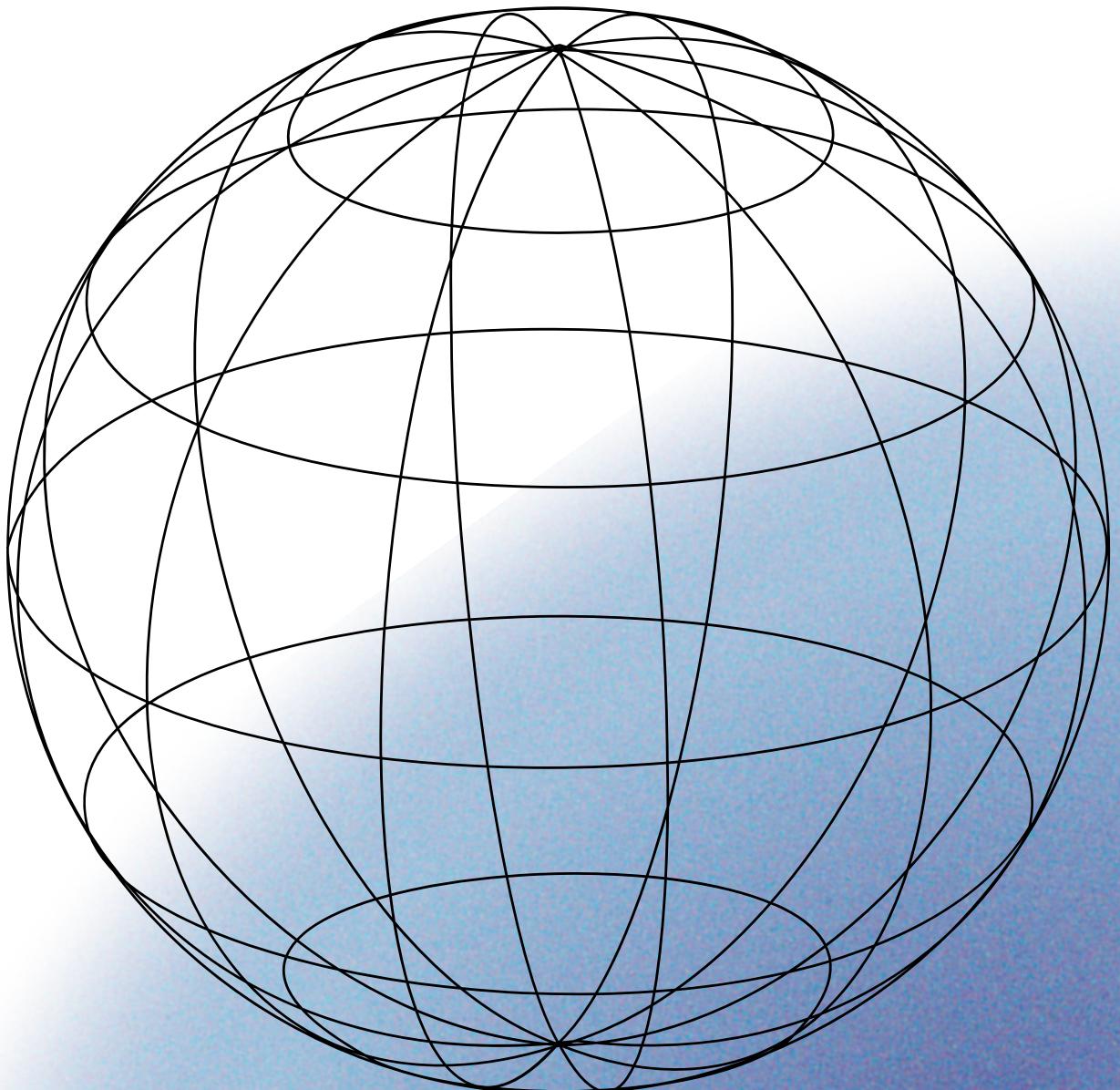


Уязвимости и способы обеспечения безопасности устройств Интернета вещей

Актуальность

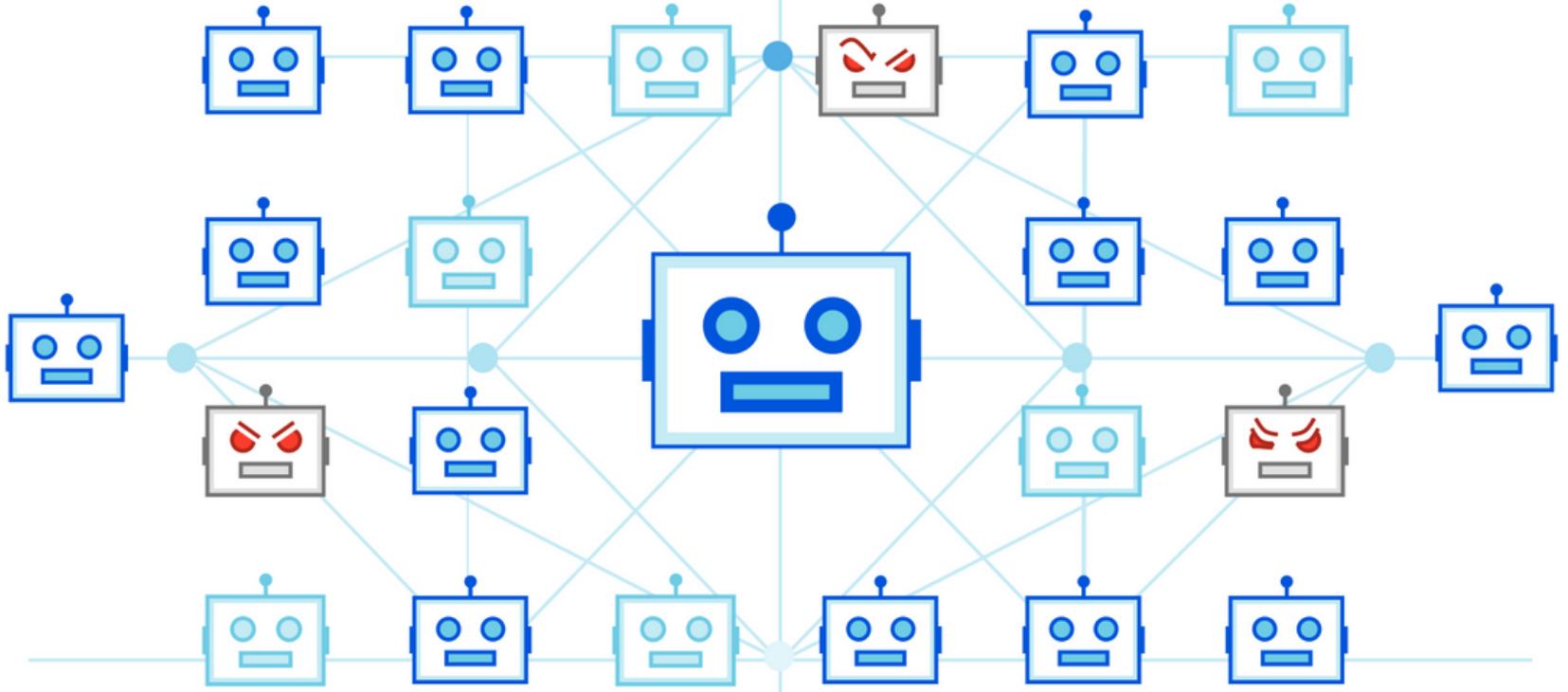
- 01 Большое количество областей применения
- 02 Наличие проблем, связанных с обеспечением безопасности и конфиденциальности
- 03 Технологии слишком важны, чтобы рисковать ими в случае взлома и других угроз





Why does the Mirai malware remain dangerous?

The Mirai is mutating.



Проблема —
продолжительное нахождение уязвимостей в
устройствах Интернета вещей, потенциальных для
эксплуатации

Задачи

- 01 Провести исследования по объему рынка Интернета вещей и существующих угроз
- 02 Определить нескольких вариантов создания продукта и реализация наилучшего
- 03 Проанализировать и оценить результаты проекта

Цель —

создание устройства с технологией обнаружения и устранения выявленных уязвимостей устройств Интернета вещей

Объем рынка и прогнозы по развитию



IoT Analytics:

К концу 2021 года по всему миру насчитывалось 12,2 млрд находящихся в эксплуатации устройств Интернета вещей, что на 8% больше, чем в 2020.

State of IoT:

К 2025-му, когда ослабнут ограничения на поставку комплектующих, произойдет дальнейшее ускорение роста, до 27 млрд подключенных IoT-устройств.

Выявленные уязвимости

- 01 Отсутствие тестирования и качественной разработки
- 02 Возможность создания и внедрения вредоносных программ
- 03 Сохранение доступа у третьих лиц к устройствам и сети
- 04 Несоблюдение рекомендаций по обеспечению безопасности
- 05 Единая сеть

Предлагаемые решения

Предэксплуатация

Ограничение доступа
третьим лицам

Инновационные
технологии защиты

Соблюдение рекомендаций:
регулярные обновления,
смена паролей,
использование надежного
метода шифрования Wi-Fi,
контроль устройств

Техническое задание

Концепция —

устройство с возможностью подключения к сети Интернет анализирует устройства, находит в них уязвимости и предлагает решения найденных проблем, опираясь на базу уязвимостей

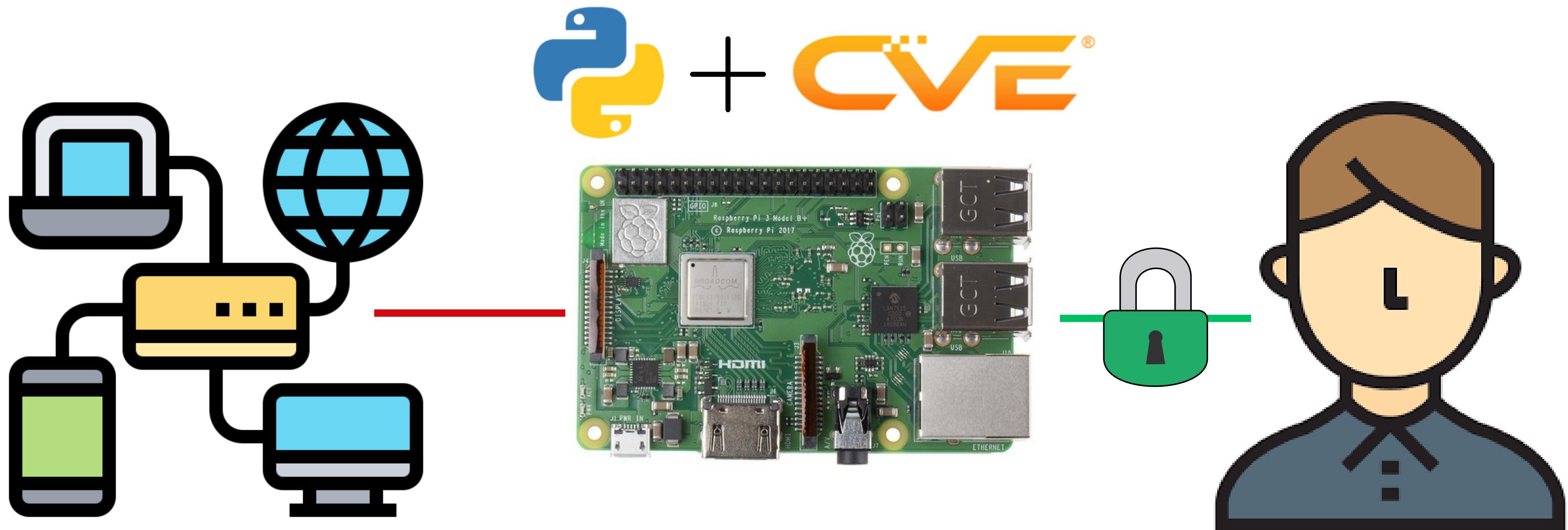
Требования к решению

- 01 Соответствие современным тенденциям
- 02 Возможность внедрения в производство и рынок
- 03 Соблюдение Федеральных законов
- 04 Наличие документации и руководства по использованию

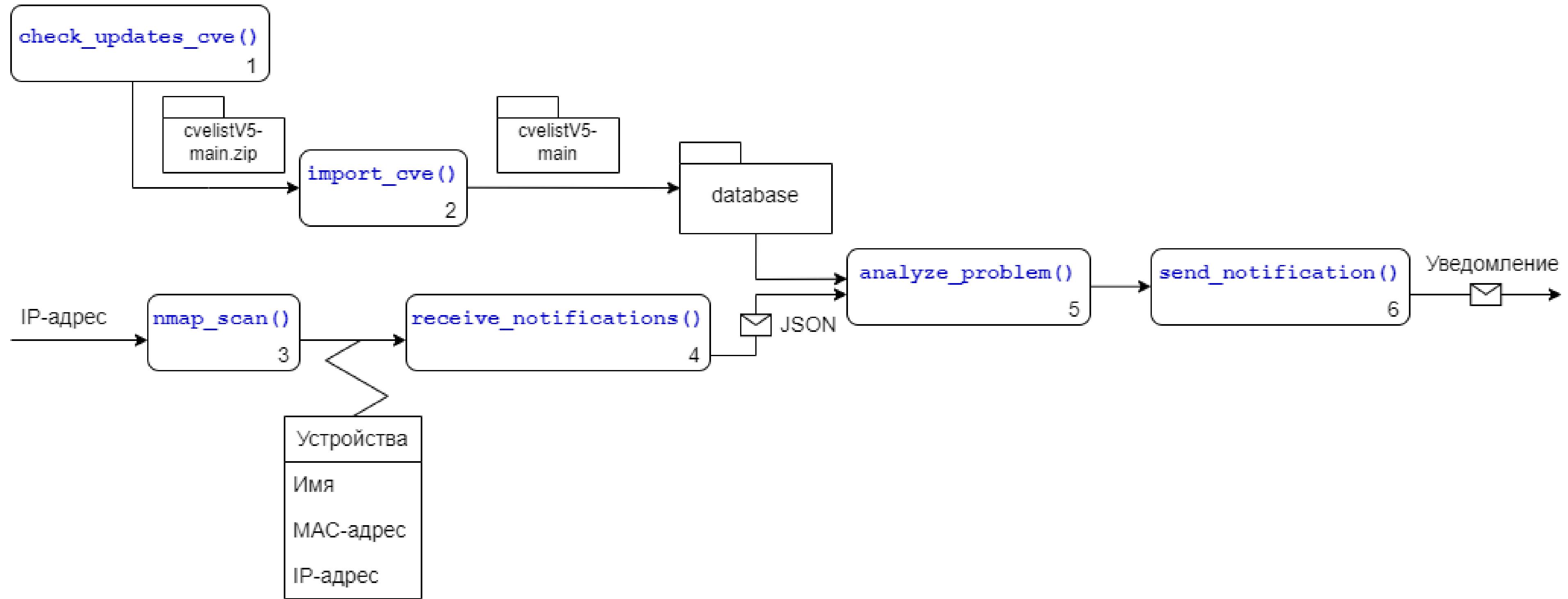
Аналоги и прототипы

FirstPoint	Защита сети	Программное решение	Работа исключительно с сетью	Великобритания
NanoLock	Блокировка вредоносных программ	Программное решение	Универсальное решение	Израиль
Bastille	Устранения радиочастотной угрозы	Набор сенсоров	Работа исключительно с сетью	США
ФСТЭК	Ресурс об уязвимостях АСУ ТП и промышленного ИВ	База данных об уязвимостях	Работа в одной области	Россия
Проектное решение – IoT SecurityPoint	Защита сети и устройств	Автономное устройство с БД об уязвимостях	Универсальное решение	Россия

Техническая составляющая



Программная составляющая



Потенциал применения

Обеспечение защиты Интернета вещей

Целевая аудитория
разработчики и иные
профессионалы

Новый продукт

Импортозамещение
Сохранение и увеличение
количества рабочих мест

Внедрение в производство, умные
дома, автомобили, здравоохранение;
аналитика данных

Современные представления

Целостность
Автономность
Производительность
Удобство в использовании

Экономическая и нормативная оценка

Raspberry Pi 3 model B	11.799 ₽
Блок питания	1499 ₽
microSD карта	399 ₽
Сенсорный дисплей	7599 ₽

	Оплата сети	1000 ₽
	Зарплата Junior Python разработчика	≥50.000 ₽

149-ФЗ «Об информации, информационных технологиях и о защите информации»
152-ФЗ «О персональных данных»
187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Итого: 72.296 ₽

Стоимость внедрения
решения для покупателя:
100.000 ₽

Прибыль ≥60.000 ₽

Демонстрация

Спасибо за внимание!
