УДК 004.738.5 DOI 10.21777/2500-2112-2025-3-70-82

АНАЛИЗ ЗАЩИТНЫХ ПРОТОКОЛОВ СИСТЕМЫ ДОМЕННЫХ ИМЁН В РАМКАХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Рахмани Джахед[1],
e-mail: jahed@mail.ru,

Кондракова Анна Денисовна[1],
e-mail: anikasynch@gmail.com,

Коренкова Ангелина Сергеевна[1],
e-mail: angelinas1703@gmail.com,
[1]*Московский технический университет связи и информатики (МТУСИ), г. Москва, Россия*

Данное исследование направлено на комплексное рассмотрение проблемы безопасности системы доменных имён (DNS) в условиях промышленного интернета вещей (IIoT), где ограниченные вычислительные ресурсы устройств сочетаются с высокими требованиями к надёжности и отказоустойчивости. В работе проведён сравнительный анализ специализированных протоколов защиты DNS, включая DNSSEC, DoH, DoT, DoQ, а также облегчённых решений DoC и mDNS, применимых в условиях ограниченных вычислительных возможностей. В ходе эксперимента протестированы протоколы как в виртуальной среде, так и на микроконтроллере, что позволило оценить их эффективность на разных уровнях инфраструктуры. Предложен научно-методический подход к анализу протоколов защиты DNS в рамках промышленного интернета вещей, включающий следующие процедуры: формирование классификации кибератак на DNS в промышленной среде; внедрение полуколичественной модели оценки рисков, адаптированной к условиям ограниченной вычислительной мощности; сопоставление традиционных и облегчённых протоколов на базе практических экспериментов. Результаты исследования могут быть применены при выборе протоколов защиты DNS в промышленных системах, а также в образовательной и методической деятельности.

Ключевые слова: промышленный интернет вещей, DNS, безопасность IIoT, кибератаки, уязвимость протоколов защиты

ANALYSIS OF DNS SECURITY PROTOCOLS IN THE CONTEXT OF THE INDUSTRIAL INTERNET OF THINGS

Rahmani J.[1],
e-mail: jahed@mail.ru,

Kondrakova A.D.[1],
e-mail: anikasynch@gmail.com,

Korenkova A.S.[1],
e-mail: angelinas1703@gmail.com,
[1]*Moscow Technical University of Communications and Informatics (MTUCI), Moscow, Russia*

This study is aimed at a comprehensive review of the security problem of the Domain Name System (DNS) in the context of the Industrial Internet of Things (IIoT), where limited computing resources of devices are combined with high requirements for reliability and fault tolerance. A comparative analysis of specialized DNS protection protocols is presented, including DNSSEC, DoH, DoT, DoQ, as well as lightweight solutions such as DoC and mDNS, applicable under resource-limited conditions. The protocols were tested both in a virtualized environment and on a microcontroller, enabling an assessment of their efficiency across different infrastructure levels. A scientific and methodological approach to the analysis of DNS protection protocols within the framework of the industrial Internet of Things is proposed, including the following procedures: the forming of a classification of cyberattacks on DNS in an industrial environment; the introduction of a semi-quantitative risk assessment model

adapted to conditions of limited computing power; the comparison of traditional and lightweight protocols based on practical experiments. The investigation results can be applied to the selection of DNS security protocols in industrial systems, as well as in educational and methodological contexts.

Keywords: Industrial Internet of Things, DNS, IIoT security, cyberattacks, vulnerability of security protocols

Введение

Цифровая трансформация оказывает ключевое влияние на промышленность. С одной стороны, она способствует автоматизации и повышению эффективности производственных систем, с другой – возникновению высоких рисков в случае нарушения работы автоматизированных информационных систем. Примером может служить энергетическая отрасль Исламской Республики Иран, где 17 энергопроизводящих станций объединены единой корпоративной инфокоммуникационной системой, включающей множество подсистем, таких как система управления рынком электроэнергии или система распределенного диспетчерского контроля. Такая архитектура требует надёжной передачи данных между компонентами, что повышает значимость промышленного интернета вещей [1; 2].

Промышленный интернет вещей (Industrial Internet of Things, IIoT) объединяет датчики, контроллеры и системы автоматизации в единую сеть для обмена данными в реальном времени с целью оптимизации производственных процессов. Промышленный IoT ориентирован на надёжность, безопасность и масштабируемость в инфраструктурах, где отказоустойчивость является ключевым требованием [3]. Однако широкое внедрение IIoT в такие сферы, как энергетика, транспорт и промышленное производство, повышает риски кибератак.

Индустрия 4.0, базирующаяся на использовании искусственного интеллекта, киберфизических систем и интернета вещей, повышает эффективность производственных процессов, но одновременно сопровождается ростом киберугроз, риском утечек данных и технологической уязвимости. Существенным ограничением является низкая вычислительная мощность многих IIoT-устройств, что затрудняет внедрение традиционных средств защиты [4]. Ограниченные ресурсы затрудняют реализацию базовых мер защиты, особенно в отношении системы доменных имён (Domain Name System, DNS), которая играет ключевую роль в маршрутизации и сетевом взаимодействии. Система доменных имён является важным элементом сетевой инфраструктуры, преобразующим доменные имена в IP-адреса. При передаче запросов в незашифрованном виде DNS остаётся уязвимой к перехвату и подмене, что критично для производственных систем с высокими требованиями к безопасности. Для защиты трафика применяются специализированные протоколы – DNSSEC, DoH, DoT, DoQ, DoC и mDNS, различающиеся по степени защищённости и требованиям к ресурсам.

С учетом изложенного актуальным является разработка научно-методического подхода для анализа защитных протоколов системы доменных имен (DNS) в промышленных технологиях интернета вещей (IOT) и проведения измерений их параметров для реализации оптимальных мер защиты в конкретных производственных условиях.

Методологическая база исследования опиралась на сочетание сравнительного анализа, полуколичественной оценки рисков и экспериментальной апробации.

Анализ угроз безопасности DNS в технологиях IIoT

IIoT-устройства разрабатываются под конкретные задачи и работают в сложных условиях, предъявляющих требования к точности, надёжности и энергоэффективности. Однако большинство из них оснащены маломощными процессорами (вплоть до 8-битных с частотой 100–400 МГц) и ограниченной оперативной памятью. Кроме того, в IIoT-устройствах применяются энергоэффективные системы связи с невысокой пропускной способностью, поскольку высокоскоростная связь потребляет больше энергии элементов питания [5; 6]. Данные аппаратные ограничения существенно затрудняют внедрение усиленных протоколов безопасности, требуя разработки специализированных решений.

Существенным фактором риска выступает продолжительная автономная работа IIoT-устройств без технического обслуживания [5]. Промышленные устройства на удаленных объектах часто могут в течение продолжительного периода эксплуатироваться без обновления программного обеспечения и диагностики квалифицированными специалистами. Это обуславливается как их физической труднодоступностью, так и общей сложностью обслуживания распределенных систем такого масштаба.

Не менее важной проблемой остается отсутствие унифицированных стандартов безопасности. Многие вендоры уделяют недостаточно внимания встроенным механизмам защиты. Значительное количество устройств изначально имеет стандартные учетные данные для входа (типа *admin/admin*), что создает серьезную уязвимость. В случае компрометации таких устройств злоумышленник получает возможность модифицировать DNS-конфигурацию, перенаправляя трафик на контролируемые им вредоносные серверы.

Таким образом, основная проблема безопасности IIoT-устройств заключается в том, что в их производстве фокус смещен на их функциональность. Отсутствие встроенных механизмов защиты и обновлений вызывает существенные уязвимости для реализации кибератак.

Показательным примером уязвимости промышленных систем стала атака вируса Stuxnet на ядерный объект в Натанзе (2010). Вредоносный код, распространявшийся через носители, эксплуатировал уязвимости SCADA-систем, переписывая код логических контроллеров и вызывая физические повреждения оборудования. Атака вывела из строя около 20 % центрифуг и существенно замедлила ядерную программу Ирана [7]. Несмотря на то, что Stuxnet поражал классические промышленные системы, его успех продемонстрировал главную уязвимость – отсутствие изоляции критической инфраструктуры. В контексте IIoT аналогичные атаки могут осуществляться удалённо, например, путём подмены DNS-записей и перенаправления трафика на вредоносные серверы. Это подчёркивает необходимость применения защищённых DNS-протоколов в промышленных сетях.

Система DNS (Domain Name System) является ключевым элементом сетевого взаимодействия. Система DNS позволяет автоматически преобразовывать доменные имена в IP-адреса, устраняя необходимость в ручном управлении. Первоначальные спецификации стандартов (RFC 882, RFC 883, RFC 1034, RFC 1035) были ориентированы на скорость и масштабируемость в условиях доверенной сетевой среды, где вопросы кибербезопасности не рассматривались как приоритетные[1].

DNS реализует два основных подхода к разрешению имён: *итеративный*, при котором клиент получает от серверов ссылки на последующие узлы и сам продолжает запрос; *рекурсивный*, при котором DNS-сервер выполняет все шаги самостоятельно. Второй вариант удобнее для клиента, но требует большей нагрузки на инфраструктуру.

Для передачи запросов чаще всего используется протокол UDP. Он обеспечивает легковесную и быструю передачу данных, не требуя установки соединения, что делает его оптимальным для работы DNS [8]. Однако данные передаются в открытом виде и не проверяется их подлинность. Из-за особенностей протокола UDP со временем появились различные типы атак, направленные на перехват, подделку или использование DNS в качестве инструмента кибератак.

Классификация кибератак через DNS на IIoT-устройства

Угрозы DNS в промышленных сетях можно классифицировать по четырём основным типам:

1. Перехват DNS-трафика (Man-in-the-Middle).

Атаки данного типа позволяют злоумышленникам анализировать незашифрованные DNS-запросы и перенаправлять соединения. IIoT-устройства, использующие открытый UDP-протокол, особенно уязвимы, так как атакующий может отслеживать и изменять данные в реальном времени.

2. Подмена записей (DNS Spoofing, Cache Poisoning).

[1] Как развивалась система доменных имен: эра ARPANET. – URL: https://habr.com/ru/companies/1cloud/articles/479452/ (дата обращения: 04.04.2025). – Текст: электронный; История системы доменных имен: первые DNS-серверы. – URL: https://habr.com/ru/companies/1cloud/articles/480514/ (дата обращения: 05.03.2025). – Текст: электронный; Олифер В.Г., Олифер Н.А. Компьютерные сети: принципы, технологии: учебник. – Санкт-Петербург: Питер, 2025. – 992 с.

В этом типе атак фальсифицированные DNS-ответы направляют устройства на вредоносные серверы. Показательным случаем служит атака DNSpionage (2018), когда злоумышленники скомпрометировали DNS-серверы нескольких ближневосточных компаний, перенаправляя трафик на серверы злоумышленников. В промышленных системах подобная атака может привести к тому, что датчики или контроллеры начнут передавать данные на фальшивые серверы, полностью нарушая технологический процесс.

3. DDoS-атаки через DNS-ботнеты.

В данном типе атак злоумышленники создают сеть заражённых IIoT-устройств (ботнет), которые одновременно отправляют огромное количество поддельных DNS-запросов к целевым серверам. Например, в 2016 году ботнет Mirai координировал атаку более 100 000 заражённых камер, генерируя свыше 1 Тбит/с фальсифицированных DNS-запросов на серверы DynDNS, что вызвало отказ в обслуживании. В контексте IIoT подобные атаки особенно опасны, так как могут вывести из строя не только отдельные устройства, но и всю промышленную сеть предприятия.

4. Фильтрация и анализ DNS-запросов.

В данном типе атак злоумышленники перехватывают и анализируют DNS-трафик IIoT-устройств, чтобы выявить уязвимые узлы сети и спланировать целенаправленную атаку. Например, в атаке на Cloudflare (2020) была использована утечка DNS-запросов через уязвимость в механизме кэширования. Полученные данные о структуре сети применялись для последующих DDoS-атак на ключевые серверы.

Для защиты DNS-запросов от подмены и перехвата были разработаны и применяются следующие протоколы: DNSSEC (Domain Name System Security Extensions), DoH (DNS over HTTP), DoT (DNS over TLS), DoQ (DNS over QUIC), DoC (DNS over CoAP), mDNS (Multicast DNS).

Сравнительный анализ протоколов защиты DNS

Несмотря на то, что для безопасной работы DNS существует достаточное количество протоколов, в контексте промышленного интернета вещей выбор DNS-протоколов требует особого баланса между безопасностью и производительностью. Далее рассматриваются свойства наиболее известных протоколов.

Протокол DNSSEC обеспечивает аутентификацию DNS-данных с помощью цифровых подписей, проверяемых по цепочке от корневой зоны до конечного домена, что предотвращает подмену записей. Однако проверка подписей на основе алгоритмов RSA или ECDSA требует значительных вычислительных ресурсов[2]. Кроме того, DNSSEC требует регулярного обновления ключей (каждые 30–90 дней) и поддержки новых хэш-алгоритмов. Эти требования делают DNSSEC неприменимым для большинства IIoT-устройств, работающих в условиях ограниченной вычислительной мощности, энергопотребления и автономного режима.

Протокол DoH обеспечивает передачу запросов через HTTPS-соединение, что делает их неотличимыми от обычного веб-трафика. Клиент отправляет DNS-запрос в формате HTTP/2 POST или GET[3]. Таким образом, происходит маскировка DNS-запросов среди HTTPS-трафика, что предотвращает перехват трафика и его анализ со стороны злоумышленника.

Протокол DoT использует TLS-соединение (Transport Layer Security) для шифрования всех DNS-запросов и ответов. Это предотвращает прослушивание и подделку DNS-трафика. Клиент должен установить TLS-соединение с DNS-сервером. После установки безопасного соединения все DNS-запросы передаются по защищенному каналу[4]. Такое шифрование предотвращает утечку данных о сетевых запросах. Однако многие IIoT-устройства, такие как датчики и контроллеры, просто не поддерживают TLS или HTTPS, либо их реализация очень сложна.

---

[2] RFC 4033-4035: DNS Security Introduction and Requirements 2005. – URL: https://www.rfc-editor.org/rfc/rfc4033 (дата обращения: 24.03.2025). – Текст: электронный.

[3] RFC 8484: DNS Queries over HTTPS (DoH). 2018. – URL: https://www.rfc-editor.org/rfc/rfc8484.html (дата обращения: 18.03.2025). – Текст: электронный.

[4] RFC 7858: Specification for DNS over Transport Layer Security (TLS). 2016. – URL: https://www.rfc-editor.org/rfc/rfc7858.html (дата обращения: 18.03.2025). – Текст: электронный.

Применение указанных DNS-протоколов в IIoT-устройствах вызывает огромные задержки. Согласно исследованиям, самые большие задержки могут достигать 606,8 % (для DoH) [6]. Это означает, что зашифрованный трафик будет передаваться практически в 6 раз медленнее по сравнению с обычным незашифрованным DNS-трафиком.

Таким образом, эти ограничения традиционных защищенных DNS-протоколов обуславливают необходимость специализированных решений для IIoT. В частности, протоколы DNS over CoAP (DoC) и Multicast DNS (mDNS) были разработаны специально для работы в условиях ограниченных ресурсов, предлагая оптимальное сочетание безопасности и эффективности для промышленных IoT-устройств.

Протокол DoC представляет собой оптимизированное решение для устройств промышленного интернета вещей, выступая легковесной альтернативой ресурсоемким протоколам, описанным ранее. Основанный на Constrained Application Protocol (CoAP), этот протокол специально разработан для работы в условиях ограниченных вычислительных ресурсов и жестких требований к энергопотреблению. Ключевое отличие DoC от традиционных DNS-решений заключается в использовании UDP вместо TCP в качестве транспортного протокола, что позволяет существенно сократить служебные накладные расходы и объем передаваемых данных[5]. Для обеспечения безопасности DoC поддерживает шифрование через DTLS (Datagram Transport Layer Security), что делает его значительно менее ресурсоемким по сравнению с решениями на основе TLS, сохраняя при этом приемлемый уровень защиты передаваемых данных. Таким образом, DTLS обеспечивает безопасность на уровне передачи данных, что делает возможным защиту DNS-запросов от перехвата и подделки.

Протокол Multicast DNS (mDNS) является эффективным решением для локального разрешения имен в промышленных сетях IIoT. В отличие от традиционных DNS-систем, mDNS полностью обходится без централизованных серверов, используя вместо этого multicast-рассылку по адресам 224.0.0.251 (IPv4) или FF02::FB (IPv6)[6]. Такой подход дает несколько ключевых преимуществ для IIoT-устройств: полная независимость от интернета и внешней инфраструктуры, минимальные задержки, а также простота настройки, поскольку mDNS не требует конфигурации.

Математический анализ рисков атак на DNS в технологиях IIoT

Надежность DNS-сервисов критически важна для промышленного IoT, поскольку компрометация доменных запросов может вызвать сбои в работе управляющих систем и остановку производства. Для количественной оценки уровня риска при использовании различных DNS-протоколов в данной работе применяется оценочная модель, описываемая формулой (1):

$$R = P \cdot (1 - E) \cdot I, \quad (1)$$

где R – уровень риска;

P – вероятность успешной реализации атаки ($0 \le P \le 1$);

E – эффективность применяемого защитного механизма ($0 \le E \le 1$);

I – уровень потенциального ущерба от реализации угрозы.

Для анализа уязвимостей DNS в условиях ограниченных вычислительных ресурсов IIoT применена полуколичественная модель оценки рисков (*semi-quantitative risk assessment*). Данный подход оптимален при отсутствии точных данных о вероятностях угроз, но наличии информации о потенциальных последствиях [9]. В контексте IIoT, где уровень наблюдаемости за угрозами ограничен, а устройства обладают малой вычислительной мощностью, использование *semi-quantitative* моделей позволяет учитывать неопределённость и ограниченные данные о событиях безопасности.

Уровень потенциального ущерба (I=8) обоснован высокой уязвимостью промышленных IoT-систем, где даже кратковременный сбой разрешения имён может вызвать сбои в передаче критически важных данных с датчиков, утрату связи с управляющей системой или задержку команд исполнительным устройствам. Ущерб может выражаться не только в простом сбое оборудования, но и в угрозе безопасности персонала.

---

[5] RFC 8323: DNS Privacy, Authorization, Special Uses, Encoding, Characters, Matching, and Root Structure: Time for Another Look? 2018. – URL: https://www.rfc-editor.org/rfc/rfc8323.html (дата обращения: 24.03.2025). – Текст: электронный.

[6] RFC 6762: Multicast DNS. 2013. – URL: https://www.rfc-editor.org/rfc/rfc6762.html (дата обращения: 24.03.2025). – Текст: электронный.

Вероятность атаки (P=0.6) определена характерными уязвимостями IIoT-устройств: отсутствием встроенных механизмов аутентификации, защиты DNS-трафика и безопасных механизмов обновления ПО, что создаёт благоприятные условия для эксплуатации слабостей сетевого уровня злоумышленниками [10]. Данное значение отражает высокий риск компрометации DNS в условиях недостаточной защищённости инфраструктуры, ограниченного контроля конфигураций и отсутствием обновлений.

Одинаковые значения I и P используются для всех протоколов, поскольку оценка направлена не на вероятность угрозы в целом, а на влияние защитных механизмов на её последствия.

Показатель эффективности защиты (E) варьируется в зависимости от особенностей реализации DNS-протоколов:

DNS (UDP) (E=0.0) не обеспечивает никакой защиты;

DNSSEC (E=0.7) гарантирует целостность данных через цифровые подписи, но уязвим к перехвату трафика;

DoT (E=0.6) обеспечивает транспортное шифрование, сохраняя риск подмены при компрометации сервера;

DoH (E=0.5), хотя и использует HTTPS-шифрование, более подвержен обходу защиты на уровне приложений из-за особенностей работы с прокси и сертификатами.

На основании этих значений расчетные уровни риска (R) демонстрируют различия по степени защищённости:

DNS (UDP) показывает максимальный уровень риска (R=4.8), подтверждая абсолютную уязвимость незащищенных запросов;

DNSSEC показывает наибольшее снижение риска (R=1.44), гарантируя целостность данных при уязвимости к перехвату;

DoT снижает риск до R=2.4 за счёт транспортного шифрования, но уязвим при компрометации сервера;

DoH демонстрирует R=1.92, оставаясь подверженным атакам на уровне приложений (через прокси и TLS).

Полученные данные подтверждают необходимость тщательного выбора DNS-протокола с учётом компромисса между безопасностью и ограничениями IIoT-среды. На рисунке 1 представлена столбчатая диаграмма с уровнями риска для каждого механизма защиты.

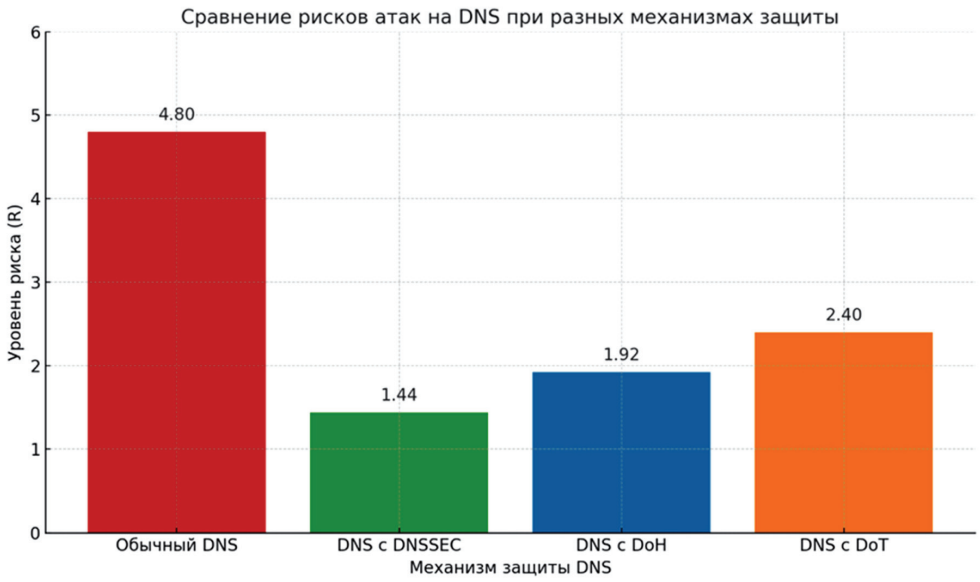

Рисунок 1 – Уровни риска на DNS при использовании различных механизмов защиты[7]

[7] Составлено авторами.

Методы и материалы исследования

В рамках эксперимента сравнивались традиционные DNS-протоколы (DNS/UDP, DoH, DoT, DNSSEC) и легковесные решения для IIoT – mDNS и DoC. Первые тестировались в виртуальной машине из-за высоких требований к ресурсам и TLS-обработке, вторые – на микроконтроллере ESP32. Это позволило оценить поведение протоколов как в условиях промышленной инфраструктуры, так и на ограниченных устройствах.

Эксперименты проводились в среде Ubuntu 22.04 LTS на виртуальной машине (4 CPU, 8 ГБ ОЗУ). Система выбрана за наличие встроенных сетевых инструментов (*dig, curl, Wireshark, stubby, cloudflared*) и широких возможностей для настройки и анализа сетевого трафика. Во всех виртуальных тестах DNS-запросы отправлялись с помощью утилиты *dig*, которая позволяет задавать тип протокола, сервер и формат ответа, а также используется для диагностики DNS.

Для анализа классического DNS использовалась команда:

dig example.com @1.1.1.1. Она отправляет DNS-запрос по умолчанию через UDP на порт 53, что видно в Wireshark при применении фильтра *udp.port == 53*. Из данных рисунка 2 видно, что пакет проходит через сеть в незашифрованном виде, его может прочитать любой, кто перехватит трафик.

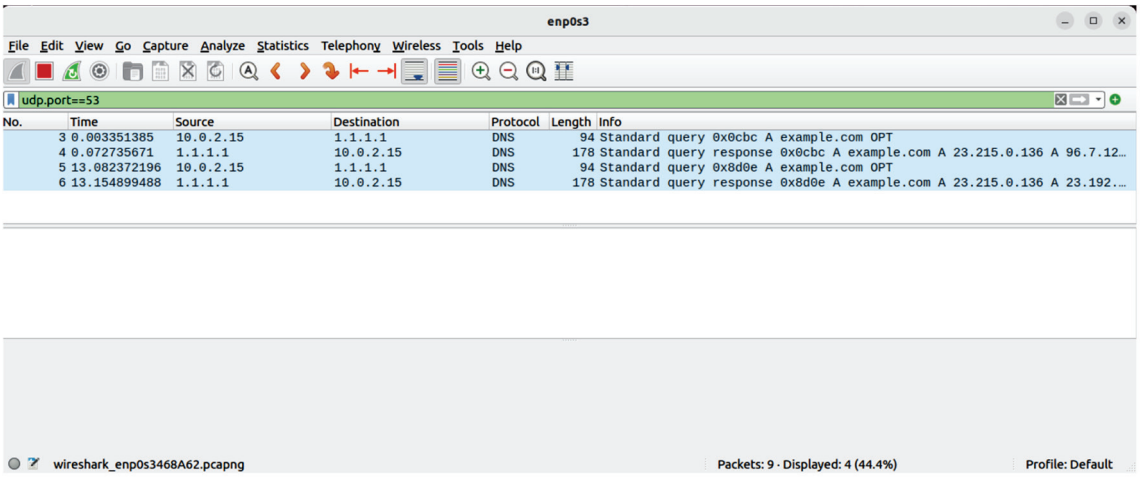

Рисунок 2 – Данные об отправке нешифрованных запросов[8]

Для проверки DoH использовалась утилита *cloudflared*, настроенная как локальный DNS-прокси. В качестве DNS-сервера был указан адрес 127.0.0.1, чтобы направить запросы на прокси. Команда *dig example.com@127.0.0.1* запускала DNS-запрос, обрабатываемый через DoH. Анализ трафика подтверждает использование DoH (рисунок 3): соединение проходит через порт 443, фиксируются TLS-пакеты (Client Hello, Server Hello, Application Data), в структуре видно поле *http-over-tls* – что подтверждает, что это именно DoH, а не обычный HTTPS, а DNS-запросы не передаются в открытом виде.

Проверка DoT проводилась с использованием локального TLS-резолвера Stubby, настроенного как DNS-сервер. Он обеспечивал шифрование запросов по протоколу TLS перед отправкой на внешние серверы. В Wireshark зафиксированы признаки DoT (рисунок 4): трафик проходит через порт 853, видны TLS-пакеты, а в зашифрованных данных в 30-м пакете указано "*Application Data Protocol: dns*" – это указывает, что внутри TLS-туннеля передаются именно DNS-запросы, а не произвольные данные. Имя домена не передаётся открыто, что подтверждает шифрование на уровне транспортного слоя.

Для проверки DNSSEC использовалась команда *dig+dnssec example.com*. В данном случае DNS-запрос отправляется через обычный протокол UDP (порт 53). Сервер в ответе добавляет криптографически подписанную запись типа RRSIG. Клиент может использовать её для проверки подлинности

[8] Составлено авторами.

полученного IP-адреса. Из рисунка 5 видно, что все данные передаются в открытом виде, но цифровая подпись защищает от подмены.

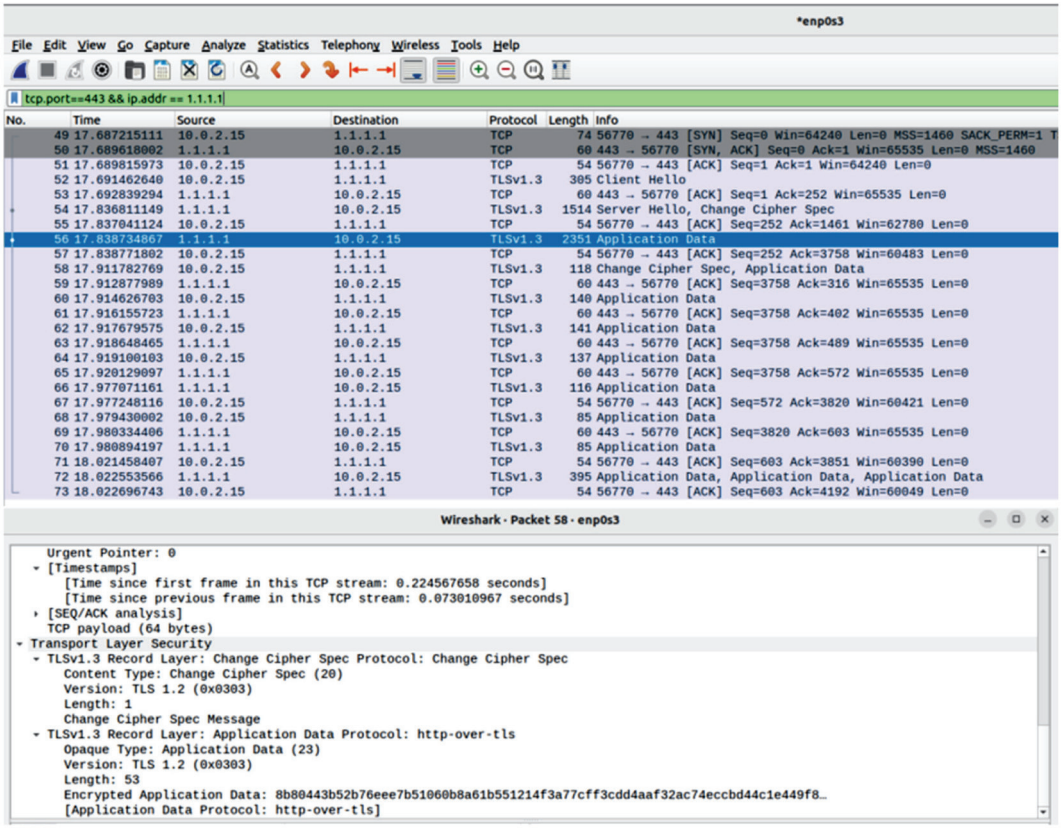

Рисунок 3 – Данные о трафике, защищенном протоколом DoH[9]

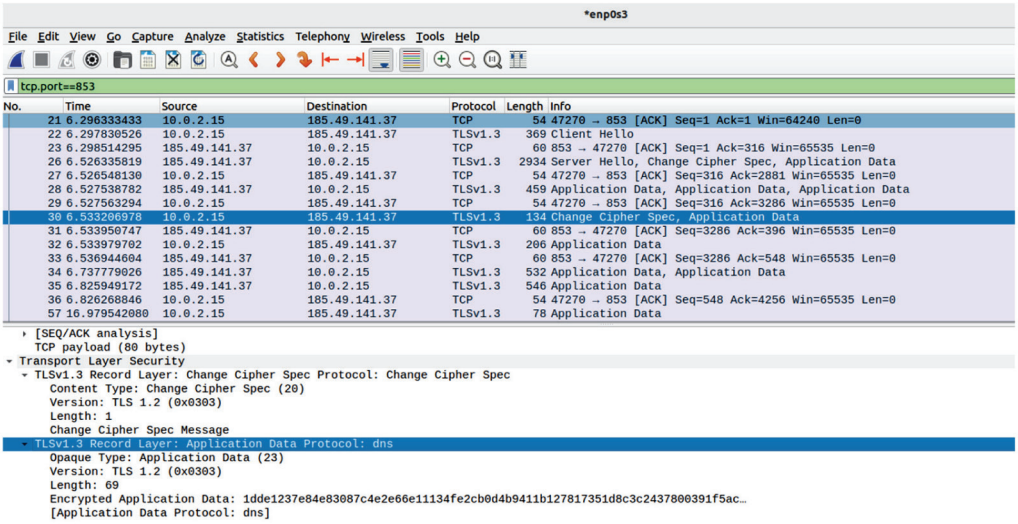

Рисунок 4 – Данные о трафике, защищенном протоколом DoT[10]

[9] Составлено авторами.
[10] Составлено авторами.

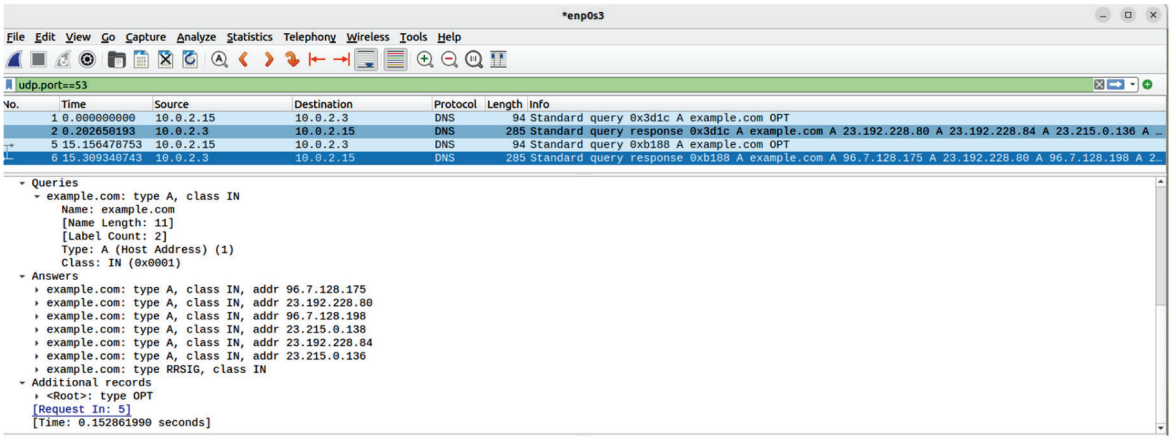

Рисунок 5 – Шифрование DNSSEC[11]

Для оценки эффективности каждого протокола в виртуальной среде измерялись три параметра: средняя нагрузка на CPU, использование RAM и задержка ответа. Тесты проводились с объёмами запросов 30, 100, 500 и 1000, по результатам которых рассчитывались средние значения. Загрузка CPU и потребление памяти отслеживались с помощью утилиты *pidstat* по PID процесса, обрабатывающего DNS-запросы: *systemd-resolved* для DNS/UDP и DNSSEC, *cloudflared* для DoH и *stubby* для DoT. Продолжительность замеров подбиралась так, чтобы охватить весь период обработки запросов. Задержка фиксировалась с помощью команды *time* в *bash*-цикле, после чего рассчитывалось среднее время отклика.

Классический DNS (UDP) показал наименьшие значения по всем метрикам. При увеличении объёма запросов до 1000, загрузка CPU составила лишь 1.28 %, RAM – около 13.2 МБ, а средняя задержка оставалась стабильной – около 38–40 мс. Эти значения подтверждают высокую производительность и минимальное влияние на ресурсы, однако при полном отсутствии защиты трафика.

Протокол DoH потребовал значительно больше ресурсов. При 1000 запросов загрузка CPU достигла почти 2.93 %, использование памяти увеличилось до 33.7 МБ. Тем не менее, задержка ответа снизилась с 47 мс при 30 запросах до 39.3 мс при 1000, что свидетельствует о стабилизации при больших объёмах трафика. Однако из-за необходимости TLS-рукопожатия и работы через HTTPS начальные накладные расходы остаются высокими.

DoT показал иную картину: несмотря на умеренные значения загрузки CPU (около 1.1 % при 1000 запросов) и RAM (в среднем 9.2 МБ), задержка была значительно выше, достигая 137 мс при малом объёме запросов и 142 мс при 1000. Это объясняется особенностями TLS-установки соединения и ограниченной оптимизацией резолвера *stubby*.

DNSSEC, в свою очередь, потреблял ресурсы, схожие с классическим DNS, поскольку использует тот же транспортный протокол (UDP), но с добавлением криптографической подписи. При 1000 запросах загрузка CPU достигала 1.37 %, использование оперативной памяти – около 13.2 МБ, а задержка оставалась на уровне 38–39 мс. Таким образом, DNSSEC даёт прирост защищённости без серьёзного увеличения времени отклика, но требует дополнительных вычислений при валидации подписей.

В качестве модели IIoT-устройства в исследовании использовался микроконтроллер ESP32 (ESP-WROOM-32), обладающий характеристиками, приближенными к реальным условиям промышленного интернета вещей: низким энергопотреблением, ограниченной оперативной памятью (520 КБ) и отсутствием полноценной операционной системы. Благодаря встроенному Wi-Fi и Bluetooth, а также двухъядерному процессору с частотой до 240 МГц, ESP32 широко применяется в IIoT-решениях и подходит для оценки сетевых протоколов в условиях ограниченных ресурсов. Однако из-за архитектурных ограничений запуск ресурсоёмких протоколов, таких как DNSSEC, DoT и DoH, оказался невозможен – в частности из-за требований к TLS-соединениям и криптографической обработке. Объём памяти и упрощённый стек не позволяют реализовать полноценную защиту на основе TLS. В связи с этим для

[11] Составлено авторами.

тестирования были выбраны два легковесных протокола – mDNS и DoC, разработанные специально для работы в условиях ограниченных вычислительных возможностей.

Для реализации mDNS на ESP32 использовался код на Arduino C++ с подключением к Wi-Fi и регистрацией доменного имени через библиотеки WiFi.h, ESPmDNS.h и WebServer.h. Вызов функции MDNS.begin(“esp32”) инициирует запуск встроенного mDNS-сервиса на устройстве, регистрируя имя esp32.local как локальное доменное имя. Это позволяет другим устройствам в сети обращаться к ESP32 без необходимости знать его IP-адрес – через механизм мультикастовых DNS-запросов, отправляемых на порт 5353.

Работоспособность протокола подтверждалась через Wireshark с фильтром *udp.port == 5353*, где фиксировались запросы и ответы на мультикаст-адрес 224.0.0.251 с использованием имени *esp32.local*. Это подтверждает корректную работу mDNS и участие устройства в локальном разрешении имён (рисунок 6).

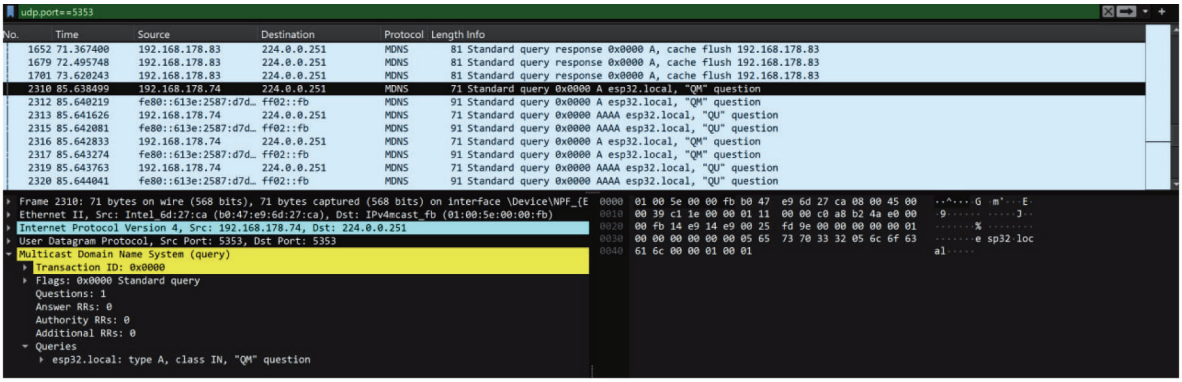

Рисунок 6 – Работа протокола mDNS[12]

Протокол DoC был реализован на ESP32 с использованием библиотеки *coap-simple*, обеспечивающей передачу по CoAP через UDP-порт 5683. Устройство регистрировало ресурс*/dns* и возвращало текстовый ответ на GET-запросы. Проверка в Wireshark с фильтром *udp.port == 5683* показала корректный обмен: клиент отправляет запрос, сервер возвращает ответ с кодом 2.05 Content. Наличие текста “Ответ от ESP32” в пакете подтверждает успешную работу CoAP-сервера и реализацию протокола DoC (рисунок 7).

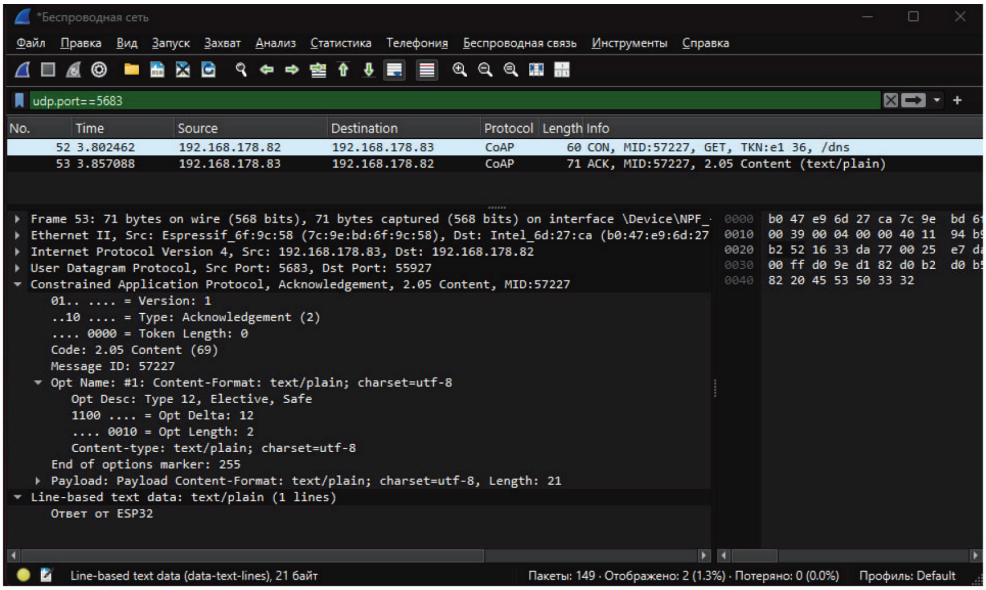

Рисунок 7 – Реализация протокола DoC[13]

[12] Составлено авторами.
[13] Составлено авторами.

Из-за ограниченной архитектуры ESP32, не поддерживающей полноценную операционную систему и мониторинг процессов, измерить загрузку процессора напрямую было невозможно. Вместо этого оценка ресурсоёмкости легковесных протоколов проводилась по задержке ответа и объёму используемой оперативной памяти. Запросы отправлялись вручную с клиентского устройства, чтобы избежать искажений от фоновой нагрузки. В ходе эксперимента mDNS показал задержку около 2.13 мс при использовании 0.21 МБ RAM, тогда как DoC продемонстрировал лучшую производительность – задержка составила всего 0.26 мс при использовании 0.226 МБ памяти. Эти результаты подтверждают высокую эффективность DoC в условиях ограниченных ресурсов.

Проведённый эксперимент подтвердил значительные различия в производительности и защищённости DNS-протоколов при работе в условиях IIoT. Протокол DNS по UDP показал минимальные значения по потреблению ресурсов, но полностью лишён механизмов защиты. DoH и DoT обеспечивают высокий уровень шифрования, однако сопровождаются увеличенной нагрузкой на процессор и оперативную память, особенно в начальной фазе соединения. DNSSEC позволяет аутентифицировать DNS-ответы, не увеличивая задержку, но требует вычислительных затрат на проверку цифровых подписей.

В среде ограниченных устройств на базе ESP32 реализация полноценных TLS-протоколов оказалась невозможной, что обусловило выбор лёгких решений – mDNS и DoC. Эти протоколы продемонстрировали наилучшее соотношение между задержкой, потреблением памяти и надёжностью работы. DoC оказался наиболее эффективным за счёт легковесного CoAP-стека и работы по UDP. Таким образом, выбор DNS-протокола для IIoT-сред должен учитывать как уровень защиты, так и ограничения аппаратной платформы. Наиболее применимыми для использования в таких условиях являются mDNS и DoC, обеспечивающие базовую защиту с минимальной нагрузкой на систему.

Оптимальное соотношение между безопасностью, производительностью и ресурсоёмкостью продемонстрировали протоколы DoC и mDNS, что делает их оптимальными для использования в реальных промышленных сценариях – например, в SCADA-системах, распределённых сенсорных сетях, энергетических установках и транспортной автоматике.

Заключение

Проблема обеспечения безопасности системы доменных имён в условиях промышленного интернета вещей требует особого внимания в силу ограниченных вычислительных возможностей устройств и высокой критичности передаваемой информации. В рамках данного исследования всесторонне рассмотрена эта проблема, проведен сравнительный анализ специализированных протоколов защиты DNS, включая DNSSEC, DoH, DoT, DoQ, а также облегчённых решений DoC и mDNS, применимых в условиях ограниченных вычислительных возможностей.

В ходе экспериментальной части проведено исследование протоколов на виртуальной машине и на микроконтроллере ESP32. Проведены измерения, которые показывают влияние протоколов на такие параметры, как нагрузка на процессор, объем оперативной памяти и задержка отклика на запрос. Полученные данные позволили выявить наиболее эффективные протоколы, которые обеспечивают приемлемый уровень защиты в ограниченных условиях. Проведённая полуколичественная оценка рисков позволила в числовой форме определить снижение уровня угрозы при использовании исследуемых протоколов защиты, усилив прикладной характер результатов. Экспериментальные данные подтверждают, что эффективная защита DNS-трафика в системах IIoT возможна при условии выбора протоколов, соответствующих архитектурным ограничениям устройств.

Предложенный авторами научно-методический подход к анализу протоколов защиты DNS в промышленных IIoT включает следующие процедуры:

– формирование классификации кибератак на DNS в промышленной среде;

– внедрение полуколичественной модели оценки рисков, адаптированной к условиям ограниченной вычислительной мощности;

– сопоставление традиционных и облегчённых протоколов на базе практических экспериментов.

Практическая значимость исследования выражается в возможности применения предложенного научно-методического обеспечения при выборе протоколов защиты DNS в промышленных технологиях интернета вещей. Перспективным направлением дальнейших исследований является расширение экспериментов на более широкие аппаратные платформы и проведение стресс-тестирования в реальных промышленных сетях, а также интеграция полученных результатов в стандарты кибербезопасности для IIoT.

Список литературы

1. *Докучаев В.А., Кальфа А.А., Рахмани Д.* Типовая структура корпоративной инфокоммуникационной системы энергопроизводящей компании ИРИ // III Научный форум телекоммуникации: теория и технологии ТТТ-2019: материалы XXI Международной научно-технической конференции, Казань, 18–22 ноября 2019 года. – Казань: Казанский государственный технический университет им. А.Н. Туполева, 2019. – Т. 1. – С. 298–299.
2. *Рахмани Д., Докучаев В.А.* Анализ тенденций развитий промышленности средств связи в ИРИ // Технологии информационного общества: сборник трудов XIV Международной отраслевой научно-технической конференции, Москва, 18–19 марта 2020 года. – Москва: ООО «Издательский дом Медиа паблишер», 2020. – С. 300–301.
3. *Рахмани Д., Рогов И.Д.* Тенденции развития сетевых технологий в 2022 году // Технологии информационного общества: сборник трудов XVI Международной отраслевой научно-технической конференции, Москва, 02–03 марта 2022 года. – Москва: ООО «Издательский дом Медиа паблишер», 2022. – С. 30–31.
4. *Рахмани Д.* Исследование методов управления рисками в инфокоммуникационной системе энергопроизводящей компании Исламской Республики Иран // T-Comm: Телекоммуникации и транспорт. – 2022. – Т. 16, № 8. – С. 30–37. – DOI 10.36724/2072-8735-2022-16-8-30-37.
5. *Тергеуов О.С., Маликова Ф.У.* Обнаружение и устранение DDoS-атаки IoT-ботнетов на основе SIEM // Universum: технические науки. – 2022. – Вып. 4 (97). – С. 54–63.
6. *Aydeger A., Hoque S., Zeydan E., Dev K.* Analysis of Robust and Secure DNS Protocols for IoT Devices // ResearchGate. – 2025. – February. – DOI 10.13149/JRG.2.3.13786.84487. – URL: https://www.researchgate.net/publication/388959543 (дата обращения: 21.03.2025). – Текст: электронный.
7. *Потапова А.В.* Вирус Stuxnet – оружие нового поколения // Вестник магистратуры. – 2014. – Т. 1, № 3 (30). – С. 10–12.
8. *Радивилова Т.А., Бушманов В.С.* Анализ основных атак на DNS-сервер и методы использования DNSSEC при защите DNS-сервера // Технологический аудит и резервы производства. – 2013. – № 2/1 (10). – С. 16–19.
9. NIST. Guide for Conducting Risk Assessments: NIST Special Publication 800-30 Revision 1 / J.F. Stine, R. Kissel, W. Barker et al. – Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2012. – 95 p.
10. European Union Agency for Cybersecurity (ENISA). Guidelines for Securing the Internet of Things / ENISA. – November, 2020. – 36 p.

References

1. *Dokuchaev V.A., Kal'fa A.A., Rahmani D.* Tipovaya struktura korporativnoj infokommunikacionnoj sistemy energoproizvodyashchej kompanii IRI // III Nauchnyj forum telekommunikacii: teoriya i tekhnologii TTT-2019: materialy XXI Mezhdunarodnoj nauchno-tekhnicheskoj konferencii, Kazan', 18–22 noyabrya 2019 goda. – Kazan': Kazanskij gosudarstvennyj tekhnicheskij universitet im. A.N. Tupoleva, 2019. – T. 1. – S. 298–299.
2. *Rahmani D., Dokuchaev V.A.* Analiz tendencij razvitij promyshlennosti sredstv svyazi v IRI // Tekhnologii informacionnogo obshchestva: sbornik trudov XIV Mezhdunarodnoj otraslevoj nauchno-tekhnicheskoj konferencii, Moskva, 18–19 marta 2020 goda. – Moskva: OOO «Izdatel'skij dom Media publisher», 2020. – S. 300–301.
3. *Rahmani D.,* Rogov I.D. Tendencii razvitiya setevyh tekhnologij v 2022 godu // Tekhnologii informacionnogo obshchestva: sbornik trudov XVI Mezhdunarodnoj otraslevoj nauchno-tekhnicheskoj konferencii, Moskva, 02–03 marta 2022 goda. – Moskva: OOO «Izdatel'skij dom Media publisher», 2022. – S. 30–31.

4. *Rahmani D.* Issledovanie metodov upravleniya riskami v infokommunikacionnoj sisteme energoproizvodyashchej kompanii Islamskoj Respubliki Iran // T-Comm: Telekommunikacii i transport. – 2022. – T. 16, № 8. – S. 30–37. – DOI 10.36724/2072-8735-2022-16-8-30-37.
5. *Tergeuov O.S., Malikova F.U.* Obnaruzhenie i ustranenie DDoS-ataki IoT-botnetov na osnove SIEM // Universum: tekhnicheskie nauki. – 2022. – Vyp. 4 (97). – S. 54–63.
6. *Aydeger A., Hoque S., Zeydan E., Dev K.* Analysis of Robust and Secure DNS Protocols for IoT Devices // ResearchGate. – 2025. – February. – DOI 10.13149/JRG.2.3.13786.84487. – URL: https://www.researchgate.net/publication/388959543 (data obrashcheniya: 21.03.2025). – Tekst: elektronnyj.
7. *Potapova A.V.* Virus Stuxnet – oruzhie novogo pokoleniya // Vestnik magistratury. – 2014. – T. 1, № 3 (30). – S. 10–12.
8. *Radivilova T.A., Bushmanov V.S.* Analiz osnovnyh atak na DNS-server i metody ispol'zovaniya DNSSEC pri zashchite DNS-servera // Tekhnologicheskij audit i rezervy proizvodstva. – 2013. – № 2/1 (10). – S. 16–19.
9. NIST. Guide for Conducting Risk Assessments: NIST Special Publication 800-30 Revision 1 / J.F. Stine, R. Kissel, W. Barker et al. – Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2012. – 95 p.
10. European Union Agency for Cybersecurity (ENISA). Guidelines for Securing the Internet of Things / ENISA. – November, 2020. – 36 p.

Статья поступила в редакцию: 19.04.2025
Статья поступила для публикации: 21.05.2025
Received: 19.04.2025
Accepted: 21.05.2025