

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ (СКУД)



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.



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.).

ОСНОВНЫЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ СКУД.



ОСНОВНЫЕ ХАРАКТЕРИСТИКИ СКУД

- Стоимость;
- Надежность функционирования;
- Быстродействие;
- Время регистрации пользователя;
- Емкость памяти;
- Устойчивость к злонамеренным действиям;
- Вероятность ошибочного отклонения законного пользователя (ошибки 1-го рода);
- Вероятность ошибочного предоставления доступа незаконному пользователю (ошибки 2-го рода).

ОСНОВНЫЕ КОМПОНЕНТЫ СКУД

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



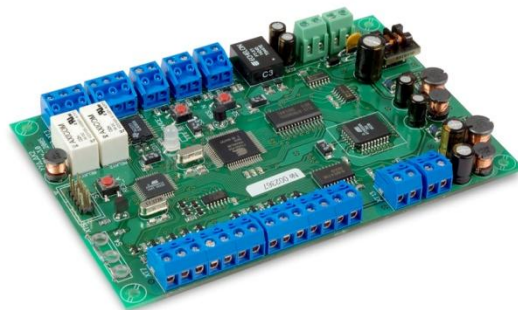


- **Считыватель** - устройство, которое считывает информацию с идентификатора и передает ее в контроллер СКУД.





▣ **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:

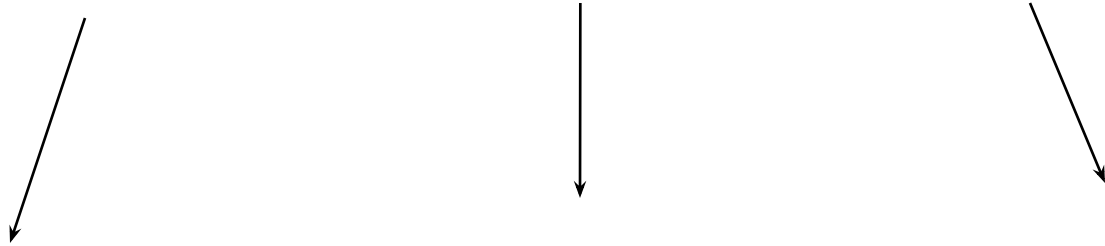
- ▣ **Программное обеспечение** - необязательный элемент, позволяющий осуществлять централизованное управление контроллерами СКУД с персонального компьютера (ПК), формирование отчетов, разнообразные дополнительные функции.
- ▣ **Конверторы** - для соединения аппаратных модулей СКУД и ПК.
- ▣ **Вспомогательное оборудование** - блоки питания, кнопки, соединительные провода.
- ▣ **Линии связи** - проводная, кабельная, волоконно-оптическая, радиосвязь.

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

Централизованные
(сетевые)

Универсальные

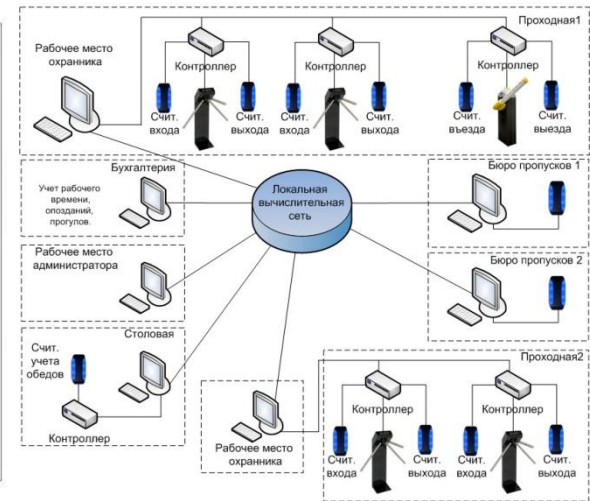
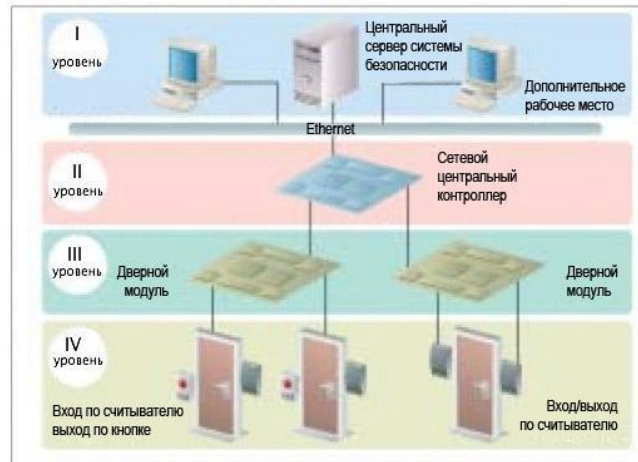
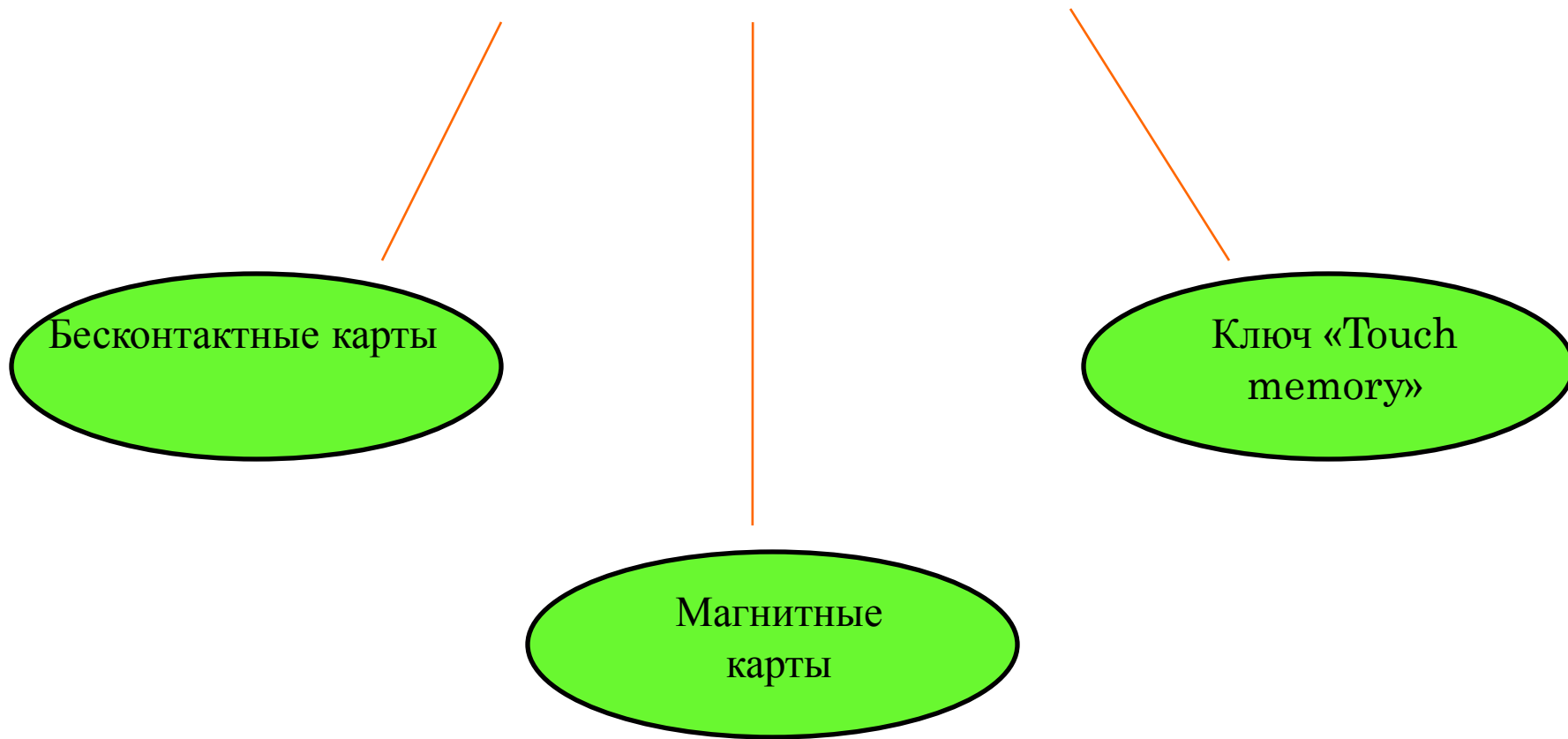
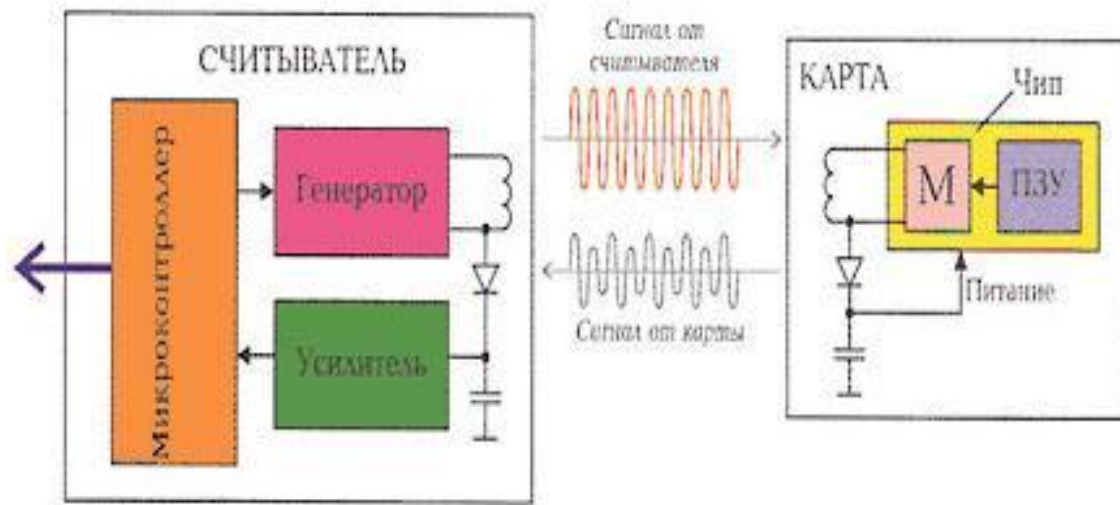


Рис. 1

ОСНОВНЫЕ ТИПЫ КАРТ



БЕСКОНТАКТНЫЕ КАРТЫ (PROXIMITY)



МАГНИТНЫЕ КАРТЫ



КЛЮЧ-БРЕЛОК «TOUCH MEMORY»(IBUTTON)



ОСОБЕННОСТИ БИОМЕТРИЧЕСКИХ СИСТЕМ КОНТРОЛЯ ДОСТУПА

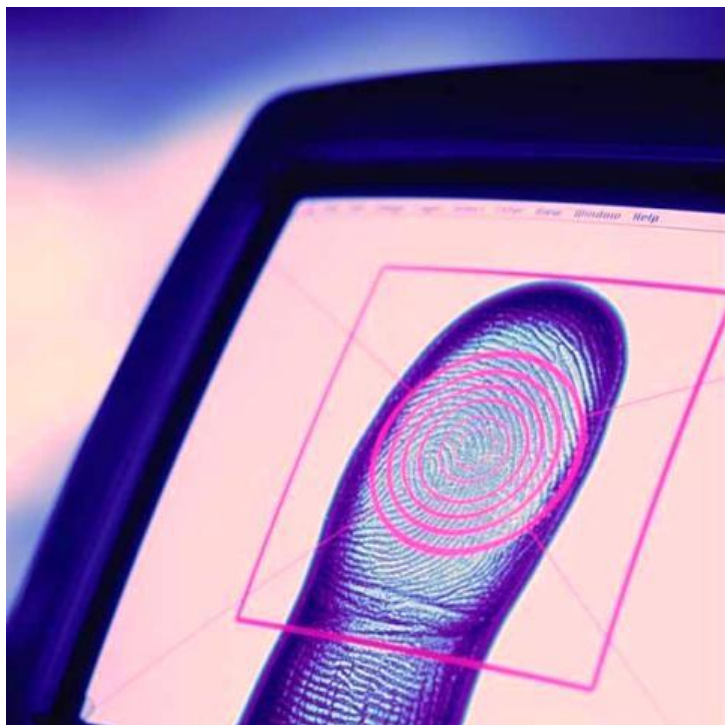
Системы контроля доступа с применением биометрической идентификации имеют ряд преимуществ:



- **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

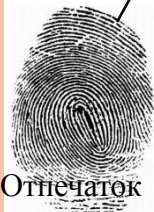
- Скорость работы биометрических терминалов, совмещение в них считывателя с контроллером, в основном зависит от мощности процессора.
- Необходимо принимать во внимание особенности биометрического распознавания:
 - Вероятностный характер распознавания: FAR (коэффициент ложного пропуска, вероятность ложной 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.
- Большой объем данных в системе



Биометрические параметры

статические

динамические



Отпечаток пальца



Форма кисти



Рисунок вен рук



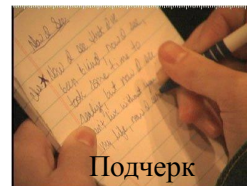
Радужная оболочка глаза



Форма лица



ДНК



Подчерк

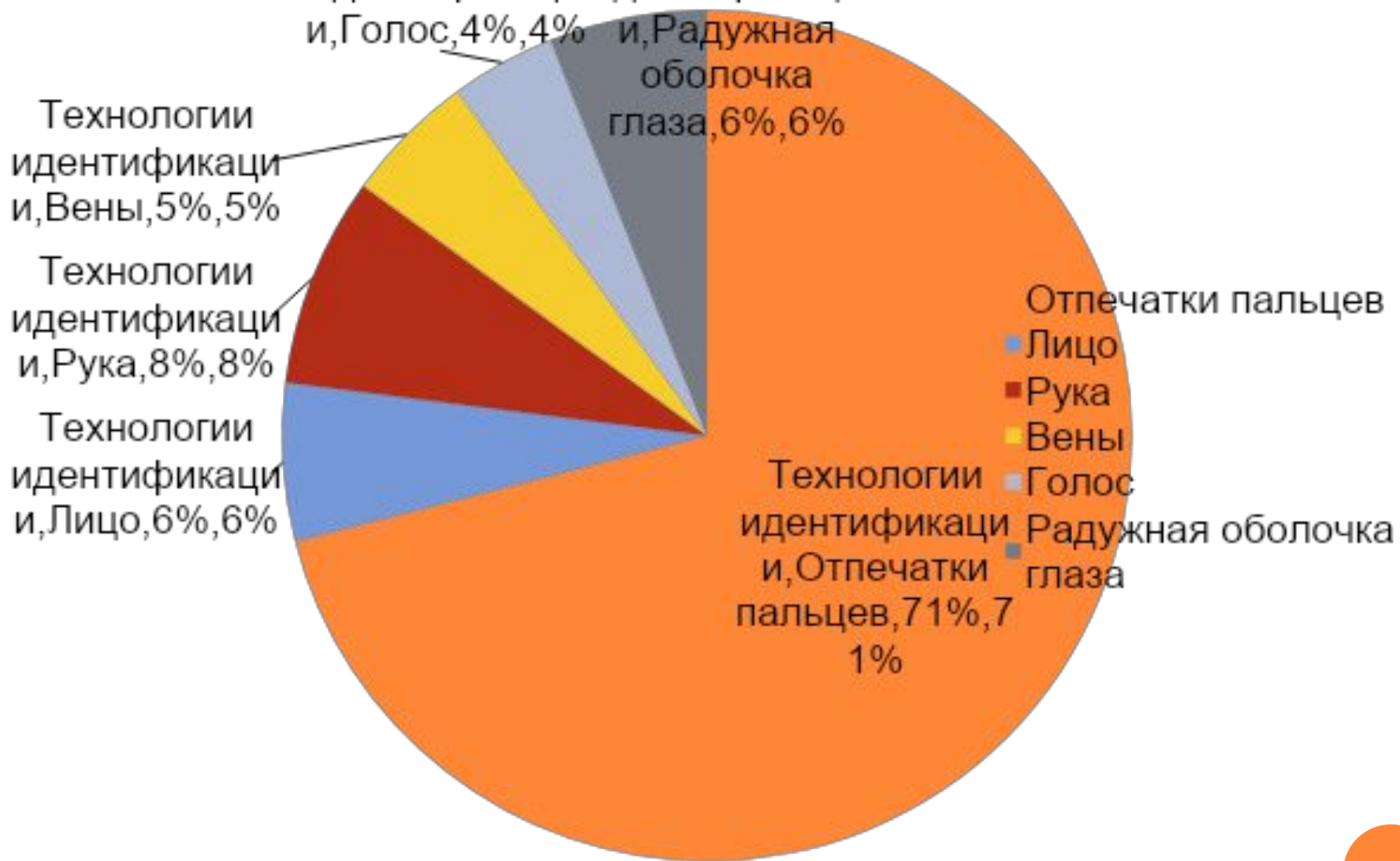


Голос

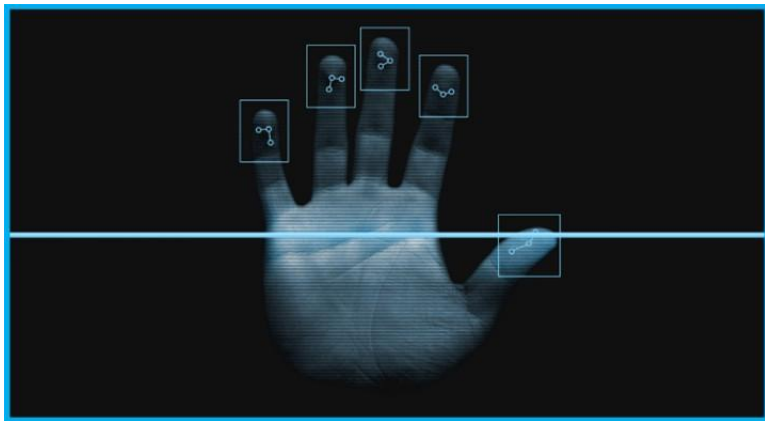


Походка

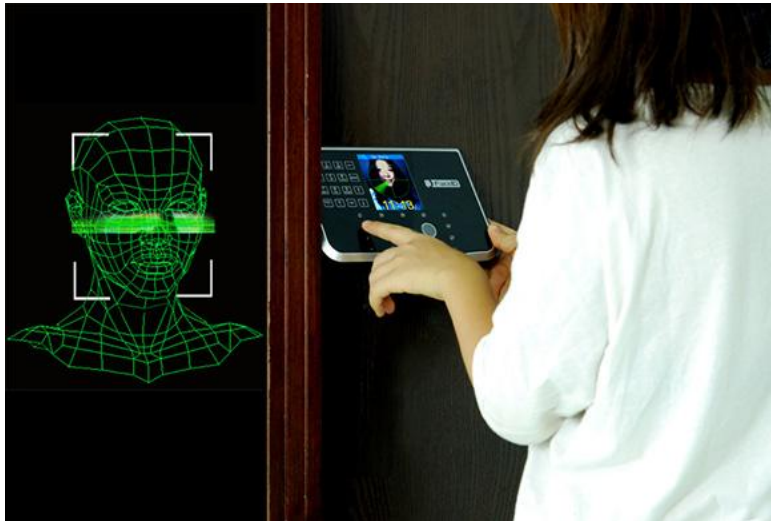
Технологии идентификации



МЕТОДЫ ЗАЩИТЫ ОТ ИМИТАЦИИ И ОШИБОК ПОЛЬЗОВАТЕЛЕЙ



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).

РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

- 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.

ПРИМЕР РАСПРЕДЕЛЕННОЙ СИСТЕМЫ

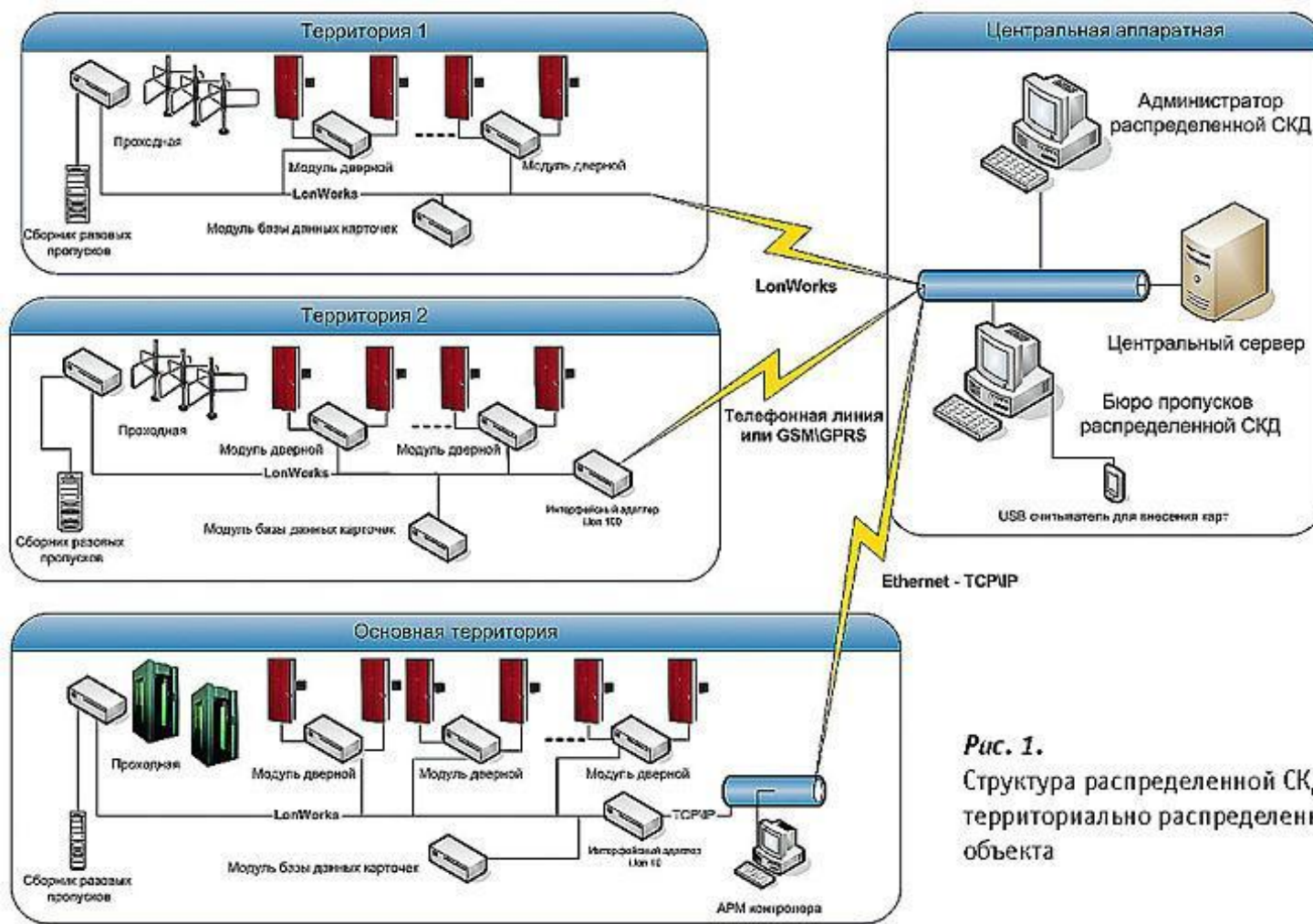


Рис. 1.
Структура распределенной СКД
территориально распределенного
объекта

ВТОРОЙ ПРИМЕР

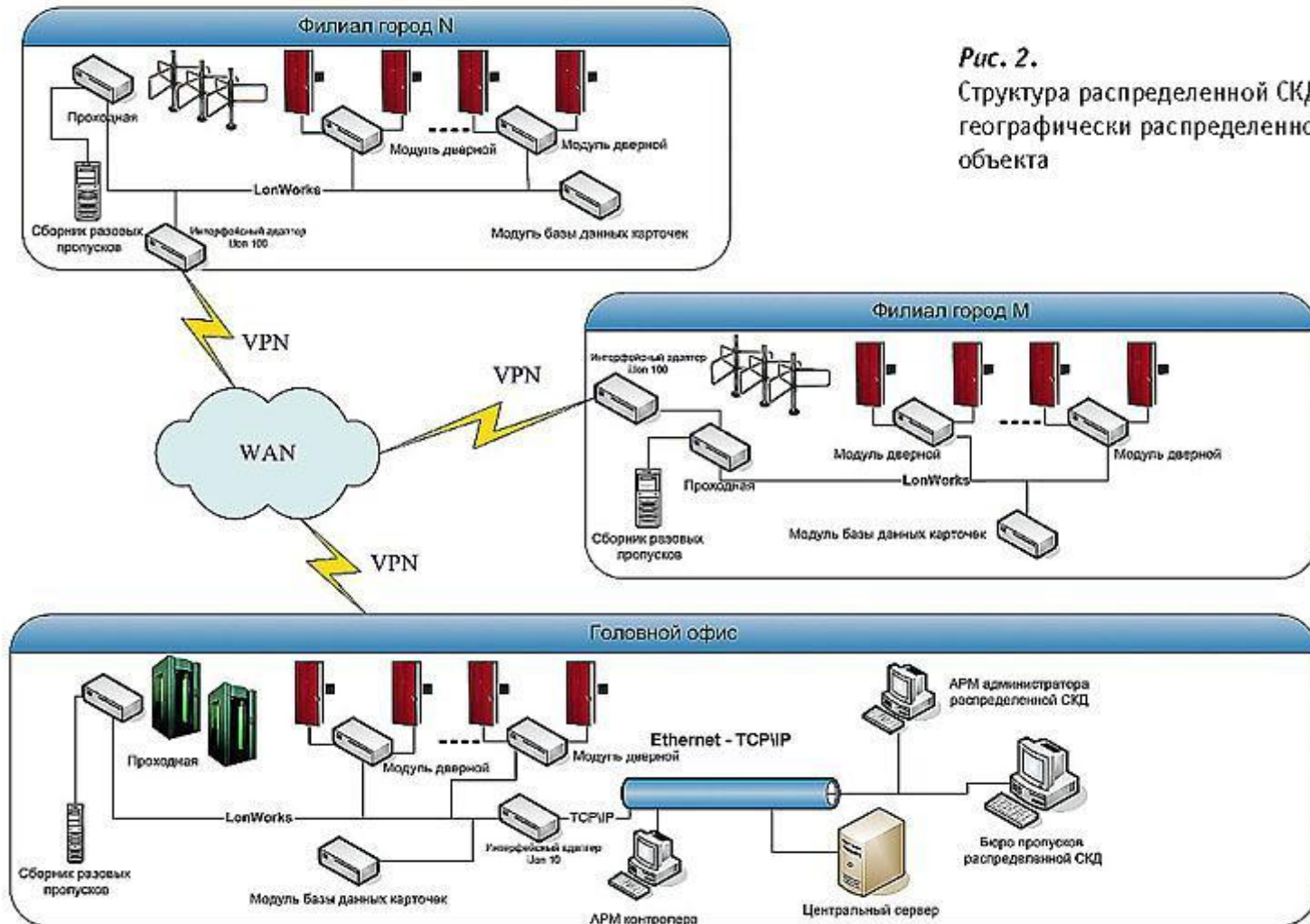
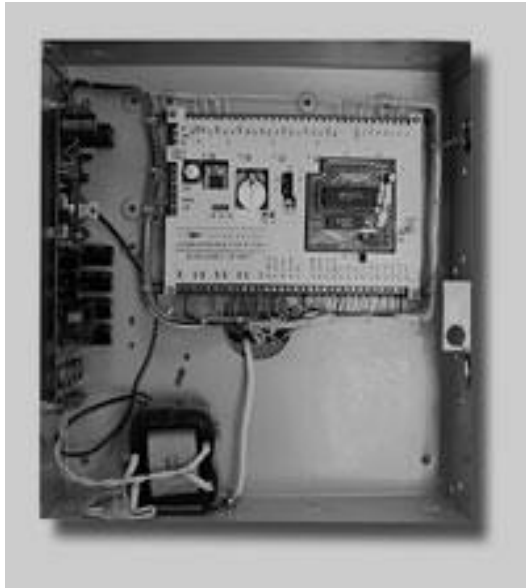


Рис. 2.
Структура распределенной СКД
географически распределенного
объекта

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"

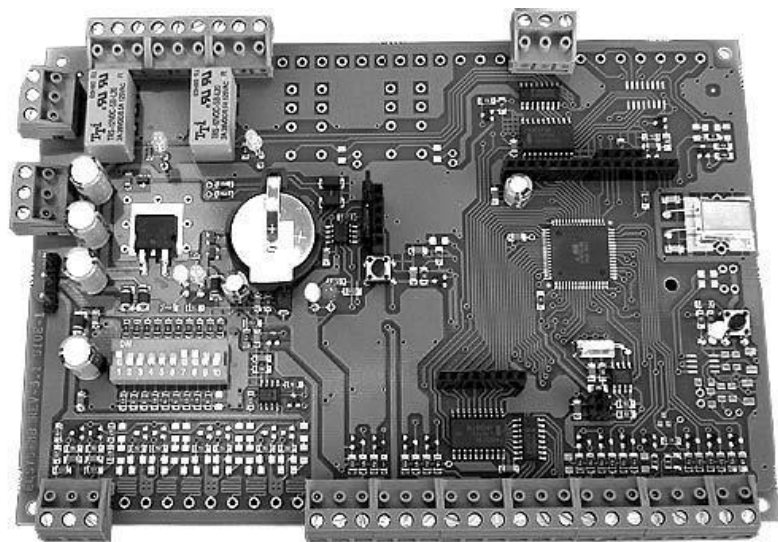
СКУД ELSYS



Система контроля и управления доступом. Предназначена для организации автоматического контроля и управления доступом на объектах различного масштаба (на проходных зданий и учреждений, в помещениях особой важности), для авторизации управления различными элементами системы безопасности, для автоматического управления исполнительными механизмами по заданным событиям и временным расписаниям. Система обеспечивает аппаратную поддержку функций охранно-пожарной сигнализации, а также работу в составе интегрированной системы обеспечения безопасности «Бастион».

В состав системы входят:

- концентраторы «ElSys-МВ», являющиеся аппаратной основой системы
- преобразователи интерфейсов (ПИ) «ElSys-IC-RS232/485», предназначенные для сопряжения сети концентраторов с персональными компьютерами (ПК)
- программное обеспечение «Бастион-ElSys»



Аппаратной основой системы являются контроллеры Elsys-MB, выпускаемые в различных по характеристикам вариантах исполнения Pro, Pro4, Standard, Light и SM. Наличие этих вариантов, а также модулей расширения памяти различной емкости к ним, позволяет при проектировании оптимизировать технико-экономические характеристики систем различного масштаба.

Сочетание ряда технических решений, принятых в системе, придает ей уникальные возможности:

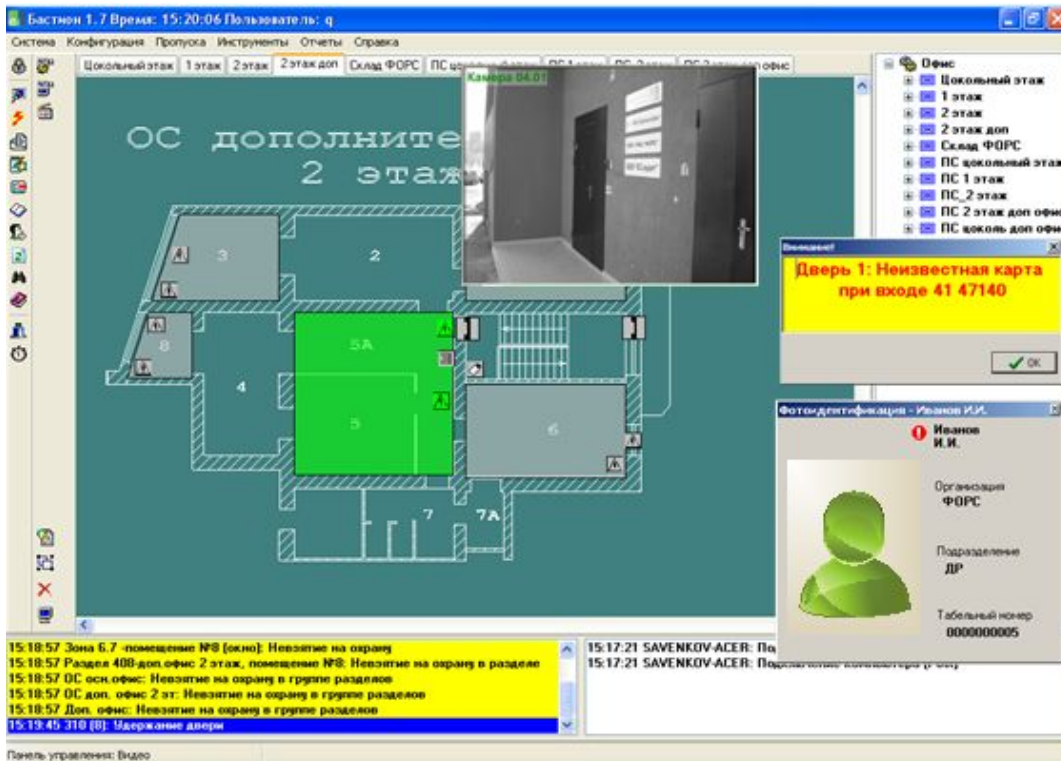
- высокая производительность и большой объем памяти контроллеров Elsys-MB, обеспечивающие обслуживание большого (до 65 тысяч) числа пользователей и длительную работу (до нескольких суток) в автономном режиме в условиях интенсивного потока событий без потери информации о событиях;
- высокая отказоустойчивость системы, обусловленная одноуровневой архитектурой;
- аппаратная реализация функции "глобальный контроль последовательности прохода" (antipassback) в масштабах системы, содержащей до 16128 контроллеров, в том числе и географически распределенной;



- Одна из отличительных особенностей СКУД Elsys – уникально гибкое управление расписаниями и полномочиями пользователей. Возможно задание как недельных, так и скользящих графиков с цикличностью до 31 дня. Механизм переноса выходных учитывает требования российского законодательства в части праздничных дней. Сложные многоэлементные расписания позволяют задавать различные графики работы для разных дней недели, разные расписания на вход и на выход для двусторонних точек доступа.

Программное обеспечение интегрированной системой безопасности «БАСТИОН».

Программное обеспечение предназначено для интеграции в единую систему безопасности подсистем управления доступом, охранной и пожарной сигнализации, теле-наблюдения, а также других систем безопасности и жизнеобеспечения здания.



ПРИМЕР ОКНА РАБОТЫ С БАСТИОНОМ

Бастيون 1.5 Время: 12:58:46 Пользователь: q

Система Конфигурация Отдел кадров Инструменты Отчеты Справка

Корпус 2 Первый этаж

Главное меню

Заголовок программы

Список устройств на планах

Закладки для переключения планов объекта

Управляющая панель активного драйвера

Панель быстрого доступа к функциям

Расширенное сообщение

План объекта

Пиктограммы устройств системы безопасности

Охраняемые зоны

Окно фотоидентификации

Окно штатных и подтвержденных тревожных сообщений

Окно тревожных сообщений

Внимание!
Турникет 1: Неизвестная карта при входе 8 48689

OK

Фотоидентификация - Исаев

Исаев Владимир Алексеевич
Документ:
Паспорт № 432298 Серия 10 04
Выдан: 10.10.2000
Октябрьский район г. Самара

Карта выдана: 31.10.2003 16:16
до: [неизвестно]
Активирована: 31.10.2003 16:16
Пригласившее лицо:
Катин Александр Валерьевич (17-99-00)
("Электронные системы")

12:44:43 Турникет 1: Отказ в доступе на вход - нет прав Бобровский 9345
12:45:18 Турникет 1: Проход под управлением охранника
12:45:18 Турникет 1: Проход под управлением охранника
12:46:41 Турникет 1: Неизвестная карта при входе 8 48689

12:45:17 Вход 1_10 (Турникет 1): Тревога
12:45:17 Турникет 1: Инициализация контроллера
12:45:32 Турникет 1: Предоставление доступа на вход Бобровский 9345
12:45:47 Турникет 1: Предоставление доступа на вход Бобровский 9345
12:45:57 Турникет 1: Предоставление доступа на выход Бобровский 9345

Текущая управляющая панель драйвера

Счетчики персонала

Панель управления Система ТВ наблюдения

В здании: 1

В классовой узле: 0

СКУД ELSYS

Число пользователей
превышает
100 тыс.

Число хранящихся событий
80 тыс.

Кол-во точек прохода
свыше
16 тыс.

**Одна из самых мощных
СКУД на отечественном
рынке!**

**СПАСИБО
ЗА ВНИМАНИЕ!**