ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

*Московский институт электроники и математики им. А.Н.Тихонова*

**Домашнее задание по теме 35. Защита компьютерных сетей и систем**

По направлению 10.04.01 – «Информационная безопасность»

Проверил:

преп. Антон Носков

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Выполнил:

Новиков В. С. МКБ 241

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2025

Часть 1. Диаграмма коммуникационного уровня

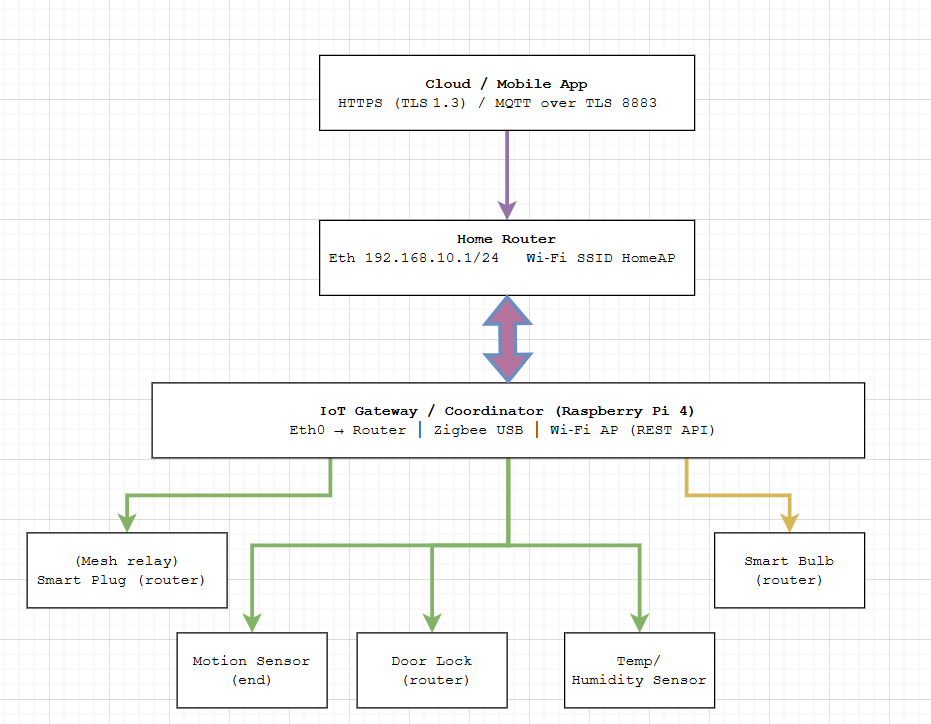
### Шаг 1. Выбор протокола для сети датчиков

Выбранный протокол: Zigbee 3.0 (IEEE 802.15.4)

Почему выбран Zigbee 3.0:

* Низкое энергопотребление — автономная работа датчиков до 10 лет.
* Топология mesh: каждое стационарное устройство‑маршрутизатор (лампа, розетка, замок) ретранслирует кадры, расширяя охват до 60‑100 м внутри помещения.
* Встроенная защита — AES‑128‑CCM, аутентификация кадров, защищённое OTA‑обновление, устранён небезопасный Touch‑Link.
* Распространённость и богатая экосистема чипов/библиотек; поддерживается в Cisco Packet Tracer 8.1.1.

### Шаг 2. Схема сети (текстовое представление)



Цвета соединений:

* Зелёный — Zigbee 3.0 (IEEE 802.15.4)
* Синий — Ethernet 802.3
* Оранжевый — Wi‑Fi 802.11ac
* Фиолетовый — TLS (HTTPS/MQTT)

Как устройства вне зоны действия шлюза обмениваются данными?

Благодаря mesh‑маршрутизации: любые Zigbee‑устройства с питанием от сети автоматически ретранслируют пакеты.

Дополнительные протоколы в сети:

|  |  |  |
| --- | --- | --- |
| Слой | Протокол | Назначение |
| Канальный | Ethernet 802.3, Wi‑Fi 802.11ac | Связь шлюза с роутером и мобильными клиентами |
| Транспортный | TCP (443, 8883), UDP (123) | HTTPS/MQTT‑TLS, NTP |
| Прикладной | MQTT 3.1.1, REST API (HTTPS/JSON) | Телеметрия и команды |
| Служебный | DHCP, DNS‑over‑TLS | Адресация, имена |

# Часть 2. Инвентарь ресурсов поверхности атаки

|  |  |  |
| --- | --- | --- |
| Сеть/устройство | Протокол(ы) | Связан с |
| Zigbee PAN 0x1A2B | IEEE 802.15.4, Zigbee 3.0, AES‑128 | ↔ IoT‑Gateway, ↔ Zigbee‑routers, ↔ end‑devices |
| IoT‑Gateway (Raspberry Pi 4) | Zigbee 3.0, Ethernet 802.3, Wi‑Fi AP 802.11ac, TCP/IP, MQTT‑TLS, HTTPS | ↔ Zigbee PAN, ↔ Home Router, ↔ Cloud |
| Домашний маршрутизатор | Ethernet, Wi‑Fi, IPv4 NAT, DHCP, DNS | ↔ Gateway, ↔ смартфон, планшет, ПК, ↔ ISP |
| Wi‑Fi LAN SSID HomeAP | 802.11ac WPA2‑PSK | ↔ Router, ↔ Gateway (REST), ↔ мобильные клиенты |
| Смартфон (Android) | Wi‑Fi, HTTPS, MQTT‑over‑WSS | ↔ Home Router, ↔ Cloud |
| Облачный брокер (AWS IoT Core) | MQTT TLS, HTTPS | ↔ IoT‑Gateway, ↔ Mobile App |
| OTA‑Update Server | HTTPS TLS 1.3 | ↔ Gateway, ↔ Zigbee OTA |

# Часть 3. POTENTIAL THREATS (STRIDE)

|  |  |  |
| --- | --- | --- |
| Тип угрозы | Сеть/устройство | Возможная угроза (OWASP IoT‑ID) |
| Spoofing | Zigbee PAN | Поддельное Zigbee‑устройство проходит в сеть через известный Link‑Key (I1 Insecure Network Services) |
|  | Wi‑Fi LAN | Evil‑Twin Wi‑Fi крадёт пароли приложения (I2 Weak Passwords) |
| Tampering | IoT‑Gateway | OTA‑апдейт без подписи → внедрение модифицированной прошивки (I5 No Secure Updates) |
|  | Zigbee‑Bulb | Exploit Touchlink‑вектора → изменение состояния ночью |
| Repudiation | Cloud API | Отсутствует аудит команд → пользователь отрицает «unlock» (I9 Insufficient Logging) |
| Information Disclosure | Zigbee PAN | Радиоперехват beacon‑кадров раскрывает PAN‑ID (I6 No Encryption in Transit) |
|  | Home Router | DNS‑сниффинг раскрывает домены облака |
| Denial of Service | Zigbee PAN | 2.4 GHz Jammer → отказ сети (I11 Lack of Physical Hardening) |
|  | IoT‑Gateway | TCP‑SYN flood → переполнение NAT таблицы |
| Elevation of Privilege | IoT‑Gateway | CVE‑2025‑12345 в zigbee2mqtt → root‑shell (I4 Insecure Components) |
|  | Smartphone App | Подмена refresh‑token → админ‑доступ к облаку |

### Рекомендации по снижению рисков

1. Отключить глобальный мастер‑ключ “ZigbeeAlliance09”; включить Trust‑Center Link‑Key.
2. Перевести Wi‑Fi на WPA3‑SAE, отключить WPS.
3. Использовать TLS 1.3 + mutual certs для MQTT, закрыть port‑forwarding.
4. Включить аудит‑логи (NIST SP 800‑92) на шлюзе, экспорт в syslog‑сервер.
5. Задействовать безопасную загрузку (U‑Boot + TPM 2.0) на Raspberry Pi.