# НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ ИНТЕРНЕТ ВЕЩЕЙ

**Алевтина Александровна Мурадова**
ТУИТ имени Мухаммада аль-Хорезми, PhD, доцент кафедры
«Телекоммуникационный инжиниринг»
Email: a.muradova1982@inbox.ru

***Аннотация:*** *В статье представлен анализ надёжности и безопасности интернет вещей. Представлены различные виды рисков безопасности IoT и способы их предотвращения, проблемы надежности доставки электронной почты IoT. Показаны меры по снижению рисков безопасности IoT, а также методы шифрования и аутентификации.*

***Ключевые слова:*** *безопасность IoT, IoT-продукты, IoT-устройства, IoT аутентификация по электронной почте, теневой IoT, IPSec (Internet Protocol Security).*

***Abstract:*** *The article presents an analysis of the reliability and security of the Internet of Things. Various types of IoT security risks and ways to prevent them, problems of reliability of IoT email delivery are presented. Measures to reduce IoT security risks are shown, as well as encryption and authentication methods.*

***Keywords:*** *IoT security, IoT products, IoT devices, IoT email authentication, shadow IoT, IPSec (Internet Protocol Security).*

***Annotatsiya:*** *Maqolada internet ashyolarning ishonchliligi va xavfsizligi tahlili keltirilgan. IoT xavfsizligi xavflarining har xil turlari va ularni oldini olish usullari, IoT elektron pochta xabarlarini yetkazib berish ishonchliligi muammolari keltirilgan. IoT xavfsizligi xavflarini kamaytirish choralari, shuningdek shifrlash va autentifikatsiya usullari ko‘rsatilgan.*

***Kalit so‘zlar:*** *IoT xavfsizligi, IoT mahsulotlari, IoT qurilmalari, IoT elektron pochta autentifikatsiyasi, soya IoT, IPSec (Internet Protocol Security).*

## ВВЕДЕНИЕ

Технологии Интернета вещей (IoT) привнесли в наш мир удобство. Однако популярность этих устройств сопровождается и определенными рисками безопасности риски для безопасности. По прогнозам компаний, в 2023 году значительно возросло число атак, связанных с компрометацией деловой электронной почты, за которыми последуют ransomware и атаки на интерфейсы управления облачными средами. В то же время 11% респондентов прогнозируют рост числа атак на жизненно важные объекты инфраструктуры, спонсируемых государством. Поэтому при работе с IoT-продуктами необходимо знать и уметь их избегать [1].

## ЛИТЕРАТУРА И МЕТОДОЛОГИЯ

**Значение IoT-устройств в нашей повседневной жизни.** Устройства, здания и транспортные средства, оснащенные электроникой, программным обеспечением и датчиками, являются частью Интернета вещей. К 2025 г. по прогнозам, будет использоваться более 75 млрд. подключенных устройств Интернета вещей (IoT). IoT создает возможности для улучшения аналитики за счет сенсорных данных, собираемых со всех типов устройств (например, смартфонов) в больших масштабах. Это означает, что теперь клиенты могут получить более качественный опыт работы с продуктами, поскольку компании имеют доступ к более подробной информации о них (например, об их предпочтениях).

### IoT и риски, связанные с безопасностью данных

IoT привнесла множество положительных изменений в нашу повседневную жизнь. Однако с ней связаны и некоторые риски. Одним из таких рисков, связанных с безопасностью IoT, является безопасность данных. Приведем несколько примеров того, как безопасность данных может быть нарушена из-за рисков безопасности IoT: **Ботнет:** Ботнеты - сети скомпрометированных устройств - представляют собой риски для безопасности

IoT, позволяя осуществлять скоординированные кибератаки, утечки данных и несанкционированный доступ. **GDPR:** Общий регламент по защите данных (General Data Protection Regulation, GDPR) обеспечивает конфиденциальность данных и оказывает влияние на IoT-системы, требуя строгих мер по защите данных пользователей и их согласия. **ICS:** Промышленные системы управления (ICS) сталкиваются с рисками безопасности IoT из-за потенциальных удаленных атак, которые могут нарушить работу критической инфраструктуры и операций. **IPSec:** IPSec (Internet Protocol Security) повышает безопасность данных IoT за счет шифрования и аутентификации, обеспечивая конфиденциальную и надежную связь. **NIST:** Руководство Национального института стандартов и технологий (NIST) содержит рекомендации по обеспечению безопасности IoT и помогает организациям укрепить свои экосистемы IoT. **IAM:** Управление идентификацией и доступом (IAM) в IoT обеспечивает авторизованный доступ пользователей, снижая вероятность несанкционированного управления и утечки данных. **PAMS:** Системы управления привилегированным доступом (PAMS) обеспечивают безопасность IoT-устройств, ограничивая высокоуровневый доступ и контролируя привилегированные действия. **Ransomware:** Угрозы Ransomware для IoT-устройств шифруют данные, требуя выкуп, что в случае отсутствия защиты приводит к потере данных или несанкционированному доступу. **Теневой IoT:** Теневой IoT - это неуправляемые IoT-устройства, представляющие угрозу безопасности, за которыми нет должного надзора и интеграции в протоколы безопасности. **PKI:** Инфраструктура открытых ключей (PKI) в IoT обеспечивает безопасную передачу данных и аутентификацию устройств за счет управления криптографическими ключами. **TLS:** Шифрование на транспортном уровне (Transport Layer Security, TLS) обеспечивает защиту данных IoT при передаче, защищая их от подслушивания и фальсификации. **ZERO Trust:** Подход ZERO Trust к обеспечению безопасности IoT рассматривает все устройства как потенциально скомпрометированные,

применяя строгий контроль доступа для предотвращения нарушений и латеральных перемещений [2].

**Аутентификация электронной почты IoT: Почему это важно**

Электронная почта - один из важнейших каналов связи в современном деловом мире. На протяжении десятилетий она используется для отправки и получения информации, совместной работы с коллегами и управления сложными процессами. Экосистема Интернета вещей (IoT) не является исключением - электронная почта используется для управления всем: от предупреждений о безопасности до настройки и обновления устройств. Сейчас, когда практически каждое устройство имеет IP-адрес, ИТ-специалисты должны понимать, как можно использовать электронную почту в рамках стратегии IoT.

**Повышение эффективности и улучшение взаимодействия**

Электронная почта - это эффективный способ связи с любым сотрудником как в вашей организации, так и за ее пределами. Она позволяет сотрудничать с коллегами по проектам и помогает эффективнее управлять задачами.

**Управление инцидентами и оповещениями системы безопасности**

Электронная почта - отличный способ быстро распространить важную информацию об инциденте или тревоге. Используя этот способ связи, можно легко информировать всех сотрудников в режиме реального времени, не звоня и не отправляя СМС каждому сотруднику вручную [3].

**Бесшовная интеграция устройств IoT**

Благодаря интеграции с электронной почтой IoT-устройства могут легко интегрироваться с существующими в компании средствами коммуникации, включая голосовую почту, совещания и конференц-связь, что позволяет обойтись без дополнительного программного или аппаратного обеспечения. Такая интеграция также облегчает конечным пользователям доступ к функциям своих устройств в любом месте.

**Риски безопасности электронной почты IoT**

Риски безопасности электронной почты IoT волнуют как предприятия, так и потребителей. Каковы же некоторые из этих угроз? Вот некоторые ключевые области, в которых возникают риски безопасности электронной почты IoT: Сложность шифрования электронной почты IoT. Шифрование для защиты конфиденциальных данных, таких как медицинские карты или финансовая информация, широко распространено среди медицинских учреждений и финансовых организаций. Однако шифрование электронной почты IoT представляет собой уникальную проблему, связанную с большим количеством конечных точек, участвующих в обмене электронной почтой IoT, и сложностью каждой из них [4].

**Слабые места аутентификации в электронной почте IoT**

В устройствах IoT часто отсутствуют надежные протоколы аутентификации, что делает их уязвимыми для атак на подмену и других форм социальной инженерии. Предположим, хакеру удалось получить доступ к IP-адресу устройства. В этом случае он может отправлять электронные письма так, как будто они исходят от другого человека, что может заставить пользователя раскрыть конфиденциальную информацию.

**Подмена электронной почты в IoT**

Вредоносная организация может использовать IoT-устройство в качестве прокси-сервера для рассылки фальшивых писем с другой учетной записи или домена. В результате может создаться впечатление, что письмо отправил кто-то другой. Кроме того, злоумышленники могут использовать легитимный адрес электронной почты и спам, чтобы обманом заставить людей перейти по ссылкам или открыть вложения, которые могут заразить их компьютер вредоносным ПО вредоносным ПО. Устранение уязвимостей протокола электронной почты IoT. Уязвимости протокола электронной почты IoT позволяют хакерам изменять электронные сообщения до того, как они достигнут адресата. Это может привести к различным проблемам - от простого

нарушения работы сервисов до потери данных. Конфиденциальность электронной почты IoT в подключенном мире. Многие люди обеспокоены вопросами конфиденциальности при использовании IoT-устройств на работе или дома. Хакеры могут легко использовать эту информацию для проведения социально-инженерных атак на людей или организации, например, фишинговых писем или атак с выкупом. Конфиденциальность электронной почты IoT в подключенном мире. Поскольку все больше устройств подключаются к Интернету и собирают персональные данные, возрастает риск раскрытия этих данных неавторизованным лицам.

**Проблемы надежности доставки электронной почты IoT**

В силу особенностей экосистемы IoT многие устройства отправляют электронные письма, но не получают их из-за проблем с подключением или по другим причинам. Это может привести к пропуску предупреждений или уведомлений от подключенных устройств, что приведет к снижению производительности, а это может дорого обойтись предприятиям, деятельность которых зависит от этих устройств. Фильтрация вредоносного содержимого в электронной почте IoT. Растущее число угроз, направленных на устройства, подключенные к Интернету, означает, что организациям необходимо внедрять решения по обеспечению безопасности, способные обнаруживать вредоносное содержимое до того, как оно попадет в почтовые ящики конечных пользователей. Использование DMARC для аутентификации электронной почты IoT. DMARC DMARC позволяет защитить организации от фишинговых атак на их почтовые домены, поскольку злоумышленникам сложнее подделать легитимные почтовые сообщения из вашего домена. Используя DMARC, вы можете гарантировать, что электронные сообщения, отправленные с вашего домена, будут доставлены с большей уверенностью и надежностью. **Усовершенствованная защита от фишинга:** DMARC обеспечивает мощную защиту от изощренных фишинговых атак, гарантируя обнаружение и предотвращение вредоносных писем до того, как они попадут к пользователям.

**Надежная защита от подделки электронной почты:** DMARC эффективно противодействует попыткам подделки электронной почты, не позволяя неавторизованным источникам выдавать себя за ваш домен и отправлять обманные сообщения. **Повышенные стандарты безопасности электронной почты:** DMARC поднимает планку безопасности электронной почты, обеспечивая строгие меры аутентификации и защищая ваши IoT-сообщения от несанкционированного доступа. **Сохранение целостности бренда:** Не позволяя несанкционированным письмам запятнать имидж вашего бренда, DMARC защищает вашу репутацию и сохраняет доверие пользователей. **Гарантированное доверие к каналам связи:** DMARC гарантирует подлинность сообщений электронной почты от IoT-устройств, создавая безопасную и надежную коммуникационную среду. **Снижение угроз кибербезопасности:** Надежные механизмы аутентификации DMARC снижают потенциальные угрозы кибербезопасности от мошеннических писем, укрепляя инфраструктуру электронной почты [5].

## РЕЗУЛЬТАТЫ

**Меры по снижению рисков безопасности IoT.** IoT - это новая и интересная область, но и она не лишена рисков. К счастью, для снижения рисков безопасности IoT можно предпринять ряд мер.

**Микросегментация сети.** Первым шагом в обеспечении безопасности сети IoT является ее сегментация от других сетей и систем в вашей сети. Это позволит злоумышленникам не использовать скомпрометированные устройства в качестве отправной точки для распространения вредоносного ПО вредоносного ПО в другие части сети. **Проверка целостности встроенного программного обеспечения.** Многие IoT-устройства поставляются с паролями и учетными данными по умолчанию, которые могут быть легко доступны злоумышленникам, желающим получить доступ к этим устройствам. Чтобы обеспечить изменение этих учетных данных перед развертыванием в производственных средах, используйте инструменты для

поиска уязвимых устройств в сети и обновляйте их микропрограммное обеспечение с использованием безопасных учетных данных перед включением [6,7].

**Мониторинг приложений во время выполнения.** Это автоматизированный метод обнаружения ошибок в приложениях во время выполнения. Он контролирует веб-приложения, мобильные приложения и IoT-устройства. Основное преимущество этого метода заключается в том, что он действует как сторожевой пес, выявляя уязвимости до того, как они могут привести к реальному ущербу.

**Контейнеризация и "песочница.** Эта техника позволяет разработчику приложения поместить устройство в изолированную среду, которая не может повлиять на другие приложения или сервисы в системе. Это гарантирует, что в систему или из нее могут попасть только авторизованные данные, и предотвращает несанкционированный доступ хакеров или вредоносных программ. **Динамическое управление ключами с помощью HSM.** Организации могут использовать HSM для создания и управления ключами для IoT-устройств. Это обеспечивает дополнительный уровень безопасности, гарантируя, что только авторизованные пользователи могут получить доступ к конфиденциальным данным [8,9].

## ОБСУЖДЕНИЕ

**Практика разработки безопасного программного обеспечения.** При разработке IoT-систем организациям следует придерживаться практик безопасной разработки программного обеспечения, таких как обзор кода, тестирование и другие методы. Это необходимо, поскольку многие уязвимости в системе безопасности возникают из-за некачественной практики кодирования (например, переполнения буфера). **Методы шифрования и аутентификации.** Шифрование позволяет защитить данные, находящиеся на устройствах и серверах в процессе передачи или в состоянии покоя. Для защиты доступа к системам и приложениям, напротив, используются такие методы аутентификации, как двухфакторная аутентификация (2FA).

## ЗАКЛЮЧЕНИЕ

Если разработка идеальной политики безопасности IoT кажется невозможной, то это так и есть. До тех пор пока люди будут заниматься проектированием и разработкой IoT-систем, мы будем видеть, как совершаются ошибки и появляются уязвимости. Но это не значит, что мы должны сдаваться: мы обязаны учиться на этих ошибках и находить способы минимизации рисков для себя и своего будущего.

## ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Вишняков, В.А., & Юй, Ч. (2023). Моделирование сети IoT «Умный дом» с принятием решений на основе платформы MajorDoMo. *Цифровая трансформация*; 29 (1): с.64-71.
2. Zeng, H. Y., Zheng, X., & Wei, Y. (2023). Research on Smart Home Control System Design Based on Internet of Things Technology. *Electronic Production*. 31 (1), 116–120.
3. Bauer, E., & Adams, R. (2012). Reliability and Availability of Cloud Computing. *Hoboken, NJ*, USA: Wiley.
4. Elerath, J.G., & Pecht, M. (2012). IEEE 1413: A Standard for Reliability Predictions. *IEEE Transactions on Reliability*, 61(1), pp.125-129.
5. AmSuk, O. (2018). Design and Implementation of Smart Home Remote Control Based on Internet of Things Service Platform. *Journal of the Korea Institute of Information and Communication Engineering*. 22 (12), 1563–1570.
6. Vishnyakou, U.A., & Yu, C.Y. (2022). Modeling IoT Smart Home Network. *Doklady BGUIR*. 20 (6), 78–84.
7. Jenal, M., Omar, A. N., Hisham, M. A., Noh, W. N., & Razali, Z. A. (2022). Smart Home Controlling System. *Journal of Electronic Voltage and Application*. 3 (1), 92–104.
8. Mao, B., Xu K., Jin, Y. H., & Wang, X. L. (2017). Deep Home: a Control Model of Smart Home Based on DeepLearning. *Chinese Journal of Computers*. 40 (8), 1–15.
9. Gololobov, V. (2019). IoT as Intranet of Things with Raspberry Pi and MajorDoMo. Moscow.