Новосибирский государственный университет экономики и управления
кафедра информационной безопасности

Защищенная система удаленного управления аудиторными проекторами и мониторинга их состояния

Лисс Александр Андреевич
Пестунов Андрей Игоревич
Линкевич Николай Александрович
Семенков Алексей Иванович
Клипов Данил Денисович
Медведев Иван Евгеньевич
Пестунова Тамара Михайловна

2016 год

Предпосылки и актуальность проекта

- Во многих социально значимых **учреждениях** наблюдается **стремительный рост** числа устройств с инфракрасным приемником, оснащенных пультами дистанционного управления (ПДУ).
- **Полные функциональные** возможности такого оборудования, как правило, могут быть получены **только через ПДУ**, поэтому при отсутствии доступа к ПДУ устройство зачастую не может быть использовано в штатном режиме.
- Если устройство расположено в **труднодоступном месте** (например, под потолком), то **невозможными** становятся даже **базовые операции**, такие как включение, выключение или регулировка.
- Отсутствие доступа к ПДУ может быть вызвано многими факторами, в частности, его **потерей, поломкой, отсутствием батарей питания** и рядом других причин.
- **Замена недоступного** ПДУ другим, имеющимся в распоряжении, **не всегда возможна** из-за того, что в одной организации могут использоваться несовместимые устройства разных производителей, разных моделей, с разным программным обеспечением и т.д.

Процесс управления состоянием проекторов (на примере НГУЭУ)

- **Аудитории типа 1.** Преподаватель получает пульт у ответственного лица и сдает его после работы.
- **Аудитории типа 2.** Выделенный сотрудник НГУЭУ самостоятельно включает заданные проекторы.

- Подобные способы могут доставлять неудобства и замедлять рабочие процессы.
- Необходимо иметь систему информирования ответственных сотрудников о том, когда включать и выключать проекторы, преподавателям необходимо посещать комнату, где выдаются ПДУ.
- При ручном управлении сложно обеспечивать синхронное переключение каналов на всех устройствах для трансляции служебных или специальных сообщений.
- В ряде случаев требуется послать устройству не команду, а серию команд (сценарий), для того чтобы привести его в заданное состояние (включить, ввести PIN-код, установить разрешение экрана или контрастность.
- При ручном управлении время работы может быть неоптимальным, что приведет к более быстрому износу проектора и необходимости его более частого обслуживания; сложно также узнать, сколько отработала лампа проектора и рассчитать ее оставшийся ресурс.

Задачи проекта

Руководство НГУЭУ поддержало инициативу коллектива авторов по разработке программно-аппаратного комплекса (далее – ПАК-УСВ) для удаленного управления состоянием аудиторных проекторов.

Создание ПАК-УСВ преследует следующие основные задачи:

- повышение оперативности включения/выключения аудиторных проекторов;
- увеличение полезного времени работы проекторов;
- защита от несанкционированного включения аудиторных проекторов;
- автоматизация управления проекторами и мониторинга их состояния;
- резервирование ПДУ на случай поломки, кражи, выхода из строя;
- персонификация сотрудников, использующих проекторы;
- учет времени использования проектором сотрудниками.

Функциональные требования к ролям пользователей ПАК-УСВ

- **Добавление новых проекторов.** Добавляется модель проектора, список доступных команд для этой модели и время задержки между отправкой команд. Формируются сценарии. Добавляется конкретный проектор. Указанием учебного корпуса, аудитории и пользователей, которым разрешено управлять проектором.
- **Управление учетными записями пользователей.**
- **Управление состоянием проекторов через сервер.**
- **Просмотр записей журнала и статистики.** Фильтрацию по определенным критериям (дате, пользователю, конкретному проектору). Просмотр состояния аудиторных проекторов (включен, выключен, неисправен).
- **Управление состоянием проекторов через ПК-ПРО.** Преподаватель, авторизуясь по своему RFID-пропуску, может отправлять доступные сценарии команд проектору.
- **Распределение функциональных возможностей по ролям.**

Распределение функциональных возможностей по ролям

Для комфортной и безопасной работы в ПАК УСВ **четыре** роли пользователей: «Администратор», «Оператор», «Аудитор» и «Преподаватель».

- Администратор, оператор и аудитор – это пользователи серверной части, преподаватель – пользователь компьютера ПК-ПРО.
- **Администратор** обладает всеми функциональными возможностями.
- **Оператор** может управлять состоянием проектором через сервер и просматривать статистику.
- **Аудитор** имеет право на просмотр статистики.
- **Преподаватель** может управлять проекторами через ПК-ПРО.

Требования к надежности ПАК-УСВ

- **Время непрерывной работы** ПК-ПРО и ПАУ должно составлять 144 ч.;
- **Коэффициент надежности сервера** (отношение числа успешных ответов к общему числу ответов) должен составлять не менее 0.8;
- **Время ответа сервера** ПАК-УСВ не должно превышать 2 с;
- ПАУ должно **функционировать 12 ч 7 дней** в неделю согласно учебному расписанию;
- ПАУ **не должно беспричинно отключаться** или посылать сигналы;
- Корпус и крепления ПАУ должны быть **устойчивым к непреднамеренным физическим воздействиям**, так как устройство будет находиться в общедоступном месте (например, в аудитории).

Модель нарушителя

Модель нарушителя основана на базовой модели из руководящего документа гостехкомиссии (документ от 30.03.1992, обновлён 01.12.2014).

- **Защищаемая информация состоит из следующих видов:** хешированные значения номеров карт (на сервере и ПК-ПРО), фамилия и инициалы пользователей (на сервере), соединение между сервером и ПК-ПРО.
- **Первый уровень** в данном случае не актуален, поскольку возможности пользователя ограничены настройками прав доступа в ОС (политика ограниченного запуска ПО в ОС MS Win.).
- Нарушителем **второго уровня** может являться преподаватель или пользователь ПК, который имеет возможность подключения сменных носителей и запуска с них стороннего ПО.
- Нарушителем **третьего уровня** может являться человек, непосредственно ответственный за состояние аудиторных компьютеров и проекторов. На компьютерах в поточных аудиториях у него есть права администратора и возможность физически вмешиваться в работу компьютера.
- Нарушителем **четвертого уровня** может являться администратор домена, т.к. у него фактически неограниченные права.

Список основных актуальных угроз ПАК УСВ

Угроза	Объект воздействия	Последствия	Способ противодействия (защиты)
1. Чтение конфигурационных файлов ПАК УСВ	ПК-ПРО	Выявление параметров системы	Настройка списков доступа и аудита Организационные меры
2. Изменение конфигурационных файлов ПАК УСВ	ПК-ПРО	Нарушение работы конкретного ПК-ПРО	Настройка списков доступа и аудита Организационные меры
3. Подмена ПО	ПК-ПРО	Нарушение работы конкретного ПК-ПРО	Настройка списков доступа и аудита Организационные меры
4. Попытка перехвата трафика между сервером и клиентом	ПК-ПРО, сервер ПАК УСВ	Несанкционированные действия с проекторами	Передача номеров карт в хешированном виде. Использование SSL TLS 1.2
5. Изменение данных на сервере ПАК УСВ вплоть до полного уничтожения всех баз данных	Сервер ПАК УСВ	Вывод из строя ПАК УСВ	Организационные меры Ведение журнала действий в ОС Регулярное резервное копирование ОС
6. Запуск вредоносного ПО	ПК-ПРО	Вывод из строя ПАК УСВ	Поддержание антивирусного ПО в актуальном состоянии

Общая схема ПАК-УСВ

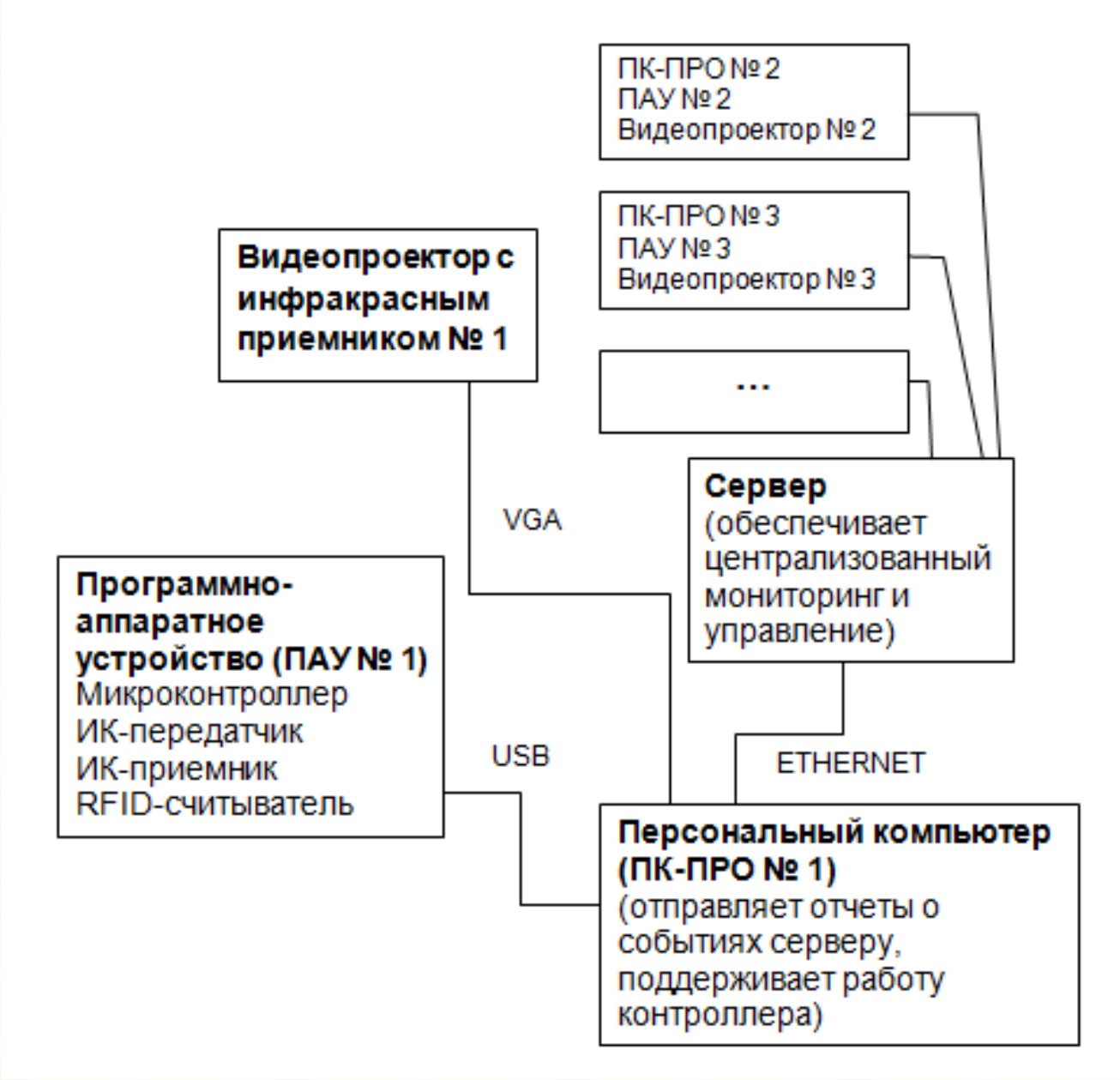
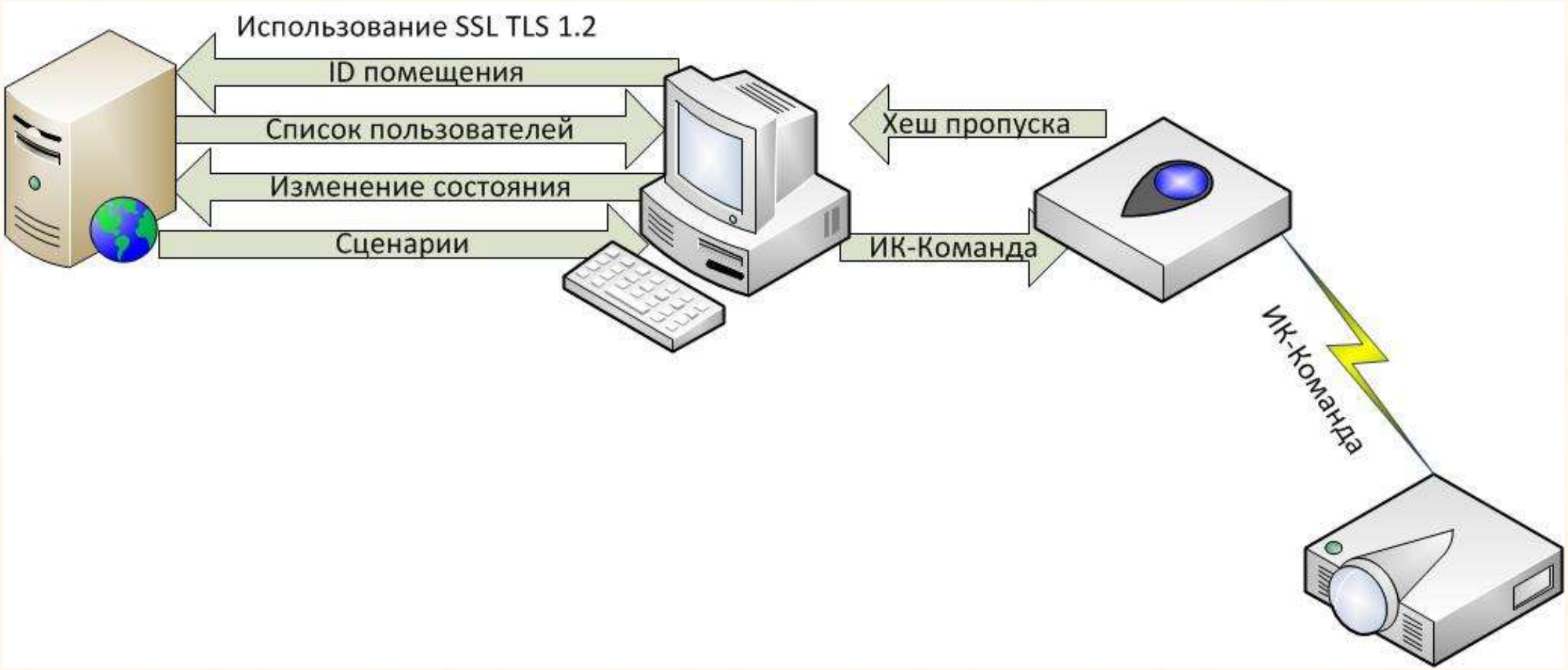
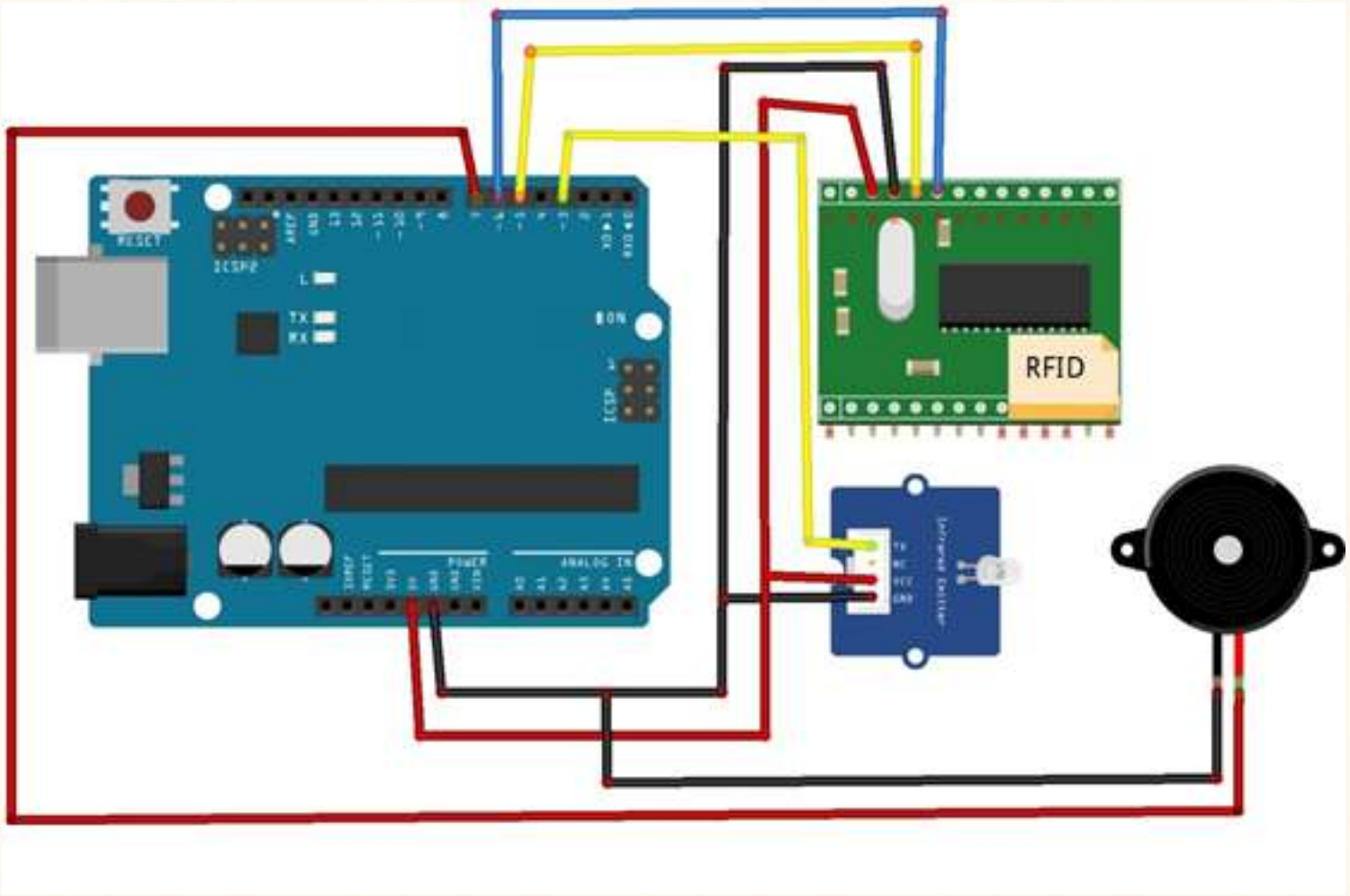


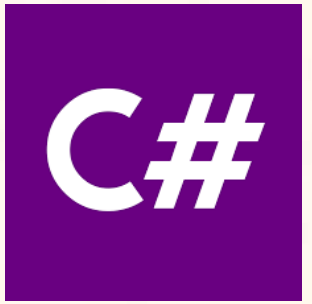
Схема бизнес-процессов ПАК-УСВ



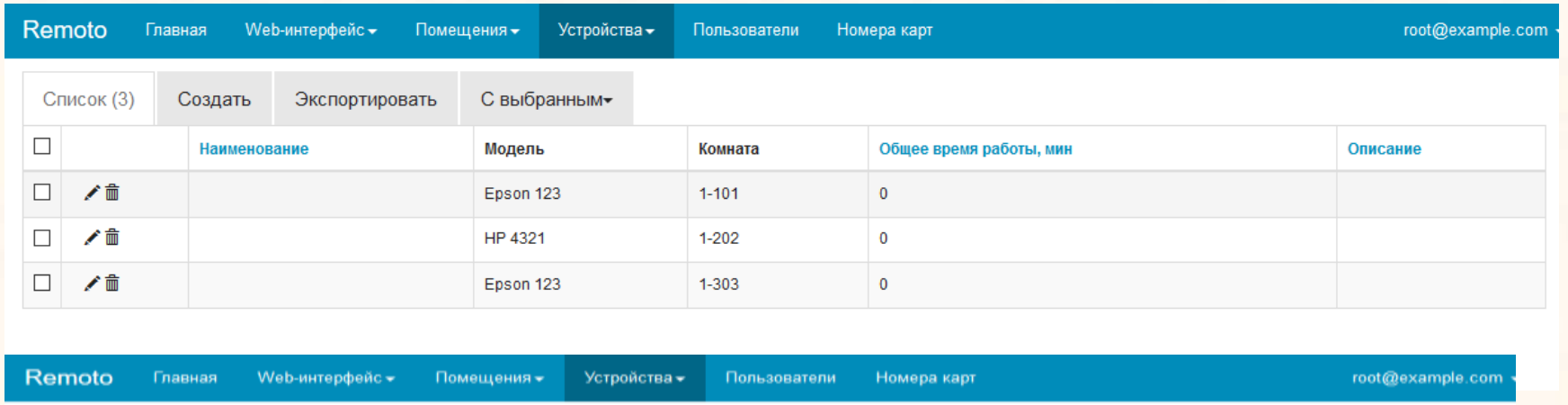
Компонентная схема ПАУ

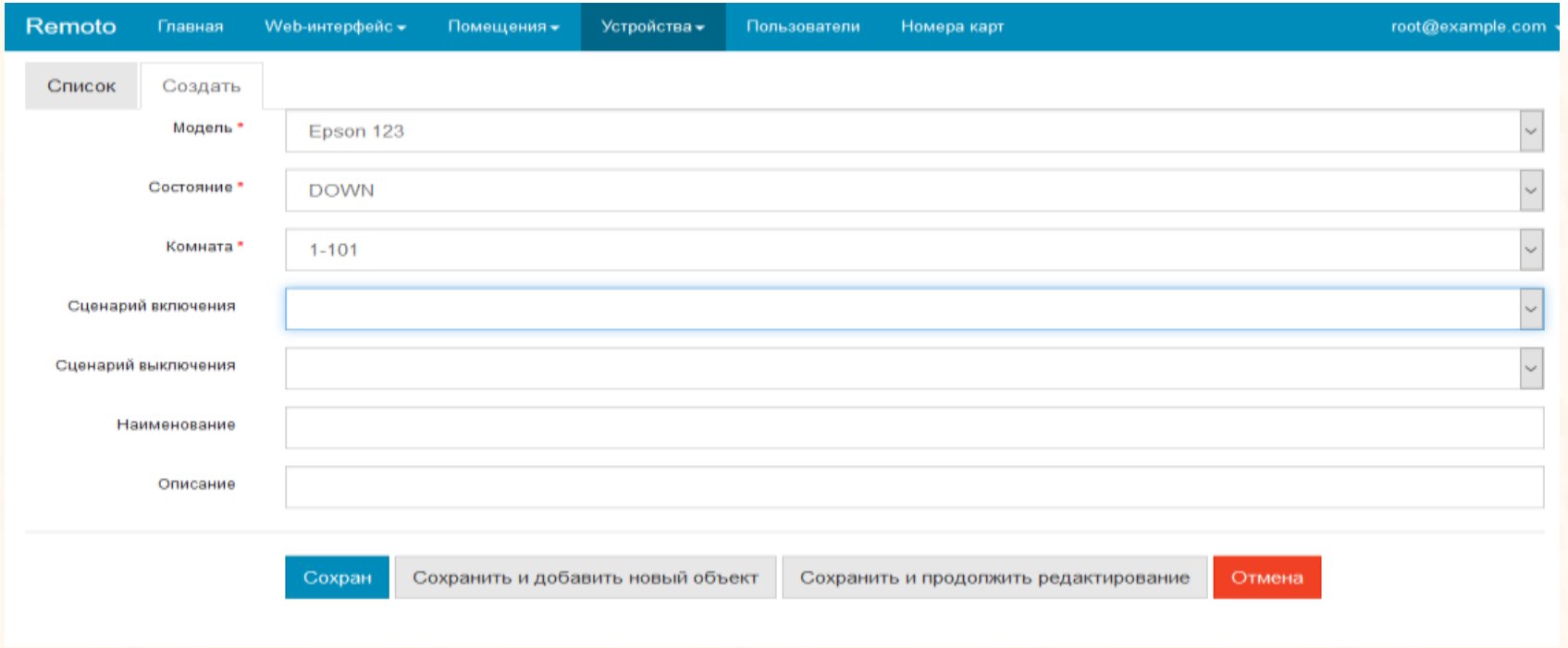


Технологии для реализации программного обеспечения

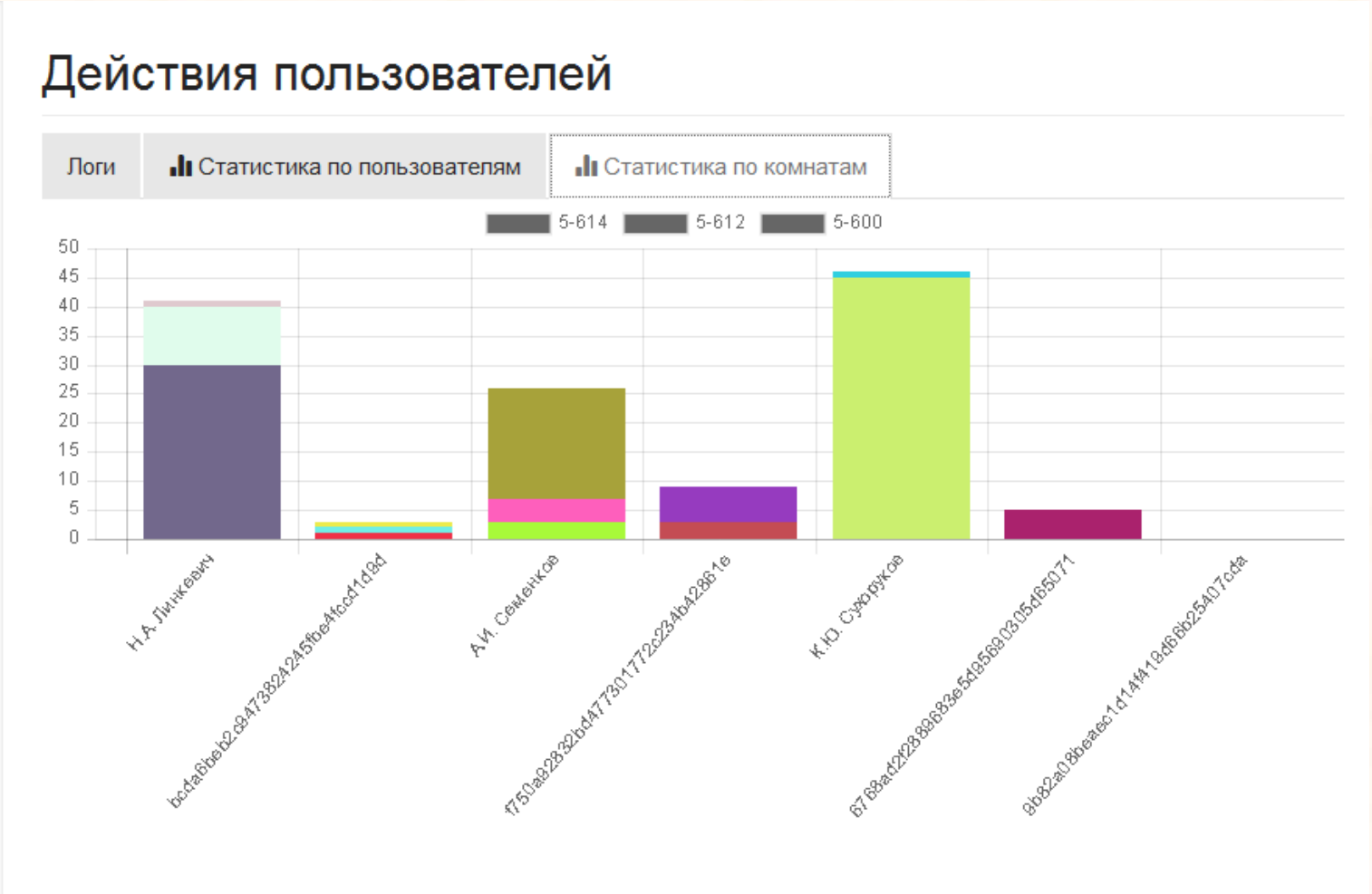


Интерфейс администратора

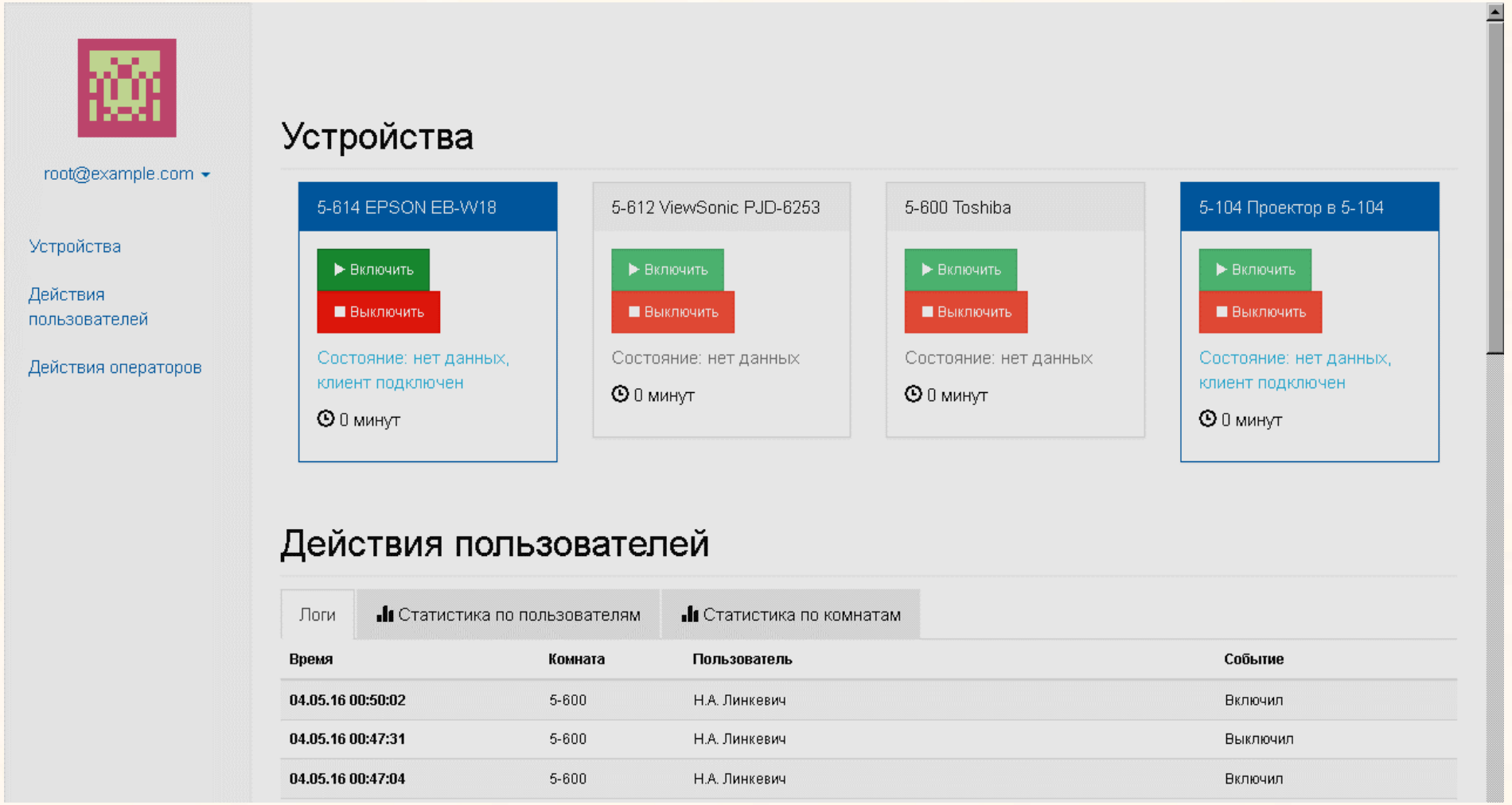




Пример сформированного отчета



Web-интерфейс серверного приложения



Заключение

- В ходе разработки представленного программно-аппаратного комплекса студенты четвертого курса (на тот момент) НГУЭУ Н. А. Линкевич (направление бакалавриата «Информационная безопасность», профиль «Информационная безопасность») и А. И. Семенков (направление бакалавриата «Фундаментальная информатика и информационные технологии», профиль «Инженерия программного обеспечения») **подготовили свои выпускные квалификационные работы**.

- Проект по разработке программно-аппаратного комплекса ПАК-УСВ может служить **примером реализации проектного обучения в вузе**.

- Существует принципиальная **возможность расширения** разработанного комплекса посредством добавления в него функциональности по управлению другими устройствами.

Спасибо за внимание

Доклад представлял:

Лисс Александр

(ведущий инженер лаб. компьютерной и сетевой безопасности кафедры информационной безопасности НГУЭУ)