SPIIRAS

Управление инцидентами и противодействие целевым кибер-физическим атакам в распределенных крупномасштабных критически важных системах
(IM&CTCPA-2015)
Санкт-Петербург, 26-28 ноября 2015

Опыт разработки распределенной системы охраны периметра на основе элементов сети Интернета вещей

Левшун Д.С., Чечулин А.А., Коломеец М.В., Котенко И.В.

Разработка системы ведется сотрудниками лаборатории проблем компьютерной безопасности ФГБУН Санкт-Петербургского института информатики и автоматизации Российской академии наук.

2015

Содержание

- Введение
  - Понятие встроенного устройства.
  - Область применения встроенных устройств.
  - Понятие систем контроля и управления доступом.
  - Инфраструктура для проведения экспериментов на основе СКУД.
- Теоретические аспекты
  - Ключевая проблема современных СКУД.
  - Методика комбинирования средств защиты ВУ.
- Практические аспекты
  - Поэтапная разработка прототипа защищенной СКУД.
  - Аварийный режим работы прототипа защищенной СКУД.
  - Фото прототипа защищенной СКУД.
- Заключение
  - Конкурентные преимущества разрабатываемой СКУД.
  - Планы на будущее.
  - Контактная информация.

Встроенное устройство

- Под **встроенным устройством** понимается электронное устройство, функциональность которого определяется в первую очередь его **аппаратной** и **программной** частями.

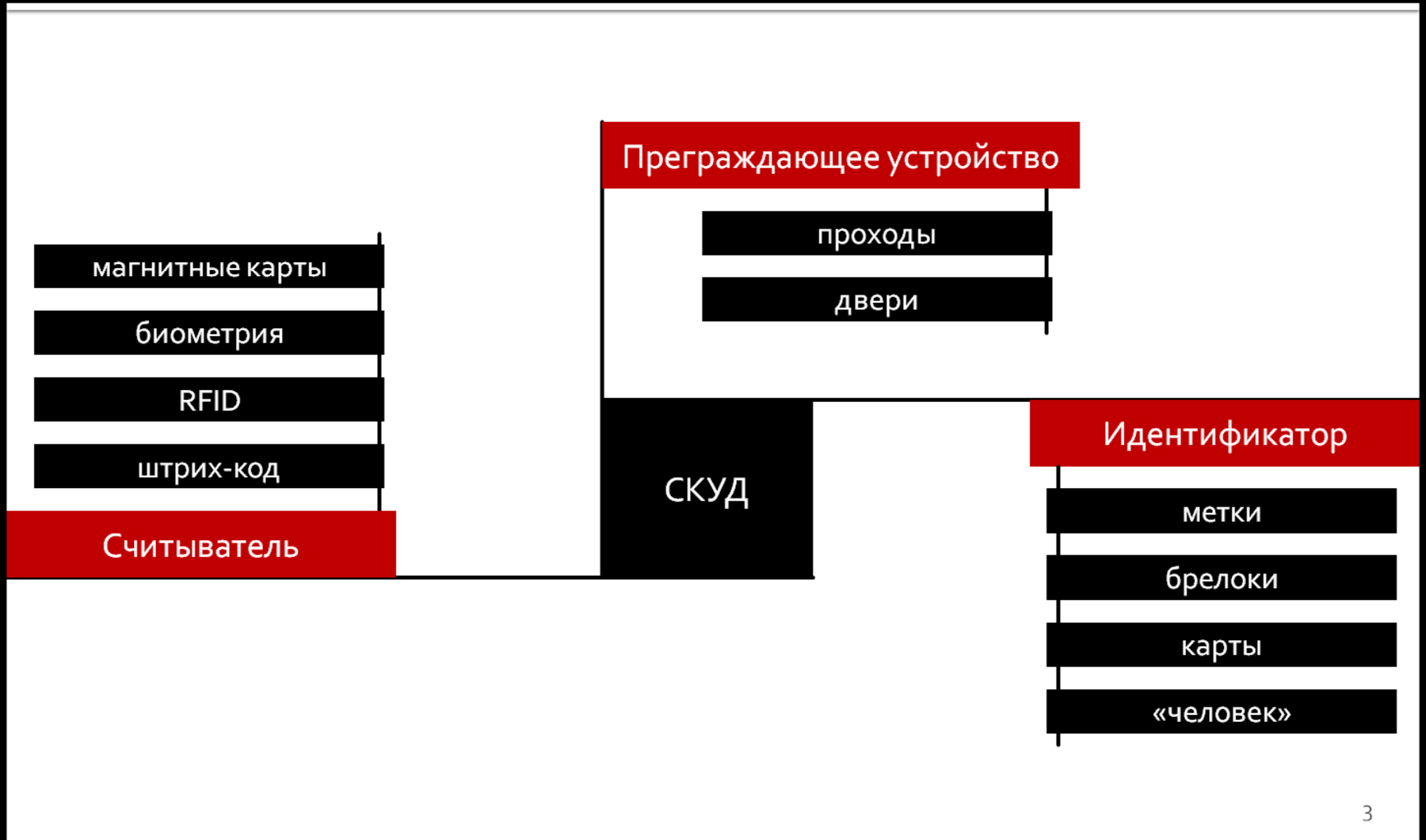
- Ключевым признаком встроенного устройства является его **узкоспециализированное назначение**, предполагающее некоторый **ограниченный набор взаимосвязанных функций**, которое устройство способно реализовать.

Область применения

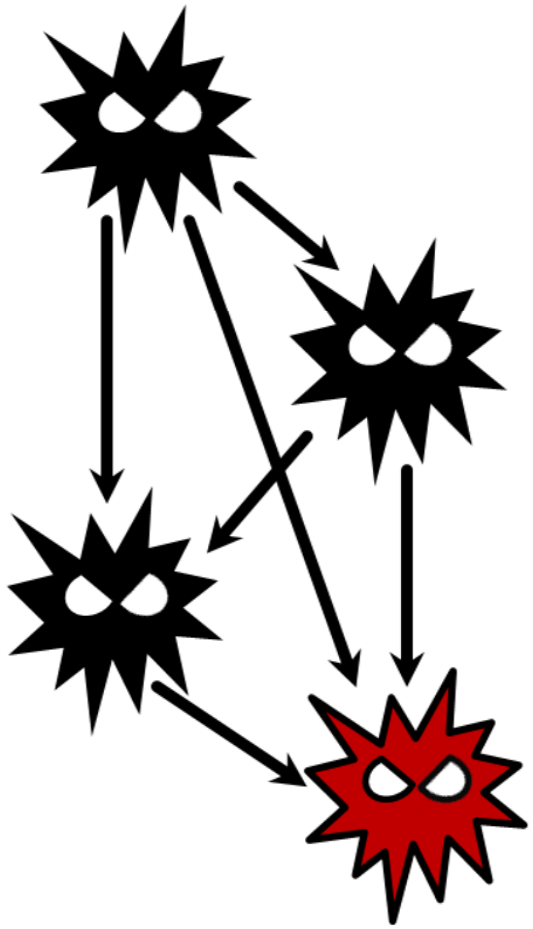
- Как правило, такие информационные системы являются **критически важными**.

- **Высокая степень взаимодействия** встроенного устройства с другими элементами программно-аппаратного окружения и пользователями системы.

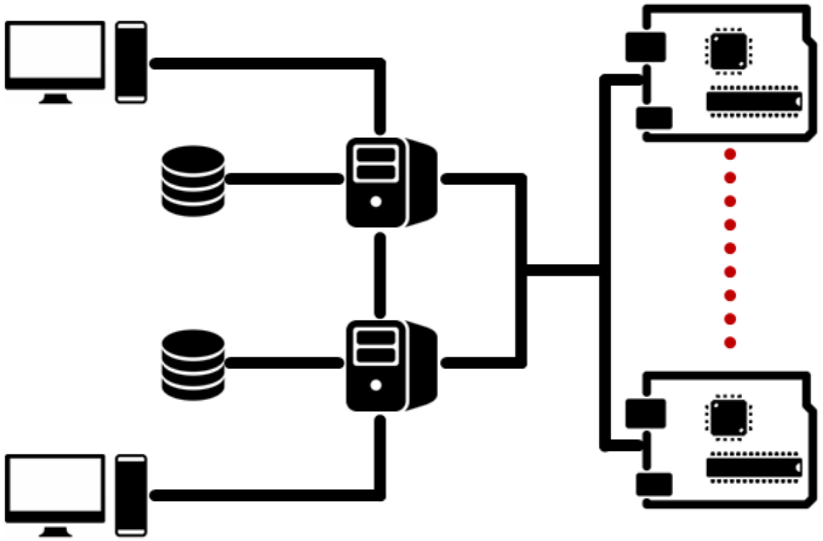
Системы контроля и управления доступом



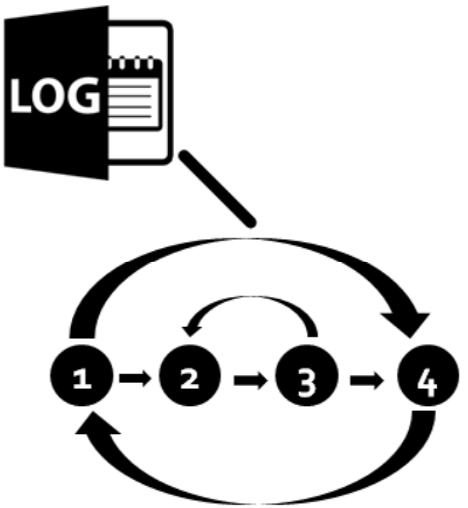
Область применения



анализ векторов атак



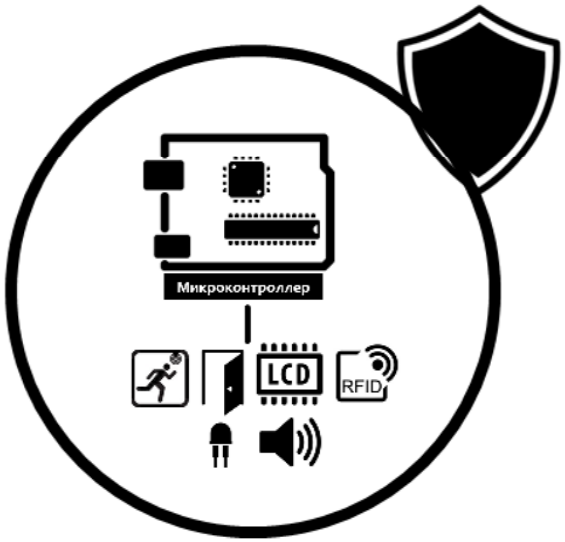
инфраструктура для проведения экспериментов



1. **вход** в помещение
2. **начало** сеанса ОС
3. **завершение** сеанса ОС
4. **выход** из помещения

корреляция событий безопасности

Проблема



Проблема:

- в современных СКУД защита внедряется **после** этапа разработки.

Проблема

Проблема:

- в современных СКУД защита внедряется **после** этапа разработки.

Цель:

- разработка прототипа **защищенной** СКУД.

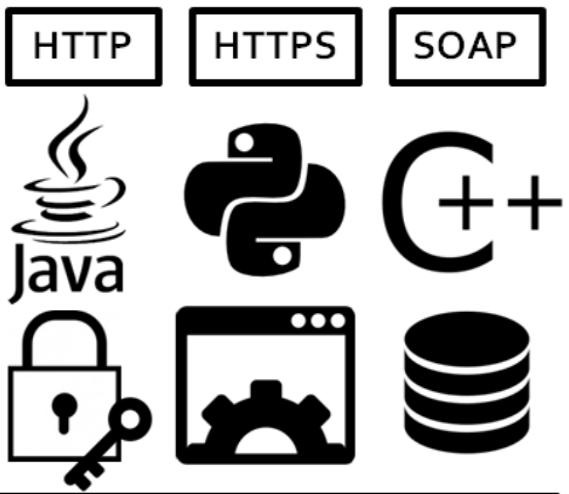
Подход к решению проблемы:

- использование новых моделей и методик комбинирования средств защиты встроенных устройств непосредственно **на этапе** разработки.

Методика разработки

Функциональные требования

к аппаратному обеспечению



к программному обеспечению

- Формирование **функциональных требований** и выбор **подходящих** программно-аппаратных компонентов.

Альтернативы

Arduino Yun, micro SD

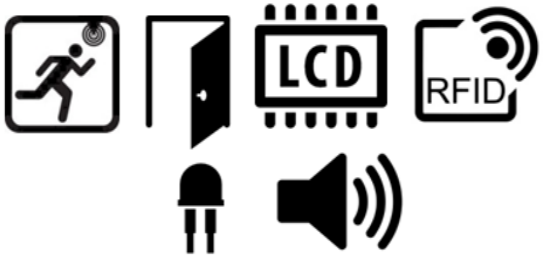
Beaglebone Black, Wi-Fi adapter

Raspberry Pi B+, Wi-Pi module

Intel Galileo, Wi-Fi Kit

Методика разработки

Платформа			
Arduino	Raspberry Pi	Beaglebone	Intel
Uno	1 A+	Bone	Edison
Mega	1 B+	Black	Galileo
Yun	2 B		
Zero			
Due			
Pro			



Поддержка взаимодействия с **внешними электронными компонентами**:

- Механическими замками.
- Сканерами бесконтактных смарт-карт.
- Инфракрасными датчиками движения
- Устройствами вывода текстовой информации, звуковых и световых сигналов.

Методика разработки

Платформа			
Arduino	Raspberry Pi	Beaglebone	Intel
Uno	1 A+	Bone	Edison
Mega	1 B+	Black	Galileo
Yun	2 B		
Zero			
Due			
Pro			

Поддержка **каналов передачи данных**:

- Беспроводного.
- Ethernet.

Методика разработки

Платформа			
Arduino	Raspberry Pi	Beaglebone	Intel
Uno	1 A+	Bone	Edison
Mega	1 B+	Black	Galileo
Yun	2 B		
Zero			
Due			
Pro			

HTTP HTTPS SOAP

Поддержка **протоколов передачи данных**:

- HTTP.
- HTTPS.
- SOAP.

Методика разработки

Платформа			
Arduino	Raspberry Pi	Beaglebone	Intel
Uno	1 A+	Bone	Edison
Mega	1 B+	Black	Galileo
Yun	2 B		
Zero			
Due			
Pro			

Поддержка **приложений**, написанных на:

- Java.
- Python.
- C++.

Методика разработки

шаг 1 | шаг 2 | шаг 3

Платформа			
Arduino	Raspberry Pi	Beaglebone	Intel
Uno	1 A+	Bone	Edison
Mega	1 B+	Black	Galileo
Yun	2 B		
Zero			
Due			
Pro			

- Поддержка и хранение **локальной резервной** копии **базы данных**.
- Поддержка **шифрования** данных, передаваемых по каналам передачи данных.
- Поддержка управления встроенным устройством через **веб-интерфейс** при **локальном Ethernet** подключении.

Методика разработки

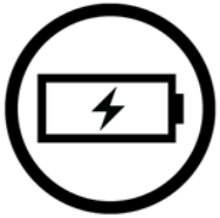
Платформа			
Arduino	Raspberry Pi	Beaglebone	Intel
Uno	1 A+	Bone	Edison
Mega	1 B+	Black	Galileo
Yun	2 B		
Zero			
Due			
Pro			

Методика разработки

шаг 1 | шаг 2 | шаг 3

Нефункциональные требования

цена



энергоэффективность

размер

- Формирование **нефункциональных требований** и выбор **наилучших** программно-аппаратных компонентов из **подходящих**.

Альтернативы

Arduino Yun, micro SD

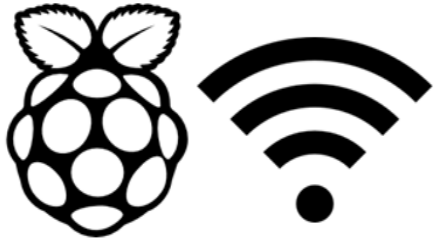
Beaglebone Black, Wi-Fi adapter

Raspberry Pi B+, Wi-Pi module

Intel Galileo, Wi-Fi Kit

Методика разработки

Arduino Yun, microSD
550 мА·ч
6782 ₽
73*53*8 мм



Raspberry Pi B+, Wi-Pi module
1350 мА·ч
5339 ₽
60*36*7 мм

- Цены конвертированы по курсу ЦБРФ от 29.10.2015: **1 € = 72,1479 ₽**.

Beaglebone Black, Wi-Fi adapter
780 мА·ч
7287 ₽
86*53*7 мм

Intel Galileo, Wi-Fi Kit
1400 мА·ч
10606 ₽
123*72*9 мм

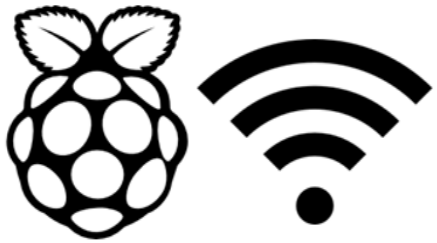
Arduino: http://arduino.cc
Raspberry-pi: http://raspberrypi.org

Amazon: http://www.amazon.com

Beaglebone: http://beagleboard.org
Intel Galileo: http://www.intel.com

Методика разработки

Arduino Yun, microSD
550 мА·ч
6782 ₽ + 1082 ₽
73*53*8 мм



Raspberry Pi B+, Wi-Pi module
1350 мА·ч
5339 ₽ + 14430 ₽
60*36*7 мм

- Цены конвертированы по курсу ЦБРФ от 29.10.2015: **1 € = 72,1479 ₽**.
- Функционирование в условиях выхода из строя электрической цепи в течение **24 часов**.

Beaglebone Black, Wi-Fi adapter
780 мА·ч
7287 ₽
86*53*7 мм

Intel Galileo, Wi-Fi Kit
1400 мА·ч
10606 ₽
123*72*9 мм

Arduino: http://arduino.cc
Raspberry-pi: http://raspberrypi.org

Amazon: http://www.amazon.com

Beaglebone: http://beagleboard.org
Intel Galileo: http://www.intel.com

Методика разработки

шаг 1 | шаг 2 | шаг 3

Статическое тестирование

типы и уровни злоумышленника

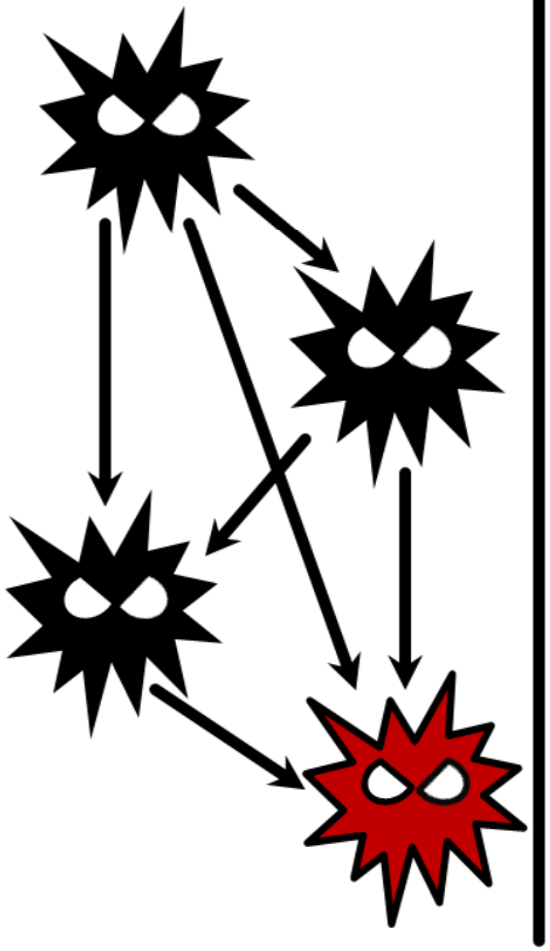
ARDUINO

компонентный состав

правила

- Анализ **выбранных** программно-аппаратных компонентов с точки зрения безопасности. **Возврат** на первый шаг, если необходимо.

Вектора атак

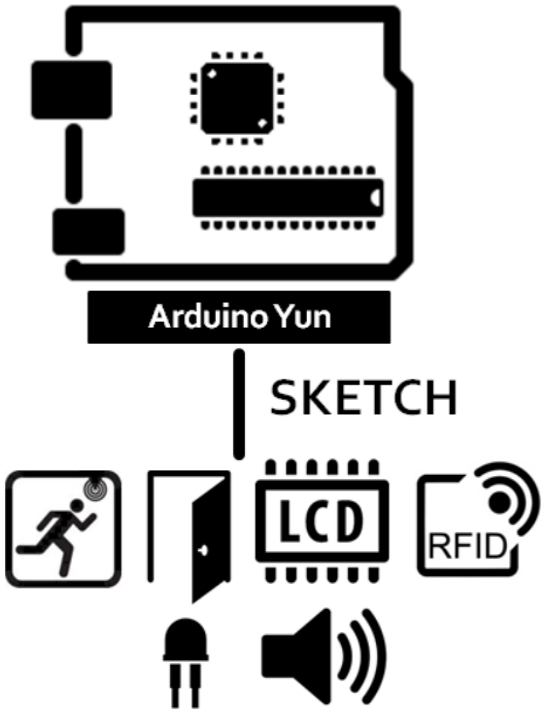


Методика разработки

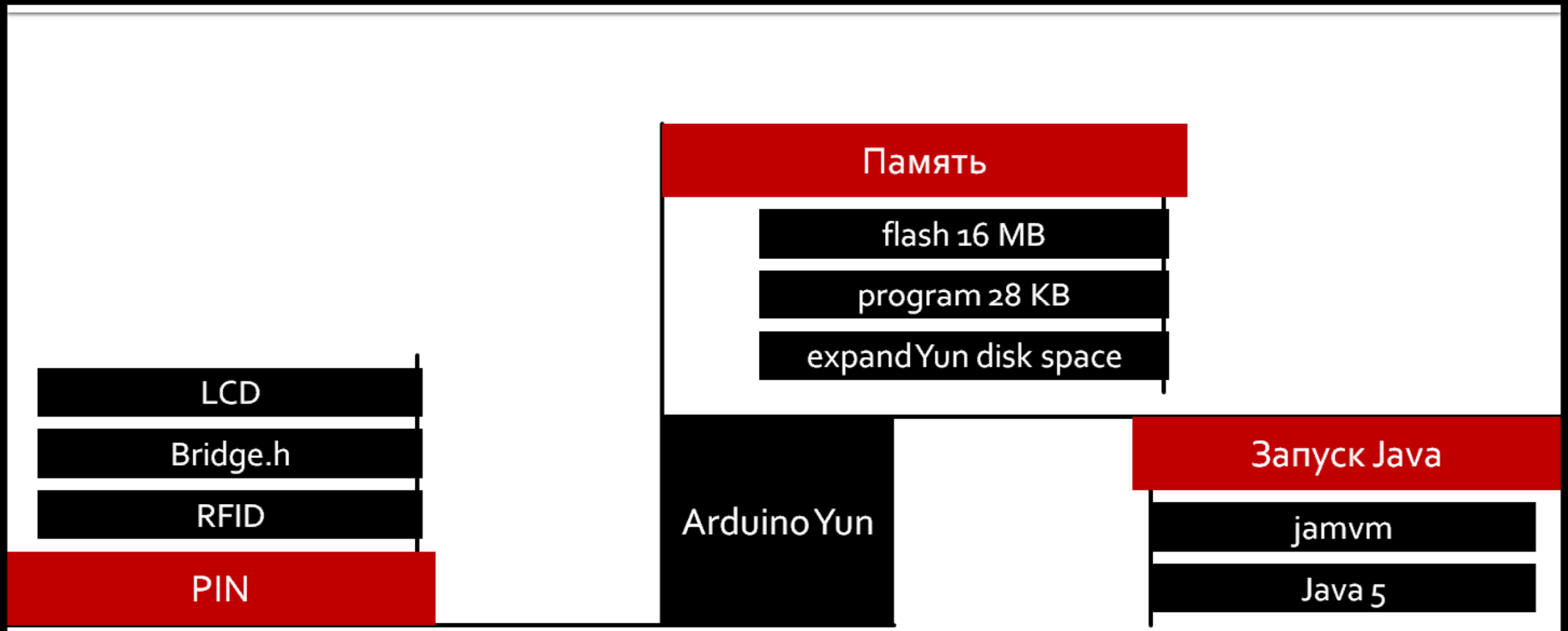
	шаг 1	шаг 2	шаг 3
типы и уровни злоумышленника	тип доступа к ВУ	тип 0: социальная инженерия	уровень возможностей злоумышленника
		тип 1: TCP/IP	уровень 1: публично доступное ПО, общеизвестные уязвимости
		тип 2: Wi-Fi, IR, Bluetooth	уровень 2: специализированное ПО, ранее неиспользуемые уязвимости
		тип 3: COM, USB	уровень 3: группа злоумышленников уровня 2
		тип 4: уровень микросхем	
компонентный состав	Arduino Yun, microSD	Ethernet	
		Wi-Fi	
		sensors	
правила	A&B&C	A: компонент	пример
		B: злоумышленник	A: sensors
		C: атака	B: type=3,lvl=3;type=4,lvl=3
			C: замена сенсора

[Десницкий В.А., Чечулин А.А. Обобщенная модель нарушителя и верификация информационно-телекоммуникационных систем со встроенными устройствами // Журнал «Технические науки — от теории к практике». Изд. НП "СибАК", №39, 2014, С.7-21.]

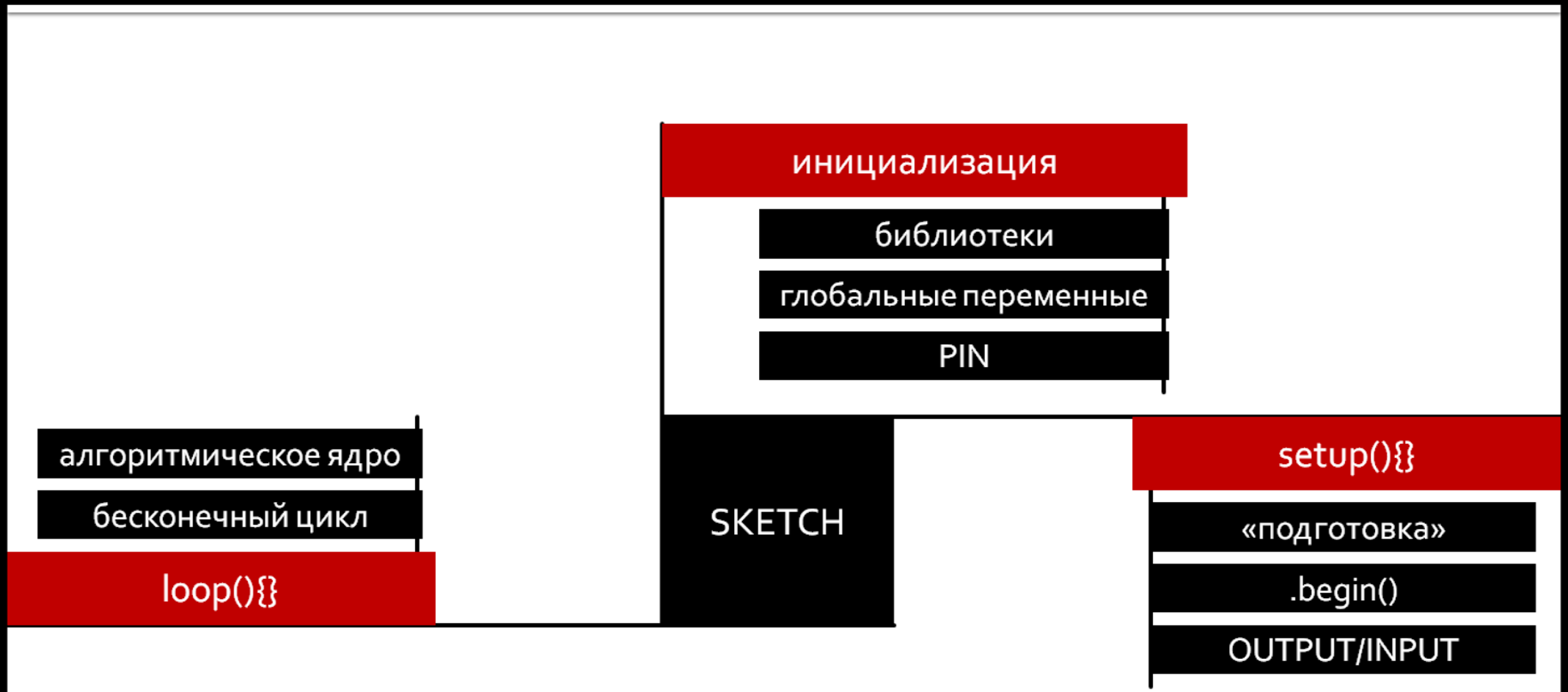
Архитектура системы



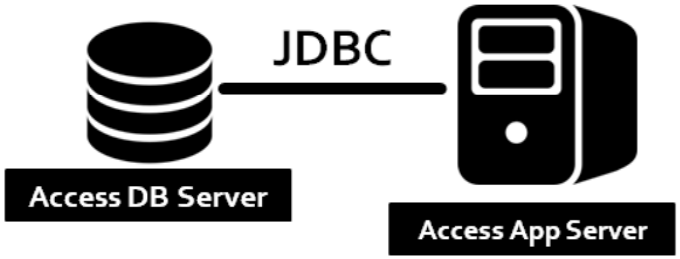
Arduino Yun

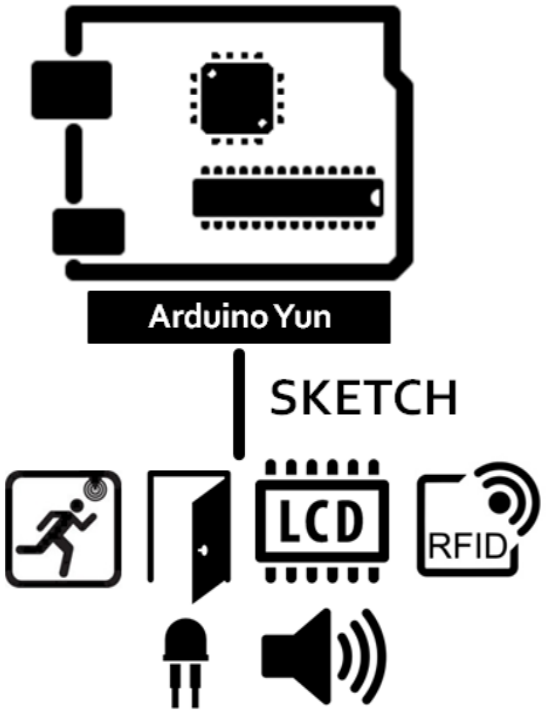

Память
flash 16 MB
program 28 KB
expand Yun disk space
LCD
Bridge.h
RFID
PIN
Arduino Yun
Запуск Java
jamvm
Java 5

SKETCH

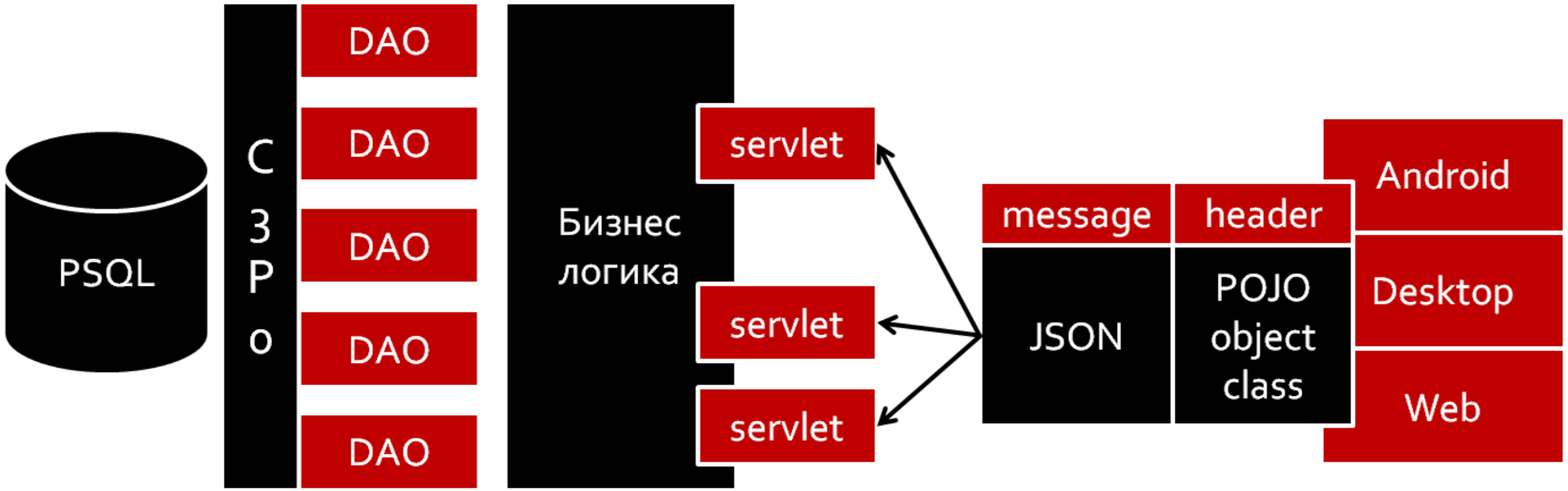

инициализация
библиотеки
глобальные переменные
PIN
алгоритмическое ядро
бесконечный цикл
loop(){}
SKETCH
setup(){}
«подготовка»
.begin()
OUTPUT/INPUT

Архитектура системы

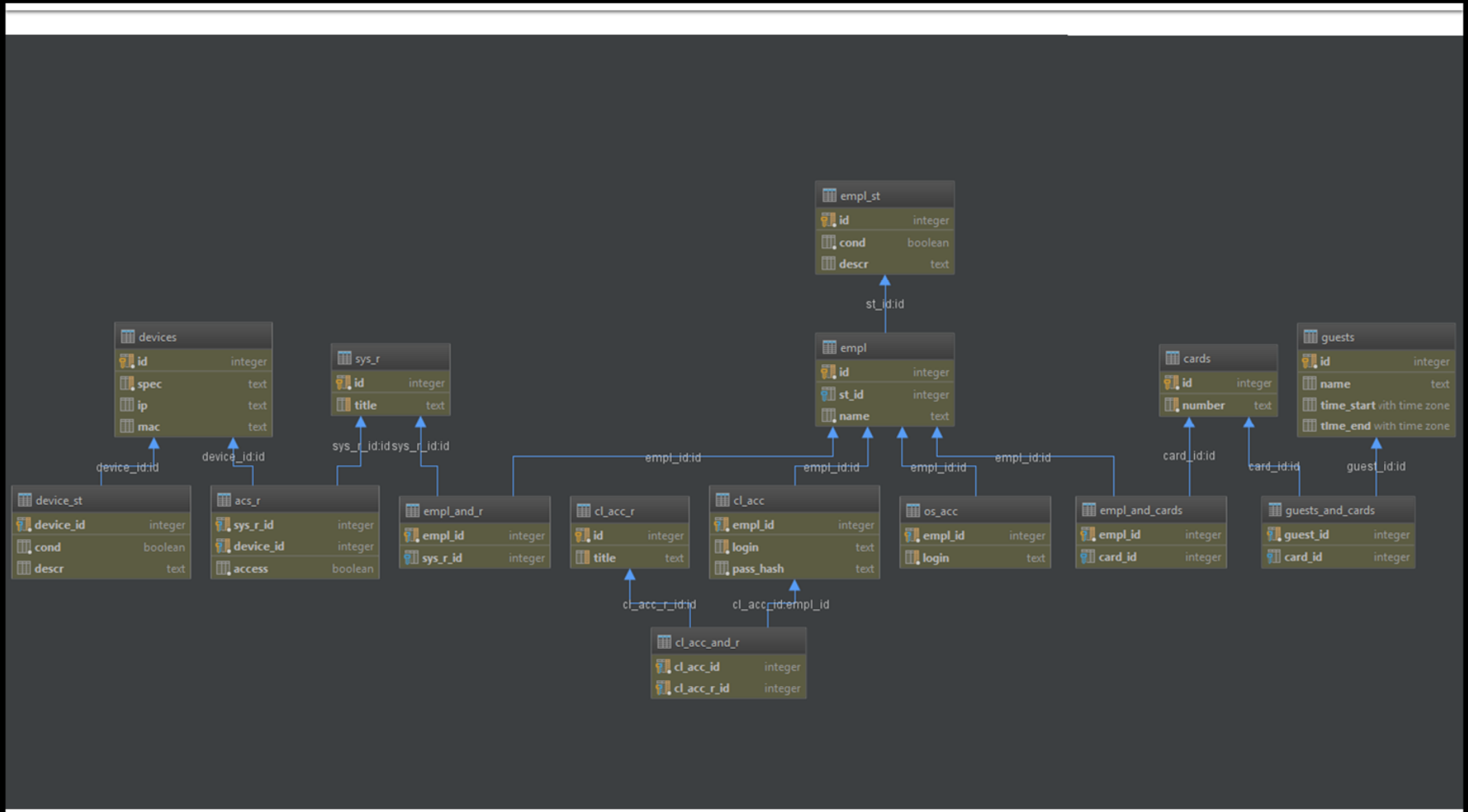




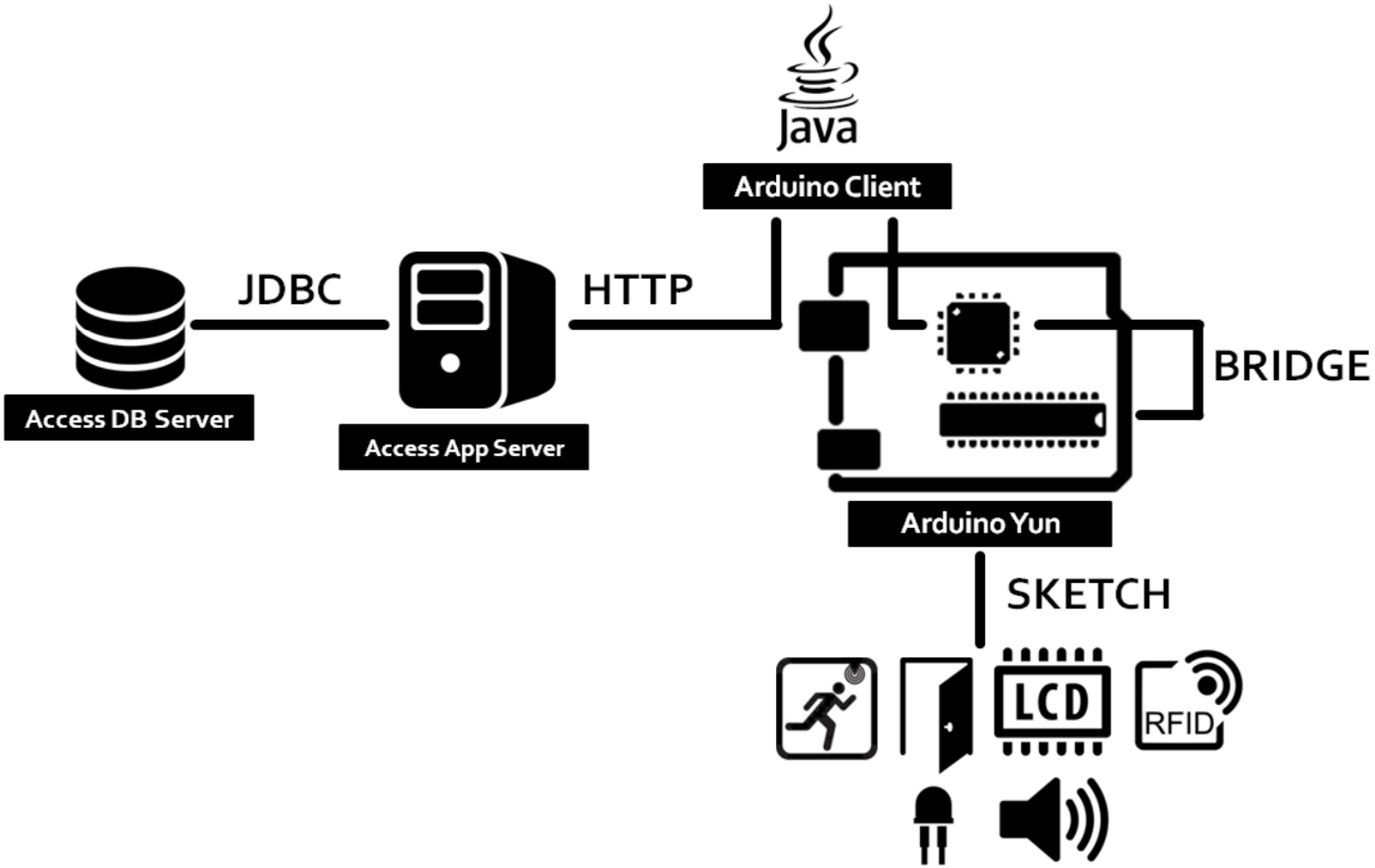
Access App Server



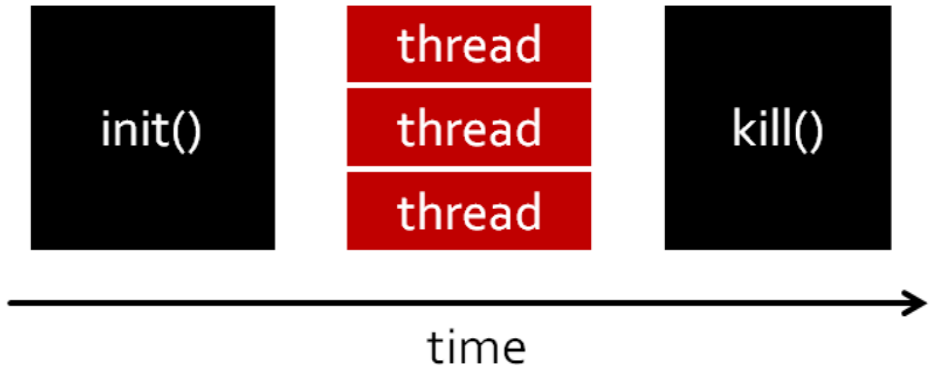
Access DB Server



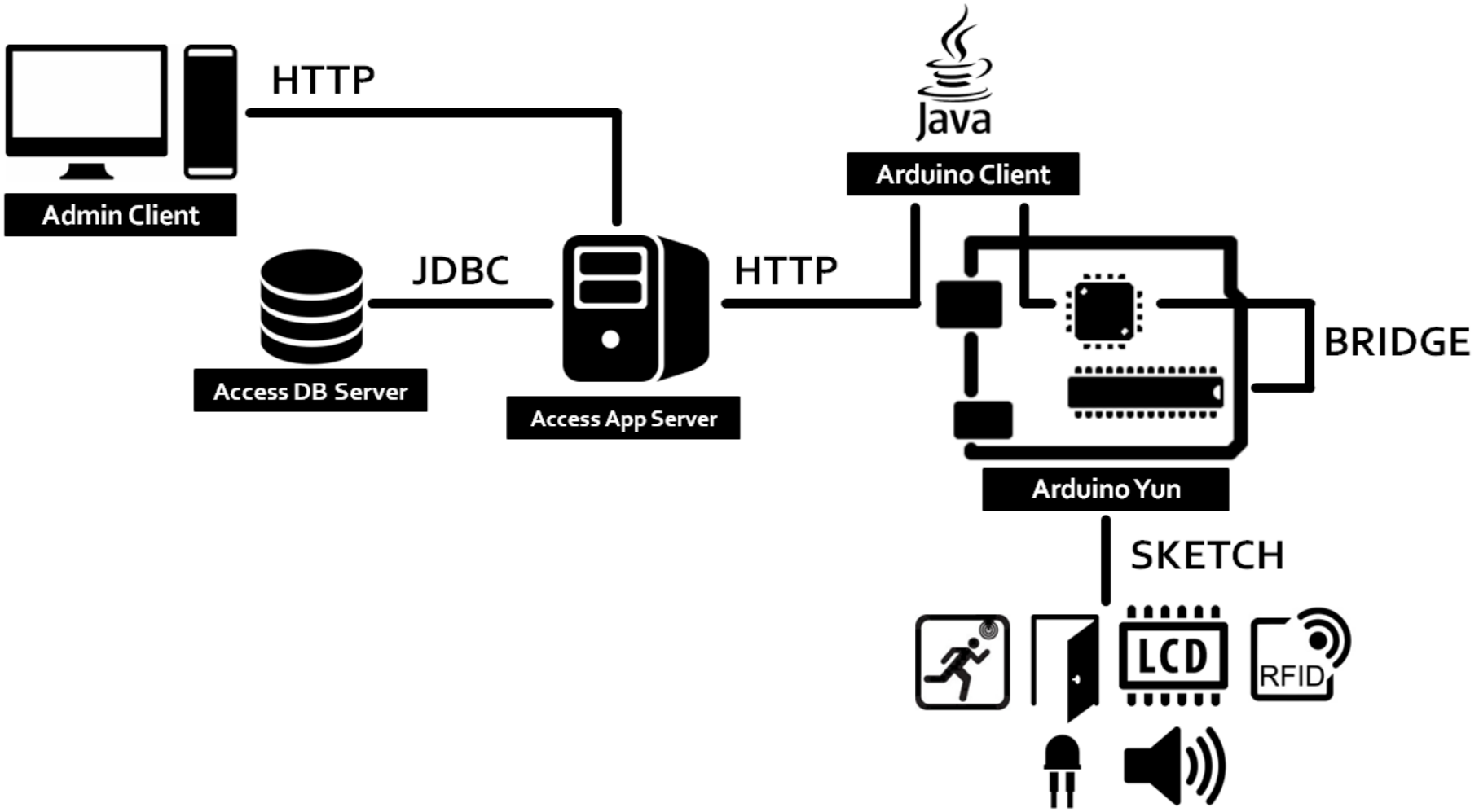
Архитектура системы



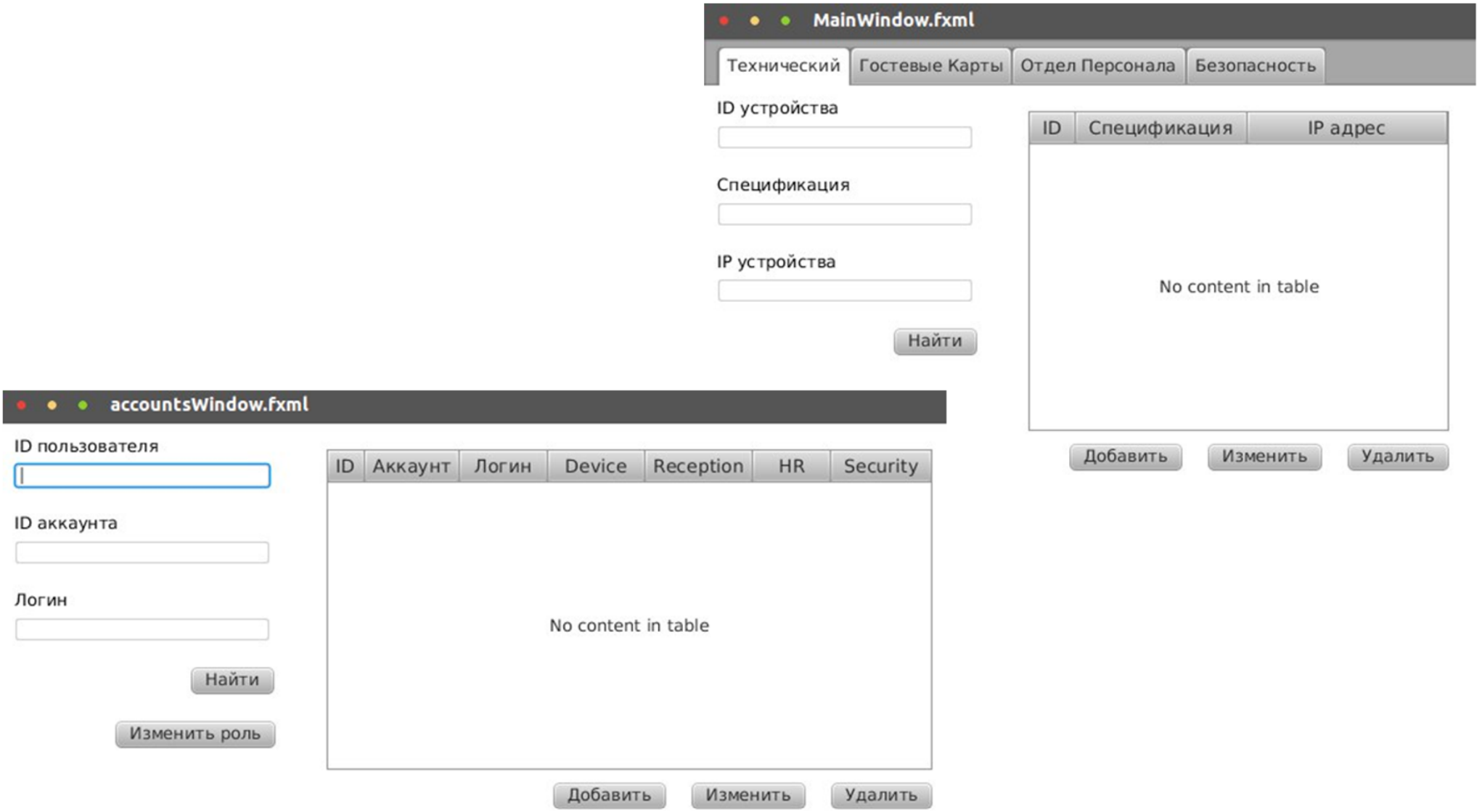
Arduino Client



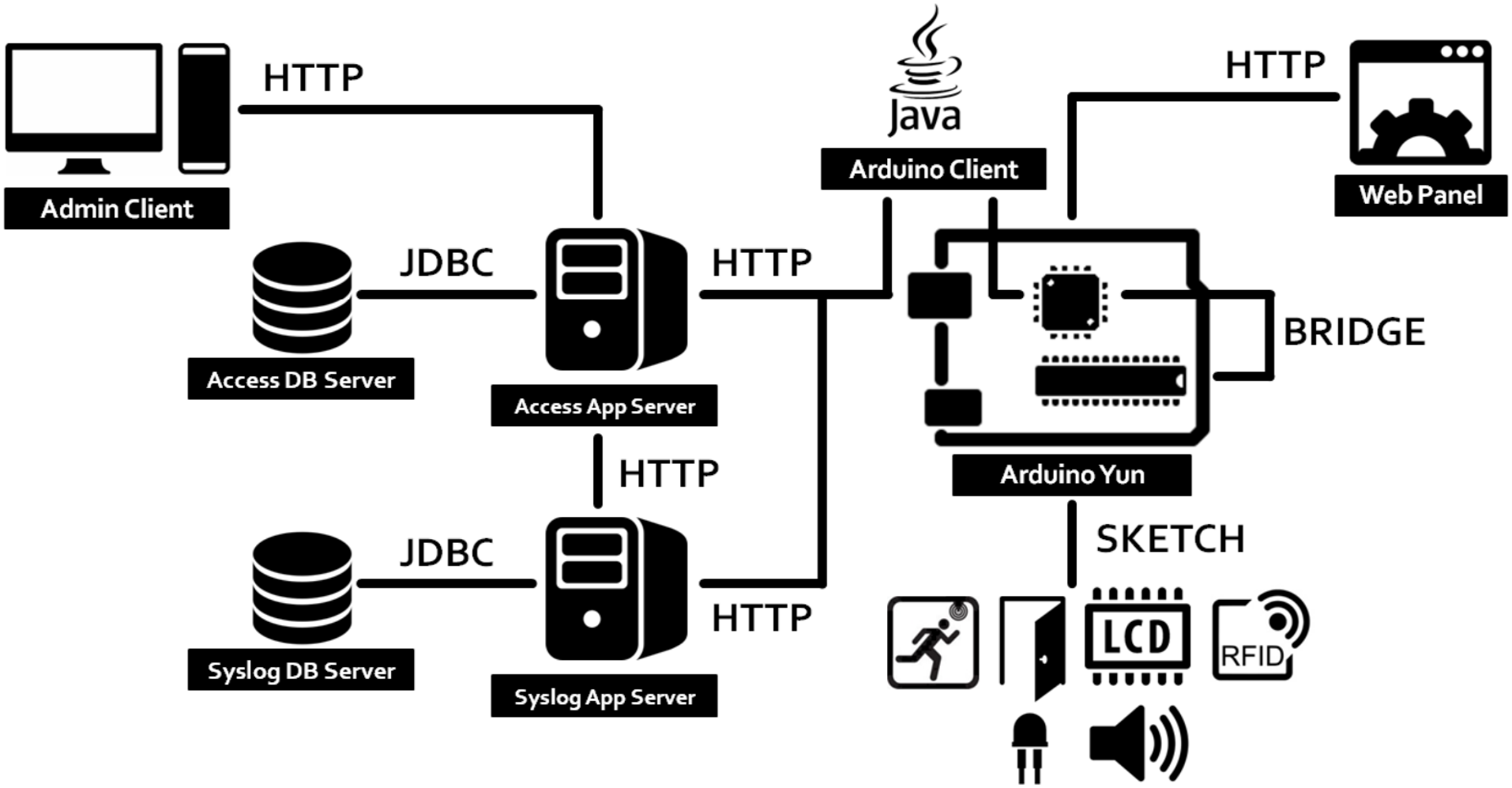
Архитектура системы



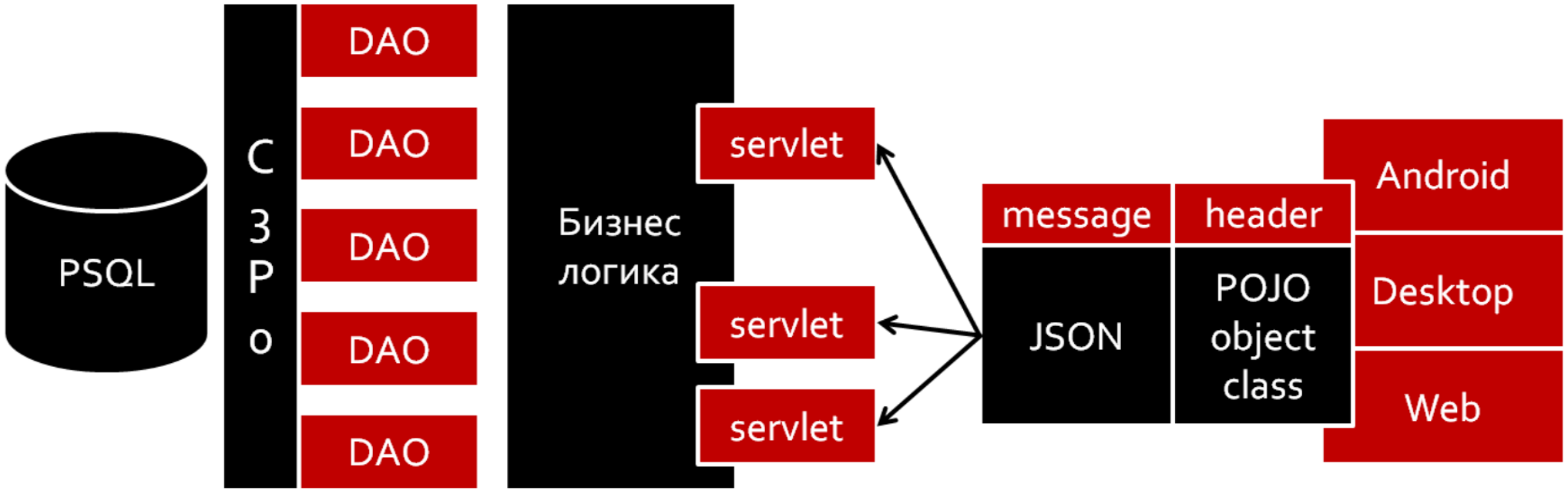
Admin Client



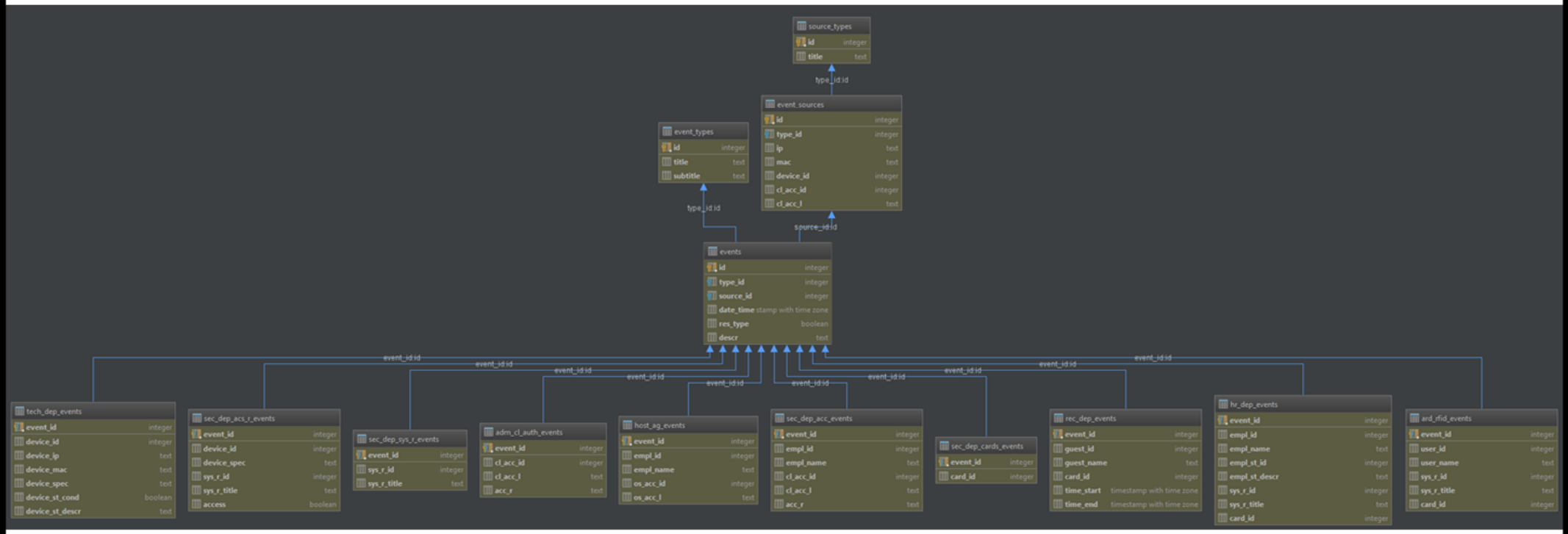
Архитектура системы



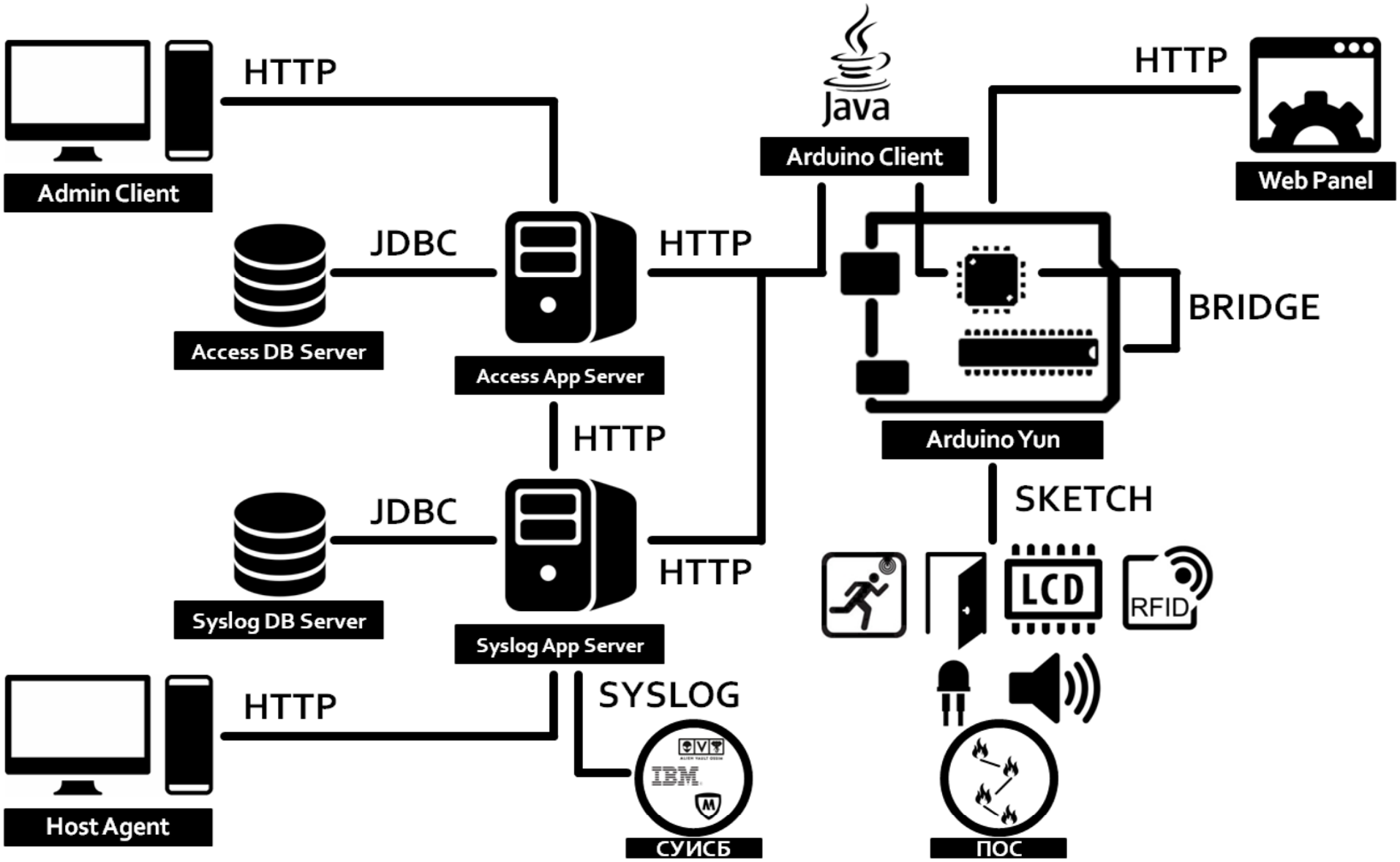
Syslog App Server



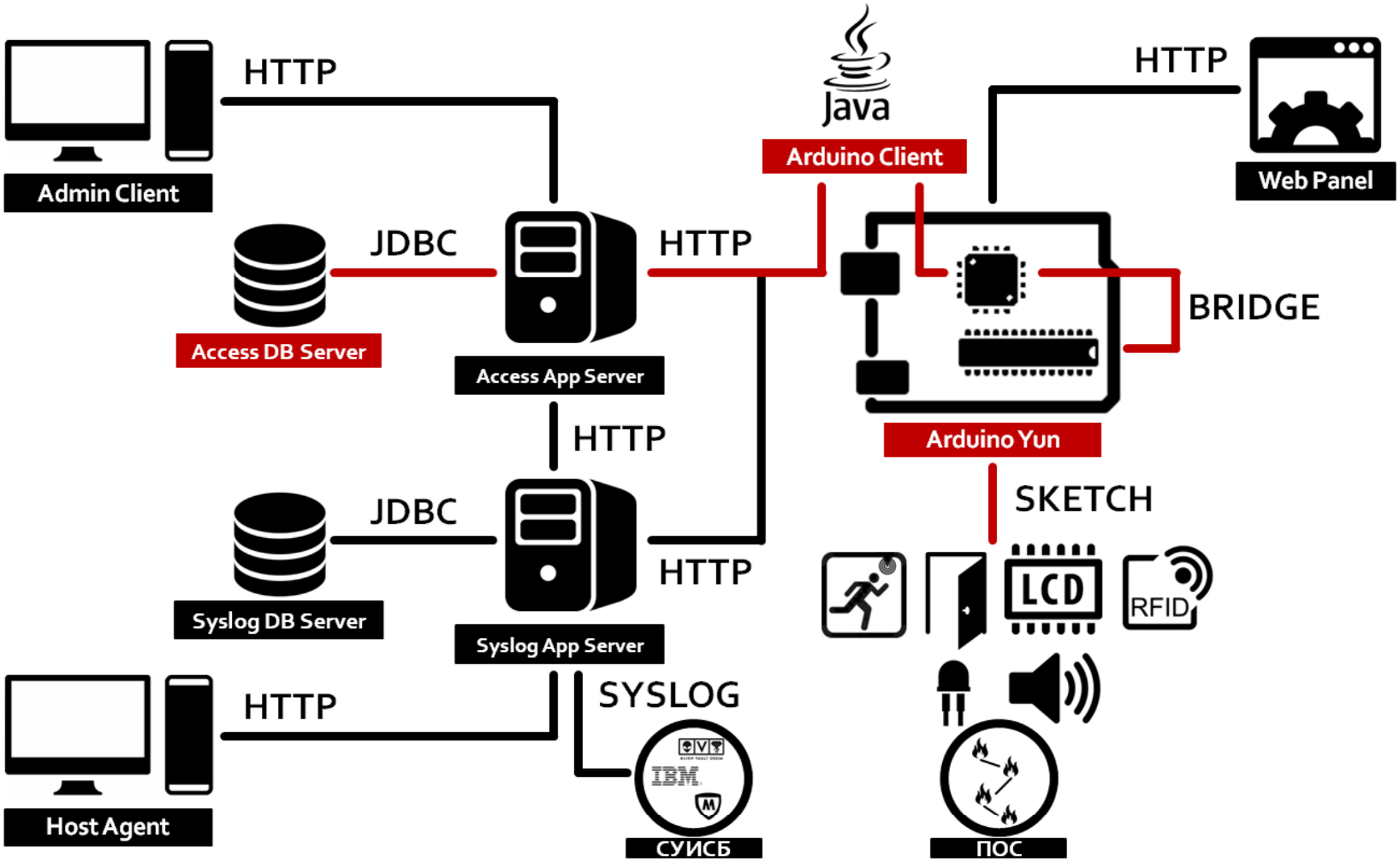
Syslog DB Server



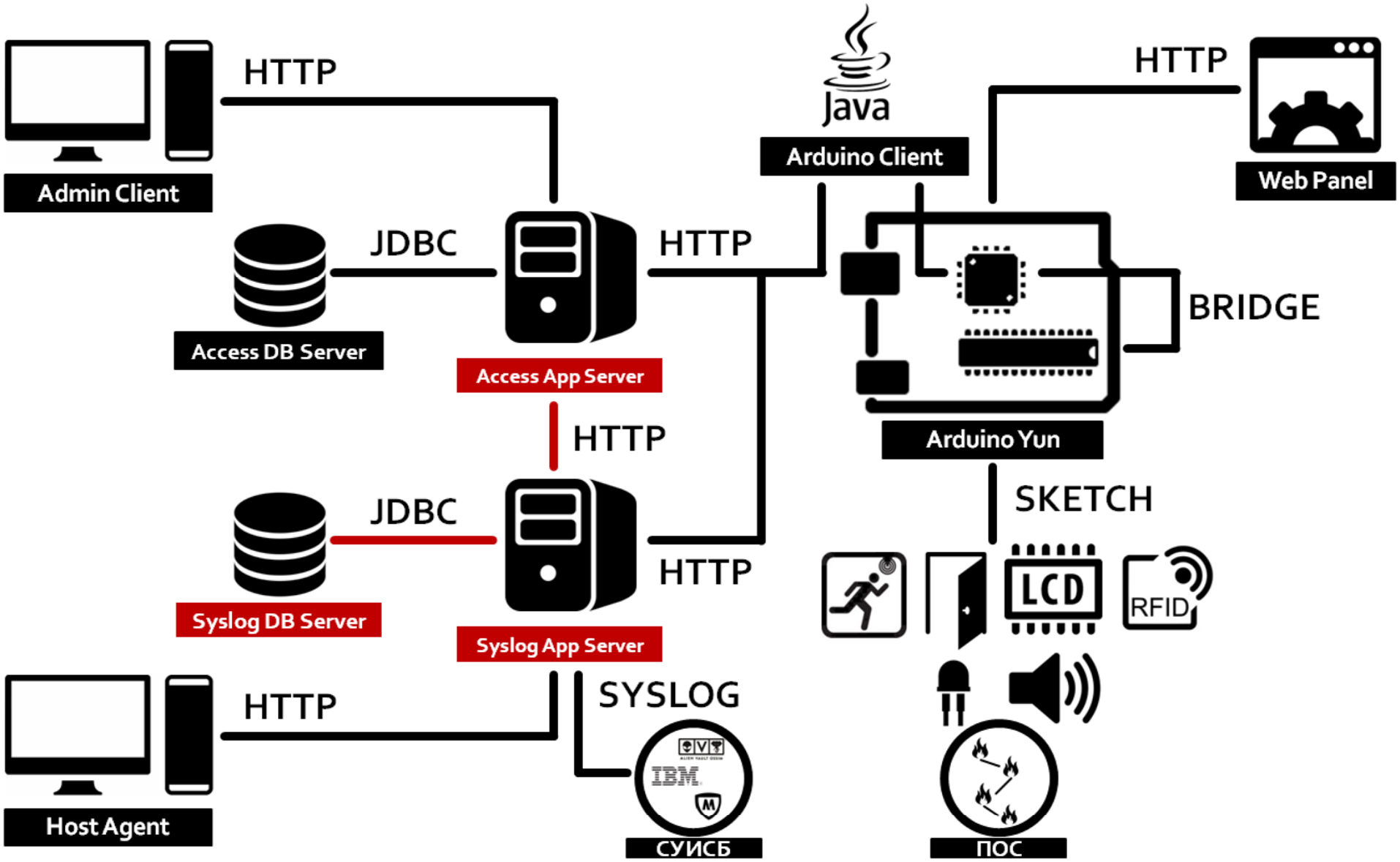
Архитектура системы



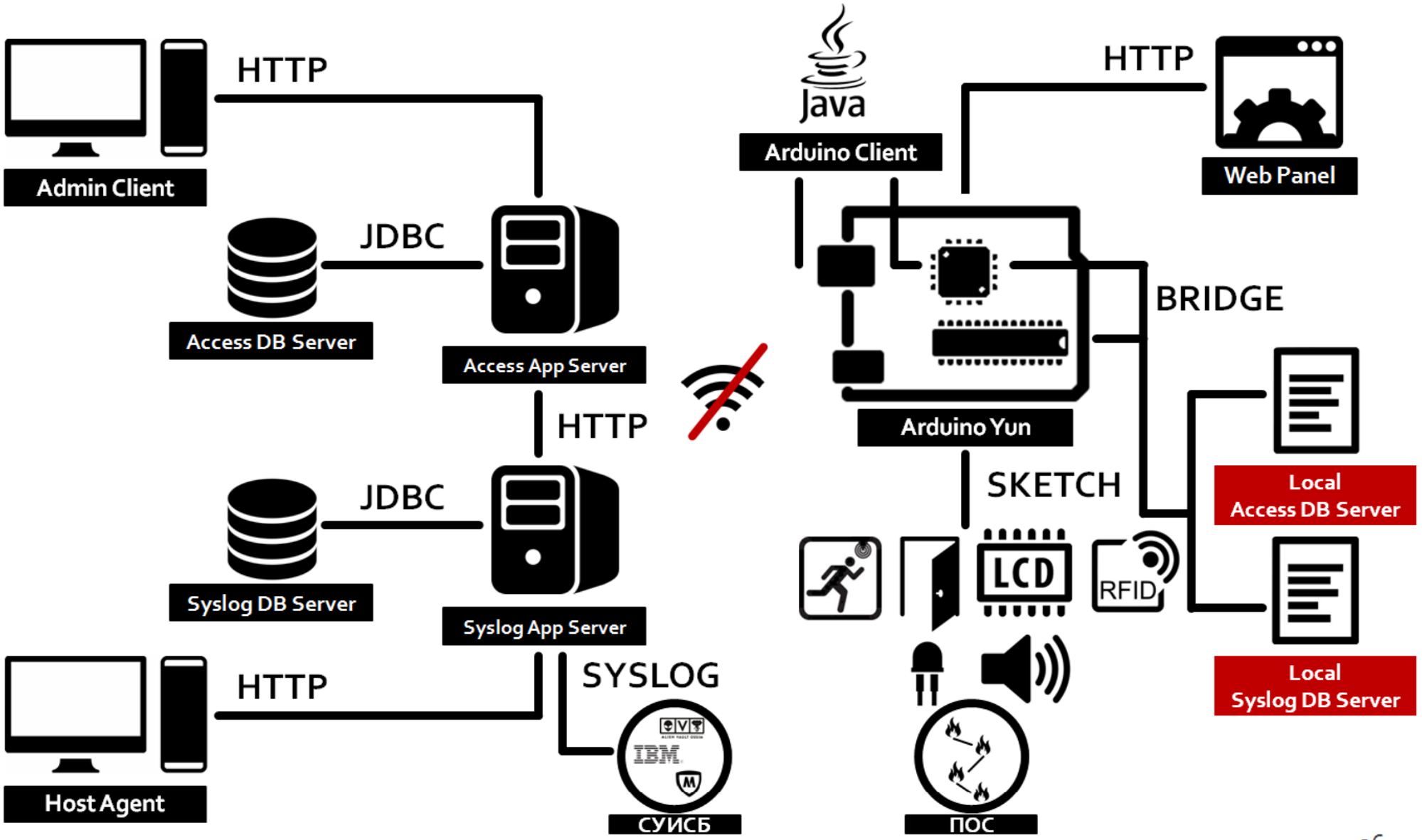
Архитектура системы



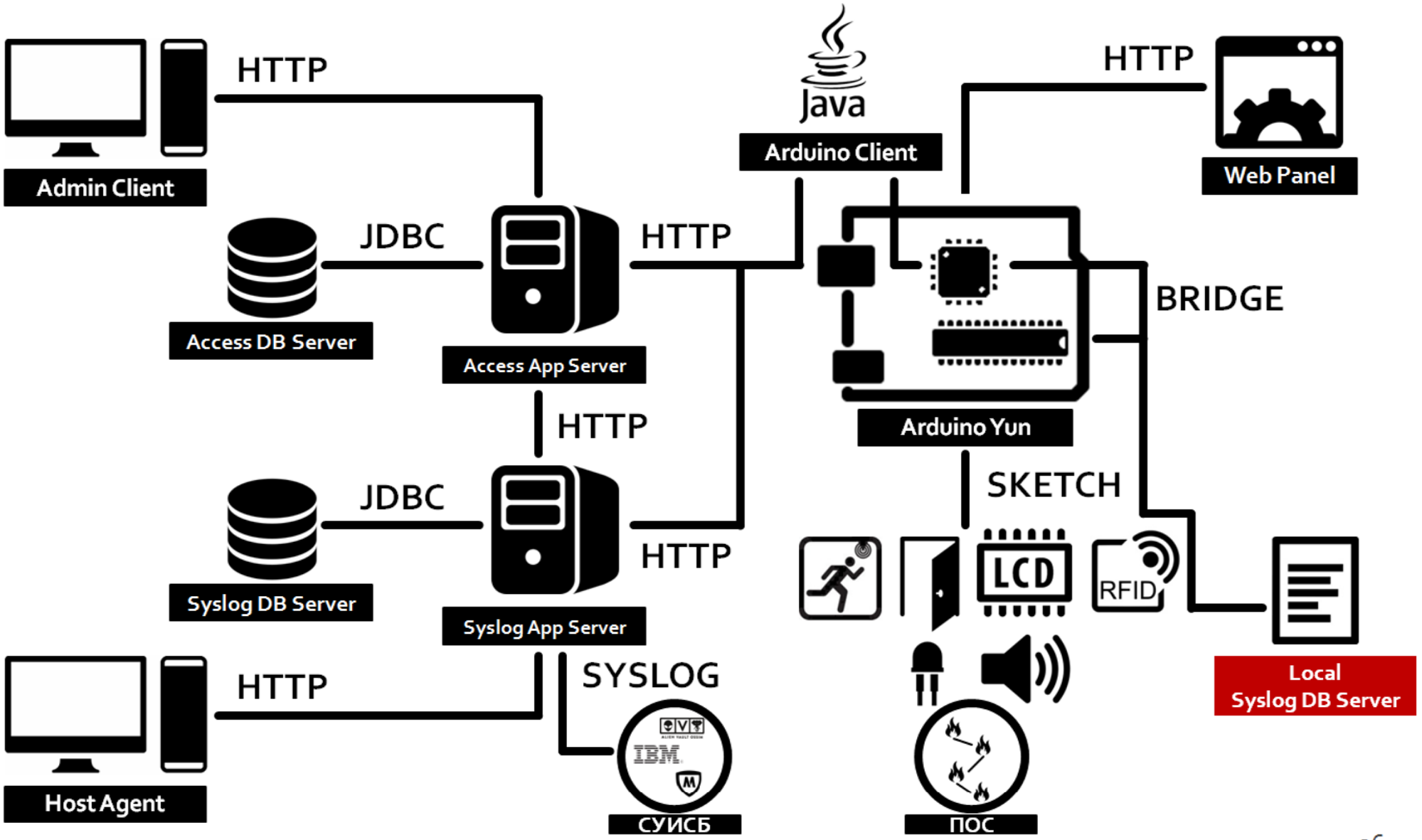
Архитектура системы



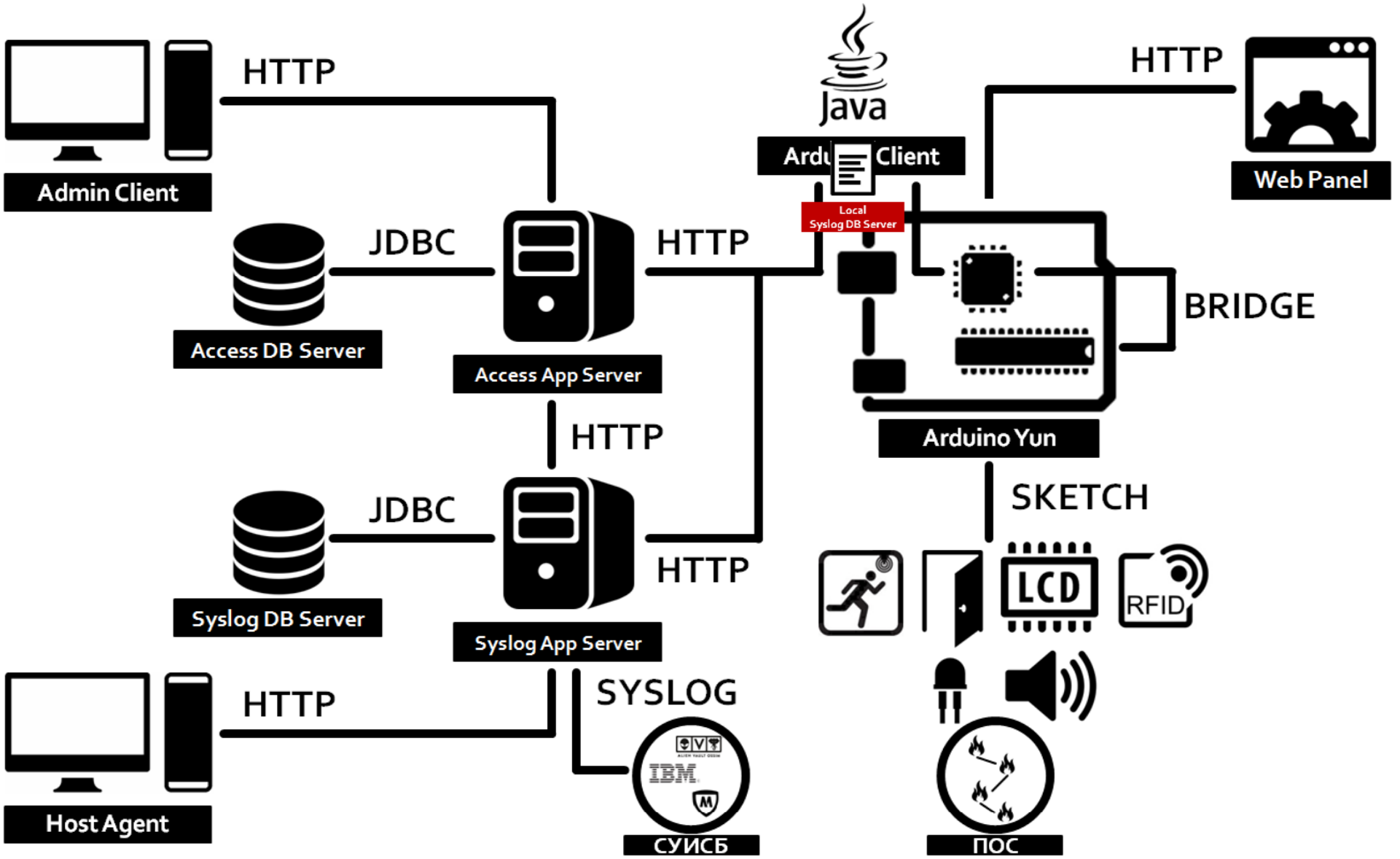
Аварийный режим



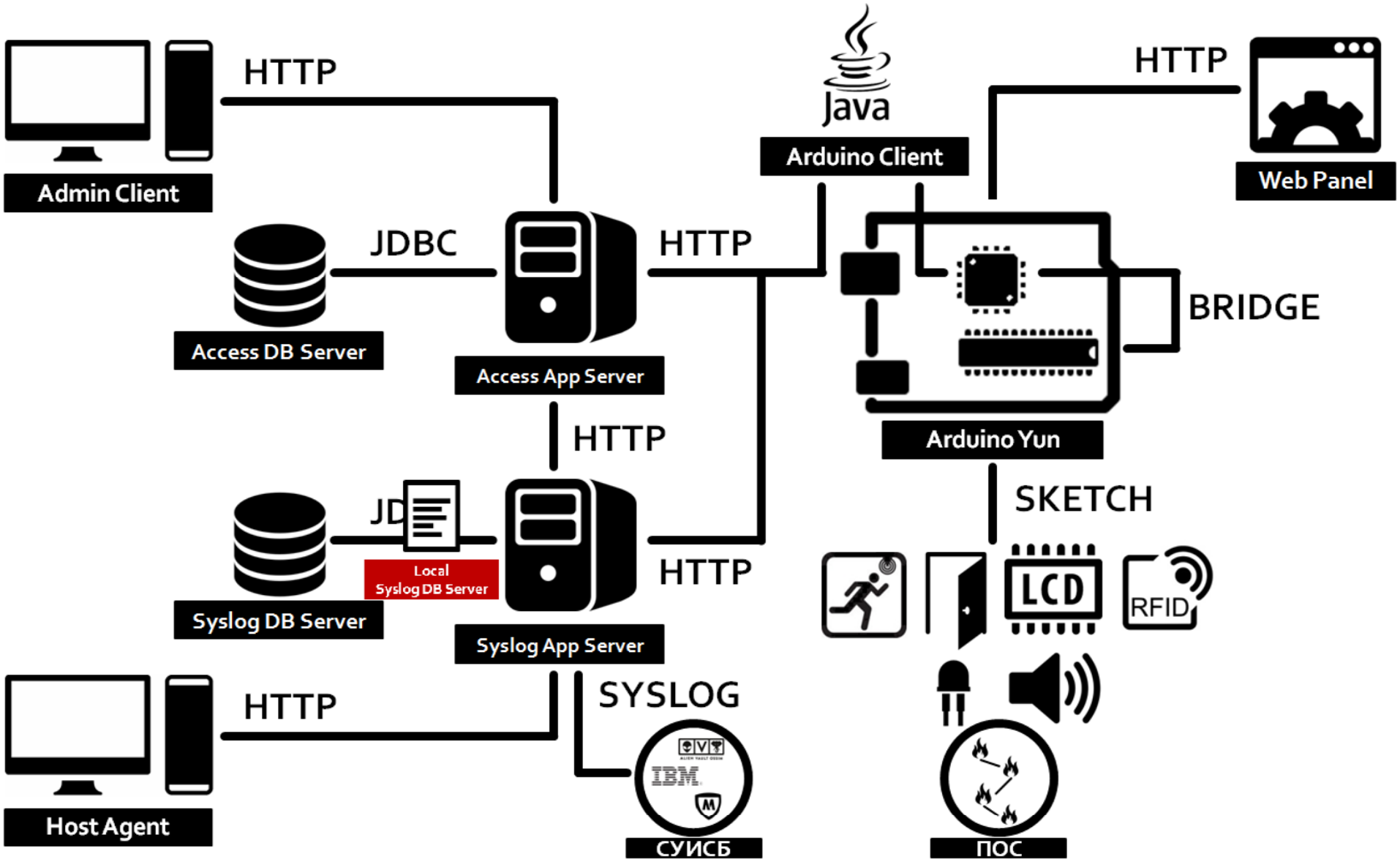
Аварийный режим



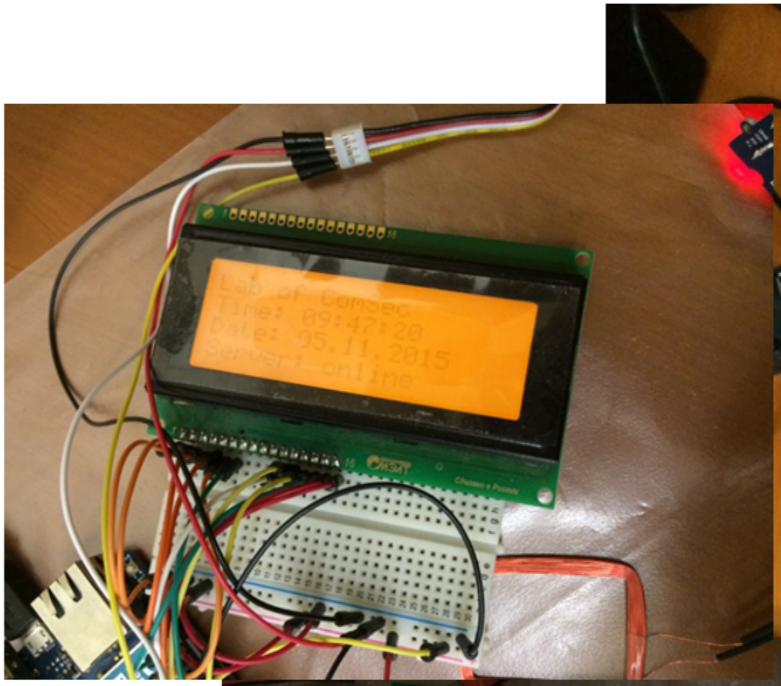
Аварийный режим

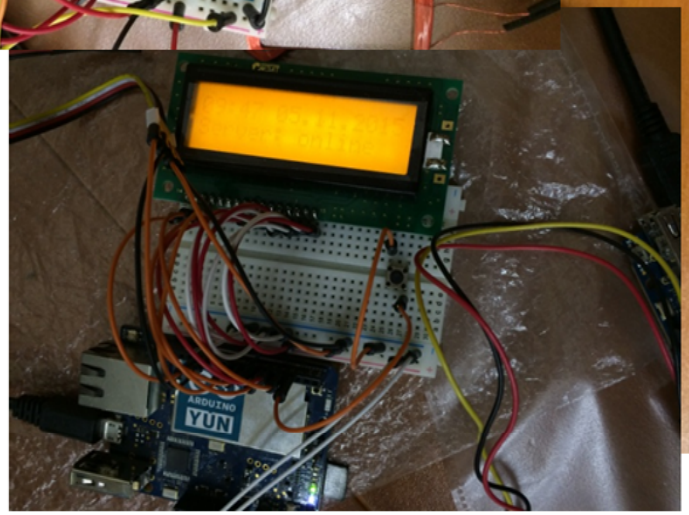


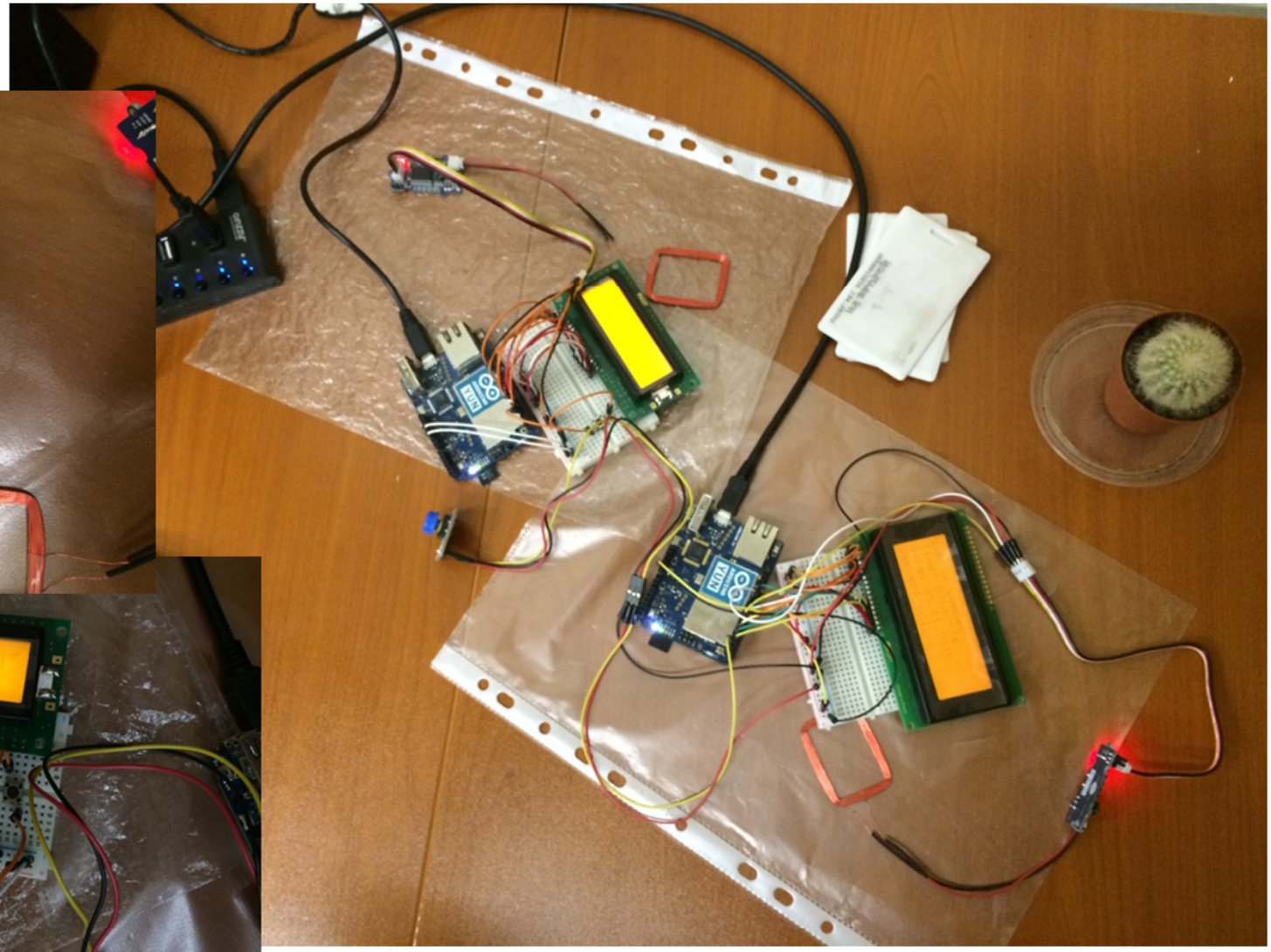
Аварийный режим



Прототип


Lab of Comsec
Time: 09:47:20
Date: 05.11.2015
Server online

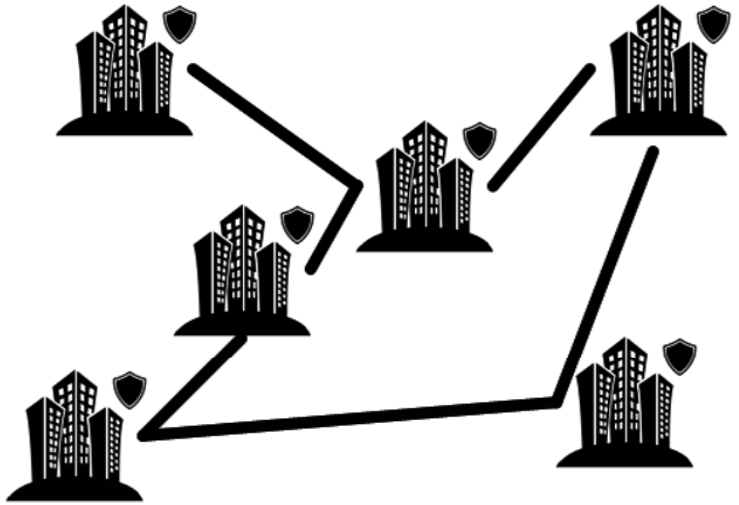

ARDUINO
YUN



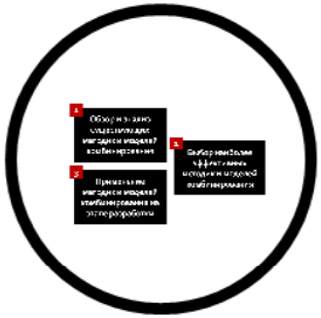
Конкурентные преимущества

1. Обзор и анализ существующих методик и моделей комбинирования
2. Выбор наиболее эффективных методик и моделей комбинирования
3. Применение методик и моделей комбинирования на этапе разработки

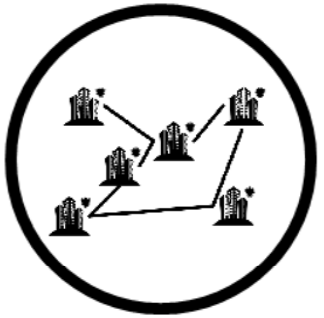
Конкурентные преимущества



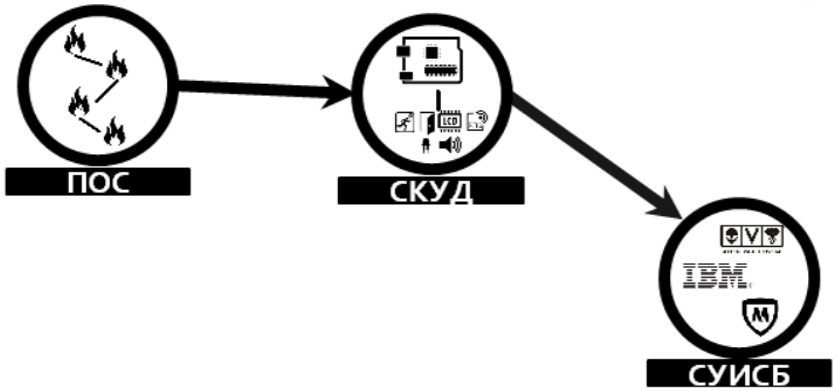
Конкурентные преимущества



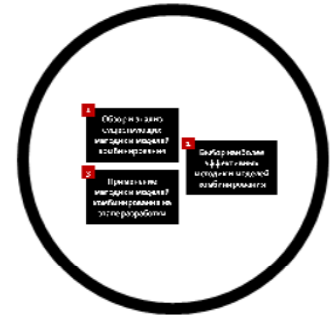
ЗАЩИЩЕННОСТЬ



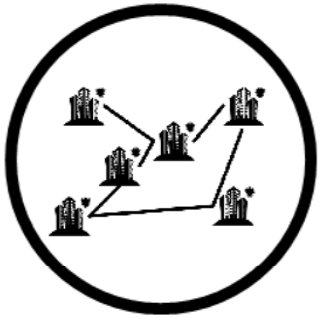
МАСШТАБИРУЕМОСТЬ



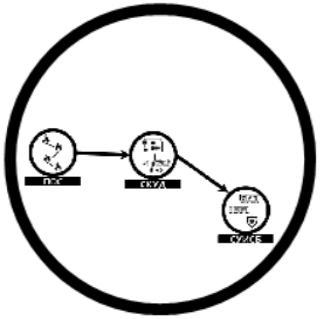
Конкурентные преимущества



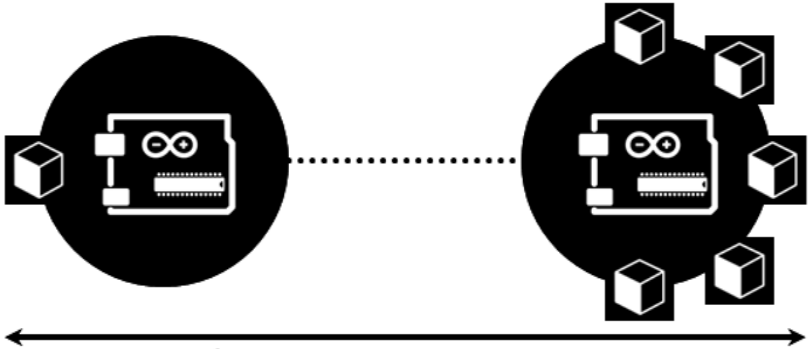
ЗАЩИЩЕННОСТЬ



МАСШТАБИРУЕМОСТЬ

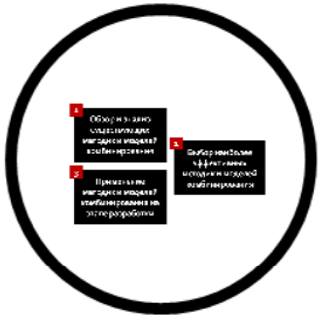


ИНТЕГРИРУЕМОСТЬ

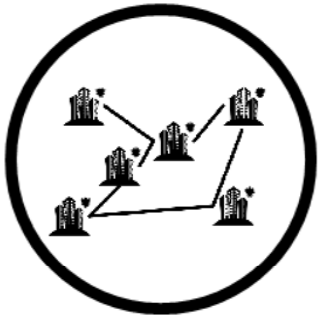


функциональность

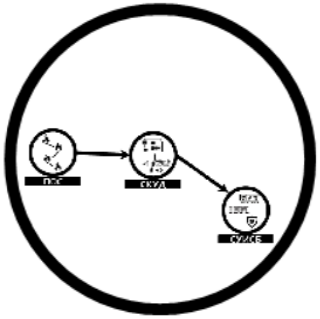
Конкурентные преимущества



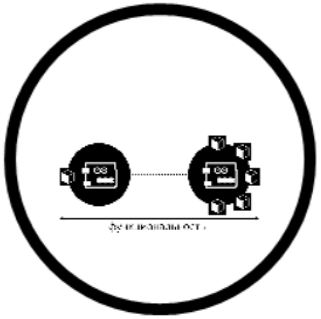
ЗАЩИЩЕННОСТЬ



МАСШТАБИРУЕМОСТЬ



ИНТЕГРИРУЕМОСТЬ

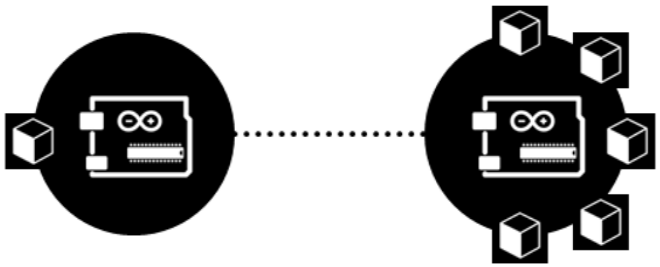


МОДУЛЬНОСТЬ

Планы на будущее

1

Развитие проекта



2

Разработка программы обучения, проведение исследований

3

Поиск инвесторов и выход на рынок

Контактная информация

Лаборатория проблем компьютерной безопасности ФГБУН СПИИРАН:

- почтовый адрес (офис): Россия, 199178, Санкт-Петербург, 14-линия В.О., д.39
- телефон: +7(812)328-26-42
- факс: +7(812)328-44-50
- URL: http://comsec.spb.ru

Авторы:

- **Левшун Дмитрий Сергеевич,** levshun@comsec.spb.ru, http://comsec.spb.ru/ru/staff/levshun
- Чечулин Андрей Алексеевич, chechulin@comsec.spb.ru, http://comsec.spb.ru/ru/staff/chechulin
- **Коломеец Максим Вадимович,** kolomeec@comsec.spb.ru, http://comsec.spb.ru/ru/staff/kolomeec
- Котенко Игорь Витальевич, ivkote@comsec.spb.ru, http://comsec.spb.ru/ru/staff/kotenko

Благодарности:

- работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451, 15-37-51126).