которые установлены для взаимодействия с IoT-системой, также могут использоваться как плацдарм для разворачивания атак на само приложение IoT. На данный момент большую часть доли рынка составляют устройства на базе ОС Android, которая в свою очередь имеет открытую архитектуру и снабжена интерфейсом программирования приложений [16]. Такая открытость позволяет злоумышленникам создавать приложения с незадекларированными возможностями и выставлять такое ПО на различных ресурсах. В результате подобная модифицированная система может попасть на устройства пользователя IoT-системы, санкционировав таким образом атаку на IoT-сеть [17].

Решения на основе ML, противодействующие атакам прикладного уровня. Атаки на уровень приложений имеют большую неоднородность, чтобы для каждого вида атак подбирать наилучшее решение в сфере ML. Поэтому хорошим вариантом будет рассмотреть алгоритмы, направленные на обнаружение различных видов атак.

В исследовании [18] представлен подход по решению дисбаланса классов для набора данных Bot-IoT, однако помимо этого представлен сравнительный анализ по обнаружению DoS и DDoS. В анализе участвовали такие алгоритмы классификации, как дерево решений (DT), случайный лес (RF), метод опорных векторов (SVM) и рекуррентные нейронные сети (RNN). В итоге модели на основе RF, DT и MLP показали точность свыше 99 % на тестовой выборке. В другом исследовании [19] проанализирована специфика сетевых данных стандарта 802.11 (Wi-Fi). Результаты работы показали, что объединение данных, полученных от проводных и беспроводных сетей, позволяет значительно улучшить точность моделей по поиску аномалий в трафике сетей последнего типа. В итоге удалось довести точность моделей на основе RF, а также ансамблей, построенных по схеме градиентного бустинга, до 96,7 % по метрике AUC (Area Under the Curve).

Нужно учесть, что у злоумышленников есть возможность создавать вредоносное ПО и доносить его до устройств управления IoT-системой. Основную опасность несет ПО, разработанное под операционную систему Android [20]. Поэтому необходимо рассмотреть решения на основе ML для обнаружения вредоносного ПО на мобильных устройствах. Здесь применяются различные подходы для обнаружения вредоносного ПО в IoT-системах, начиная от использования классических видов алгоритмов ML в статическом и динамическом анализах и заканчивая биоинспирированными подходами, т.е. использованием алгоритмов, вдохновленных биологическими системами, например, генетические алгоритмы. Первые позволяют покрыть большую часть современных угроз, вторые же показывают свою пользу в адаптивном реагировании на неизвестные угрозы (использование уязвимостей 0-day) [21]. Также стоит отметить, что отдельным направлением обеспечения безопасности IoT, в том числе на уровне приложений, является оценка уровня безопасности подобных систем. Здесь интересна работа [22], в которой

авторы используют интеллектуальные системы для анализа рисков, которым могут быть подвержены системы.

3. МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ КАК ОДИН ИЗ ТИПОВ УГРОЗ ДЛЯ ИОТ-СИСТЕМ

Социальная инженерия как инструмент атаки. Социальная инженерия (SE) – это воздействие с применением методов манипулирования, направленное как на одного человека, так и на группу лиц, целью которого является получение доступа к конфиденциальной информации либо контроль поведения объекта воздействия [23]. Примерами SE являются фишинговые письма, поддельные веб-страницы, поддельные звонки и т.д. Отметим, что показатель защищенности от атак с использованием методов социальной инженерии в основном зависит от самого человека. В исследовании [24] автор проводит опрос, в результате которого выясняется, что даже при наличии самых передовых средств защиты человек все равно остается уязвим для атак. Здесь имеет значение степень осведомленности самого человека о методах социальной инженерии.

Отдельно стоит отметить, что научный прогресс в течение последних лет вывел возможности социальной инженерии на новый уровень. Речь о больших языковых моделях (Large Learning Model – LLM), которые способны обучаться на паттернах общения между людьми, что позволяет им подстраиваться под диалог с жертвой, т.е. значительно уменьшить необходимые усилия, которые будут применены злоумышленником.

Так, например, ChatGPT способен генерировать фишинговые письма, в которых будет имитирован стиль и официальный тон коммуникации, что в результате не позволяет пользователям отличить такие письма от действительно легитимных. В исследовании [25] авторы обсудили возможности и риски использования ChatGPT

в рамках атак СИ. Также большие языковые модели способны персонализировать сообщения [26], т.е. генерировать сообщения от имени знакомых человека, против которого направлена атака. Зачастую для этой цели алгоритм обучают на переписке человека, в роли которого необходимо представиться в фишинге. Также хорошим примером возможностей LLM является работа [27], в которой авторы исследуют применение LLM в симуляции атак социальной инженерии.

Решения ML, противодействующие угрозам социальной инженерии в области IoT. Существующие механизмы ML способны помочь пользователям защититься от такого метода манипулирования, как фишинг. В исследовании [28] проводилась разработка механизма определения фишинговых писем с помощью ансамбля алгоритмов классификации по схеме Adaboost. В ходе исследования авторы объединяют такие алгоритмы, как k -ближайших соседей (KNN), логистическая регрессия (Logistic Regression – LR), линейная регрессия и наивный байесовский классификатор (NB). В заключении авторы приводят следующие результаты: среди одиночных классификаторов наибольшей точности удалось достичь алгоритму KNN – 96 %, сам же ансамбль показал точность в 98,3 %, из 1000 значений тестового набора алгоритм дал всего девять ложноотрицательных и восемь ложноположительных ответов.

Отдельно стоит отметить, что большие языковые модели помимо генерации фишинга способны ему же и противодействовать. Так, в работе [29] авторы исследовали возможности различных LLM к обнаружению фишинговых писем. В результате выявлено, что модели OpenAI (GPT-3.5, GPT-3.5-Turbo-Instruct, ChatGPT) способны качественно распознавать фишинговые электронные письма. Обусловлен данный результат широким диапазоном параметров, что позволяет понимать языковые нюансы.

Заслуживает внимания работа [30], в которой предлагается система под названием ChatPhishDetector, которая спо-

собна распознавать фишинговые сайты. Эта система собирает информацию с веб-сайта, нормализует ее, генерирует запрос в LLM и получает результат обнаружения из ответа. При использовании GPT-4V достигнуты следующие результаты: точность (precision) – 98,7 %, полнота (recall) – 99,6 %.

4. РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Машинное обучение безусловно открывает широкий спектр возможностей для обеспечения безопасности IoT-систем. В контексте выявления и предотвращения атак на пользователя системы алгоритмы ML предлагают большую гибкость. Это позволяет охватить большую разнородность атак, что свойственно для уровня приложений IoT, поскольку на данном уровне имеется широкий стек протоколов передачи ПО, разработанного в рамках OpenSource и распространяемого через различных поставщиков (например, GooglePlay или AppStore). Также стоит отметить, что немалую роль в проблемах безопасности играют человеческие ошибки.

В рамках работы рассмотрены различные подходы, основанные на использовании алгоритмов ML для обеспечения информационной безопасности IoT-систем. Предлагались варианты с использованием нейронных сетей (NN), деревьев решений (DT), метода опорных векторов (SVM). Однако наибольшей эффективности удастся добиться при объединении нескольких алгоритмов, иными словами, при использовании ансамблей.

При распознавании атак социальной инженерии ансамбли также показывают успехи, но могут терять эффективность против фишинговых сообщений, сгенерированных с помощью больших языковых моделей (LLM), которые способны улавливать языковые нюансы. Однако сами LLM показывают большие результаты в распознавании контента, сгенерированного с помощью модели, а также в целом в распознавании фишинга как для сообщений, так для сайтов.

5. ЗАКЛЮЧЕНИЕ

Все чаще появляются утверждения, что человек является одной из главных уязвимостей информационных систем и IoT-системы не исключение. Пользовательский уровень IoT подвержен большой разнородности атак. Часть уязвимостей закрывается, однако развитие данных систем приносит уже новые уязвимости в эти системы. Но не всегда необходимо владеть техническими навыками, чтобы получить несанкционированный доступ к системе, порой этого можно добиться воздействием на человека (так называемая атака социальной инженерии). С появлением больших языковых моделей необязательно взаимодействовать с человеком, можно переложить эту работу на данные модели.

В представленной работе алгоритмы машинного обучения рассматриваются как средства обнаружения и предотвращения атак на пользователя (атаки на пользовательские приложения, атаки социальной инженерии) в контексте IoT-систем. Учитывая, что данный уровень архитектуры IoT не имеет серьезных ограничений в вычислительных ресурсах по сравнению с тем же физическим, это позволяет прибегнуть к таким методам, как ансамбли алгоритмов ML, а также использовать большие языковые модели. Однако перед внедрением методов машинного обучения стоит помнить о необходимости предварительного расчета вычислительных ресурсов, поскольку задержка передачи данных в рамках IoT-систем является критически важной, иными словами системы безопасности не должны оказывать какое-либо воздействие на производительность.

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

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

СПИСОК ИСТОЧНИКОВ

1. **Арбузов А. М.** Анализ экономической перспективы использования автономных надводных судов // Современные вызовы транспортной отрасли: новые возможности : материалы межвузовской научно-практической конференции транспортных вузов, 27–28 февраля 2024 г., Москва, Россия. М. : Издательско-торговая корпорация «Дашков и К», 2024. С. 12–15. EDN: AAXHFE.
2. **Арбузов А. М., Нырков А. П., Терехов А. Н. и др.** Применение алгоритмов машинного обучения в обеспечении безопасности сетевой инфраструктуры IoT-систем на водном транспорте // Проблемы информационной безопасности. Компьютерные системы. 2025. № 2(64). С. 131–142. DOI: 10.48612/jisp/3zat-fd5f-vemt. EDN: TNQZDE.
3. Apple inc. URL: <https://developer.apple.com/homekit/> (дата обращения: 14.01.2026).
4. **Prantl T., Iffländer L., Herrnleben S. et al.** Performance Impact Analysis of Securing MQTT Using TLS // Proceedings of the ACM/SPEC International Conference on Performance Engineering (ICPE '21): Association for Computing Machinery, New York, NY, USA. 2021. P. 241–248. DOI: 10.1145/3427921.3450253.
5. **Gentile A., Macri D., Carnì D. et al.** A Network Performance Analysis of MQTT Security Protocols with Constrained Hardware in the Dark Net for DMS // Applied Sciences. 2024. Vol. 14. № 18. № 8501. DOI:10.3390/app14188501.
6. **Husnain M., Hayat K., Cambiaso E. et al.** Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System // Sensors. 2022. Vol. 22. № 2. № 567. DOI:10.3390/s22020567.

7. **Hintaw A., Manickam S., Abomaali M., Karuppayah S.** MQTT Vulnerabilities, Attack Vectors and Solutions in the Internet of Things (IoT) // IETE Journal of Research. Latest Articles. 2023. Vol. 69. № 6. P. 3368–3397. DOI: 10.1080/03772063.2021.1912651.
8. **Raikar M. M., Meena S. M.** Vulnerability assessment of MQTT protocol in Internet of Things (IoT) // 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), 21–23 May 2021, Jalandhar, India. 2021. P. 535–540. DOI: 10.1109/ICSCCC51823.2021.9478156.
9. **Jinze Du, Chengtai Gao, Tao Feng.** Formal Safety Assessment and Improvement of DDS Protocol for Industrial Data Distribution Service // Future Internet. 2022. Vol. 15. № 1. № 24. DOI:10.3390/fi15010024.
10. A Security Analysis of the Data Distribution Service (DDS) Protocol. URL: https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-the-data-distribution-service-dds-protocol.pdf (дата обращения: 14.01.2026).
11. **Altulaihan E., Almaiah M., Aljughaiman A.** Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions // Electronics. 2022. Vol. 11. № 20. № 3330. DOI: 10.3390/electronics11203330.
12. **Lombardi M., Pascale F., Santaniello D.** Internet of Things: A General Overview between Architectures, Protocols and Applications // Information. 2021. Vol. 12. № 1. № 87. DOI: 10.3390/info12020087.
13. CVE-2024-46957. URL: <https://nvd.nist.gov/vuln/detail/CVE-2024-46957> (дата обращения: 14.01.2026).
14. **Altulaihan E., Almaiah M., Aljughaiman A.** Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions // Electronics. 2022. Vol. 11. № 20. № 3330. DOI: 10.3390/electronics11203330.
15. **Sharma G., Vidalis S., Anand N. et al.** A Survey on Layer-Wise Security Attacks in IoT: Attacks, Countermeasures, and Open-Issues // Electronics. 2021. Vol. 10. № 19. № 12. DOI:10.3390/electronics10192365.
16. **Маликов М. С., Соболев Н. В., Зегжда Д. П.** Программный комплекс для статического анализа безопасности и модификации Android приложений в процессе их установки // Методы и технические средства обеспечения безопасности информации. 2024. № 33. С. 77–78. EDN: IKPAJA.
17. **Chatzoglou E., Kambourakis G., Smiliotopoulos C.** Let the Cat out of the Bag: Popular Android IoT Apps under Security Scrutiny // Sensors. 2022. Vol. 22. № 2. № 513. DOI: 10.3390/s22020513.
18. **Almaraz-Rivera J. G., Pérez-Díaz J. A., Cantoral-Ceballos J. A.** Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models // Sensors. 2022. Vol. 22. № 9. № 3367. DOI: 10.3390/s22093367.
19. **Chatzoglou E., Kambourakis G., Smiliotopoulos C., Kolias C.** Best of Both Worlds: Detecting Application Layer Attacks through 802.11 and Non-802.11 Features // Sensors. 2022. Vol. 22. № 15. № 5633. DOI: 10.3390/s22155633.
20. **Солдатова А. Ю., Зегжда Д. П., Павленко Е. Ю.** Обнаружение мошенничества с мобильной рекламой на основе анализа работы Android-приложений // Материалы конференции «Информационные технологии в управлении» (ИТУ-2022): 15-я мультиконференция по проблемам управления, 4–6 октября 2022 г., Санкт-Петербург, Россия. СПб. : «Концерн «Центральный научно-исследовательский институт «Электроприбор»», 2022. С. 246–249. EDN: HQKIXL.
21. **Wolsey A.** The State-of-the-Art in AI-Based Malware Detection Techniques: A Review // arXiv:2210.11239. 2022. DOI: 10.48550/arXiv.2210.11239.
22. **Зегжда Д. П., Москвин Д. А., Орел Е. М.** Автоматизация управления безопасностью интеллектуальных систем с использованием графа атак и анализа рисков // Защита информации. Инсайд. 2022. № 2(104). С. 22–28. EDN: HUFAIM.
23. **Годунова М. С., Копосова М. С.** Социальная инженерия как метод киберпреступления // StudNet. 2022. Т. 5. № 6. С. 5573–5580.
24. **Малькута А. М., Радыгин В. Ю., Манаенкова Т. А.** Социальная инженерия – уязвимость современных систем // Финансовая безопасность. Современное состояние и перспективы развития : материалы VIII Международной научно-практической конференции Международного сетевого института

- в сфере ПОД/ФТ, 14–15 декабря 2022 г., Москва, Россия. М. : Национальный исследовательский ядерный университет «МИФИ», 2022. Т. 2. С. 305–310. EDN: YZMDXM.
25. **Стрижков В. А.** Применение методов машинного обучения для противодействия инсайдерской угрозе информационной безопасности // Вопросы безопасности. 2023. № 4. С. 152–165. DOI: 10.25136/2409-7543.2023.4.68856. EDN: JZMNXQ.
 26. **Haque M. A., Li Shuai.** Exploring ChatGPT and its impact on society // AI and Ethics. 2024. № 5. P. 791–803. DOI: 10.1007/s43681-024-00435-4.
 27. **Богина В. М., Борисов Г. И., Братко В. В. и др.** Анализ применимости больших языковых моделей к моделированию реалистичных диалогов в целях симуляции атак социальной инженерии // Проблемы ин-формационной безопасности. Компьютерные системы. 2025. № 4(67). С. 9–22. DOI: 10.48612/jisp/kfvm-3811-vmk4. EDN: NPB MIX.
 28. **Baldassarre M., Caivano D., Fernández N. B. et al.** The Social Impact of Generative AI: An Analysis on ChatGPT // GoodIT '23 : Proceedings of the 2023 ACM Conference on Information Technology for Social Good. 2023. P. 363–373. DOI: 10.1145/3582515.3609555.
 29. **Patel H., Rehman U., Iqbal F.** Evaluating the Efficacy of Large Language Models in Identifying Phishing Attempts // 2024 16th International Conference on Human System Interaction (HSI), Paris, France. 2024. P. 1–7. DOI: 10.1109/HSI61632.2024.10613528.
 30. **Koide T., Fukushi N., Nakano H., Chiba D.** Detecting Phishing Sites Using ChatGPT // arXiv.2306.05816. 2023. DOI: 10.48550/arXiv.2306.05816.

REFERENCES

1. **Arbuzov A. M.** Analysis of the economic prospects for using autonomous surface vessels. *Sovremennye vyzovy transportnoj otrasli: novye vozmozhnosti : materialy mezhdvuzovskoj nauchno-prakticheskoy konferencii transportnyh vuzov*, 27–28 fevralya 2024 g., Moscow, Russia. Moscow : Izdatel'sko-torgovaya korporaciya "Dashkov i K", 2024, pp. 12–15. EDN: AAXHFE. (In Russian)
2. **Arbuzov A. M., Nyrkov A. P., Terekhov A. N. et al.** The application of machine learning algorithms in securing IoT-systems network infrastructure in water transport systems. *Problems of information security. Computer systems*. 2025. No. 2(64), pp. 131–142. DOI: 10.48612/jisp/3zatfd5f-vemt. EDN: TNQZDE. (In Russian)
3. Apple inc. URL: <https://developer.apple.com/homekit/> (accessed: 14.01.2026).
4. **Prantl T., Iffländer L., Herrnleben S. et al.** Performance Impact Analysis of Securing MQTT Using TLS. *Proceedings of the ACM/SPEC International Conference on Performance Engineering (ICPE '21)*: Association for Computing Machinery, New York, NY, USA. 2021, pp. 241–248. DOI: 10.1145/3427921.3450253.
5. **Gentile A., Macri D., Carnì D. et al.** A Network Performance Analysis of MQTT Security Protocols with Constrained Hardware in the Dark Net for DMS. *Applied Sciences*. 2024. Vol. 14. No. 18. No. 8501. DOI:10.3390/app14188501.
6. **Husnain M., Hayat K., Cambiaso E. et al.** Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System. *Sensors*. 2022. Vol. 22. No. 2. No. 567. DOI:10.3390/s22020567.
7. **Hintaw A., Manickam S., Abomaali M., Karuppayah S.** MQTT Vulnerabilities, Attack Vectors and Solutions in the Internet of Things (IoT). *IETE Journal of Research. Latest Articles*. 2023. Vol. 69. No. 6, pp. 3368–3397. DOI: 10.1080/03772063.2021.1912651.
8. **Raikar M. M., Meena S. M.** Vulnerability assessment of MQTT protocol in Internet of Things (IoT). 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), 21–23 May 2021, Jalandhar, India. 2021, pp. 535–540. DOI: 10.1109/ICSCCC51823.2021.9478156.
9. **Jinze Du, Chengtai Gao, Tao Feng.** Formal Safety Assessment and Improvement of DDS Protocol for Industrial Data Distribution Service. *Future Internet*. 2022. Vol. 15. No. 1. No. 24. DOI: 10.3390/fi15010024.
10. A Security Analysis of the Data Distribution Service (DDS) Protocol. URL: <https://>

- documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-the-data-distribution-service-dds-protocol.pdf (accessed: 14.01.2026).
11. **Altulaihan E., Almaiah M., Aljughaiman A.** Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. *Electronics*. 2022. Vol. 11. No. 20. No. 3330. DOI: 10.3390/electronics11203330.
 12. **Lombardi M., Pascale F., Santaniello D.** Internet of Things: A General Overview between Architectures, Protocols and Applications. *Information*. 2021. Vol. 12. No. 1. No. 87. DOI: 10.3390/info12020087.
 13. CVE-2024-46957. URL: <https://nvd.nist.gov/vuln/detail/CVE-2024-46957> (accessed: 14.01.2026).
 14. **Altulaihan E., Almaiah M., Aljughaiman A.** Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. *Electronics*. 2022. Vol. 11. No. 20. No. 3330. DOI: 10.3390/electronics11203330.
 15. **Sharma G., Vidalis S., Anand N. et al.** A Survey on Layer-Wise Security Attacks in IoT: Attacks, Countermeasures, and Open-Issues. *Electronics*. 2021. Vol. 10. No. 19. No. 12. DOI: 10.3390/electronics10192365.
 16. **Malikov M. S., Sobolev N. V., Zegzhda D. P.** Software complex for static security analysis and modification of Android applications during their installation. *Metody i tehnikeskie sredstva obespecheniya bezopasnosti informacii*. 2024. No. 33, pp. 77–78. EDN: IKPAJA. (In Russian)
 17. **Chatzoglou E., Kambourakis G., Smiliotopoulos C.** Let the Cat out of the Bag: Popular Android IoT Apps under Security Scrutiny. *Sensors*. 2022. Vol. 22. No. 2. No. 513. DOI: 10.3390/s22020513.
 18. **Almaraz-Rivera J. G., Pérez-Díaz J. A., Cantoral-Ceballos J. A.** Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models. *Sensors*. 2022. Vol. 22. No. 9. No. 3367. DOI: 10.3390/s22093367.
 19. **Chatzoglou E., Kambourakis G., Smiliotopoulos C., Koliass C.** Best of Both Worlds: Detecting Application Layer Attacks through 802.11 and Non-802.11 Features. *Sensors*. 2022. Vol. 22. No. 15. No. 5633. DOI: 10.3390/s22155633.
 20. **Soldatova A. Yu., Zegzhda D. P., Pavlenko E. Yu.** Detection of mobile advertising fraud based on an analysis of Android app performance. *Materialy konferencii "Informacionnye tehnologii v upravlenii"* (ITU-2022) : 15-ya mul'tikonferenciya po problemam upravleniya, 4–6 oktyabrya 2022 g., St. Petersburg, Russia. St. Petersburg : "Koncern "Central'nyj nauchno-issledovatel'skij institut "Ehlektropribor", 2022, pp. 246–249. EDN: HQKIXL. (In Russian)
 21. **Wolsey A.** The State-of-the-Art in AI-Based Malware Detection Techniques: A Review. *arXiv:2210.11239*. 2022. DOI: 10.48550/arXiv.2210.11239.
 22. **Zegzhda D. P., Moskvina D. A., Orel E. M.** Automatic security management of smart infrastructures using attack graph and risk analysis. *Zashita informacii. Inside*. 2022. No. 2(104), pp. 22–28. EDN: HUFAIM. (In Russian)
 23. **Godunova M. S., Koposova M. S.** Social engineering as a method of cybercrime. *Stud-Net*. 2022. Vol. 5. No. 6, pp. 5573–5580. (In Russian)
 24. **Malkota A. M., Radygin V. Yu., Manaenkova T. A.** Social engineering – a vulnerability of modern systems. *Financial security. Sovremennoe sostoyanie i perspektivy razvitiya* : materialy VIII Mezhdunarodnoj nauchno-prakticheskoy konferencii Mezhdunarodnogo setevogo instituta v sfere POD/FT, 14–15 dekabrya 2022 g., Moscow, Russia. Moscow : Nacional'nyj issledovatel'skij yadernyj universitet "MIFI", 2022. Vol. 2, pp. 305–310. EDN: YZMDXM. (In Russian)
 25. **Strizhkov V. A.** Application of machine learning methods to counter insider threat to information security. *Security Issues*. 2023. No. 4, pp. 152–165. DOI: 10.25136/2409-7543.2023.4.68856. EDN: JZMHXQ. (In Russian)
 26. **Haque M. A., Li Shuai.** Exploring ChatGPT and its impact on society. *AI and Ethics*. 2024. No. 5, pp. 791–803. DOI: 10.1007/s43681-024-00435-4.
 27. **Bogina V. M., Borisov G. I., Bratko V. V. et al.** Analysis of the applicability of large language models to the simulation of realistic dialogues for the purpose of simulating social engineering attacks. *Problems of information security. Computer systems*. 2025. No. 4, pp. 9–22. DOI: 10.48612/jisp/kfvm-3811-vmk4. EDN: NPB MIX. (In Russian)

28. **Baldassarre M., Caivano D., Fernández N. B. et al.** The Social Impact of Generative AI: An Analysis on ChatGPT. GoodIT '23 : Proceedings of the 2023 ACM Conference on Information Technology for Social Good. 2023, pp. 363–373. DOI: 10.1145/3582515.3609555.
29. **Patel H., Rehman U., Iqbal F.** Evaluating the Efficacy of Large Language Models in Identifying Phishing Attempts. 2024 16th International Conference on Human System Interaction (HSI), Paris, France. 2024, pp. 1–7. DOI: 10.1109/HSI61632.2024.10613528.
30. **Koide T., Fukushi N., Nakano H., Chiba D.** Detecting Phishing Sites Using ChatGPT. *arXiv.2306.05816*. 2023. DOI: 10.48550/arXiv.2306.05816.

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

АРБУЗОВ Артем Максимович – аспирант, Государственный университет морского и речного флота имени адмирала С. О. Макарова, Россия, 198035, Санкт-Петербург, Двинская ул., д. 5/7
E-mail: artarbuzv@gmail.com
ORCID: 0000-0003-0123-010X

ARBUZOV Artem M. – Postgraduate Student, Admiral Makarov State University of Maritime and Inland Shipping, Russia, 198035, St. Petersburg, Dvinskaya str., 5/7

НЫРКОВ Анатолий Павлович – д-р техн. наук, профессор, заведующий кафедрой, Государственный университет морского и речного флота имени адмирала С. О. Макарова, Россия, 198035, Санкт-Петербург, Двинская ул., д. 5/7
E-mail: kaf.koib@gmail.com, nyrkowap@gumrf.ru
ORCID: 0000-0002-9803-6284

NYRKOV Anatoliy P. – Doctor of Engineering Sciences, Professor, Head of Department, Admiral Makarov State University of Maritime and Inland Shipping, Russia, 198035, St. Petersburg, Dvinskaya str., 5/7

ГАСКАРОВ Дилияур Вагизович – д-р техн. наук, профессор, Государственный университет морского и речного флота имени адмирала С. О. Макарова, Россия, 198035, Санкт-Петербург, Двинская ул., д. 5/7

GASKAROV Dilyaur V. – Doctor of Engineering Sciences, Professor, Admiral Makarov State University of Maritime and Inland Shipping, Russia, 198035, St. Petersburg, Dvinskaya str., 5/7

ЛИ Изольда Валерьевна – канд. техн. наук, доцент, Санкт-Петербургский государственный морской технический университет, Россия, 190121, Санкт-Петербург, Лоцманская ул., д. 3
E-mail: LiIV@gumrf.ru
ORCID: 0000-0002-3661-9417

LI Izolda V. – Candidate of Engineering Sciences, Associate Professor, State Marine Technical University, Russia, 190121, St. Petersburg, Lotsmanskaya str., 3