Система контроля и управления доступом (СКУД).

1.1. СКУД. Понятие. Основные задачи.

СКУД- совокупность совместимых между собой аппаратных и программных средств, направленных на ограничение и регистрацию доступа людей, транспорта и других объектов в(из) помещения, здания, зоны и территории.

Существует много задач, решаемых с помощью СКУД.

Типовые задачи, решаемые с помощью систем контроля доступа

- идентификация сотрудников, входящих на территорию (в здание) компании и/или покидающих офис;
- регистрация, учет и контроль посетителей на предприятии;
- разграничение доступа в помещения (зоны) усиленной защиты (производственные участки, хранилища материальных ценностей и т.п.);
- организация прохода к ячейкам депозитариев, сейфам и т.д. с обеспечением доступа к ним только при одновременном подтверждении своих полномочий несколькими независимыми лицами (сотрудник банка и его клиент, офицер безопасности и работник функционального подразделения);

- защита квартир, частных владений, апартаментов, гостиничных номеров от проникновения нежелательных лиц;
- распознавание посетителей торговых и развлекательных центров с дальнейшей дифференциацией их обслуживания (привилегии постоянным клиентам, недопущение прохода ранее выявленных нарушителей, предотвращение продаж алкоголя несовершеннолетним и т.п.).

1.2. Основные компоненты СКУД

Идентификатор - определенное устройство или личный физический признак, по которому система может определить пользователя.

Считыватель - устройство, которое считывает информацию с идентификатора и передает ее в контроллер СКУД.

Контроллер - устройство, предназначенное для обработки информации со считывателей идентификаторов и принятия решения, пропустить или нет данного пользователя в данную дверь.

Исполнительные (преграждающие) устройства - турникеты, двери оборудованные управляемыми замками, ворота, шлагбаумы, шлюзы.

А также:

Программное обеспечение - необязательный элемент, позволяющий осуществлять централизованное управление контроллерами СКУД с персонального компьютера (ПК), формирование отчетов, разнообразные дополнительные функции.

Конверторы - для соединения аппаратных модулей СКУД и ПК.

Вспомогательное оборудование - блоки питания, кнопки, соединительные провода.

Линии связи - проводная, кабельная, волоконно-оптическая, радиосвязь.

1.3. Основные принципы функционирования СКУД.

Для сотрудников, посетителей и клиентов компании изготавливается электронный ключ (идентификатор) в виде пластиковой карты или брелка с индивидуальным кодом. Картотеки организуются в виде электронных баз данных, в которых идентификатор связывается с персональной информацией.

Считыватели устанавливаются либо у входа в здание, либо у входа в помещения, доступ к которым ограничен. Система сопоставляет полученную от считывателя информацию и ситуацию, при которой эта информация поступила и отправляет разрешающий либо запрещающий сигнал на исполнительное устройство, в результате замки (двери, турникеты) открываются либо блокируются. Также система может активировать функцию перехода помещения в режим охраны, тревоги и т.п.

Каждый факт активизации считывателя (предъявления идентификаторов) фиксируется в контроллере и ведется история, обычно сохраняющаяся на жестком диске в компьютере в виде, позволяющем с помощью специального программного обеспечения получать необходимую информацию – отчёты о учете рабочего времени, нарушениях трудовой дисциплины и других.

1.4Основные характеристики СКУД. Классификации.

Основными характеристиками СКУД можно назвать:

- Стоимость;
- Надежность функционирования;
- Быстродействие;
- Время регистрации пользователя;
- Емкость памяти;
- Устойчивость к злонамеренным действиям;

А также такие важные показатели как:

- Вероятность ошибочного отклонения законного пользователя (ошибки 1-го рода);
- Вероятность ошибочного предоставления доступа незаконному пользователю (ошибки 2-го рода).

Классифицировать системы контроля доступа можно по многим признакам. Например:

По идентификаторам, используемым в системе:

- *механические* - идентификационные признаки представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);
- *магнитные* - идентификационные признаки представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т. д.);
- *оптические* - идентификационные признаки представляют собой нанесенные на поверхности или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении, помогающие осуществлять контроль доступа к охраняемому объекту (карты со штриховым кодом, голографические метки и т. д.);
- *электронные* - идентификационные признаки представляют собой электронный код , записанный в микросхеме идентификатора (дистанционные карты, электронные ключи и т. д.);
- *акустические* - идентификационные признаки представляют собой кодированный акустический сигнал;
- *биометрические* - идентификационные признаки для биометрических устройств представляют собой индивидуальные физические признаки человека (отпечатки пальцев, геометрия ладони, рисунок сетчатки глаза, голос, динамика подписи и т.д.);
- *комбинированные* - для идентификации используются одновременно несколько идентификационных признаков.

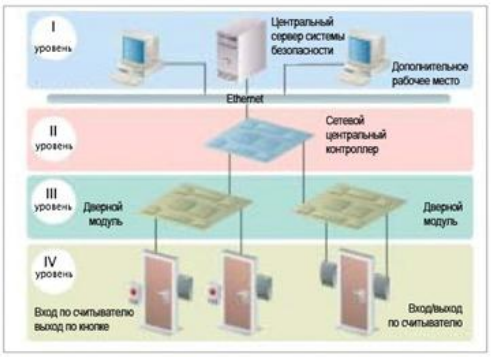
По способу управления системой контроля доступа:

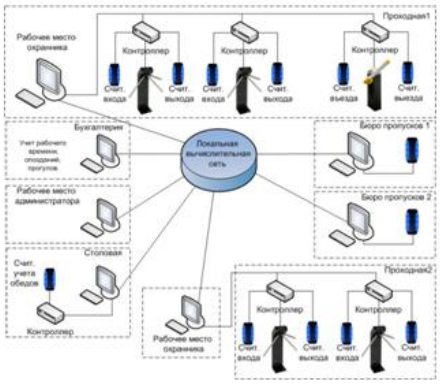
- *автономные* - для управления одним или несколькими управляемыми преграждающими устройствами без передачи информации на центральный пульт и без контроля со стороны оператора;
- *централизованные (сетевые)* - для управления управляемыми преграждающими устройствами с обменом информацией с центральным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

Автономные

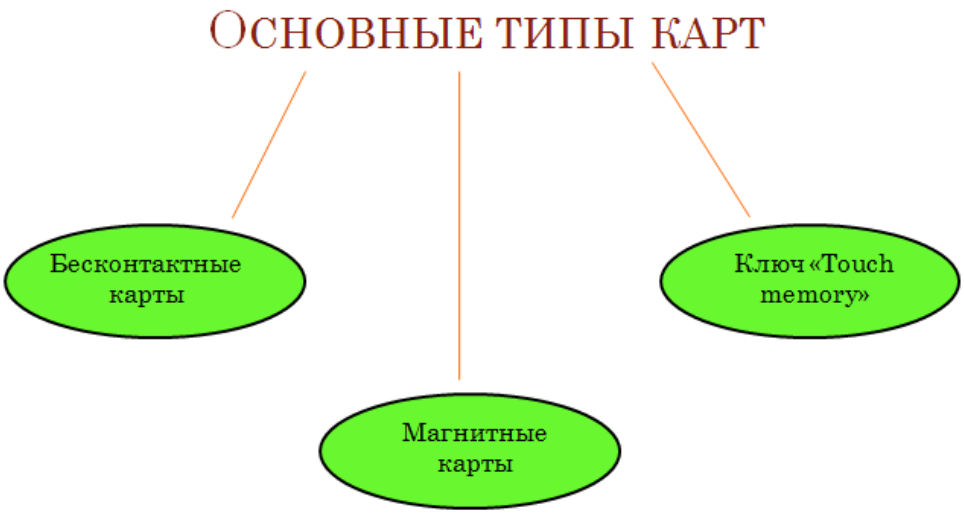
Централизованные (сетевые)

Универсальные

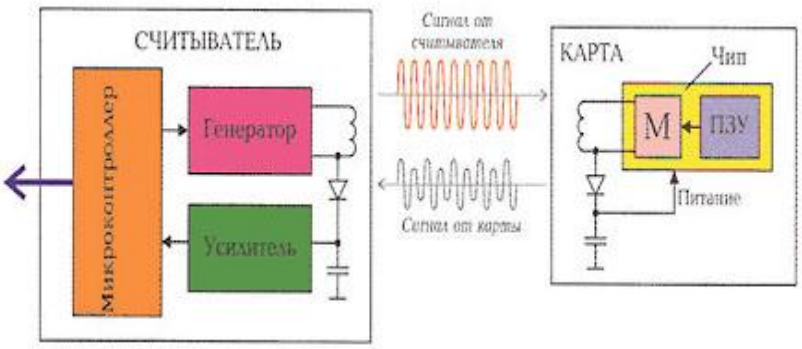




2.1 Идентификаторы. Магнитные карты



Наиболее перспективными на сегодняшний день типами карт считаются **бесконтакнтые радиочастотные карты – PROXIMITY.** Они работают на расстоянии, при нетребовательности к чёткому позиционированию объекта, поэтому их использование достаточно стабильно, удобно и эффективно. Принцип работы достаточно прост .



Считыватель содержит генератор, который записывает антенну считывателя. Излучаемая антенной считывателя энергия принимается антенной карты и используется для питания микросхемы

(чип), которая при появлении питания с помощью модулятора (М) начинает модулировать сигнал считывателя кодом, записанным в постоянном запоминающем устройстве (ПЗУ) карты.

Модулированный сигнал в считывателе детектируется, усиливается и поступает на микроконтроллер, который преобразует принятый от карты сигнал к виду, удобному для передачи на внешнее устройство, к которому подключен считыватель.

Магнитные карты. В магнитном слое располагаются отрезки проволоки из сплава и именно они несут информацию при перемещении вдоль считывающей головки. Такие карты имеют меньшую изнашиваемость, однако есть у них и минус, ограничивающий применение – код в карту нельзя поменять, он вносится при изготовлении карты раз и навсегда. Существуют также штрих-кодовые карты, где штрих-код виден, либо закрыт материалом, прозрачным только в инфракрасном свете.

Ещё одним типом карт, получившим широкое распространение, является **ключ-брелок «Touch memory».** Обычно он выглядит как металлическая таблетка, в которой монтируется чип ПЗУ. Для активизации ключа необходимо приложить таблетку плоской поверхностью к считывателю. В этот миг посылается уникальный код идентификатора. Эти виды карт удобны тем, что одна и та же «таблетка» может открывать не одну дверь, а несколько.

2.2 Идентификаторы. Биометрия. Особенности. Типы.

Системы контроля доступа с применением биометрической идентификации имеют ряд преимуществ:

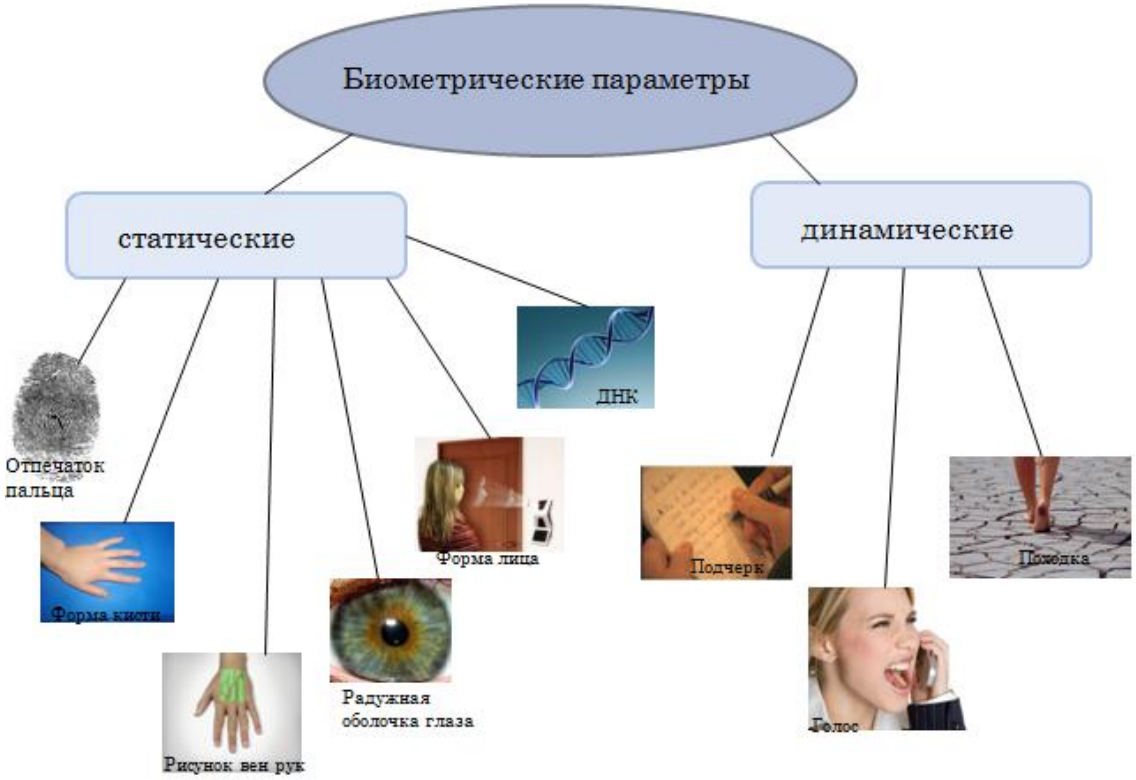
- Безопасность. Самое важное свойство биометрии - это возможность идентифицировать именно личность человека. Биометрические идентификаторы нельзя передать или похитить.

- Удобство. Обязательно, определенный процент сотрудников забывает или теряет карточки для входа в офис и тратит и свое время, и время секретарей или службы охраны на организацию своего доступа. С биометрическими идентификаторами такого не может случиться.

- Имидж. Помимо прочего, внедрение биометрических технологий с использованием преимуществ системы и соответственно с извлечением пользы создает компании дополнительный технологический и современный имидж.

Особенности

- Скорость работы биометрических терминалов, совмещение в них считывателя с контроллером, в основном зависит от мощности процессора.
- Необходимо принимать во внимание особенности биометрического распознавания:
    - Вероятностный характер распознавания: FAR (коэффициент ложного пропуска, вероятность ложной идентификации); FRR (коэффициент ложного отказа доступа — вероятность того, что система биоидентификации не признает подлинность отпечатка пальца зарегистрированного в ней пользователя);
    - Требования к производительности: например скорость считывания.
- Больший объем данных в системе



На схеме приведены биометрические параметры, которые могут быть использованы в системах распознавания (системах идентификации). Параметры можно подразделить на статические и динамические. Примерами статических является отпечатки пальцев, форма лица, форма кисти, радужная оболочка глаза. Примерами динамических –походка, подчерк, голос.

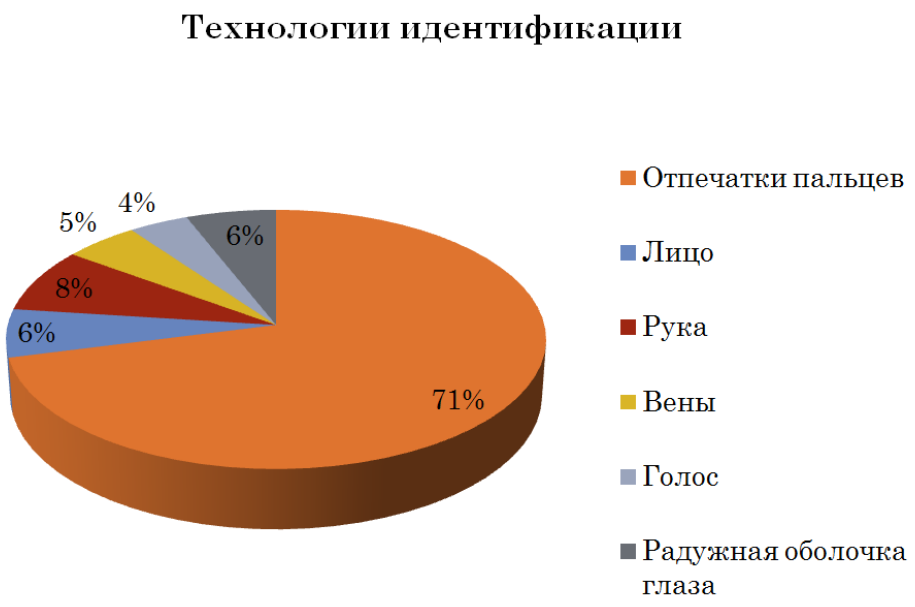
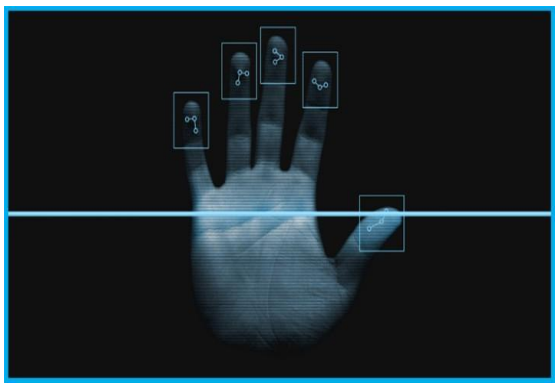


Диаграмма. Процентное соотношение биометрических параметров в зависимости от их использования в системах распознавания.

2.3 Идентификаторы. Биометрия. Методы защиты от имитации и ошибок пользователей.



Очевидно что при всех своих преимуществах использование биометрической информации автоматически не гарантирует абсолютную надежность системы контроля доступа. Существует определенная вероятность задействования злоумышленниками биометрических имитаторов для «обмана» БиоСКУД. Например, муляжи пальцев с нанесенным рисунком отпечатка, цветные фотографии лица.

Современные БиоСКУД имеют средства защиты от подобных биоимитаторов. Вот некоторые из них:

- Измерение температуры (пальца, ладони);
- Измерение электрических потенциалов (пальца);
- Измерение наличия кровотока (ладони, пальцы);
- Сканирование внутренних параметров (рисунок вен рук);
- Использование трехмерной модели (лица).

3. Распределенные системы контроля управления доступом

Еще несколько лет назад основной функцией СКД являлась задача по управлению доступом в рамках одного здания. С развитием экономики страны и появлением необходимости централизованного управления СКД у крупных распределенных организаций сформировались новые требования к СКД, которые можно объединить и назвать требованиями к распределенным системам контроля доступа.

Один из вариантов построения СКУД территориально-распределенного предприятия – это **использование единой базы данных, содержащей информацию об объектах, сотрудниках и правах доступа**.

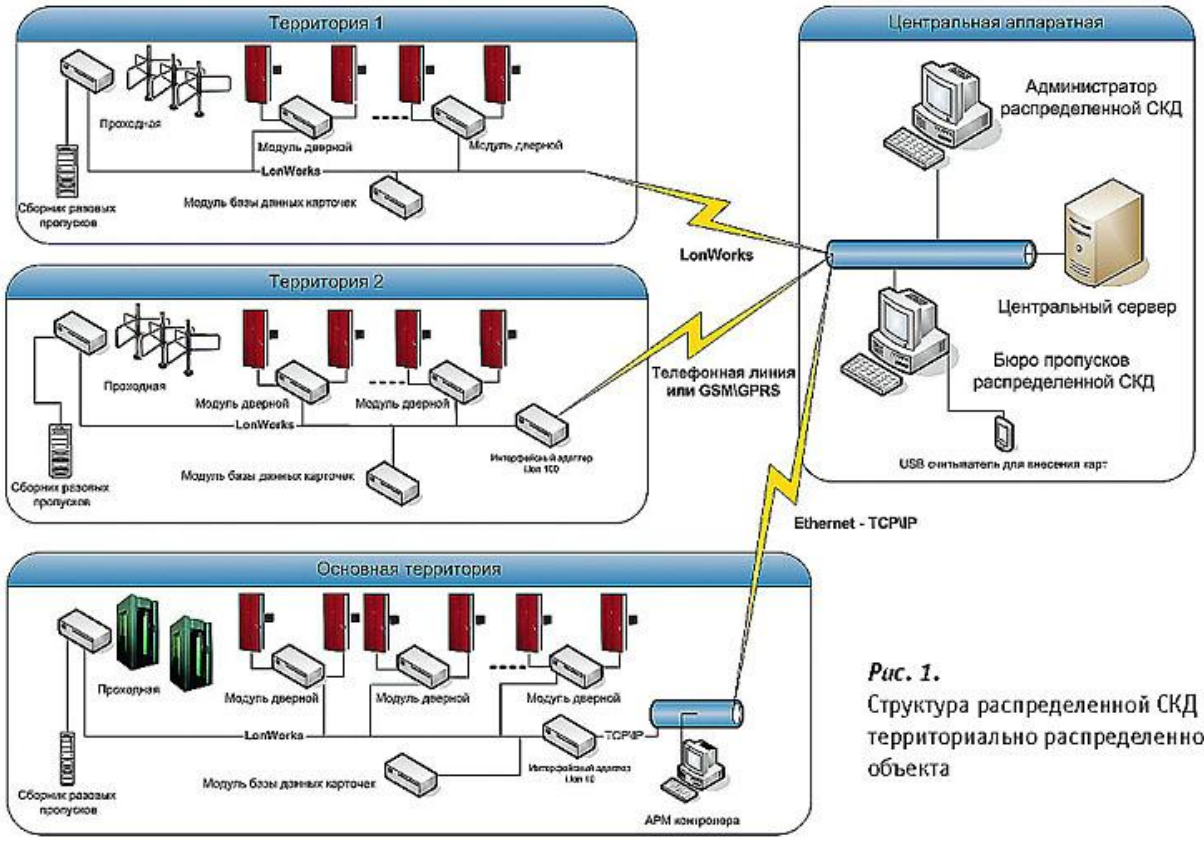


Рис. 1.
Структура распределенной СКД территориально распределенного объекта

Кроме того, есть вариант использования множества баз данных и серверов системы, обменивающихся информацией (синхронизирующихся) между собой.

В чем плюсы такого подхода?

- Обеспечивается возможность централизованного управления и мониторинга состояния пропускного режима на всех объектах компании.
- Полностью сохраняется пропускной функционал проходной при отсутствии связи с центром обработки данных, в котором находится сервер базы данных.
- Используется оптимальный состав эксплуатируемого оборудования.
- Обеспечивается высокая степень масштабируемости системы при изменении количества и (или) местонахождения объектов и эксплуатируемого оборудования.

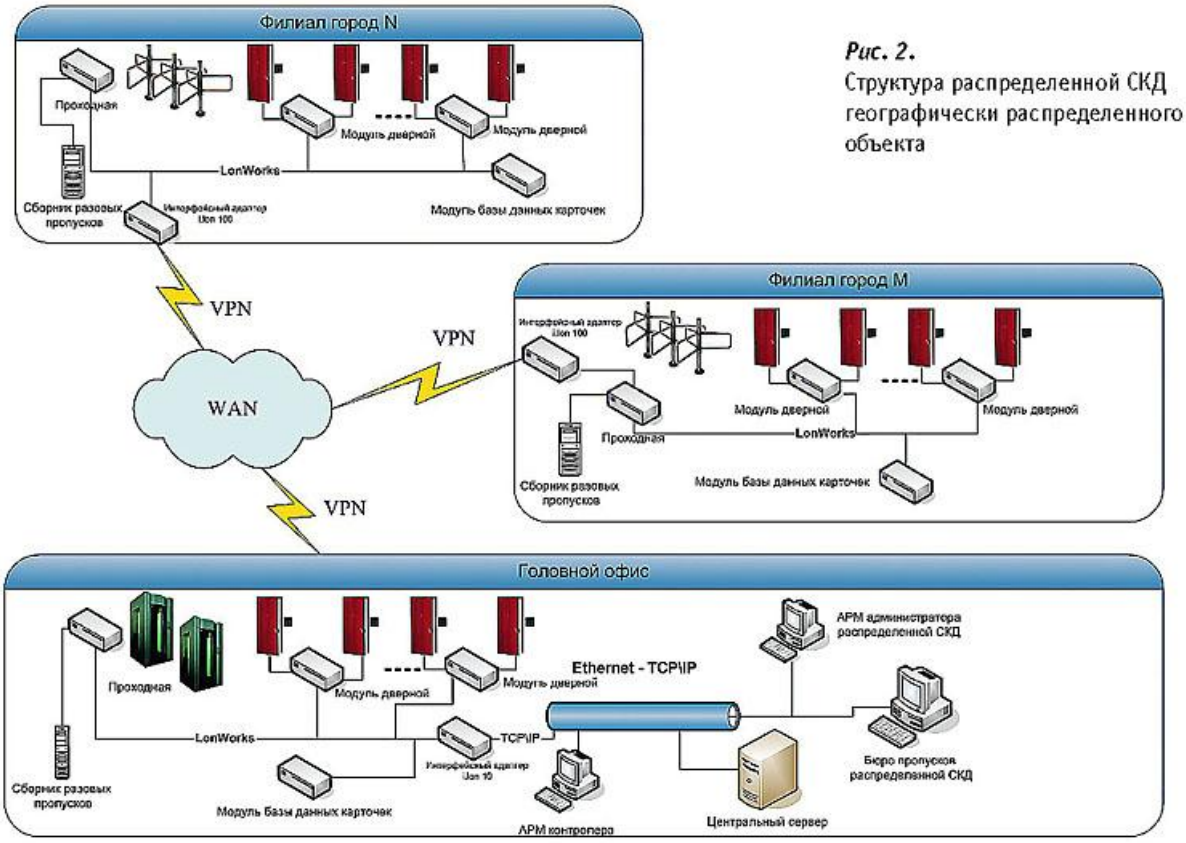


Рис. 2.
Структура распределенной СКД географически распределенного объекта

В установке географически-распределенных систем контроля доступа нуждаются такие типы организация, как то:

- большие торговые сети;
- аэропорты и морские порты;
- организации с разветвленной филиальной сетью и другими территориально разбросанными пунктами организации технологического процесса;
- предприятия, занимающиеся транспортировкой энергоресурсов (газо- и нефтепроводы и т.п.);
- крупные промышленные предприятия.

Один из способов централизованной работы такой системы – это передача данных через интернет.

Нормативные документы

- ГОСТ Р 51241-98 "Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. "
- Р 78.36.005-99 "Выбор и применение систем контроля и управления доступом"