**4. Системы контроля и управления доступом**

**Система контроля и управления доступом (СКУД)** – совокупность совместно действующих средств (механических, электромеханических, электрических, электронных), обеспечивающих контроль и управление доступом и обладающих технической, информационной, программной и эксплуатационной совместимостью, предназначенных для ограничения и санкционирования перемещения людей, предметов, транспорта в помещениях, зданиях, сооружениях и по территории охраняемых объектов.

|  |
| --- |
| Безымянный  Рисунок 4.13. – Структурная схема системы видеонаблюдения |

**Идентификатор** – уникальный признак субъекта доступа.

**Устройство ввода идентификационных признаков (УВИП)** – электронные устройства для ввода идентификатора.

**Устройство управления** – устанавливают режим доступа и обеспечивают прием и обработку информации с УВИП, управление УПУ, отображение и регистрацию информации.

**Управляемые преграждающие устройства (УПУ)** – обеспечивающие физическое препятствие доступу людей, транспорта и других объектов.

**Виды идентификаторов**

**Пароль** - последовательность символов, известная только одному человеку, вводимая вручную;

**Устройство** - малогабаритное техническое средство, содержащее последовательность символов, вводимых контактным или бесконтактным способом;

**Биометрия** - физиологические или поведенческие характеристики человека вводимые контактным или бесконтактным способом.

**Способы ввода идентификатора**

* Ручной – ввод идентификатора субъектом путем набора пароля на клавиатуре;
* Контактный – использование устройства аутентификации (touch memory, карта с магнитной полосой и т.д.);
* Бесконтактный (RFID, proximity устройства и т.д.).

По способу управления преграждающими устройствами (дверьми, турникетами, шлюзами и т.д.) все системы можно классифицировать следующим образом:

* автономные (локальные) — для управления одним или несколькими преграждающими устройствами, без передачи информации на центральный пульт и без контроля со стороны оператора;
* централизованные (сетевые) — для управления преграждающими устройствами с обменом информацией с центральным пультом, контролем и управлением системой со стороны оператора;
* универсальные, включающие функции как автономных, так и сетевых систем, работающие в сетевом режиме под руководством центрального устройства управления и переходящие в автономный режим при возникновении отказов в сетевом оборудовании или центральном устройстве.

По количеству точек доступа и пользователей СКУД можно подразделять на:

* малые — единица точек доступа (офисы);
* средние — десятки точек доступа и тысячи пользователей (банки, предприятия, учреждения, гостиницы);
* большие — сотни точек доступа и десятки тысяч пользователей (крупные промышленные предприятия, аэропорты).

Автономные системы предназначены для обеспечения контроля и управления доступом в отдельное помещение (рисунок 4.13).

|  |
| --- |
| skd1  Рисунок 4.13. - Структурная схема автономной СКУД |

Такая система состоит из автономного контроллера, хранящего в себе базу данных идентификаторов и управляющего работой остальных элементов системы. В качестве исполнительного устройства используется электромагнитный замок, либо защелка. Для идентификации пользователя используются различные типы карт с соответствующими считывателями (магнитные, Proximity, штриховые). Контроллер работает, как правило, с одним считывателем на вход (считыватель на выход используется лишь в особо важных помещениях); для открытия замка изнутри помещения обычно используется либо кнопка, либо датчик-коммутатор движения. Для обеспечения правильности работы всей системы используется датчик положения двери.

Для обеспечения нормального режима работы системы контроля доступа, дверь оснащается доводчиком, а контроллер — резервным источником питания.

Типичным примером автономного контроллера является контроллер обеспечивающий работу с одним считывателем Proximity карточки или Touch Memory считывателем, позволяющий обеспечить автономный контроль за доступом в отдельное помещение.

Автономные системы с накоплением информации, выполняют те же задачи, что и системы описанные выше. Единственным отличием является возможность системы накапливать информацию обо всех проходах через точку прохода (дверь, турникет) — время, дата, идентификационный номер. Данная информация хранится в памяти контролера и может быть по необходимости востребована. Для получения информации и представления её в наглядном виде используется специальное программное обеспечение (ПО). ПО позволяет оператору системы решать задачи: отслеживания перемещения сотрудников по территории, учета рабочего времени сотрудников, визуально контролировать личность владельца Proximity карточки или брелка Touch Memory.

Характерным примером данной системы служит контролер с программным обеспечением. Контролеры являются переходным звеном к сетевым системам, так как, могут они объединятся в единую сеть, для получения накопленных данных от многих точек прохода.

|  |
| --- |
| skd2  Рисунок 4.14. - Автономная СКУД с накоплением информации |

Сетевые системы предназначены для обеспечения контроля и управления доступом на крупных объектах (банки, учреждения, предприятия и т.п.).

Выделяют четыре характерных типа точек доступа, где может быть применен контроль:

* проходные;
* офисные помещения;
* помещения с повышенным уровнем безопасности;
* объекты на улице (ворота, шлагбаумы для автостоянок и т.д.).

|  |
| --- |
| skd3  Рисунок 4.15. Сетевая СКУД |

Управляемые преграждающие устройства (турникеты) могут быть полуростового типа, реже используются турникеты с перекрытием проема в полный рост. Турникеты в большинстве своем не обеспечивают физического препятствия для проникновения, а служат только для упорядочивания потока людей и помогают службе охраны контролировать вход на объект. Таким образом, основная их задача — ограничить возможность прохода нескольких человек по одному допуску (идентификатору). Турникеты могут быть оборудованы средствами сигнализации, срабатывающими при попытках обхода. Шлюзы или кабины относятся к преграждающим устройствам блокирующего типа. Они могут при необходимости сдержать человека в точке доступа. Шлюзы применяются на объектах с повышенным уровнем безопасности. При этом они часто оснащаются дополнительными средствами контроля (металлодетекторами, детекторами взрывчатых и радиоактивных веществ и т.п.). На проходных может возникнуть потребность в телевизионном контроле. При этом ввод кода, или считывание идентификатора пользователя, сопровождается вводом изображений из базы данных и с телекамеры на монитор охранника, (режим видеоидентификации), который производит их равнение.

Основной особенностью построения СКУД на больших объектах, является организация нескольких автоматизированных рабочих мест (АРМ) на базе персональных компьютеров, объединенных в локальную компьютерную сеть. Весь персонал, обслуживающий СКУД, имеет доступ к единой базе данных, находящейся на сервере системы. Такие системы обычно содержат АРМы: «проходная» (с возможностью видеоидентификации), бюро пропусков, администратор, дежурный службы безопасности. В системе используется несколько сетей контроллеров, каждая из которых подключается к территориально ближайшему компьютеру, но управление всей системой может осуществляться с любого рабочего места при наличии соответствующих прав у оператора.

Построенная по такой схеме СКУД может обеспечить централизованное управление на объекте, содержащем несколько зданий, значительно удаленных друг от друга.

|  |
| --- |
| skd4  Рисунок 4.16. Сетевая СКУД большого объекта |