МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАТАРСТАН

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ЛИЦЕЙ ИННОПОЛИС»

ОТЧЕТ  
О ПРАКТИКО-ОРИЕНТИРОВАННОЙ РАБОТЕ

заключительного этапа Всероссийской олимпиады школьников по технологии  
профиль: «Информационная безопасность»

по теме:  
RegulIoT – умное обеспечение безопасности Интернета Вещей

Выполнила:  
ученица 11 класса ГАОУ «Лицей Иннополис»  
Юрина Виктория Никитична

Научный руководитель:  
Михайлов Михаил Леонидович  
заместитель директора по информатизации

Иннополис 2024**РЕФЕРАТ**

Отчет 39 с., 2 ч., 13 рис., 1 чертеж, 13 источников, 6 прил.

БЕСПРОВОДНЫЕ СЕТИ, ИНТЕРНЕТ ВЕЩЕЙ, ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ, УГРОЗЫ БЕЗОПАСНОСТИ, УСТРОЙСТВО, УЯЗВИМОСТИ, ЭКСПЛУАТАЦИЯ.

Объектом исследования является Интернет вещей – система взаимосвязанных физических объектов (устройств), которые могут собирать, обрабатывать и передавать данные без участия человека.

Цель работы – создание комплекса технологий для обнаружения и устранения выявленных уязвимостей устройств Интернета вещей с применением искусственного интеллекта.

В процессе работы проводились теоретические исследования структуры и отдельных областей применения Интернета вещей. Производился сбор и анализ информации об использовании искусственного интеллекта в Интернете вещей.

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

Степень внедрения – продукт, готовый к внедрению в системы потенциальной аудитории с использованием умеренных ресурсов.

Эффективность продукта определяется достижением всех поставленных задач, а также проведенным тестированием на определенном круге лиц как из сферы информационной безопасности, так и из других сфер, не связанных с ИБ.

**СОДЕРЖАНИЕ**

[**ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ И АББРЕВИАТУРЫ** 2](#_Toc163141779)

[**ВВЕДЕНИЕ** 5](#_Toc163141780)

[**ОСНОВНАЯ ЧАСТЬ ОТЧЕТА** 6](#_Toc163141781)

[1 Теоретическое исследование 6](#_Toc163141782)

[1.1 Архитектура 6](#_Toc163141783)

[1.2 Объем рынка и прогнозы по развитию 7](#_Toc163141784)

[1.3 Возможные и выявленные уязвимости 9](#_Toc163141785)

[1.4 Способы обеспечения безопасности 10](#_Toc163141786)

[1.5 Искусственный интеллект и Интернет вещей 11](#_Toc163141787)

[1.6 Результаты исследования 12](#_Toc163141788)

[2 Разработка технологического процесса 13](#_Toc163141789)

[2.1 Формулировка технического задания 13](#_Toc163141790)

[2.2 Предложения решения выявленной проблемы 14](#_Toc163141791)

[2.3 Концепция продукта и обоснование выбора оптимального решения 15](#_Toc163141792)

[2.4 Аналоги и прототипы 16](#_Toc163141793)

[2.5 Описание технологического процесса 18](#_Toc163141794)

[2.6 Потенциал применения 25](#_Toc163141795)

[2.7 Способы внедрения 28](#_Toc163141796)

[2.8 Экономическая и нормативная оценка реализации и внедрения 29](#_Toc163141797)

[2.9 Тестирование и оценка результатов 31](#_Toc163141798)

[**ЗАКЛЮЧЕНИЕ** 33](#_Toc163141799)

[**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** 36](#_Toc163141800)

[**ПРИЛОЖЕНИЯ** 38](#_Toc163141801)

[Приложение А. Структура мирового рынка Интернета вещей 38](#_Toc163141802)

[Приложение Б. Аналоги проектного решения 39](#_Toc163141803)

[Приложение В. Представление технологического процесса в виде uml-диаграммы 42](#_Toc163141804)

[Приложение Г. Программная составляющая (код) на языке программирования Python 43](#_Toc163141805)

[Приложение Д. Сведения о разработанном комплексе 47](#_Toc163141806)

[Приложение Е. Итоги тестирования продукта 49](#_Toc163141807)

**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" \o "Компьютерная сеть) множества [датчиков](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%82%D1%87%D0%B8%D0%BA" \o "Датчик) 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" \o "Исполнительное устройство), 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" \o "Радиоканал).

*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" \o "Связный список)), 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" \o "Компьютерная сеть), состоящая из некоторого количества [хостов](https://ru.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82" \o "Хост) 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)" \o "Робот (программа)) — 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" \o "Программное обеспечение).

*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.

*Дарквеб* (англ. *dark web*) – часть всемирной паутины (англ. *WWW – World Wide Web*), которая находится в [даркнетах](https://encyclopedia.kaspersky.ru/glossary/darknet/), и доступ к которой можно получить только при помощи специального программного обеспечения (такого как Tor). Дарквеб относится к [глубокой сети](https://encyclopedia.kaspersky.ru/glossary/deep-web/), то есть является частью сети, недоступной для поисковиков.

*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.

*Интернет вещей* (англ. *IoT* – *Internet of Things*) – система взаимосвязанных физических объектов (устройств), которые могут собирать, обрабатывать и передавать данные без участия человека. [8]

*ИИ* (сокр. *искусственный интеллект*; англ. *AI – Artificial Intelligence*) – технология, позволяющая системе, машине или компьютеру выполнять задачи, требующие разумного мышления, то есть имитировать поведение человека для постепенного обучения с использованием полученной информации и решения конкретных вопросов. Позволяет автоматизировать некоторые процессы.

*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" \o "Узел сети) [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" \o "Сегмент сети). 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" \o "Канальный уровень) 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.

*ФСТЭК* (сокр. *Федеральная служба по техническому и экспертному контролю*) – орган защиты государственной тайны, наделенный полномочиями по распоряжению сведениями, составляющими государственную тайну.

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

**ВВЕДЕНИЕ**

Актуальность данной работы обусловлена необходимостью развития устойчивой и безопасной экосистемы, адаптированной под требования современного общества и производства.

Цель работы – создание комплекса технологий для обнаружения и устранения выявленных уязвимостей устройств Интернета вещей с применением искусственного интеллекта.

Задачи:

1. Разобрать архитектуру Интернета вещей;
2. Проанализировать объем рынка и прогнозы по развитию Интернета вещей;
3. Определить существующие угрозы безопасности при использовании Интернета вещей, проанализировать преложенные методы устранения уязвимостей;
4. Выяснить, как стоит использовать искусственный интеллект для анализа и улучшения работы устройства;
5. Определить несколько вариантов создания продукта и выбрать наиболее подходящую технологию;
6. Обучить искусственный интеллект для анализа некоторых задач устройства и для улучшения его работы;
7. Проанализировать потенциал применения результата проекта, предложить способы внедрения продукта;
8. Дать экономическую и нормативную оценку реализации и внедрения продукта, провести тестирование на фокус-группе; подвести итоги проекта.

**ОСНОВНАЯ ЧАСТЬ ОТЧЕТА**

1. Теоретическое исследование
   1. Архитектура

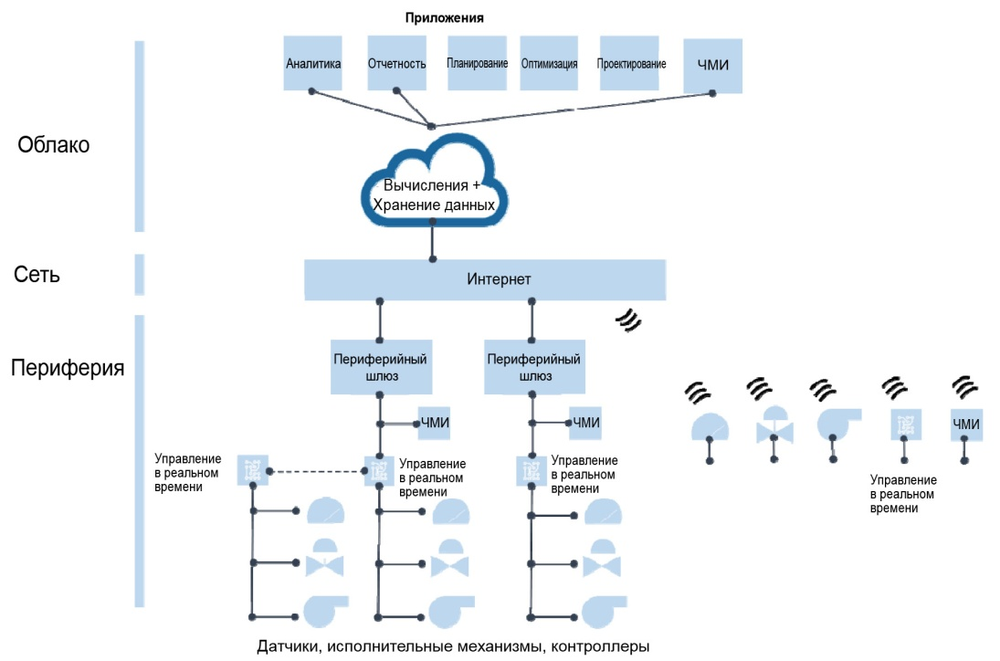
 Архитектура Интернета вещей состоит из нескольких уровней, в которых показано, как разные технологии связаны между собой (рисунок 1).

Рисунок 1 – Архитектура Интернета вещей

Источник, в котором представлена информация об уровнях архитектуры Интернета вещей, представлен по ссылке в списке использованной литературы под номером 9.

* 1. Объем рынка и прогнозы по развитию

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

Согласно статистике от Statista, к 2025 году количество устройств, подключенных к Интернету, превысит 38 миллиардов. [4] Рост IoT-индустрии, предсказанный IDC, приведет к увеличению объемов собираемой информации до 73 зеттабайт к 2025 году. [3]

Согласно последнему отчету IoT Analytics "State of IoT – Spring 2023", количество глобальных подключений к IoT выросло на 18% в 2022 году до 14,3 млрд активных устройств IoT. Также IoT Analytics сообщало, что в 2023 году общее количество подключенных устройств Интернета вещей вырастет еще на 16%, до 16,7 млрд активных устройств. Даже несмотря на то, что в 2023 году рост количества активных устройств Интернета вещей был немного медленней, чем в 2022, IoT Analytics ожидают активного роста данной технологии в течение еще нескольких лет.

Вышеупомянутая аналитическая компания сообщила о трех технологиях подключения, которые займут 80% рынка Интернета вещей в ближайшие годы, а именно Wi-Fi, Bluetooth и Cellular IoT.

Также в своем отчете IoT Analytics отметила несколько компаний, которые вкладывали наибольшее количесвто ресурсов в развитие технологии Интернета вещей:

1. China Mobile переместилась с пятого места в 2012 году на первое место в 2021 году и, как ожидается, будет оставаться в лидерах еще долгие годы;
2. АТ&Т, Verizon и Deutsche Telekom неизменно входили в пятерку лидеров с 2010 по 2022 год и, как ожидается, сохранят свои позиции до 2027 года;
3. China Unicom вошла в пятерку лидеров в 2022 году и, по прогнозам, останется в числе ведущих сетевых операторов и поставщиков до 2027 года.

В рассматриваемом отчете IoT Analytics также отметила то, что стартапы, ориентированные на разработки в сфере Интернета вещей, испытывают трудности с обеспечением финансирования. За последние 12 месяцев объем средств, вложенных в глобальные стартапы Интернета вещей, значительно сократился. В первом квартале 2023 года на развитие Интернета вещей поступили финансирования на общую сумму 840 миллионов долларов, что на 45% меньше, чем в первом квартале 2009 года. [6]

* 1. Возможные и выявленные уязвимости

Согласно исследованию Positive Technologies, в 2022 году было зафиксировано 223 инцидента в промышленных компаниях, вызванных кибератаками, что на 7% больше, чем в предыдущем году. Почти все атаки на организации промышленного сектора (97%) были целевыми (APT). В *дарквебе* количество объявлений о продаже доступа к инфраструктуре промышленных организаций выросло на 40%, и стоимость одного доступа колеблется от $500 до $5 тыс.

Среди атак на промышленные организации 87% направлены на компьютеры, серверы и сетевое оборудование. Злоумышленники в 44% случаев осуществляли атаки на персонал промышленных организаций через вредоносные рассылки по электронной почте (94%) и фишинговые сайты (10%, веб-ресурсы промышленных организаций - 12%).

В 70% успешных атак на промышленные организации злоумышленники использовали вредоносное программное обеспечение. Почти половина кибератак (445) на промышленность включала методы социальной инженерии. Эксплуатация уязвимостей программного обеспечения составила 43% всех атак.

Наиболее распространенными видами вредоносного ПО стали шифровальщики, которые были использованы в двух третях атак с применением вредоносного ПО. Тремя наиболее популярными видами программ-вымогателей в промышленной отрасли в 2022 году стали LookBit, BlackCat (ALPHV) и Conti, все они имеют реализации как для Windows, так и для Linux. [12]

Вредоносные программы типа *ботнетов* встречаются не реже, чем шифровальщики, упомянутые выше. 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 Mēris. *Meris* (с латышского – чума) – ботнет, который стоит за серией DDoS-атак, направленных на тысячи сайтов по всему миру. Первый раз он был обнаружен в конце июня 2021 года QRator в ходе совместных исследований, которые они проводили с Яндексом. Их первоначальные исследования выявили от 30000 до 56000 роботов, но повторный подсчет показал, что их число гораздо выше, на уровне 250000 ботов. Ботнет Meris формируется из зараженных маршрутизаторов и сетевого оборудования, изготовленного латвийской компанией MikroTik. Согласно блогу компании MikroTik, злоумышленники использовали уязвимость в операционной системе маршрутизатора RouterOS, которая позволила злоумышленникам получить неаутентифицированный удаленный доступ для чтения и записи произвольных файлов (CVE-2018-14847). [1]

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*. [11]

Уже установлено, что для нормальной работы системы Интернета вещей требуется единая сеть в предприятии или доме. Это обязательное условие, но в то же время оно представляет дополнительный риск, поскольку неправильная настройка даже одного параметра безопасности на одном из устройств может поставить под угрозу безопасность всей домашней сети.

* 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*. 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]

Намеренный взлом может являться способом 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. [11]

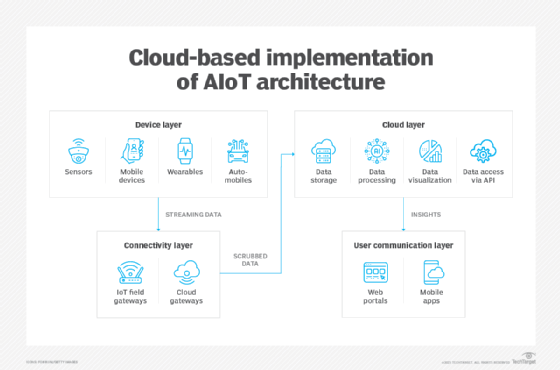
Есть ряд рекомендаций, соблюдая которые можно минимизировать риск взлома устройства: регулярные обновления, смена паролей «по умолчанию» и использование надежных, использование надежного метода шифрования Wi-Fi, контроль устройств (их параметров конфиденциальности и функций) и т.д. [7]

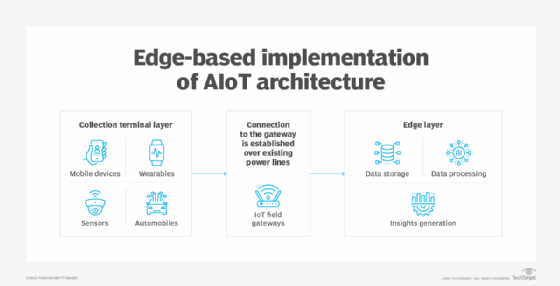
Также применяются инновационные и надежные технологии защиты. Например, комбинация *блокчейна* и Интернета вещей часто рассматривается как один из наиболее перспективных сценариев применения технологии обеспечения безопасности.

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. [10]

* 1. Искусственный интеллект и Интернет вещей

Направление разработки устройств и ПО Интернета вещей с применением искусственного интеллекта выделяют как отдельную категорию – Artificial Intelligence of Things (AIoT). Системы искусственного интеллекта в интернете вещей (AIoT) обычно настраиваются как облачные (cloud-based) (рисунок 3) или «краевые» (edge-based) (рисунок 4) системы. Ознакомится с теоретическим описанием данных систем можно по ссылке в списке использованной литературы под номером 2.





*Рисунок 4 – уровни edge-based AIoT [2]*

*Рисунок 3 – уровни cloud-based AIoT [2]*

* 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.

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.

Рекомендации по использованию устройств Интернета вещей не всегда обеспечивают защиту данных от несанкционированного доступа, так как многие базы данных и инструменты для взлома находятся в публичном доступе, что требует постоянного обновления методов защиты.

Artificial Intelligence of Things (AIoT) – одно из самых актуальных и востребованных направлений разработки решений Интернета вещей. Вскоре мы будем все чаще и чаще встречать искусственный интеллект как главного помощника в обеспечении безопасности «умных» устройств.

# Разработка технологического процесса

## Формулировка технического задания

Перед определением возможных вариантов решения проблемы необходимо обозначить 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 дополнительных средств защиты как применяемой и анализируемой информации, так и самого устройства в целом;
6. Применение ИИ для анализа работы устройства и повышения качества его работы;
7. Соблюдение Федеральных Законов Российской федерации:
   1. 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
   2. 152-ФЗ «О персональных данных»;
   3. 98-ФЗ «О коммерческой тайне»;
   4. 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
8. 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, значительное количество уязвимостей 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. Это обосновано тем, что другие аспекты не могут быть эффективно решены в рамках данного проекта. Например, повышение уровня осведомленности пользователей – обязанность каждой компании, занимающейся производством умных устройств, а также ответственность самого пользователя. Угрозы со стороны злоумышленников и вредоносного программного обеспечения неизбежны – наша задача заключается в обеспечении защиты разработок и оперативном устранении выявленных уязвимостей, а также в информировании пользователей о порядке взаимодействия с устройством и ПО, чтобы это взаимодействие оставалось безопасным.

Предложения решения выявленной проблемы:

1. Реализация намеренной эксплуатации устройств и их проверки на уязвимости;
2. Регулярное автоматическое сканирование сети и 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

Оптимальным решением выбранной проблемы является реализация регулярного автоматического сети и устройств на наличие уязвимостей или вредоносного программного кода. Данное решение считается наиболее оптимальным, так как в остальных предложенных вариантах имеются противоречия.

При реализации намеренной эксплуатации устройств и их проверки на уязвимости всегда существует угроза появления «дыр» в безопасности гаджетов, что может привести к еще большему нарушению конфиденциальности и сохранности данных. Также данный способ занимает много времени, ведь обычный пользователь не сможет до конца разобраться в предложенном решении – придется вызывать специалиста и тратить дополнительные ресурсы. Проектное решение должно быть автономным.

Первоначальное создание абсолютно безопасного устройства невозможно технически: даже если оно будет безопасным, то останутся уязвимости в сети, которые также должны быть найдены и решены.

Разделение одной сети на несколько подсетей противоречит архитектуре Интернета вещей, где устройства находятся в единой сети.

Концепция продукта основывается на устранении уязвимостей, потребностях потенциальных пользователей и стоимости решения. Будет предложено три варианта использования комплекса решений. Потенциальный пользователь сможет выбрать подходящий вариант, основываясь на своих потребностях и бюджете:

1. Использование исключительно ПО, которое представляет собой графическую панель усправления всеми устройствами Интернета вещей в одной сети.

В данном ПО будет реализован инструмент сканирования сети на наличие уязвимостей в устройствах с применением ИИ, а также обновляемая база уязвимостей и руководство пользователя. В данном варианте пользователю приедтся использовать собственное «железо», на котором будет установлено данное ПО (ПК, планшет и т.п.).

1. Использование исключительно устройства, которое имеет возможность подключиться к сети Интернет, в которой находятся проверяемые устройства.

Данное устройство будет использовать ПО, описанное выше. Устройство сможет просканировать сеть и гаджеты на наличие уязвимостей и, если таковы были найдены, предложить решения найденных проблем, опираясь на загруженную базу уязвимостей; следовательно, пользователю не придется применять собственное «железо».

1. Использование комплекса решений, описанных выше.

Данный вариант будет актуален, например, на больших производствах: на малых предприятиях можно будет использовать только ПО, на больших же – автономное устройство.

* 1. Аналоги и прототипы

В ходе анализа рынка продуктов по обеспечению безопасности устройств Интернета вещей было найдено несколько готовых решений. Полученные данные представлены в таблице 2 (Приложение Б). Также в Приложении представлены ссылки на официальные сайты производителей и изображения рассмотренных решений.

К решениям, схожим с RegulIoT, можно отнести такие рассмотренные решения, как Symantec Industrial Control System Protection и SecPoint Penetrator. Они используют схожие технологии анализа и защиты устройств: например, в них также используется искусственный интеллект для анализа сети и нахождения уязвимостей в ней. Но остаются некоторые различия между этими решениями: например, Symantec ICSP USBприменяют преимущественно на больших производствах – использование в малой сети не предусмотрено или не является целесообразным; SecPoint Penetrator имеет не самую удобную реализацию в виде сетевого коммутатора, а панель управления реализована в виде веб-страницы. В свою очередь проектное решение RegulIoT может применяться на производствах разных масштабов и любых сфер, а также имеет удобную реализацию: отдельное устройство, с которым человек взаимодействует только по необходимости, в совокупности с разработанным ПО и интерфейсом, что означает возможность интерактивного взаимодействия при помощи сенсорного экрана.

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 одинаково схожих и качественных технологий.

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.

Проектный продукт так же, как и существующие аналоги будет решать поставленную проблему безопасности Интернета вещей (соответственно, проблемы информационной безопасности в целом) – проблему продолжительного наличия уязвимостей и их поиска, а также будет отвечать поставленной цели – созданию комплекса технологий для обнаружения и устранения выявленных уязвимостей устройств Интернета вещей с применением искусственного интеллекта.

* 1. Описание технологического процесса

Реализация продукта поделена на 2 части: программную и техническую. В программной части описан процесс разработки ПО в виде *standalone-приложения*. В технической части описан процесс настройки и отладки устройста.

Программная часть:

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 CSV, так как его можно наиболее просто и быстро обновлять путем импортирования с официального источника, а также данный формат таблицы наиболее удобно использовать в ходе обучения модели искусственного интеллекта. Целесообразно хранить данные об уязвимостях за последние 2-3 года, так как уязвимости регулярно обновляются, например – устраняются.

1. Концепция ПО и определение функций

Разрабатываемое устройство будет постоянно подключено к локальной сети Интернета вещей. После сканирования сети, при нахождении уязвимостей (согласно базе уязвимостей CVE) устройство будет отправлять уведомление пользователю с предложенным решением устранения уязвимости, если такого было найдено в БД CVE, иначе будет предложено отключение скомпрометированного устройства от сети до появления обновления от разработчика.

Искусственный интеллект будет применен на этапе поиска уязвимостей: анализ должен происходить быстро и без нагрузки на сети, что возможно сделать только с использованием ИИ. Можно использовать «ручные» методы нахождения уязвимостей – через условные операторы и циклы – но это не является целесообразным решением, так как появляется большая нагрузка на устройство (или другое устройство, где развернуто ПО) и сеть. Также ИИ будет собирать данные о работе устройства – время сканирования сети, нахождени уязвимостей, реакции на найденные неполадки – и предоставлять данные в отчете, где будут указаны предложенные решения для повышения качества работы продукта.

В программной составляющей необходимо реализовать следующее:

* 1. Обновление, хранение и использование базы уязвимостей CVE в формате CSV;
  2. Реализация сканирования определенной сети Интернета вещей;
  3. Алгоритм по нахождению ошибок и/или уязвимостей и их обработке;
  4. Реализация уведомлений о выявленных уязвимостях, а также найденных решениях и обновлениях;
  5. Автоматизация пункта 2.3 путем применения искусственного интеллекта;
  6. Представление системы в виде standalone-приложения;
  7. 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, catboost, ipywidgets, pyinstaller.

По итогу определенны следующие функции:

1. check\_updates\_cve() – проверка обновления базы уязвимостей;
2. import\_cve() – выдержка из .csv файла уязвимостей за последние 2 года;
3. nmap\_scan(ip=”127.0.0.1”) – сканирование сети. На вход подается IP-адрес сети, в которой находятся устройства Интернета вещей. На выходе функция сохраняет данные об устройствах (MAC и IP адреса, имя, производитель, версия прошивки) в новом файле формата CSV;
4. ai\_analyze() – проверка устройств на наличие уязвимостей. Если в сохраненной базе уязвимостей было найдено имя устройства или его прошивка, то данные об устройстве (если было найдено решение в CVE, то и описание устранения уязвимости; значение по умолчанию – “Deactivate device”) отправляются в следующую функцию;
5. create\_message(info) – функция получает данные об уязвимом устройстве в виде списка и формирует сообщение пользователю;
6. send\_notification(message) – функция отправляет пользователю уведомление об ошибке.

Написание кода производилось в редакторе Visual Studio Code. Использовалось приложение Qt Designer для разработки интерфейса standalone-приложения (со скриншотом главного меню можно ознакомиться в Приложении Д).

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

При отладке разработанного кода были выявлены трудности с отправкой уведомлений пользователю. Было рассмотрено несколько вариантов отправки уведомлений, но самым простым в реализации оказалось всплывающее окно с текстом ошибки. В дальнейшем планируется отправление уведомлений на почту пользователя и на смартфон.

1. Обеспечение защиты от угроз

Угрозы могут быть реализованы через эксплуатацию уязвимостей. Стоит использовать межсетевой экран, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами (использование iptables), а также *DLP-* и *SIEM-системы*, которые предотвращают несанкционированный доступ к информации и ее утечку.

1. Обучение модели ИИ

Для решения задач, описанных выше, необходим правильный процесс обучения модели, который включает несколько ключевых этапов. Первым этапом является подготовка данных для обучения и тестирования модели. На этом этапе данные из файла с описаниями уязвимостей по CVE в формате CSV и список устройств объединяются и предварительно обрабатываются. Подготовка данных включает в себя удаление ненужных признаков, обработку пропущенных значений, а также преобразование категориальных признаков в числовые. Затем данные разделяются на обучающий и тестовый наборы, чтобы оценить качество работы модели.

На следующем этапе происходит обучение модели. Для этого выбирается подходящий алгоритм машинного обучения и подбираются оптимальные гиперпараметры модели. Затем модель обучается на обучающем наборе данных. В процессе обучения модель постепенно адаптируется к данным, пытаясь минимизировать ошибку предсказания. После завершения обучения модели производится оценка ее качества на тестовом наборе данных. Это позволяет проверить обобщающую способность модели и оценить ее эффективность в решении поставленных задач.

Для анализа уязвимостей в устройствах хорошо подходят алгоритмы градиентного бустинга, такие как CatBoost, XGBoost или LightGBM. Оптимальные гиперпараметры модели могут быть подобраны с помощью методов Grid Search или Random Search, а также методов оптимизации, например, Bayesian Optimization. Кросс-валидация, такая как K-fold Cross-Validation, помогает оценить производительность модели и избежать переобучения.

В проекте использовался алгоритм градиентного бустинга CatBoost. Для программирования на языке программирования Python использовался редактор кода Visual Studio Code и среда разработки Jupyter для визуального контроля за обучением модели.

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. Ссылку на разработанную документацию можно найти в Приложении Д.

Техническая часть:

1. Основа продукта

За основу берется Raspberry Pi 3 model B – одноплатный компьютер.

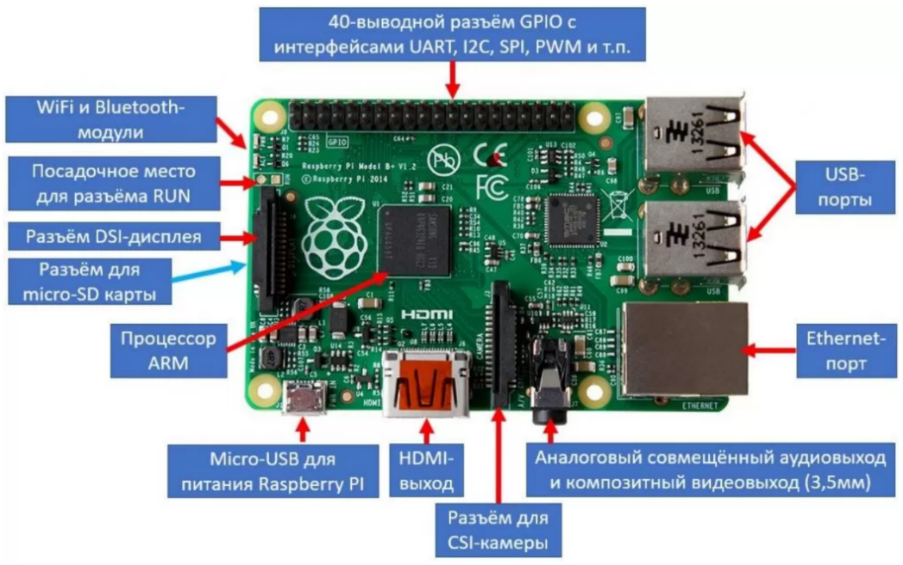


Рисунок 5 – Составные элементы Raspberry Pi [5]

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.

1. Подключение к сети Интернет

Raspberry Pi оснащается модулем Wi-Fi начиная модели 3 Model B. За основу будет взята данная модель, так как отпадает необходимость дополнительных затрат и установки *донгла*, а также данная версия является самой дешевой в розничной закупке на данный момент. 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 и открыть консоль. Затем запустить утилиту вывода информации о USB-устройствах путем ввода lsusb | grep wireless и убедиться, что в выводе есть запись, содержащая строки 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.

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. Внешняя составляющая

При обсуждении внешнего дизайна устройства, особенно его корпуса, следует отметить важность выбора надежного и огнестойкого материала, который обеспечит безопасность пользователя от возможных коротких замыканий и внешних повреждений, таких как вмятины при транспортировке или монтаже. На текущем этапе разработки было принято решение использовать пластик и 3D-печать для создания корпуса, поскольку это один из самых доступных методов. Однако, при наличии дополнительных ресурсов рассматривается возможность применения более прочных материалов, таких как алюминий или металл, для повышения безопасности устройства и создания более эстетичного вида.

Чертежи корпуса устройства можно найти в приложении Д.

1. Установка ПО

Так как ПО для устройства представлено в виде standalone-приложения, был настроен канал передачи данных по SSH, по которому были переданы файлы и само приложение на разработанное устройство при помощи утилиты scp. Настроен автозапуск приложения в полноэкранном режиме.

* 1. Потенциал применения

При оценке потенциала применения результата проекта стоит учитывать несколько факторов.

В настоящее время востребованность Интернета вещей подчеркивается путем анализа областей, где данная технология находит свое применение. Устройства, взаимодействующие в рамках этой системы, активно внедряются в различные сферы: датчики интегрированы в автомобили и используются на производственных площадках, сенсоры тщательно контролируют функциональность медицинских устройств и интегрируются в домашние приборы.

Стоит отметить, что роль искусственного интеллекта в устройствах Интернета вещей придает им не только дополнительные функции, но и повышает уровень анализа данных, принятия решений и автоматизации процессов. Таким образом, в рамках технологического рынка появляется необходимость разработки инновационных подходов к обеспечению безопасности в критических структурах, а также продвижения передовых решений в области искусственного интеллекта в устройствах Интернета вещей.

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 программным решением продукта. 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 ходе проекта, может работать автономно (без участия человека), оно будет достаточно удобным в использовании людьми, неспециализированных в ИТ-сфере. Выполнена визуализация системы и процесса выполнения некоторых этапов (действий), что также повыщает удобство применения, так как человек доверяет больше продуктам, которые имеют визуальное и понятное представление. Этот факт является еще одним преимуществом, выделяющим разработанный продукт RegulIoT на фоне конкурентов: например, в сравнении с SecPoint Penetrator, который представлен в виде сетевого коммутатора с необходимостью дополнительной, умеренно сложной настройкой ПО, легко установить и настроить, так как ПО уже предустановленно на устройстве.

Можно предположить, что разработанный продукт сможет заместить импортные решения, обеспечивая дальнейшую безопасность при использовании устройств Интернета вещей на производстве и в других различных сферах на территории Российской Федерации и стран СНГ. Данное преимущество позволит оставить современные технологии в стране и продолжить их развитие с малыми потерями.

Одним из дополнительных преимуществ продукта является снижение вероятности утраты кадров. Однозначно можно сказать, что при разработке и внедрении продукта на широкий рынок потребуется высококвалифицированная команда специалистов. Этот процесс также исключит утрату текущих кадров, поскольку Интернет вещей будет сохранять свою актуальность, продолжая развиваться. Таким образом, профессионалы в области Интернета вещей, разработки программного обеспечения, искусственного интеллекта, машинного обучения и аналитики сохранят возможности для трудоустройства, а также появятся новые рабочие места.

* 1. Способы внедрения

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

RegulIoT может быть 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 и дальнейшее решение проблемы.

Продукт может быть 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 проблем.

Говоря о применении в медицине, можно предположить, что устройство сможет контролировать, например, автоматизированный процесс подачи лекарств и контроль устройств, которые используются во время наблюдения за пациентом или реабилитации больного.

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 беспилотных автомобилей.

Самым неординарным способом внедрения является сбор статистики. Проектное решение может быть реализовано не только для своих основных задач, но и в целях сбора статистических данных для создания новых решений по повышению безопасности Интернета вещей.

* 1. Экономическая и нормативная оценка реализации и внедрения

Разработка трех различных вариантов внедрения продукта была проведена ради более гибкого внедрения продукта в производство: покупатель может сам выбрать комплектацию и количество необходимых продуктов, что повышает удобство дальнейшего использования и сокращает стоимость. В затраты на реализацию и внедрение RegulIoT включаются стоимость технических составляющих устройства и оплата труда сотрудников. Была проведена оценка трех вариантов внедрения RegulIoT – ПО, автономное устройство, использование комплекса ПО и устройств.

Таблица 1 – смета стоимости разработки продукта (в условиях розничной закупки и малой команды); ПО

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование траты | Единица измерения | Количество | Цена, рубли | Сумма, рубли |
| 1 | Зарплата junior-разработчика (Python) | рубли | 1 | 50.000 | 50.000 |
| 2 | Специалист по информационной безопасности | рубли | 1 | 70.000 | 70.000 |
| **Итого:** | | | | | 120.000 |

Рассчитывается, что на рынке Интернета вещей RegulIoT в виде исключительно ПО будет более востребован, чем устройство или комплекс решений, поэтому стоимость внедрения для покупателей сокращается до 10.000 рублей.

Таблица 2 – смета стоимости разработки продукта (в условиях розничной закупки и малой команды); в комплексе

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование траты | Единица измерения | Количество | Цена, рубли | Сумма, рубли |
| 1 | Raspberry Pi 3 model B | шт | 1 | 15.399 | 15.399 |
| 2 | Блок питания | шт | 1 | 1.550 | 1.550 |
| 3 | microSD карта 8 ГБ | шт | 1 | 550 | 550 |
| 4 | Сенсорный дисплей 7” | шт | 1 | 4.527 | 4.527 |
| 5 | Зарплата junior-разработчика (Python) | рубли | 1 | 50.000 | 50.000 |
| 6 | Специалист по информационной безопасности | рубли | 1 | 70.000 | 70.000 |
| **Итого:** | | | | | 142.026 |

Зарплата сотрудников указана в месяц (по данным <https://hh.ru>); после вычисления часов человческой работы в стоимость продукта будет включаться меньшая оплата труда. Рассчитывается, что материалы будут закупаться по оптовой цене. При учете двух факторов, описанных выше, стоимость внедрения для покупателей будет составлять 70.00 рублей.

Смета стоимости разработки продукта в комплексе будет рассчитываться после обсуждения заказа с покупателем. В зависимости от количества предоставляемых продуктов цена комплекса может начинаться от 80.000 рублей (учитывается оптовая закупка материалов и оплата труда после вычисления потраченных часов).

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 составлен план дальнейшего развития продукта.

* 1. Тестирование и оценка результатов

Было проведено планирование функционального тестирования продукта. В качестве критериев можно выделить такие пункты, как:

* Степень удовлетворенности потенциальных пользователей самостоятельным подключением и саомстоятельной настройкой устройства (где 1 – очень проблематично, а 10 – очень просто);
* Степень удовлетворенности потенциальных пользователей сканированием сети и нахождением устройств в ней (где 1 – все устройства были не найдены, а 10 – найдены все устройства)
* Степень удовлетворенности потенциальных пользователей взаимодействия с искусственным интеллектом (где 1 – ИИ абсолютно не помог в решении задачи анализа сети и улучшения работы устройства, а 10 – ИИ выполнил все поставленные задачи);
* Степень удовлетворенности потенциальных пользователей реакцией устройства на найденную уязвимость (где 1 – устройство повело себя абсолютно не так, как ожидалось, а 10 – устройство смогло корректно сообщить пользователю об уязвимости).

Было проведено планирование пользовательского тестирования продукта. Полная фокус-группа состоит из нескольких групп пользователей:

* Группа 1: специалисты информационной безопасности, имеющие опыт работы с уязвимостями Интернета вещей и с искусственным интеллектом;
* Группа 2: специалисты по машинному обучению, которые смогут оценить степень внедрения искусственного интеллекта в разработанном продукте;
* Группа 3: пользователи, имеющие опыт работы с устройствами умного дома, но не имеющие опыта работы в сферах ИБ и ИИ.

Стоит отметить, что при следующих тестированиях продукта планируется увеличение фокус-группы, пригласив специалистов в сфере промышленного Интернета вещей.

Была проведена оценка результатов тестирования продукта; подведенные итоги представлены в графиках (Приложение Е). Согласно результатам можно сделать вывод, что устройство снижает вероятность реализации существенных угроз в локальной сети Интернета вещей. Тестирование было проведено на 5-ти устройствах системы умного дома: умной станции, пылесосе, чайнике, весах, домофоне.

Для эксперимента по нахождению уязвимости была вручную понижена версия платформы Home Assistant, к которой был подключен умный домофон. До версии 2023.01.1 в данной платформе находилась уязвимость CVE-2023-27482, позволяющая обойти аутентификацию и получить полный доступ к привилегированному API [Supervisor](https://github.com/home-assistant/supervisor), через который можно менять настройки, устанавливать/обновлять ПО, управлять дополнениями и резервными копиями.

Профильные специалисты отметили, что уровень обучения ИИ – на среднем уровне. Это является существенным недостатком продукта, который необходимо устранить в дальнейшей разработке. Определена степень внедрения RegulIoT – продукт готов к внедрению в системы потенциальной аудитории с использованием умеренных ресурсов (с большими временными затратами на более глубокое обучение ИИ).

**ЗАКЛЮЧЕНИЕ**

В результате проведенного теоретического исследования можно сделать вывод, что Интернет вещей представляет собой новую и стремительно развивающуюся технологию. На текущем этапе особое внимание следует уделять обеспечению ее достаточной безопасности, учитывая ее влияние на различные отрасли промышленности и рынка. В ходе работы были выявлены ключевые аспекты Интернета вещей, такие как структура, области применения, существующие уязвимости, и методы борьбы с угрозами безопасности. При формулировке технического задания в процессе исследования были выделены плюсы и минусы нескольких подходов к решению проблемы, учитывая целесообразность их внедрения, нагрузку на сеть и возможные проблемы.

Разработанный в результате практико-ориентированной работы продукт RegulIoT готов к внедрению в системы потенциальной аудитории устройством с использованием умеренных ресурсов. Определено, что трудностей с тиражированием и масштабируемостью продукта возникнуть не должно: увеличение производства и затраты на данный процесс являются прямой задачей при развитии продуктов подобного рода. Были определены несколько решений по развитию и внедрению проектного продукта.

Спроектированный продукт имеет ряд свойств, которые уступают по глубине разработки (в сравнении с другими решениями в области разработки безопасного Интернета вещей). Связано это с собственной недостаточной наработкой в создании данных технологий, в то время как компании, специализирующиеся на разработке устройств и ПО для Интернета вещей, уже несколько лет предоставляют готовые решения и обеспечивают безопасностб данной технологии. Размышляя над возможными улучшениями системы, можно упомянуть такие предложения по развитию, как создание отдельной операционной системы для устройства взамен standalone-приложения и более глубокое обучение искусственного интеллекта на реальных промышленных кейсах. Планируется разработка веб-сайта продукта с подробной информацией о нем – данное введение поможет повысить узнаваемость продукта и привлечь инвесторов.

Поставленные задачи были выполнены в полной мере. Цель работы – создание комплекса технологий для обнаружения и устранения выявленных уязвимостей устройств Интернета вещей с применением искусственного интеллекта – выполнена.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. A Brief History of the Meris Botnet – <https://blog.cloudflare.com/meris-botnet> (дата обращения: 16.02.2024)
2. Artificial intelligence of things (AIoT) – <https://www.techtarget.com/iotagenda/definition/Artificial-Intelligence-of-Things-AIoT>
3. Don’t Let Storage Be an Afterthought in Designing for IoT, the Metaverse, and Automotive – <https://embeddedcomputing.com/technology/storage/dont-let-storage-be-an-afterthought-in-designing-for-iot-the-metaverse-and-automotive> (дата обращения: 18.02.2024)
4. Internet of Things: Key stats for 2022 – <https://techinformed.com/internet-of-things-key-stats-for-2022/> (дата обращения: 18.02.2024)
5. Raspberry Pi – Режим доступа: <https://3d-diy.ru/wiki/arduino-platy/obzor-plat-raspberry-pi/> (дата обращения 10.02.2024)
6. State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally – <https://iot-analytics.com/number-connected-iot-devices/#:~:text=The%20latest%20IoT%20Analytics%20%E2%80%9CState,to%2016.7%20billion%20active%20endpoints> (дата обращения: 16.02.2024)
7. 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: 30.01.2024)
8. What is the Internet of Things (IoT)? – Режим доступа: <https://aws.amazon.com/what-is/iot/> (дата обращения: 28.01.2024)
9. Введение в концепцию «интернета вещей» (IoT) – Режим доступа: <https://nag.ru/material/38920> (дата обращения: 28.01.2024)
10. 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: 02.02.2024)
11. Поиск и взлом уязвимых устройств интернета вещей – Режим доступа:<https://spy-soft.net/hack-vulnerable-iot-devices/#__IoT> (дата обращения: 03.02.2024)
12. Россия даст 400 млн руб. на безопасность промышленного интернета вещей – <https://russianelectronics.ru/2023-03-28-interneta-veshhej/> (дата обращения: 17.02.2024)
13. Что такое безопасность интернета вещей? – Режим доступа: <https://www.kaspersky.ru/resource-center/preemptive-safety/best-practices-for-iot-security> (дата обращения: 03.02.2024)

**ПРИЛОЖЕНИЯ**

Приложение А. Структура мирового рынка Интернета вещей

*Рисунок 6 – Структура мирового рынка* Интернета вещей

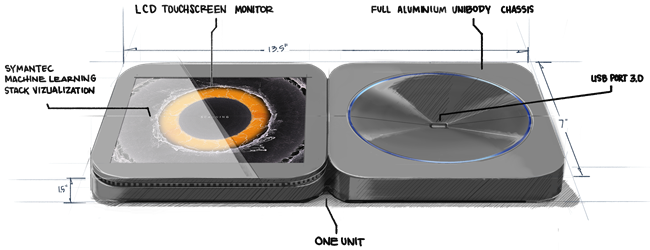
Приложение Б. Аналоги проектного решения

Таблица 3 – Аналоги проектного решения

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Название продукта | | Параметры сравнения | | | | | | |
| Вид решения (ПО или физическое устройство) | | | Универсальность решения (сферы применения) | | Стоимость | Страна-производитель |
| SecPoint Penetrator | | ПО с применением ИИ + сетевой коммутатор | | | Промышленный Интернет вещей (IIoT), умный дом (в некоторых случаях) | | $219 или €199 или ₽21.900 | Дания |
| **Kaspersky IoT Secure Gateway (KISG)** | | ПО + специальная аппаратная платформа (Siemens SIMATIC IOT2040) | | | IIoT, умный город, транспорт и навигация | | По запросу | Россия |
| Symantec Industrial Control System Protection (Symantec ICSP USB) | | Сканирующая станция в автономном алюминиевом корпусе с сенсорным экраном | | | IIoT | | $2.200 или ₽220.000 | США |
| БДУ ФСТЭК | | База данных уязвимостей | | IIoT | | | В открытом доступе | Россия |
| Продолжение таблицы 3 | | | | | | | | |
| Название продукта | Параметры сравнения | | | | | | | |
| Вид решения (ПО или физическое устройство) | | Универсальность решения (сферы применения) | | | Стоимость | | Страна-производитель |
| RegulIoT | ПО с применением ИИ + небольшое устройство с сенсорным экраном | | IIoT, умный дом, здравоохранение, беспилотные автомобили, транспорт | | | от ₽10.000 | | Россия |

Данные о продуктах были взяты из официальных источников:

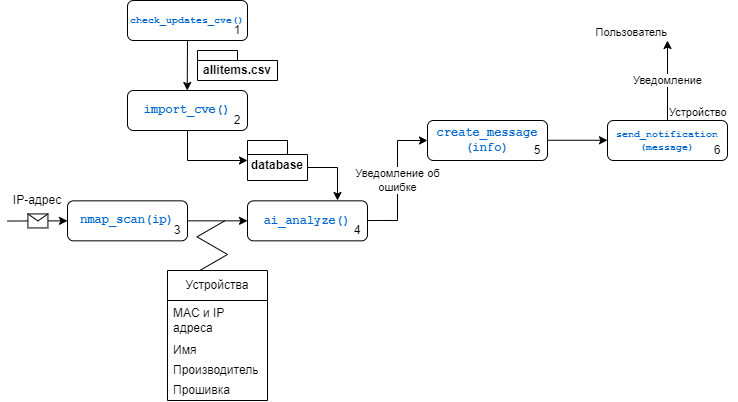
1. SecPoint Penetrator. Режим доступа: <https://www.secpoint.com/penetrator.html> (дата обращения 17.02.2024)
2. **Kaspersky IoT Secure Gateway (KISG). Режим доступа:** <https://os.kaspersky.com/solutions/kaspersky-iot-infrastructure-security/> (дата обращения: 17.02.2024)
3. Symantec Industrial Control System Protection (Symantec ICSP USB). Режим доступа: <https://docs.broadcom.com/doc/internet-of-things-protecting-against-industrial-cyber-attacks-en>, страница 4 (дата обращения: 17.02.2024)
4. ФСТЭК. Режим доступа: <https://bdu.fstec.ru/threat> (дата обращения: 17.02.2024)



*Рисунок 9 – Symantec Industrial Control System Protection (Symantec ICSP USB) и его физические характеристики*

*Рисунок 8 –* ***Kaspersky IoT Secure Gateway (KISG) и его физические характеристики***

*Рисунок 7 – SecPoint Penetrator*

Приложение В. Представление технологического процесса в виде  
uml-диаграммы

*Рисунок 10 – Представление технологического процесса в виде  
uml-диаграммы*

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

Листинг 1 – Проверка на наличие обновлений на официальном сайте CVE

main\_date = "Wed, 03 Apr 2024 18:55:44 GMT"

def check\_updates\_cve():

global main\_date

update = False

date = feedparser.parse("https://cve.mitre.org/data/downloads/index.html").updated

if date != main\_date:

update = True

main\_date = date

if update:

url = "<https://cve.mitre.org/data/downloads/allitems.csv>"

wget.download(url) # >> allitems.csv

Листинг 2 – Создание и обновление базы уязвимостей на устройстве

import datetime as dt

import csv

def import\_cve():

year = dt.now().year

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

with open(“allitems.csv”, “r”, newline=””, encoding=”utf-8”) as csvfile, \

open(“database.csv”, “w”, newline=””, encoding=”utf-8”) as newcsvfile:

# Создаем объекты для чтения и записи CSV

reader = csv.reader(csvfile)  
 writer = csv.writer(newcsvfile)

# Записываем заголовок в новый файл

writer.writerow([“CVE”, “Status”, “Description”, “References”, “Comments”, “Votes”, “Phase”])

# Пропускаем заголовок в исходном файле

next(reader)

# Читаем каждую запись в исходном файле

for row in reader:

# Проверяем, содержит ли запись дату в формате года

if len(row) > 1 and row[1].startswith("Modified"):

# Извлекаем год из строки Modified

year = row[1].split("(")[1][:4]

# Фильтруем записи за последние 2 года

if year in years:

# Записываем запись в новый файл

writer.writerow(row[:7])

Листинг 3 – сканирование сети и нахождение устройств

import socket

import nmap

def nmap\_scan(ip=”127.0.0.1”):

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])

Листинг 4 – анализ подключенных устройств и поиск по сохраненной БД

Листинг 5 – отправка пользователю уведомлений о найденных уязвимостях

import sys

from PyQt5.QtWidgets import QApplication, QWidget, QVBoxLayout, QLabel, QPushButton, QMessageBox

class ErrorMessageBox(QWidget):

def \_\_init\_\_(self, error\_text):

super().\_\_init\_\_()

self.error\_text = error\_text

self.initUI()

def initUI(self):

layout = QVBoxLayout()

label = QLabel("Произошла ошибка:")

layout.addWidget(label)

error\_label = QLabel(self.error\_text)

layout.addWidget(error\_label)

detail\_button = QPushButton("Подробнее")

detail\_button.clicked.connect(self.showDetail)

layout.addWidget(detail\_button)

close\_button = QPushButton("Закрыть")

close\_button.clicked.connect(self.close)

layout.addWidget(close\_button)

self.setLayout(layout)

self.setWindowTitle("Ошибка")

def showDetail(self):

QMessageBox.information(self, "Подробнее", self.error\_text)

def send\_notification(message):

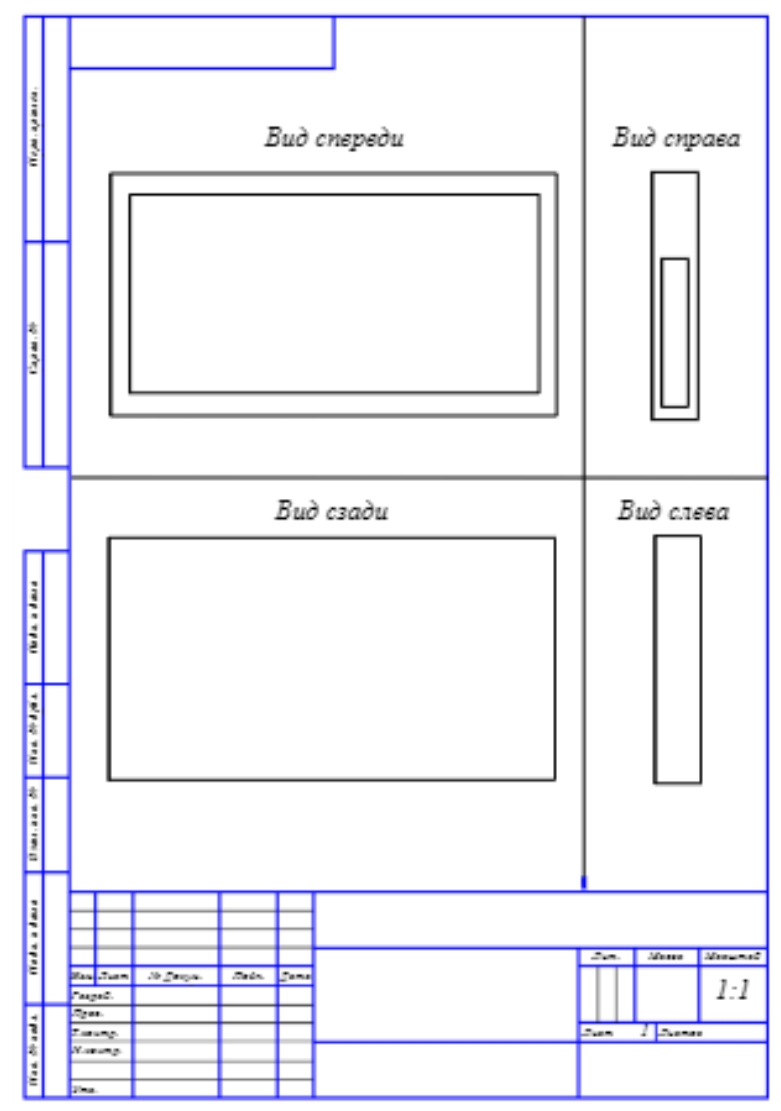
error\_text = create\_message(info)

window = ErrorMessageBox(error\_text)

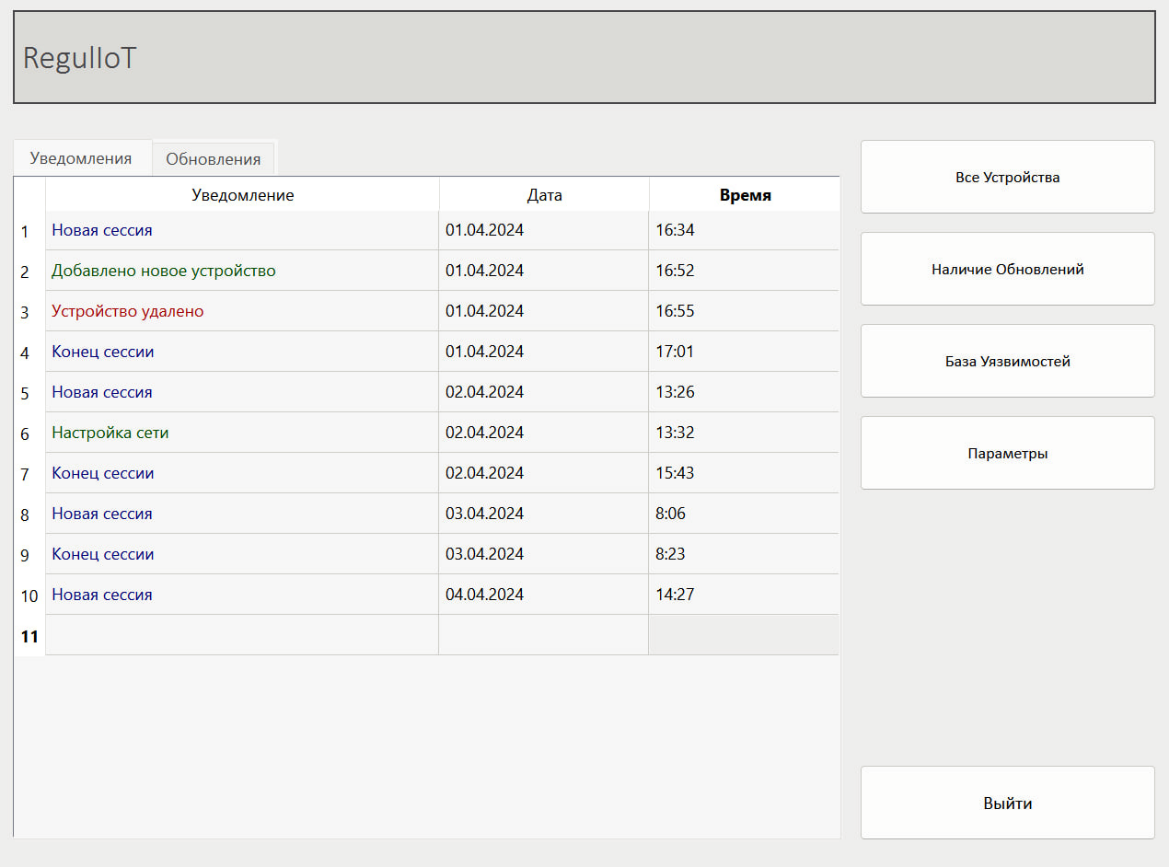
window.setGeometry(500, 300, 400, 200)

window.show()

sys.exit(app.exec\_())

Приложение Д. Сведения о разработанном комплексе

Чертеж 1 – корпус устройства

Ссылка на документацию и материалы, используемые в разработке продукта: <https://github.com/shersh-is/RegulIoT>.

*Рисунок 12 – лэйбл RegulIoT*

*Рисунок 11 – Главное меню*

Приложение Е. Итоги тестирования продукта

*Рисунок 13 – Оценка положительного эффекта от использования продукта*