**РЕФЕРАТ**

Отчет 35 с., 2 ч., 6 рис., 12 источников, 3 прил.

БЕСПРОВОДНЫЕ СЕТИ, ИНТЕРНЕТ ВЕЩЕЙ, СТАНДАРТ БЕЗОПАСНОСТИ, УГРОЗЫ БЕЗОПАСНОСТИ, УСТРОЙСТВО, УЯЗВИМОСТИ, ЭКСПЛУАТАЦИЯ.

Объектами исследования являются Интернет вещей, находящиеся в нем устройства и уязвимости данной технологии.

Цель работы – создание устройства с технологией обнаружения и устранения выявленных уязвимостей устройств Интернета вещей.

В процессе работы проводились теоретические исследования структуры и отдельных областей применения Интернета вещей.

В результате исследования было создано техническое решение проблемы продолжительного нахождения уязвимостей, выявленных в устройствах Интернета вещей.

Степень внедрения – прототип, в дальнейшем возможно развитие разработанной технологии.

Эффективность продукта определяется актуальностью Интернета вещей и работоспособностью проектного продукта.

**СОДЕРЖАНИЕ**

[**ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ И АББРЕВИАТУРЫ** 3](#_Toc131155535)

[**ВВЕДЕНИЕ** 6](#_Toc131155536)

[**ОСНОВНАЯ ЧАСТЬ ОТЧЕТА О НИР** 8](#_Toc131155537)

[1 Теоретическое исследование 8](#_Toc131155538)

[1.1 Сбор и анализ информации по исследуемой проблеме 8](#_Toc131155539)

[1.1.1 Архитектура 8](#_Toc131155540)

[1.1.2 Объем рынка и прогнозы по развитию 10](#_Toc131155541)

[1.1.3 Области применения 11](#_Toc131155542)

[1.1.4 Возможные и выявленные уязвимости 14](#_Toc131155543)

[1.1.5 Способы обеспечения безопасности 16](#_Toc131155544)

[1.1.6 Результаты исследования 18](#_Toc131155545)

[1.2 Формулировка технического задания 19](#_Toc131155546)

[1.2.1 Требования к проектному решению 19](#_Toc131155547)

[1.2.2 Предложения решения выявленной проблемы 19](#_Toc131155548)

[1.2.3 Концепция продукта и обоснование выбора оптимального решения 20](#_Toc131155549)

[2 Разработка технологического процесса 21](#_Toc131155550)

[2.1 Аналоги и прототипы 21](#_Toc131155551)

[2.2 Описание технологического процесса реализации проектного решения 22](#_Toc131155552)

[2.3 Потенциал применения 27](#_Toc131155553)

[2.4 Способы внедрения 29](#_Toc131155554)

[2.5 Экономическая и нормативная оценка реализации и внедрения 30](#_Toc131155555)

[**ЗАКЛЮЧЕНИЕ** 33](#_Toc131155556)

[**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** 34](#_Toc131155557)

[**ПРИЛОЖЕНИЯ** 36](#_Toc131155558)

**ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ И АББРЕВИАТУРЫ**

В настоящем проекте применяются следующие термины с соответствующими определениями:

*DLP-система* (англ. *Data Leak Prevention*) – программные продукты, защищающие организации от утечек конфиденциальной информации.

*DoS-атака* – попытка причинить вред, сделав недоступной целевую систему, например веб-сайт или приложение, для обычных конечных пользователей.

*Mesh-сети* – топология сети, отдельные узлы которой напрямую, в динамическом режиме и в отсутствие какой-либо строгой иерархии подключаются к максимально возможному количеству других узлов с целью эффективной передачи данных.

*SIEM-система* (англ. *Security Information and Events Management*) – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности.

*Standalone приложение* - программное обеспечение, которое не нуждается в каких-либо дополнительных программах и зависимостях для его установки и функционирования.

*RFID (*англ. *Radio Frequency Identification)* – способ автоматической идентификации объектов, который посредством радиосигналов считывает и записывает данные.

*Беспроводные сенсорные сети* (англ. *WSN – Wireless Sensor Network*) – распределённая, самоорганизующаяся [сеть](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) множества [датчиков](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%82%D1%87%D0%B8%D0%BA) и [исполнительных устройств](https://ru.wikipedia.org/wiki/%D0%98%D1%81%D0%BF%D0%BE%D0%BB%D0%BD%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B9%D1%81%D1%82%D0%B2%D0%BE), объединённых между собой посредством [радиоканала](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D0%B8%D0%BE%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB).

*Блокчейн* (англ. *block chain*) – выстроенная по определённым правилам непрерывная последовательная цепочка блоков ([связный список](https://ru.wikipedia.org/wiki/%D0%A1%D0%B2%D1%8F%D0%B7%D0%BD%D1%8B%D0%B9_%D1%81%D0%BF%D0%B8%D1%81%D0%BE%D0%BA)), содержащих информацию.

*Ботнет* (англ. *botnet*; образовано от слов *robot* и *network*) – [компьютерная сеть](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), состоящая из некоторого количества [хостов](https://ru.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82) с запущенными [ботами](https://ru.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B1%D0%BE%D1%82_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0)) — автономным [программным обеспечением](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5).

*Брутфорс* (англ. brute force) – метод подбора пароля (или ключа, используемого для шифрования), предполагающий систематический перебор всех возможных комбинаций символов до тех пор, пока не будет получена правильная комбинация.

*ИБ* (сокр. *Информационная безопасность*) – практика предотвращения несанкционированного доступа, использования, исследования записи или уничтожения информации.

*Интеллектуальные сети* (англ. *IN – Intelligent Network* или *Smart Grid*) – способ организации сети связи, ориентированный на введение в сеть услуг и управление ими. Определяют архитектуру аппаратных и программных средств, которая позволяет выполнять обмен данными между системой коммутацией и сетью во время организации связи между узлами.

*Интернет вещей* (англ. *IoT* – *Internet of Things*) – система взаимосвязанных физических объектов (устройств), которые могут собирать, обрабатывать и передавать данные без участия человека.

*ИТ* (сокр. *Информационные технологии*) – процессы, использующие совокупность средств и методов сбора, обработки, накопления и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса, явления, информационного продукта.

*Кросс-совместимость* – способность устройств работать в одной сети и безопасно обмениваться данными.

*Промышленный интернет вещей* (англ. *IIoT – Industrial Internet of Things*) – интернет вещей для корпоративного / отраслевого применения; система объединенных компьютерных сетей и подключенных промышленных (производственных) объектов со встроенными датчиками и ПО для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека.

*Реверс-инжиниринг* (англ. *Reverse Engineering*) – процесс анализа скомпилированного бинарного файла с целью понять, как программа работает.

*Сетевой коммутатор –* устройство, предназначенное для соединения нескольких [узлов](https://ru.wikipedia.org/wiki/%D0%A3%D0%B7%D0%B5%D0%BB_%D1%81%D0%B5%D1%82%D0%B8) [компьютерной сети](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) в пределах одного или нескольких [сегментов сети](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D0%B3%D0%BC%D0%B5%D0%BD%D1%82_%D1%81%D0%B5%D1%82%D0%B8). Коммутатор работает на [канальном (втором) уровне](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) сетевой [модели OSI](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI).

*Смарт-контракт* – компьютерные программы, хранящиеся в блокчейне, позволяющие конвертировать традиционные контракты в цифровые аналоги.

С*тандарт безопасности –* нормативно-технический документ, регламентирующий аспекты, связанные с безопасностью продукции, процессов, технологий, устанавливающий условия эксплуатации и технического обслуживания средств производства, а также исключения неприемлемого риска.

*ФСТЭК* (сокр. *Федеральная служба по техническому и экспертному контролю*) – орган защиты государственной тайны, наделенный полномочиями по распоряжению сведениями, составляющими государственную тайну. ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею.

*Цифровая трансформация* – процесс внедрения организацией цифровых технологий, позволяющий оптимизировать системы управления основными технологическими процессами.

*Шлюз* (англ. *Gateway*) – аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы (например, локальной и глобальной).

**ВВЕДЕНИЕ**

*Интернет вещей* соединяет миллиарды физических устройств по всему миру, которые подключены к Интернету, а данные могут передаваться и обрабатываться по сети без участия человека. С появлением новых удобств появились новые угрозы – по всему миру происходят взломы устройств, подключенных к Интернету, ведь не все уязвимости были устранены в силу новизны технологии.

Проведенное исследование поспособствует решению проблемы безопасности, а именно проблему продолжительного нахождения уязвимостей в устройствах Интернета вещей. Продукт будет содержать в себе основу для дальнейшего развития систем защиты устройств, подключенных к Интернету вещей. В ближайшее время проблема будет актуальна, так как рынок технологий постоянно развивается и всегда есть место новым решениям, которые также должны быть безопасными при использовании.

Цель работы – создание устройства с технологией обнаружения и устранения выявленных уязвимостей устройств Интернета вещей.

Задачи:

1. Разобрать строение (архитектуру) Интернета вещей;
2. Проанализировать объем рынка и прогнозы по развитию Интернета вещей;
3. Определить области применения Интернета вещей;
4. Определить возможные и выявленные угрозы безопасности при использовании Интернета вещей;
5. Проанализировать существующие методы устранения уязвимостей;
6. Определить несколько вариантов создания продукта;
7. Выбрать наиболее подходящую технологию;
8. Проанализировать потенциал применения результата проекта;
9. Предложить способы внедрения продукта;
10. Дать экономическую и нормативную оценку реализации и внедрения продукта.

**ОСНОВНАЯ ЧАСТЬ ОТЧЕТА О НИР**

1. Теоретическое исследование
   1. Сбор и анализ информации по исследуемой проблеме
      1. Архитектура

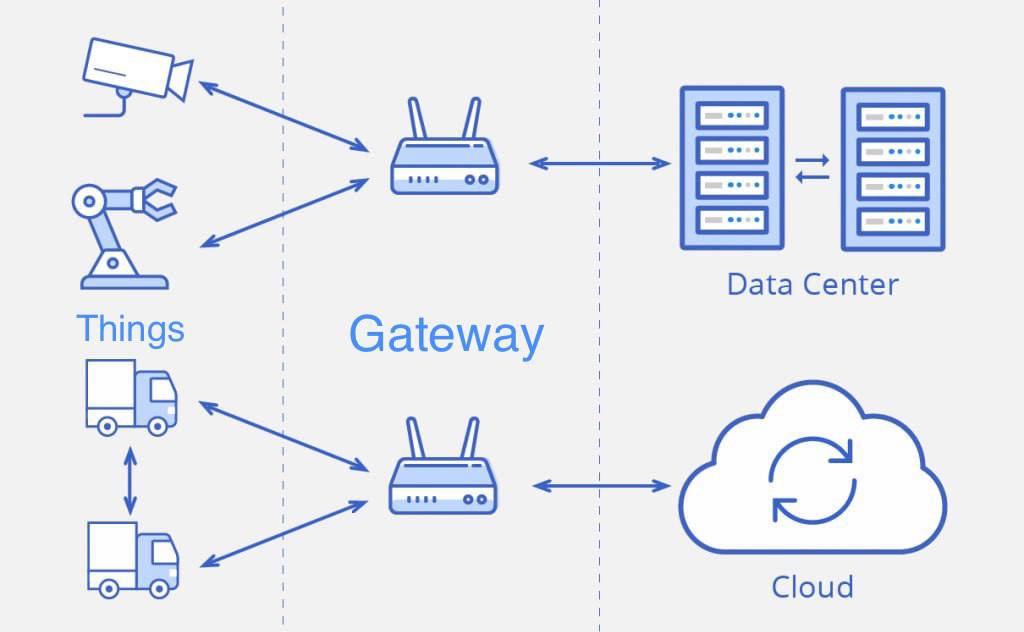
 Архитектура Интернета вещей состоит из нескольких уровней, в которых показано, как разные технологии связаны между собой (рисунок 1).

Рисунок 1 – Архитектура Интернета вещей

1. Уровень устройств (Things)

Состоит из объектов, соединенных с сенсорами. Обеспечивает сбор и обработку информации в реальном времени: измерение температуры, давления, влажности, скорости движения и других показателей.

Устройства имеют соединение со *шлюзами*, подключаемыми к локальной или глобальной вычислительной сети. Но есть и самодостаточные устройства, которые могут работать на базе сетей сотовых операторов (подключение с помощью Wi-Fi или Ethernet) – для координации с облаком им хватает доступа в интернет через провод, GSM/3G/LTE, NB-IoT, Wi-Fi и т.д. Сами шлюзы являются *коммутаторами*, поддерживающими определенный стандарт или протокол, обеспечивающий связь с приборами.

Беспроводные *сенсорные сети* состоят из сенсоров, характеризующимися низким электропотреблением и скоростью передачи данных. Они набирают все большую популярность, потому что могут содержать гораздо больше датчиков с поддержкой работы от батарей и охватывают большие площади – достигается это путем применения топологии *mesh-сети*. [8]

1. Уровень шлюзов и сетей (Gateway)

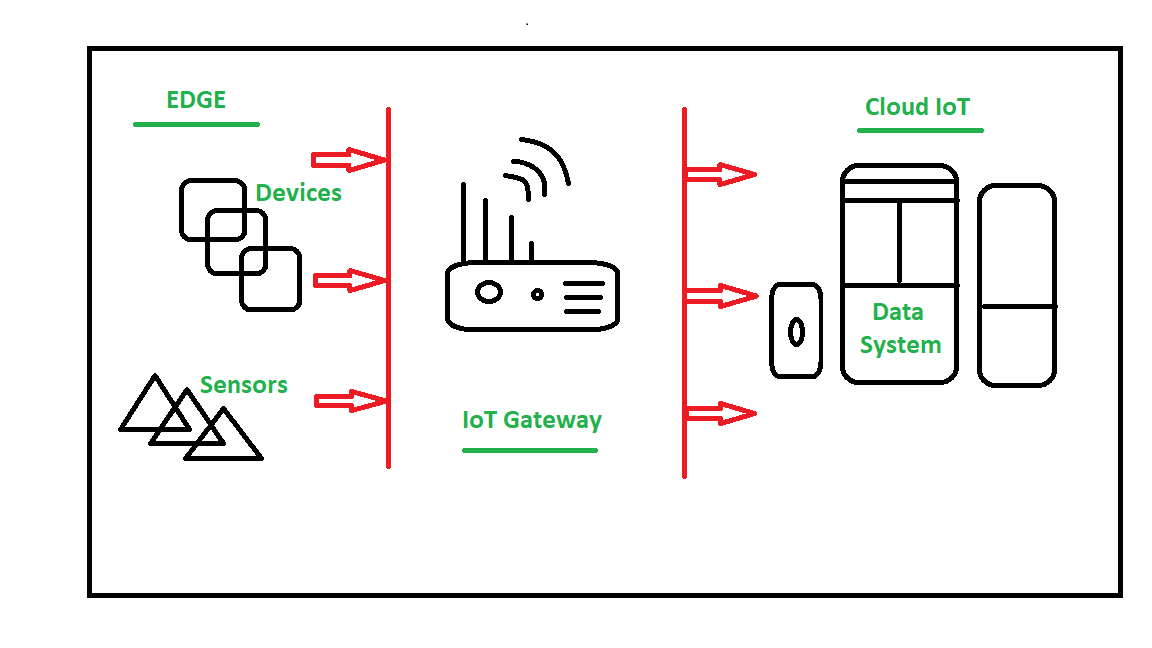
 Предназначен для соединения разнородных сетей в единую платформу (рисунок 2). Реализация широкого спектра задач в Интернете вещей достигается обеспечением совместной работы множества различных технологий и протоколов. Сети доступа должны обеспечивать требуемые значения передачи данных по задержке, пропускной способности и безопасности.

Рисунок 2 – Gateway Интернета вещей

Сетевые шлюзы обеспечивают взаимодействие пользователя или автоматизированных систем с элементами Интернета вещей посредством поддерживаемого стандарта связи. [8]

1. Сервисный уровень (Cloud)

Содержит набор информационных услуг, обеспечивающих автоматизацию технологических и бизнес-операций в Интернете вещей:

* приложение (API);
* централизованная панель управления элементами Интернета вещей;
* интерфейс хранения, ввода/вывода данных из внешней системы;
* различная аналитическая обработка информации;
* управление и поддержка операционной и бизнес-деятельностей;
* обеспечение информационной безопасности;
  + 1. Объем рынка и прогнозы по развитию

С объемом и структурой мирового рынка Интернета вещей можно ознакомиться в Приложении А.

Из прошлогодних исследований следует, что к концу 2021 года по всему миру насчитывалось 12,2 млрд находящихся в эксплуатации устройств Интернета вещей, что на 8% больше, чем в прошлом году – исследования были проведены компанией IoT Analytics.

Из прогноза вышеупомянутой исследовательской организации следует, что в 2021 году наблюдалась повсеместная перегруженность портов, что связано с карантинными мерами во время пандемии. Также были трудности с транспортировкой аппаратуры грузовым и судоходным транспортом, с контейнерными перевозками.

Были названы главные факторы, влияющие на развитие рынка Интернета вещей, из них:

1. Инфляция. С ростом инфляции в большинстве крупных стран ухудшается экономический рост рынка, что также затрагивает рынок Интернета вещей;
2. Дефицит ИТ-кадров. В 2021 году значительно уменьшилось количество специалистов в сфере искусственного интеллекта, интернета вещей и облачных вычислений.
   * 1. Области применения

Концепция Интернета вещей может существенно улучшить многие сферы жизни, а также создать более умный и удобный мир. Уже сейчас заметно повсеместное использование данной технологии.

Можно выделить несколько основных сфер, в которых применяется технология Интернета вещей:

1. Промышленность

Интернет вещей в промышленности выделяют в отдельный термин – *Промышленный интернет вещей*.

На производстве устанавливаются датчики, исполнительные механизмы, контроллеры и интерфейсы (для удобства восприятия человеком). После осуществляется сбор информации, которая впоследствии дает объективные и точные данные о состоянии производства. Далее обработанные данные распределяются по отделам, что помогает наладить взаимодействие между сотрудниками предприятия.

Имеются определенные условия внедрения Интернета вещей в производство: например, определенные потребности в повышении качества, значительная энергоемкость производства и т.п.

На сегодняшний день существуют разработанные *стандарты безопасности*, которые необходимо соблюдать при внедрении промышленного Интернета вещей: «Протокол защищенного обмена для индустриальных систем (CRISP 1.0)», [ISO/TR 22100-4:2018](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:ISO/TR_22100-4:2018_%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%BF%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BE%D0%B1%D0%BE%D1%80%D1%83%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F_%E2%80%93_%D0%A1%D0%B2%D1%8F%D0%B7%D1%8C_%D1%81_ISO_12100_%E2%80%93_%D0%A7%D0%B0%D1%81%D1%82%D1%8C_4) «Безопасность производственного оборудования — Связь с ISO 12100 — Часть 4: Руководство для производителей оборудования по рассмотрению соответствующих аспектов [информационной безопасности](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C) ([кибербезопасности](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8))». [2]

1. Электроэнергетика

В электроэнергетике в Интернет вещей входят *интеллектуальные сети* и счетчики. Преимущества использования Интернета вещей в энергетике направляются на более оптимальную планировку загрузки генерирующих мощностей и их объем.

Более широкое внедрение интеллектуальных технологий, особенно с учетом протяженности линейных объектов, могло бы привести к повышению надежности и снижению операционных расходов. Это позволило бы перейти к управлению сетью «по состоянию», а не проводить ремонты в соответствии с жесткими регламентными сроками.

Некоторые частные энергетические компании также активно оснащают свои объекты системами удаленного контроля и диагностики с целью повысить надежность и снизить расходы на эксплуатацию.

1. Автомобилестроение

Интернет вещей применяется сразу в нескольких процессах автомобилестроения.

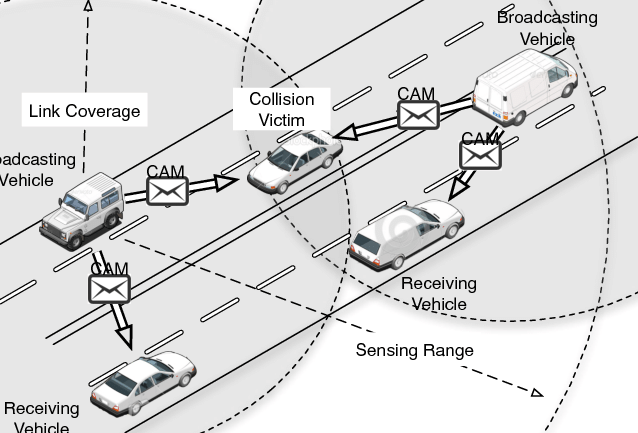
 Встроенные сенсоры Интернета вещей позволяют обмениваться данными с другими автомобилями (технология *V2V – vehicle-to-vehicle,* рисунок 4). [1]

Рисунок 3 – Структура V2V

Датчики и сенсоры применяются, например, для контроля за состоянием колес и подвески автомобиля. Такие данные, как скорость, давление воздуха в шинах, нагрузка при вождении, собираются в реальном времени и отправляются на бортовой компьютер, а при неисправностях сразу сообщают пользователю (водителю). Данное нововведение позволяет свести к минимуму дорогостоящий ремонт и регулярные проверки автомобиля, а также исключают операции, выполнение которых не обойдется без человека.

1. Транспорт и логистика

Более серьезные системы интеллектуального мониторинга транспорта внедряются благодаря установке в автомобили систем удаленного мониторинга передвижения на базе датчиков [ГЛОНАСС](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:%D0%93%D0%9B%D0%9E%D0%9D%D0%90%D0%A1%D0%A1)/[GPS](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:GPS) и систем контроля за расходом топлива. Такие устройства позволяют существенно сократить затраты и контролировать целевое использование транспорта, анализировать и оптимизировать маршруты движения, что крайне важно для логистики.

Благодаря использованию систем мониторинга и навигации (те же датчики ГЛОНАСС/GPS) становится возможным построение оптимальных и безопасных маршрутов. Такой подход помогает менеджерам улучшать контроль над работой транспортных средств и сводить к минимуму влияние на операции человеческого фактора.

1. Умный дом

Дом можно назвать умным, когда он имеет ряд интеллектуальных устройств, которые объединены в одну сеть и могут управляться удаленно.

С каждым годом концепция Умного дома реализуется все в большем количестве домов и квартир. Подобные высокотехнологичные дома повышают комфорт проживания, ведь большинство процессов автоматизируются и управляются удаленно.

Несмотря на то, что технологии домашней автоматизации и Интернета вещей существуют уже достаточно долгое время, многие решения остаются в режиме тестирования, и всегда есть возможность улучшения какого-либо аспекта. Одной из наиболее обсуждаемых проблем интеллектуальной домашней автоматизации является проблема *кросс-совместимости* – это является основным препятствием для успешного, полного и повсеместного внедрения Умного дома.

1. Здравоохранение

Спрос на более качественные медицинские услуги, распространение хронических заболеваний, рост численности гериатрического населения увеличивают расходы в отрасли здравоохранения. Ключевыми драйверами роста рынка Интернета вещей в здравоохранении являются: необходимость контроля затрат в секторе здравоохранения, растущее внимание к уходу, ориентированному на пациента, развитие высокоскоростных сетевых коммуникационных технологий.

Интернет вещей может применяться в медицине для удаленного мониторинга здоровья, отслеживания приема лекарств, мониторинга медицинских активов на основе Интернета вещей, умного больничного пространства.

Исходя из анализа областей применения Интернета вещей, можно сделать вывод, что данную технологию используют люди практически всех возрастов и профессий – непосредственно или косвенно.

* + 1. Возможные и выявленные уязвимости

Высокое проникновение промышленного Интернета вещей в критически важную инфраструктуру и производственный сектор привело к увеличению числа потенциальных кибератак. Об этом свидетельствуют данные исследования, проведенного аналитиками компании [Frost & Sullivan](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Frost_%26_Sullivan), о чем стало известно 13 декабря 2018 года.

Не секрет, что некоторые производители систем и устройств Интернета вещей торопятся вывести свои продукты на продажу как можно скорее, исходя из коммерческого интереса. Это означает, что есть место отсутствию тестирования и доброкачественной разработки «умных» вещей – в процессе разработки могли быть не учтены угрозы безопасности устройств, а после запуска могут отсутствовать обновления безопасности. [12]

Компании часто связывают поставщиков для предоставления услуг и доставки. Однако, это непреднамеренный вход для субъектов угрозы, если полномочия скомпрометированы. Необходимо контролировать сторонний доступ, который включает в себя поставщиков.

Исходя из предыдущей проблемы безопасности Интернета вещей следует еще одна – злоумышленникам предоставляется возможность создания и внедрения вредоносных программ и программ-вымогателей для устройств Интернета вещей. Вредоносные программы для *ботнетов* из устройств интернета вещей встречаются наиболее часто. Такие программы могут захватывать контроль над целыми сетями устройств, впоследствии нарушая работу приборов, что приводит к угрозам безопасности и конфиденциальности самого пользователя.

Примером уязвимости, при которой сеть устройств становится ботнетом, является Mirai Botnet. Mirai – это вредоносная программа, которая заражает устройства в сети и удаленно управляет ими. Часто такая схема используется для реализации дальнейших атак – например, DDoS-атак. Mirai сканирует сеть устройств Интернета вещей, основанных на ARC процессорах (как правило, данные процессоры используют операционную систему Linux). Если базовые имя пользователя и пароль не были изменены, то злоумышленники могли получить доступ к сети и заражали программой Mirai. [7]

Как упоминалось выше, главной ошибкой пользователя при первичной настройке системы или части системы Интернета вещей является пренебрежение сменой базового пароля. Такие пароли можно легко подобрать существующими и открытыми инструментами для *брутфорса*. [12]

Уже выяснено, что система Интернета вещей работает в единой сети предприятия или дома – это необходимое условие для работы, но также это является еще одной «лазейкой» злоумышленников. Достаточно неправильно настроить всего лишь один параметр безопасности на одном из устройств, и вся домашняя сеть окажется в опасности.

* + 1. Способы обеспечения безопасности

Чтобы понять, как защитить систему, необходимо понять, как искать уязвимые устройства Интернета вещей.

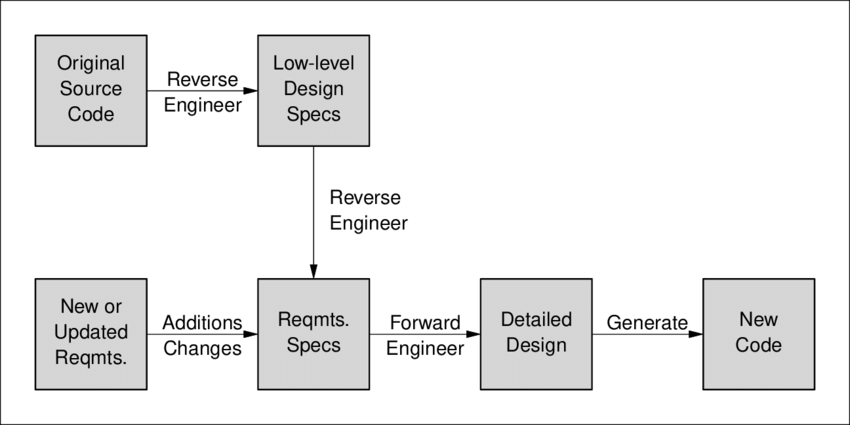
Взломать «умное» устройство можно несколькими путями – например, через уязвимости в прошивке, которые были найдены путем *реверс-инжиниринга* (рисунок 5). Первым шагом будет поиск отличительной черты устройства – можно найти уязвимость интересующего нас устройства в существующих базах данных (например, от компаний MITRE или Rapid7), а уже через уязвимость добраться до «центра» устройства. [11]

Рисунок 4 – Процесс реверс-инжиниринга

Данный способ («намеренный взлом») может являться методом обеспечения безопасности: разработчик (или же человек, не являющийся злоумышленником) опережает преступника – эксплуатирует уязвимость и находит решение данной проблемы, тем самым перекрывая доступ к устройству злоумышленнику. Процесс эксплуатации при должной настройке может производиться автоматически.

Есть ряд рекомендаций, соблюдая которые можно минимизировать риск взлома устройства: регулярные обновления, смена паролей «по умолчанию» и использование надежных, использование надежного метода шифрования Wi-Fi, контроль устройств (их параметров конфиденциальности и функций) и т.д.

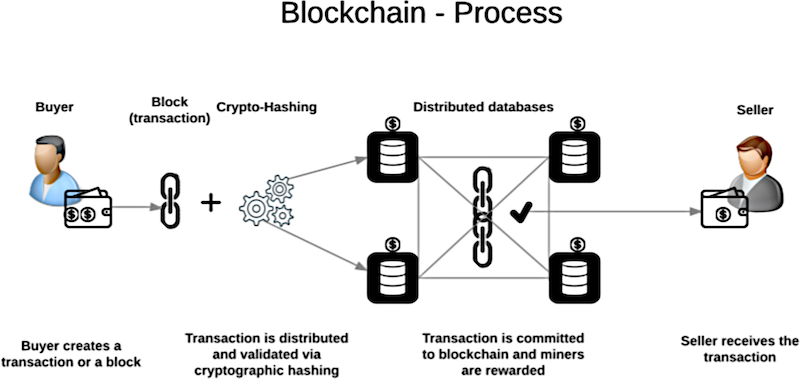
Также применяются инновационные и надежные технологии защиты. Например, комбинация *блокчейна* (рисунок 6)и Интернета вещей часто рассматривается как один из наиболее перспективных сценариев применения технологии обеспечения безопасности.

Рисунок 5 – Процесс блокчейна

Количество вариантов использования блокчейна в IoT-приложениях велико: можно обеспечивать защиту цепей поставок, центрального сервера, транспорта, умных замков и т.д. Предлагается использование *смарт-контрактов* Ethereum: весь процесс, например, оплаты аренды при помощи смартфона автоматизирован и следует инструкциям, прописанным в умном контракте. [9]

Специалисты советуют ограничивать доступ к устройствам поставщикам и третьим лицам. Это можно сделать, инициируя MFA (Multi-factor Authentication) от мобильного телефона или настольного приложения. Необходимо разработать протоколы в отношении того, кто будет иметь доступ, и они должны разграничить уровень доступа, который будет иметь третья сторона. Это одна из политики «нулевого доверия», которую должны принять как можно скорее. [5]

* + 1. Результаты исследования

Интернет вещей – относительно новая технология, которая уже обладает преимуществами для повсеместного использования.

Архитектура Интернета вещей представляет собой определенную иерархию, каждые части которой соединены необходимыми технологиями (коммутатор, mesh-сети, шлюзы).

Для создания и поддержания безопасности Интернета вещей были установлены специальные стандарты безопасности.

Устройства Интернета вещей можно найти в самых различных областях современного рынка, а по прогнозам различных исследований данная технология будет только развиваться.

Несмотря на все существующие рекомендации по использованию устройств Интернета вещей, все равно остается риск несанкционированного доступа к данным, которые обрабатываются и передаются в единой сети.

Важным упоминанием будет то, что все необходимые для взлома инструменты и базы данных находятся в открытом доступе и, следовательно, нет возможности полностью ограничиться от них – для защиты необходимо создавать новые методы обеспечения безопасности.

## Формулировка технического задания

Исходя из теоретического исследования можно определить характерные черты разработки будущего продукта.

* + 1. Требования к проектному решению

1. Выполнение поставленной цели исследования;
2. Соблюдение архитектуры Интернета вещей;
3. Возможность внедрения в производство и рынок Интернета вещей;
4. Соответствие современным тенденциям развития технологии;
5. Использование хотя бы одного способа защиты;
6. Соблюдение Федеральных Законов Российской федерации (149-ФЗ «Об информации, информационных технологиях и о защите информации», 152-ФЗ «О персональных данных», 98-ФЗ «О коммерческой тайне», 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»);
7. Наличие документации на программное обеспечение и технической документации на оборудование.
   * 1. Предложения решения выявленной проблемы

В ходе исследования было выявлено несколько проблем Интернета вещей: неосведомленность пользователей, безответственное отношение компаний к разработке продуктов Интернета вещей, значительное количество уязвимостей (*CVE* – Common Vulnerabilities and Exposures) в устройствах, увеличение числа потенциальных атак со стороны злоумышленников, создание и внедрение вредоносных программ.

Для решения выбрана проблема продолжительного наличия уязвимостей, потенциальных для дальнейшей эксплуатации и взлома устройств, так как оставшиеся проблемы не подлежат решению в данной исследовательской работе.

Предложения решения выявленной проблемы:

1. Реализация намеренной эксплуатации устройства посредством получения сообщения об ошибке и использования существующей базы уязвимостей;
2. Регулярное автоматическое сканирование сетей устройств на наличие уязвимостей или вредоносного программного кода;
3. Первоначальное создание абсолютно безопасного устройства, в котором не будет каких-либо уязвимостей;
4. Разделение одной сети на несколько подсетей, которые будут регулярно сканироваться.
   * 1. Концепция продукта и обоснование выбора оптимального решения

Мною было выбрана реализация намеренной эксплуатации устройства посредством получения сообщения об ошибке и использования существующей базы уязвимостей. Я считаю данное решение наиболее оптимальным, так как в остальных идеях имеются противоречия:

1. При реализации регулярного автоматического сканирования сетей будет необоснованная нагрузка на всю систему, что приведет еще к большему количеству сбоев;
2. Первоначальное создание абсолютно безопасного устройства невозможно технически: даже если оно будет безопасным, то останутся уязвимости в сети, которые также должны быть найдены и решены;
3. Разделение одной сети на несколько подсетей противоречит самой концепции Интернета вещей, где устройства находятся в единой сети.

Концепция продукта состоит из устройства, которое имеет возможность подключиться к сети Интернет и сети Интернета вещей, в котором находится проверяемое устройство, проэксплуатировать уязвимости, опираясь на существующую базу данных, и предложить решения найденных проблем.

# Разработка технологического процесса

* 1. Аналоги и прототипы

При анализе рынка решений по обеспечению безопасности устройств Интернета вещей было найдено несколько готовых продуктов:

1. FirstPoint – программное решение, сосредоточенное на защите устройств Интернета вещей от атак, которые исходят из сотовой сети или которые общаются через сотовую сеть. FirstPoint является победителем IoT Evolution Expo 2022 года в номинации Security Excellence.
2. NanoLock – нацелен на блокировку вредоносных программ, программ-вымогателей, атак «отказ в обслуживании» (*DoS-атака*) и других угроз. Может использоваться не только на мелких, но и на крупных производствах. Основан на концепции «нулевого» доверия.
3. Armis – комплекс решений, который обрабатывает весь трафик для последующего выявления уязвимостей, выполнения автоматических политик безопасности и обеспечения непрерывного мониторинга управляемых и неуправляемых устройств.
4. Bastille – набор сенсоров, которые предназначены для устранения радиочастотной угрозы путем обнаружения, анализа и классификации устройств, подключенных к сети устройств Интернета вещей, и предоставления инструментов для принятия мер, необходимых для защиты. [4]

К аналогам продукта исследовательского проекта можно отнести такие рассмотренные решения, как FirstPoint и Bastille, так как они основаны на схожих концепциях работы с сетью, анализа и защиты устройства. Одновременно с этим можно утверждать, что наилучшим существующим решением из рассмотренных является FirstPoint, что подтверждается общепризнанными наградами.

Исходя из анализа подобранных решений можно сделать вывод, что продукт данного исследовательского проекта будет отличаться своей новизной, так как в настоящее время существует малое количество схожих технологий и реализаций.

Важным упоминанием будет то, что проектный продукт будет являться одной из немногих отечественных разработок в области Интернета вещей, так как в настоящее время используются не только зарубежные устройства Интернета вещей, но и зарубежные решения по обеспечению безопасности данной технологии.

Продукт данного исследовательского проекта так же, как и существующие аналоги будет решать поставленную проблему безопасности Интернета вещей (соответственно, проблемы информационной безопасности в целом) – проблему продолжительного наличия уязвимостей, их поиск и предложение решений по устранению, а также будет отвечать поставленной цели – создание технологии для устранения выявленных уязвимостей устройств Интернета вещей.

* 1. Описание технологического процесса реализации проектного решения

Реализация продукта будет осуществлена следующим образом:

1. Основа продукта

За основу берется Raspberry Pi – одноплатный компьютер. Несмотря на свои малые размеры, плата имеет высокую производительность, что позволяет ей выйти на один уровень со стационарными ПК. Благодаря своей комплектации, на современном Raspberry Pi можно реализовать множество задач и проектов.

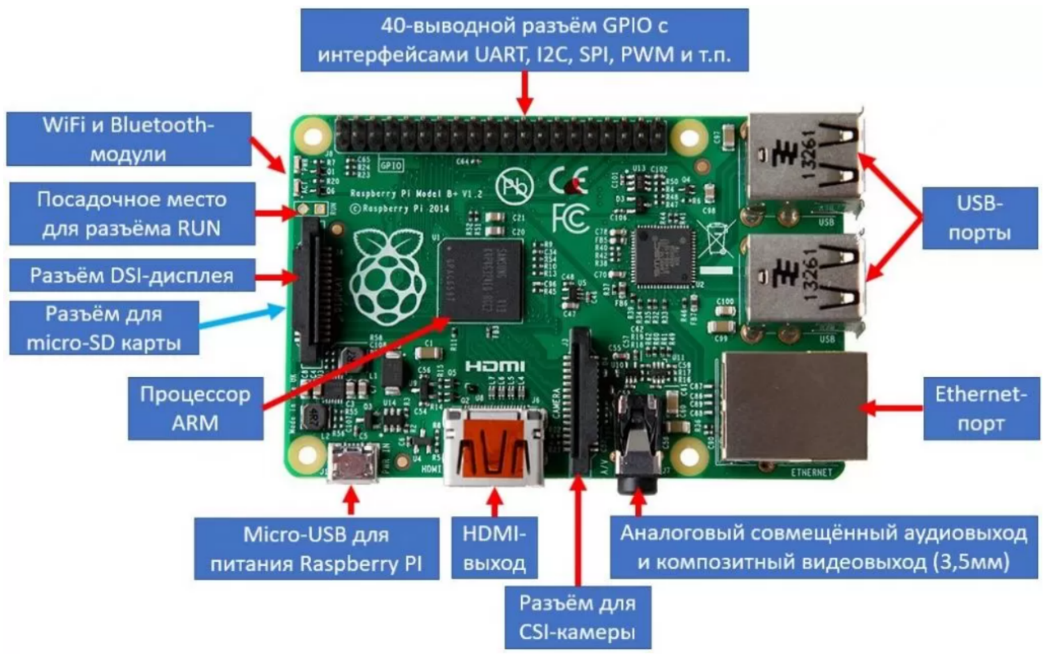
В разрабатываемом решении будет осуществлена реализация подключения устройства к Wi-Fi (следовательно, подключение к единой сети устройств Интернета вещей), хранения и обновления существующей базы уязвимостей, алгоритма для выявления уязвимостей, использующего базу уязвимостей, и программы по определению и предложению решений по обеспечении безопасности (устранения уязвимостей). Все функции будут представлены графически в виде приложения для удобства в использовании пользователем.

Рисунок 6 – Составные элементы Raspberry Pi [3]

1. Подключение к сети Интернет

Raspberry Pi оснащается модулем Wi-Fi начиная модели 3 Model B, следовательно, за основу будет взята данная модель, так как отпадает необходимость дополнительных затрат и установки *донгла*. После настройки Raspberry Pi (установки программного обеспечения и обновлений) станет возможным настройка подключения к сети Интернет.

Сначала устанавливается модуль Wi-Fi. После этого необходимо подключить монитор, открыть консоль и ввести команду «Terminal». Затем запустить утилиту вывода информации о USB-устройствах путем ввода «lsusb | grep wireless» и убедиться, что в выводе есть запись, содержащая строки «Wireless Adapter». Запустить консоль. Далее ввести команду «lsusb» и посмотреть, есть ли в списке запись Wireless Adapter. Если интерфейс находится в состоянии «down», надо его «поднять» вводом команды «ifconfig wlan0 up» от имени суперпользователя. После успешного определения совместимости можно настраивать микрокомпьютер. Для получения всей информации может потребоваться запуск команды от имени суперпользователя. [10]

После настройки модуля Wi-Fi на Raspberry Pi, необходимо найти сеть, к которой подключены все устройства необходимой сети Интернета вещей, и подключиться к ней.

1. Хранение и обновление базы данных

Существует множество качественно разработанных баз данных уязвимостей.

Стоит рассмотреть существующие российские базы уязвимостей, так как продукт будет являться отечественной разработкой и должен быть максимально независимым от зарубежных разработок. Основными, если не единственными, российскими базами данных являются база данных *ФСТЭК* и база данных от российской компании Positive Technologies. База уязвимостей от Positive Technologies обновляется чаще, чем база ФСТЭК – это является главным преимуществом. Обе базы данных представлены в затруднительном для применения в проектном продукте виде – база уязвимостей от Positive Technologies представляет собой веб-страницу, а базу данных ФСТЭК можно загрузить только в двух форматах – XML и XLSX. Соответственно, использование зарубежной базы данных – вынужденная мера до тех пор, пока не появится качественная отечественная база данных уязвимостей, представленная в удобном для использования формате.

В разработке продукта была выбрана база данных CVE. Главными преимуществами данной базы в сравнении с другими являются возможности организациям использовать единую систему для взаимодействия между собой и совместимыми с CVE инструментами, что повышает удобство пользования продуктом, и получать информацию о конкретной уязвимости из различных источников. Базу данных CVE можно скачать и использовать в различных форматах (CSV, HTML, Text, XML, JSON). Наиболее удобным для использования в проектном продукте является формат JSON, так как его можно наиболее просто и быстро обновлять путем импортирования с официального источника. Целесообразно будет хранить данные об уязвимостях за последние 2-3 года, так как уязвимости регулярно обновляются, например – устраняются.

1. Программная составляющая

При возникших неполадках устройство, находящееся в сети, отправляет входной сигнал на приемщик (т.е. проектное решение) через шлюз. Данный приемщик обрабатывает сигнал с ошибкой, находит описание проблемы в базе уязвимостей CVE, определяет решение проблемы (которое также представлено в используемой базе) и отправляет текст с ошибкой и необходимым решением на разработанное устройство сети Интернета вещей.

В программной составляющей необходимо реализовать следующие пункты:

1. Обновление, хранение и использование базы уязвимостей CVE в формате JSON;
2. Реализация приема сообщений об ошибках от устройств в определенной сети Интернета вещей;
3. Алгоритм по обработке полученных сообщений об ошибках и нахождению решений полученных ошибок;
4. Реализация уведомлений о выявленных уязвимостях, найденных решениях, обновлениях;
5. Представление системы в виде *standalone-приложения*;
6. Реализация понятного и удобного пользователю интерфейса.

Исходя из критериев, необходимых для реализации технологии, можно составить список используемых библиотек для использования в языке программирования Python: sys, PyQt5, os, wget, json, datetime, plyer, pyinstaller. Данный список может пополняться и изменяться.

Описание разработки программной составляющей представлено в виде uml-диаграммы в Приложении Б. С фрагментами кода можно ознакомиться в Приложении В.

1. Обеспечение защиты от угроз

Стоит учитывать угрозы не только искусственного, но и естественного характера. В случае с естественными угрозами стоит обеспечивать защиту продукта таким же образом, как и системы, в котором оно используется: крепкий корпус, противопожарная защита, защита от влаги. Обусловлено это тем, что устройства сети Интернета вещей может применяться в различных условиях, и исходя из этих условий обеспечивается необходимая защита.

Искусственные угрозы могут быть реализованы двумя способами: эксплуатация уязвимостей (использование вредоносного года и т.п.) и несанкционированный доступ. При реализации взлома первым способом стоит использовать такой метод защиты, как межсетевой экран. При реализации второго способа необходимо использовать *DLP-* и *SIEM-системы*, которые предотвращают несанкционированный доступ к информации и ее утечку (взлом с нарушением работы в устройстве посредством электромагнитных и электрических каналов и т.п.).

1. Разработка документации

Документация на разработанное программное обеспечение должна включать в себя руководство по использованию программы и справочный текст к функциям приложения. Техническая документация на разработанное оборудование должна включать в себя характеристики устройства, руководство по эксплуатации.

* 1. Потенциал применения

При оценке потенциала применения результата проекта стоит учитывать несколько факторов.

Актуальность применения Интернета вещей в настоящее время освещена путем анализа областей, в которых используется данная технология. Устройства, являющиеся частью данной системы, применяются повсеместно: датчики установлены в автомобилях и на производствах, сенсоры контролируют работу медицинских приборов и встроены в приборы умного дома. Соответственно, угроза взлома может присутствовать в любой критической структуре, а значит, современный рынок технологий нуждается в решениях для защиты той или иной структуры, в которой используется Интернет вещей. Также это означает, что продукт сможет использоваться в любой точке мира, где он необходим – нет ограничений по местоположению реализации.

К современным представлениям о решении данной проблемы относятся такие факторы, как целостность решения, его автономность, производительность (какое максимальное количество устройств поддерживает), длительность жизненного цикла продукта.

Целостность решения, его автономность и производительность обусловлены основной составляющей и программного решения созданного результата проекта. Стоит предположить, что после реализации продукта на рынке технологий его жизненный цикл продолжит расти в течение нескольких лет, так как актуальность Интернета вещей будет только набирать обороты и находить новые сферы применения. При дальнейших обновлениях и улучшениях продукта он не потеряет свою актуальность в течение длительного срока, а значит конец жизненного цикла будет сложно предугадать.

Целевой аудиторией будут являться, в первую очередь, рабочие промышленных предприятий и медицинских учреждений, работа которых тесно связана с Интернетом вещей и где важна безопасность данной технологии, так как любые нарушения могут привести к фатальным последствиям. Также решение проекта может применяться и в системе Умного дома, следовательно, целевую аудиторию предложенного решения дополнят обычные пользователи, которые ценят комфорт в доме и его цифровизацию.

Так как устройство, спроектированное в решении проекта, может работать автономно (без участия человека), оно будет достаточно удобным в использовании людей, неспециализированных в ИТ-сфере. Возможно внедрение визуализации системы или процесса выполнения некоторых этапов (действий), что также повысит удобство применения, так как человек доверяет больше продуктам, которые имеют визуальное и понятное представление.

В связи с обстановкой на российском рынке технологий, которая сформировалась после определенных событий в мире, можно предположить, что разработанный продукт сможет заместить импортные решения, обеспечивая дальнейшую безопасность при использовании устройств Интернета вещей на производстве и в других различных сферах. Данное преимущество позволит оставить современные технологии в стране и продолжить их развитие без каких-либо потерь.

Исходя из предыдущего описанного преимущества продукта следует еще один плюс – понижается вероятность потери кадров. Наиболее вероятно, что при разработке продукта и выведении его на большой рынок понадобиться команда специалистов. При реализации продукта будет исключена потеря уже существующих кадров, так как Интернет вещей останется и продолжит развиваться, а соответственно, профессионалы в данной сфере смогут остаться при работе или найти новую, связанную с их родом деятельности.

* 1. Способы внедрения

Исходя из особенностей продукта (в частности его многофункциональности и универсальности применения) и проведенного анализа, можно предложить несколько способов по внедрению:

1. Повсеместное использование в системе Умного дома

Разработанное устройство будет подключено к сети устройств Умного дома. При нарушении работы какого-либо устройства будет посылаться сигнал о проблеме. Продукт будет принимать данный сигнал, подключаться к устройству и находить уязвимость или решение проблемы.

1. Внедрение в технологии производства

Продукт будет напрямую связан с каждым прибором в циклах производства (данное решение о реализации большого количества устройств обусловлено тем, что на данной стадии нет гарантии того, что один продукт сможет поддерживать всю нагрузку единого производства). При выявлении неполадок будет незамедлительная реакция от разработанного продукта и дальнейшее решение проблемы.

1. Использование в приборах медицинского сектора

Устройство сможет контролировать, например, автоматизированный процесс подачи лекарств и контроль устройств, которые используются во время наблюдения за пациентом или реабилитации больного.

1. Контроль за процессами в автомобилях

Ранее рассматривалось применение устройств Интернета вещей в контроле за процессами в автомобилях. С применением разработанного продукта можно сделать данное использование Интернета вещей более безопасным, что уменьшит количество аварий с участием «умных» автомобилей.

1. Внедрение для сбора статистики

Проектное решение может быть реализовано не только для своих основных задач, но и в целях сбора статистических данных для создания новых решений по улучшению безопасности Интернета вещей.

* 1. Экономическая и нормативная оценка реализации и внедрения

В затраты на реализацию и внедрение проектного решения включаются стоимость технических составляющих устройства и траты на дальнейшую поддержку в сети.

* В настоящее время одноплатный компьютер Raspberry Pi 3 model B (минимально возможный для использования в продукте) стоит 11.799 рублей (источник: <https://www.dns-shop.ru/product/f7f069de01303330/mikrokomputer-raspberry-pi-3-model-b/>);
* К одноплатному компьютеру для работы прилагается блок питания стоимостью 1499 рублей (источник: <https://www.dns-shop.ru/product/348deb7ab4a03330/blok-pitania-raspberry-pi-3-power-supply/>);
* Образ Raspberry Pi OS устанавливается на microSD карту емкостью не менее 8 Гб. Стоимость карты: 399 рублей и выше (источник: <https://www.dns-shop.ru/product/3a935fdbf7ef3330/karta-pamati-smartbuy-sdhc-8-gb-sb8gbsdhccl10/>);
* Дисплей, который используется для визуализации в процессе настройки (может использоваться и в дальнейшей эксплуатации), не имеет определенных требований. Главный критерий: поддержка HDMI. Мною был выбран сенсорный дисплей, предназначенный для Raspberry Pi, стоимостью 7599 рублей;
* Сумма для оплаты Интернета зависит от места, в котором будет реализовываться продукт. В среднем это значение равно 1000 рублей;
* Средняя зарплата junior-разработчика на Python в России составляет 50.000 рублей (источник: <https://hh.ru>).

Стоимость внедрения данного решения без наценок составляет 72.296 рублей. Для покупателя базовое решение обойдется в 100.000 рублей (сумма стоимостей составляющих \* 2 + оплата труда разработчика). Следовательно, полная окупаемость продукта будет осуществлена после одного внедрения продукта. Прибыль будет составлять 60.000 рублей и более.

Нормативная оценка решения будет производиться по нескольким критериям:

1. Соблюдение 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Данный критерий соблюдается, так как, следуя ключевым моментам закона, информация о жизни человека не собирается и не распространяется без его согласия, вся информация, доступ к которой нельзя ограничивать, не скрывается, а также обеспечивается безопасное хранение информации.

1. Соблюдение 152-ФЗ «О персональных данных»

Данный критерий соблюдается, так как перед началом использования и настройки продукта спрашивается разрешение на сбор и обработку персональных данных, и полученные данные не передаются третьим лицам.

1. Соблюдение 98-ФЗ «О коммерческой тайне»

На данном этапе данный критерий не может быть учтен, так как продукт не является разработкой определенной коммерческой компании – решение является разработкой в рамках исследовательского проекта.

1. Соблюдение 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

При разработке IT-инфраструктуры критически важные предприятия должны руководствоваться 239 приказом ФСТЭК. В нем прописаны основные требования к защите информации на таких предприятиях.

Важным упоминанием будет тот факт, что данная нормативная оценка выполнена, основываясь на теоретических знаниях и знании разработки продукта. Официальную нормативную оценку должны проводить специалисты определенных организаций, в том числе ФСТЭК.

Оценивая конкурентоспособность разработанного продукта, можно прийти к выводу, что проектное решение будет являться перспективной разработкой на рынке Интернета вещей, так как соблюдены современные представления о продукте и определена его возможная рыночная стоимость, определена целевая аудитория и способы внедрения продукта. Безусловно, устоявшиеся компании являются серьезными конкурентами на данный момент, но при внедрении новых технологий в продукт и, вероятно, спонсирование решения выведут разработку на один уровень с уже существующими решениями.

**ЗАКЛЮЧЕНИЕ**

По результатам научно-исследовательской работы можно сделать вывод, что Интернет вещей – новая и быстроразвивающаяся технология, и на данном этапе необходимо обеспечить ее достаточную безопасность, так как она проникает во все сферы промышленности и рынка. После теоретического исследования темы были определены все важные аспекты Интернета вещей: структура, области применения, существующие уязвимости, методы решения угроз безопасности. При исследовании в течение формулировки технического задания были выявлены преимущества и недостатки нескольких путей решения проблемы: учитывалась целесообразность реализации того или иного решения, нагрузка сети, возможные проблемы.

Разработанный в результате практико-ориентированной исследовательской работы продукт находится на стадии прототипа, который является основой для дальнейшей разработки методики защиты устройств Интернета вещей и устройств, способствующих поддержанию безопасности технологии. Были определены несколько решений по развитию и внедрению проектного продукта. В сравнении с лучшим достижением в области разработки безопасного Интернета вещей спроектированный продукт имеет ряд свойств, которые уступают по глубине разработки. Связано это с моей собственной недостаточной наработкой в создании данных технологий, в то время как компании, специализирующиеся на данной разработке, уже несколько лет предоставляют готовые решения и обеспечивают безопасность Интернета вещей. Размышляя над возможными улучшениями системы, можно упомянуть такие предложения по развитию, как создание отдельной операционной системы для устройства и реализация полного анализа сети.

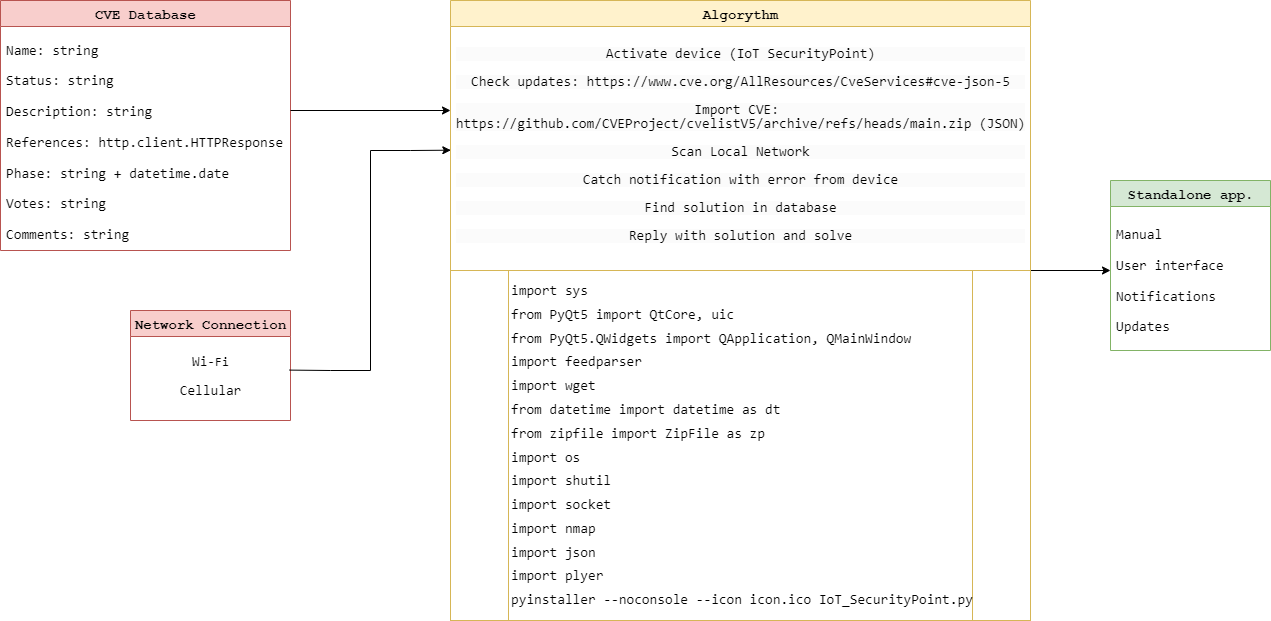
Поставленные задачи были выполнены в полной мере. Цель работы – создание устройства с технологией обнаружения и устранения выявленных уязвимостей устройств Интернета вещей – выполнена.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Automotive IoT: Smarter Vehicles, Optimized Car Manufacturing – Режим доступа: <https://www.scnsoft.com/blog/iot-in-automotive-industry> (дата обращения: 30.01.2023)
2. Industrial Internet of Things – IIoT Промышленный интернет вещей – Режим доступа: <https://www.tadviser.ru/index.php/IIoT_-_Industrial_Internet_of_Things> (дата обращения: 30.01.2023)
3. Raspberry Pi – Режим доступа: <https://3d-diy.ru/wiki/arduino-platy/obzor-plat-raspberry-pi/> (дата обращения 10.02.2023)
4. The Top 19 Internet of Thing (IoT) Security Solutions – Режим доступа: https://www.firstpoint-mg.com/blog/top-19-iot-security-solutions/ (дата обращения: 09.02.2023)
5. Top Security Techniques to Protect Internet of Things Infrastructure – Режим доступа: <https://www.stealthlabs.com/blog/top-security-techniques-to-protect-internet-of-things-infrastructure/> (дата обращения: 30.01.2023)
6. What is the Internet of Things (IoT)? – Режим доступа: <https://aws.amazon.com/what-is/iot/> (дата обращения: 28.01.2023)
7. What is the Mirai Botnet? – Режим доступа: <https://www.cloudflare.com/en-gb/learning/ddos/glossary/mirai-botnet/> (дата обращения: 11.02.2023)
8. Введение в концепцию «интернета вещей» (IoT) – Режим доступа: <https://nag.ru/material/38920> (дата обращения: 28.01.2023)
9. Интернет вещей и блокчейн: проблемы, преимущества и сферы применения – Режим доступа: <https://forklog.com/internet-veshhej-i-blokchejn-problemy-preimushhestva-i-sfery-primeneniya> (дата обращения: 02.02.2023)
10. Подключение и настройка интернета Wi-Fi на Raspberry Pi – Режим доступа: <https://vpautinu.com/wifi/raspberry-pi> (дата обращения: 10.02.2023)
11. Поиск и взлом уязвимых устройств интернета вещей – Режим доступа:<https://spy-soft.net/hack-vulnerable-iot-devices/#__IoT> (дата обращения: 03.02.2023)
12. Что такое безопасность интернета вещей? – Режим доступа: <https://www.kaspersky.ru/resource-center/preemptive-safety/best-practices-for-iot-security> (дата обращения: 03.02.2023)

**ПРИЛОЖЕНИЯ**

Приложение А. Структура мирового рынка Интернета вещей

Приложение Б. Представление технологического процесса в виде  
uml-диаграммы

Приложение В. Программная составляющая (код) на языке программирования Python

Листинг 1 – Проверка на наличие обновлений на официальном сайте

main\_date = "Wed, 29 Mar 2023 18:54:43 GMT"

def check\_updates\_cve():

global main\_date

update = False

date = feedparser.parse("https://www.cve.org/AllResources/CveServices#cve-json-5").updated

if date != main\_date:

update = True

main\_date = date

if update:

url = "https://github.com/CVEProject/cvelistV5/archive/refs/heads/main.zip"

wget.download(url) # >> cvelistV5-main.zip

Листинг 2 – Создание базы уязвимостей на устройстве

def import\_cve():

with zp("cvelistV5-main.zip") as zf:

zf.extractall("./")

year = dt.now().year

years = [str(year - 1), str(year)] # install db's only for last and current years

for f in os.listdir("./database"):

os.remove(os.path.join("./database", f))

for by\_year in os.listdir("./cvelistV5-main/cves"):

if by\_year in years:

for folders in os.listdir(f"./cvelistV5-main/cves/{by\_year}"):

for file in os.listdir(f"./cvelistV5-main/cves/{by\_year}/{folders}"):

shutil.copy(f"./cvelistV5-main/cves/{by\_year}/{folders}/{file}", "database")

else:

continue

Листинг 3 – сканирование Сети и нахождение устройств

def scan\_net():

ip = socket.gethostbyname(socket.gethostname())

# scans and founds all devices in network

hosts = []

scanner = nmap.PortScanner()

scanner.scan(ip, arguments="-sn")

for host in scanner.all\_hosts():

name = socket.gethostbyname\_ex(socket.gethostname())[0]

address = scanner[host][ "adresses"]["ipv4"]

if "mac" in address:

mac = scanner[host][ "adresses"]["mac"]

hosts.append([name, mac, address]) # hosts of all devices in network

else:

hosts.append([name, "Неизвестно", address])