

Мирсаитов Сергей Фаритович

канд. техн. наук, доцент, доцент

Коротких Алексей Владимирович

магистрант

Чернышова Оксана Александровна

магистрант

ФГБОУ ВО «Московский технологический университет»

г. Москва

АЛЬТЕРНАТИВНЫЙ ПОДХОД В ОРГАНИЗАЦИИ МНОГОУРОВНЕВОЙ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

Аннотация: статья посвящена альтернативному подходу в организации многоуровневой системы контроля доступа. Авторы приводят пример решения реализации многоуровневой системы контроля с созданием локальной схемы подсетей и системы в целом. В данной статье не затрагиваются вопросы обучения.

Ключевые слова: контроль доступом, многоуровневая система.

Для организации системы контроля доступа применяется, как правило, многоуровневая система. Помимо системы контроля доступа, контролируемый периметр оснащается системой видеонаблюдения, которая как правило интегрирована в систему.

Первой задачей многоуровневой системы контроля и управления доступом (СКУД) является – контроль доступа в контролируемый периметр первого уровня доступа, а так же контроль для входа в отдельные помещения первого уровня доступа. Если организация обладает парковкой, то добавляется система контроля парковки (турникеты, шлагбаумы).

Возможен вариант, когда каждый турникет входа оснащен считывателями для учета рабочего времени сотрудников. Предполагается, что данная система поддерживает функцию Antipassback (или запрет повторного прохода) – это функциональная возможность системы, исключающая проход по одной карточке

двух сотрудников, или проход без использования карточки. Благодаря этому, мы решим задачу получать точные данные о времени прихода и ухода сотрудников.

Второй задачей многоуровневой системы контроля доступа – контроль доступа в контролируемый периметр второго (n-уровня) уровня – доступ в особо важные помещения контролируемого периметра с использованием технологий:

- организация доступа при условии: ключ Touch Memory + Pin код и карта;
- доступ по двум картам (войти могут только два человека, встретившись вместе).

Для доступа могут использоваться две эти технологии многоуровневого метода, при этом предполагается что, вход в помещение 1 будет использоваться метод по двум картам одна из, которых является главной. Доступ в помещение 2 будет осуществлять с помощью ключа Touch Memory + Pin код и карта. Для повышения уровня защиты возможно (по определенному временному алгоритму) изменение кодов ключа Touch Memory и Pin кода.

Так же предполагается, что контролируемый периметр будет оснащен системой видеонаблюдением. Данная задача решается установкой по всему контролируемому периметру камер видеонаблюдения с программным распознаванием образов с интеграцией в СКУД.

Вариант многоуровневой системы контроля приведен на рисунке 1.

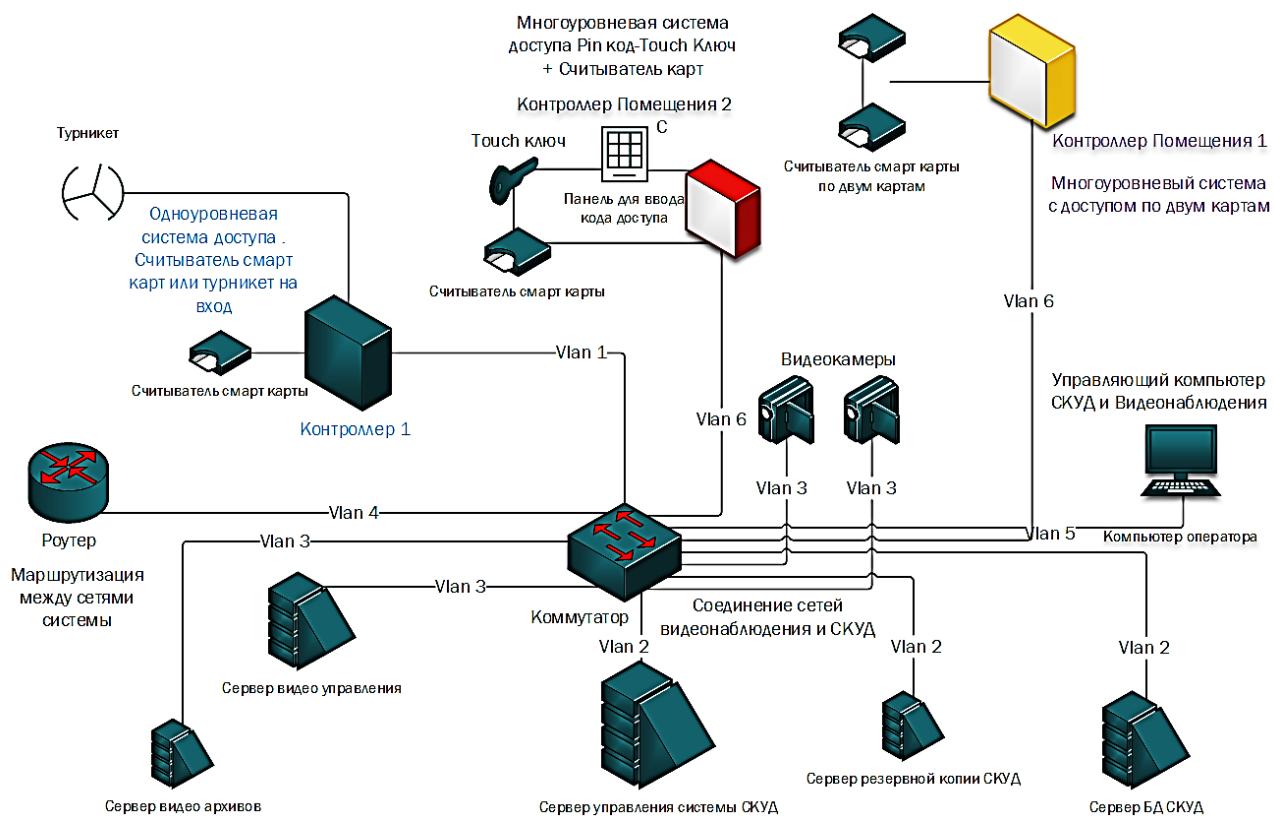


Рис. 1. Системы контроля и управления доступом и видеонаблюдения

На рисунке 1, изображена схема системы локальных виртуальных подсетей системы контроля и управления доступом и видеонаблюдения. Данная система находится в собственной (без подключения к общественным) сети для обеспечения безопасности системы от внешнего проникновения. На схеме изображены сервера для управления, и хранения данных. Коммутатор отвечает за соединение подсетей системы контроля и управления доступом и видеонаблюдения, роутер отвечает за маршрутизацию между сетями системы. Контроллер 1 отвечает за доступ в контролируемый периметр первого уровня доступа. Контроллер помещений 2 обеспечивают доступ в помещения с усиленным контролем доступа. Управляющий компьютер СКУД отвечает за управление системой контроля и управления доступом, а так же управлением системой видеонаблюдения.

Система контроллеров помещений 1, 2 была смоделирована на платформе Arduino Uno, с датчиками:

- arduino Ethernet Shield Rev3 безPoE;
- считыватель RFIDRC522;

- считыватель Touch Memory DS9002;
- эластичная клавиатура 4x4 кнопки.

Верификация предлагаемого подхода построения СКУД показала, что достоинством подхода является разделение участков виртуальной локальной подсети, что позволяет разделить права доступа и уменьшить вероятность проникновения в систему. Данный подход позволяет создать многообразие любых вариантов построения многоуровневой системы защиты, исходя из конкретных требований.

Недостатком предлагаемого подхода в организации СКУД является необходимость создания уникального кода системы для каждого типа используемого контроллера.

Список литературы

1. Jonathan Oxer, Hugh Blemings, Practical Arduino. Technology in action. – С. 269–278.
2. Michael Margolis, Arduino Cookbook. O’REILLY. – С. 187–190, С. 451–466.
3. Victor Olifer, Natalia Olifer, Компьютерные сети.
4. Ulli Sommer, Программирование микроконтроллерных плат Arduino/Freeduino. – С. 52–78.