

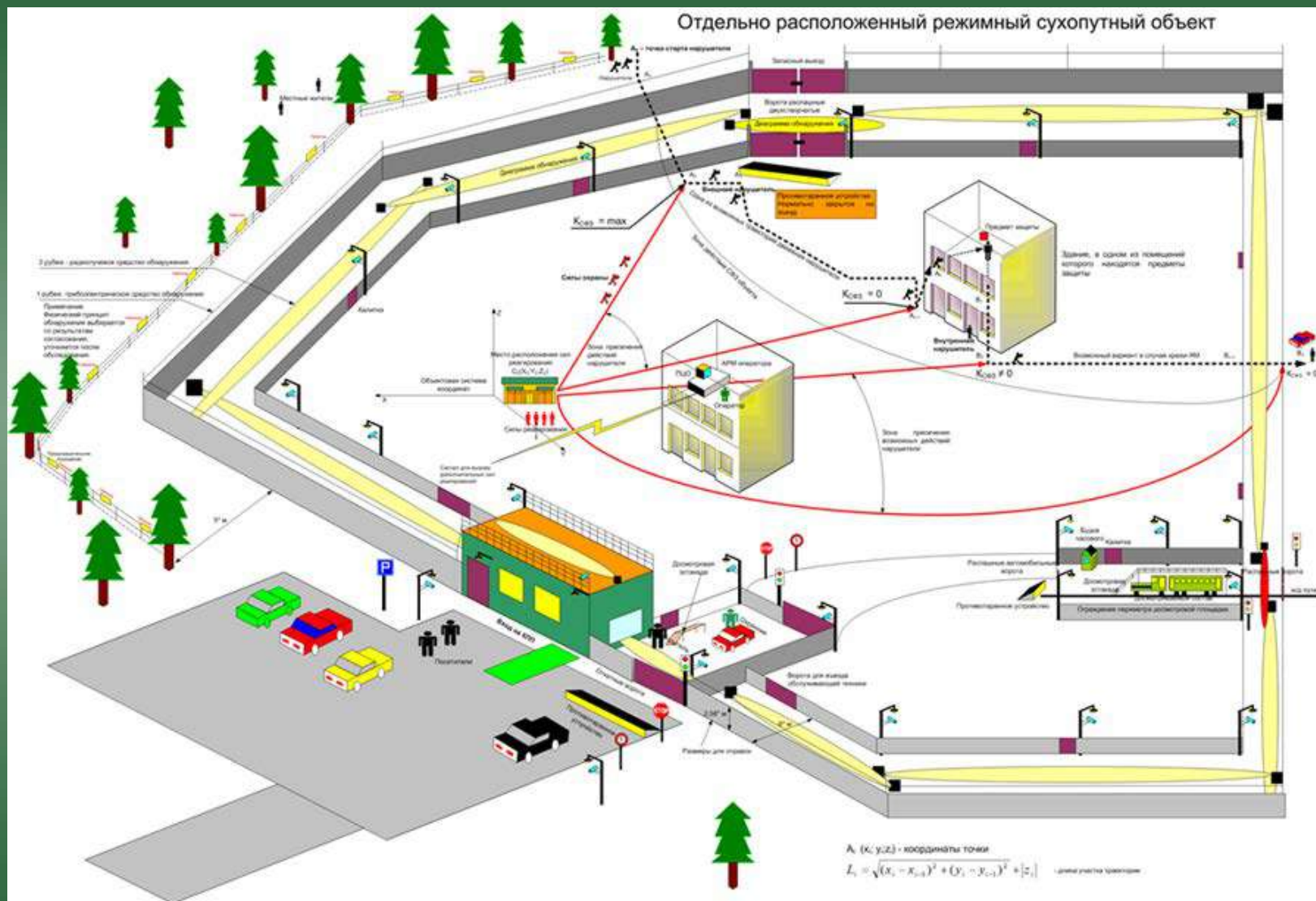
«Обеспечение безопасности и антитеррористической защищенности объектов образования и науки»

Учебные вопросы:

- Структура и состав систем контроля и управления доступом.
- Требования Постановления Правительства РФ №1235 от 07.11.2017 г. «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства образования и науки РФ...».
- Типовые технические решения системы контроля и управления доступом объектов Минобразования и науки различных категорий опасности в соответствии с требованиями Постановления Правительства РФ №1235 от 07.11.2017 г.

Структура и состав современных систем контроля и управления доступом.

Пример гипотетического объекта



Основные задачи, решаемые СКУД



Контроль и управление доступом – комплекс мероприятий, направленных на ограничение и санкционирование доступа людей, транспорта и других объектов в (из) помещения, здания, зоны охраны и территории.

ГОСТ Р 51241 -2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»

Основная нормативно-правовая база

1. Федеральный Закон «О противодействии терроризму» от 06.03.2006 № 35-ФЗ;
2. Постановление Правительства РФ № 1235 от 7 ноября 2017 г. «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства образования и науки РФ...».
3. Постановление Правительства РФ №272 от 25 марта 2015 г. «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий).....».
4. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

Вахтер

Ручная система пропуска. Система ручного учета (табель, журнал и т.п.)

Домофон

Автоматизированная система пропуска Система ручного учета (табель, журнал и т.п.)

Автономные СКУД

Автоматическая система пропуска Автоматизированная система учета (электронный журнал, ручная обработка и т.п.)

Сетевые СКУД

Автоматическая система пропуска Полуавтоматическая система учета (электронный журнал, электронная обработка, автоматизированный перенос данных в бухгалтерские системы и т.п.)

СКУД в составе интегрированных систем

Автоматическая система пропуска Полуавтоматическая система учета (электронный журнал, электронная обработка, автоматизированный перенос данных в бухгалтерские системы и т.п.) \автоматическое взаимодействие с другими подсистемами безопасности

Системы управления предприятием

Автоматическая система пропуска Полуавтоматическая система учета (электронный журнал, электронная обработка, автоматический перенос данных в бухгалтерские системы)

Общая структура СКУД:

- а) подсистема ввода идентификационных признаков;
- б) подсистема управления точкой доступа;
- в) подсистема преграждения прохода;
- г) подсистема обработки данных (АРМ СКУД...)



Классификация СКУД

1. По способу управления.
2. По количеству контролируемых точек доступа.
3. По функциональным характеристикам.
4. По виду объектов контроля.
5. По уровню защищенности системы от НСД к информации.

1. По способу управления.

- автономные - для управления одним или несколькими УПУ без передачи информации на центральный пульт и без контроля со стороны оператора;
- централизованные (сетевые) - для управления УПУ 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.

2. По количеству контролируемых точек доступа.

- малой емкости (менее 16 точек);
- средней емкости (не менее 16 и не более 64 точек);
- большой емкости (64 точки и более).

Классификация СКУД

3. По функциональным характеристикам.

- 1 - системы с ограниченными функциями;
- 2 - системы с расширенными функциями;
- 3 - многофункциональные системы.

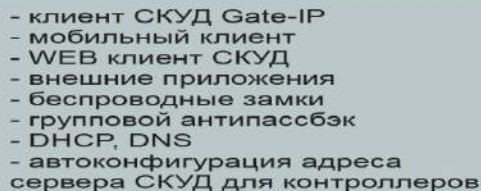
4. По виду объектов контроля.

- для контроля доступа физических объектов;
- для контроля доступа к информации.

5. По уровню защищенности системы от НСД к информации.

Классификацию систем КУД по защищенности от несанкционированного доступа к информации проводят по таблице А.1 приложения А [5].

Классификацию средств КУД по устойчивости от несанкционированного доступа к информации проводят по таблице Б.1 приложения Б [5].



«Требования Постановления Правительства РФ
№1235 от 07.11.2017 г. «Об утверждении требований
к антитеррористической защищенности объектов
(территорий) Министерства образования и науки
РФ...»

Основные требования (п.17 – 19)

Постановление Правительства РФ № 1235 от 7 ноября 2017 г.

п.17 Антитеррористическая защищенность объектов (территорий) независимо от их категории опасности обеспечивается путем осуществления комплекса мер, направленных:

а) на воспрепятствование неправомерному проникновению на объекты (территории);

П.18 Воспрепятствование неправомерному проникновению на объекты (территории) достигается посредством:

а) разработки и реализации комплекса мер по выявлению, предупреждению и устранению причин неправомерного проникновения на объекты (территории), локализации и нейтрализации последствий их проявления;

б) организации и обеспечения пропускного и внутриобъектового режимов, контроля их функционирования;

П.19. Выявление потенциальных нарушителей установленных на объектах (территориях) режимов и (или) признаков подготовки или совершения террористического акта обеспечивается путем:

а) неукоснительного соблюдения на объектах (территориях) пропускного и внутриобъектового режимов;

Основные требования (п.20 – 22)

Постановление Правительства РФ № 1235 от 7 ноября 2017 г.

П.20. Пресечение попыток совершения террористических актов на объектах (территориях) достигается посредством:

- а) организации и обеспечения пропускного и внутриобъектового режимов на объектах (территориях);
- б) своевременного выявления фактов нарушения пропускного режима, попыток вноса (ввоза) и проноса (провоза) запрещенных предметов (взрывчатых, отравляющих веществ, оружия, боеприпасов, наркотических и других опасных предметов и веществ) на объекты (территории);
- в) организации санкционированного допуска на объекты (территории) посетителей и автотранспортных средств;
- г) поддержания в исправном состоянии инженерно-технических средств и систем охраны, обеспечения бесперебойной и устойчивой связи на объектах (территориях);
- д) исключения фактов бесконтрольного пребывания на объектах (территориях) посторонних лиц и нахождения транспортных средств на объектах (территориях) или в непосредственной близости от них;

П.22. В целях обеспечения антитеррористической защищенности объектов (территорий) независимо от присвоенной им категории опасности осуществляются следующие мероприятия:

- в) обеспечение пропускного и внутриобъектового режимов и осуществление контроля за их функционированием;

Основные требования (п.п.23 – 211)

Постановление Правительства РФ № 1235 от 7 ноября 2017 г.

П.23. В отношении объектов (территорий) второй категории опасности дополнительно к мероприятиям, предусмотренным [пунктом 22](#) настоящих требований, осуществляются следующие мероприятия:

б) оборудование объектов (территорий) инженерно-техническими средствами и системами охраны (системой видеонаблюдения, контроля и управления доступом, охранной сигнализацией);

П.24. В отношении объектов (территорий) первой категории опасности дополнительно к мероприятиям, предусмотренным [пунктами 22](#) и [23](#) настоящих требований, осуществляются следующие мероприятия:

а) обеспечение особого порядка доступа на объект (территорию);

г) оборудование контрольно-пропускных пунктов и въездов на объект (территорию) телевизионными системами видеонаблюдения, обеспечивающими круглосуточную видеофиксацию, с соответствием зон обзора видеокамер целям идентификации и (или) различения (распознавания);

д) оснащение въездов на объект (территорию) воротами, обеспечивающими жесткую фиксацию их створок в закрытом положении, а также при необходимости средствами снижения скорости и (или) противотаранными устройствами.

«Типовые технические решения системы контроля и управления доступом объектов образования и науки различных категорий опасности в соответствии с требованиями Постановления Правительства РФ №1235 от 07.11.2017 г.»

Преграждающие устройства

по виду перекрытия проёма в проходе:

*с частичным
перекрытием:*

Турникеты

- трехштанговые
- полупрофильные
- полнопрофильные
- турникеты-калитки
- скоростные турникеты

Калитки

Шлагбаумы

*с полным
перекрытием:*

Сплошные двери

- раздвижные
- распашные

Ворота

- раздвижные
- распашные
- подъемно-:
 - * поворотные, гелютинные
 - * секционные
 - * рулонные (рольворота)

Полноростовые турникеты

*с блокированием
объекта в проёме*

Тамбур-шлюзы

Роторные шлюзовые кабины

Средства автоматизации
управления
преграждающими
устройствами:

- автоматические приводы;
- элементы дистанционного управления;
- элементы обеспечения безопасности.

**по способу
управления:**

с ручным управлением

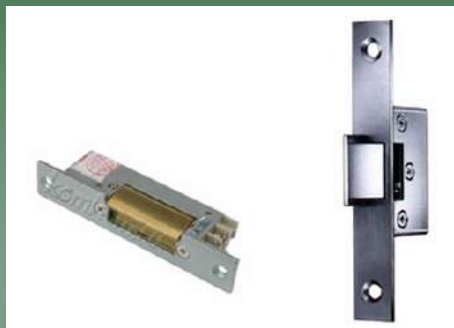
с полуавтоматическим управлением

с автоматическим управлением

Исполнительные устройства

а) Замки с электрическим управлением (электрозамки) – самый массовый тип исполнительных устройств

Электрозащелки



Электромеханические замки



Соленоидные электрозамки



Моторные электрозамки



Электромагнитные замки

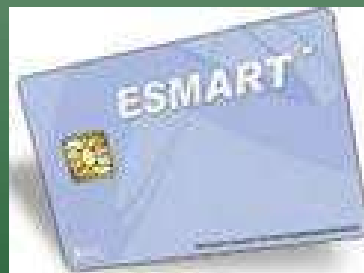


б) Гидравлические и электромеханические приводы

Идентификаторы

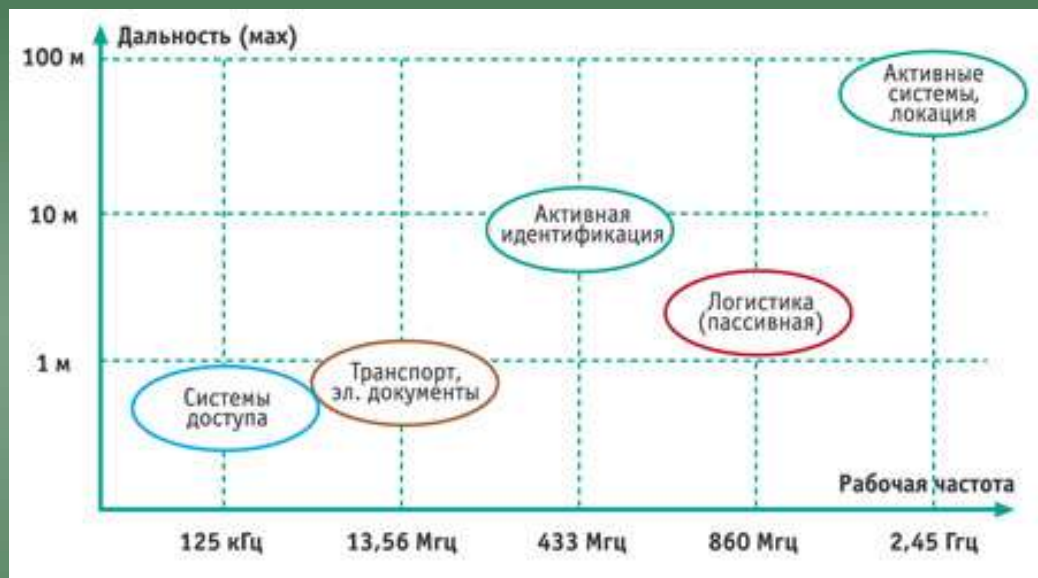
Идентификаторы - носители идентификационных признаков

- 3.1. *Вещественные идентификаторы*, реализованные в виде предмета (технического устройства), на которое с помощью специальной технологии занесен идентификационный признак в виде кодовой информации, например, ключи к механическим замкам, магнитные карты, Виганд-карты, Proximity-карты, смарт-карты, браслеты, метки, электронные ключи Touch Memory, радиобрелки и т. д.;
- 3.2. *Биометрические идентификаторы*;
- 3.3. *Запоминаемый человеком уникальный код*.



Особенности радиочастотной идентификации.

Классификация систем RFID



б) Дальность связи

ДИАПАЗОН	РАЗМЕР АНТЕННЫ	МАКСИМАЛЬНАЯ ДАЛЬНОСТЬ	ПРИМЕЧАНИЕ
125 кГц	100 x 50 см	60–80 см	Пассивная
13,56 МГц	100 x 50 см	80–120 см	Пассивная
433 МГц	10 x 10 см	20–100 м	Активная
800–900 МГц	20 x 20 см	200–400 см	Пассивная
2,45 ГГц	10 x 10 см	10–150 м	Активная

а) Рабочие F:

- 125 кГц
- 13,56 МГц
- 433 МГц
- 860 МГц
- 2,45 ГГц

Применяемые идентификаторы:

Карты: HID,
 Indala (Motorola),
 EM Marin (EM),
 Mifare®,

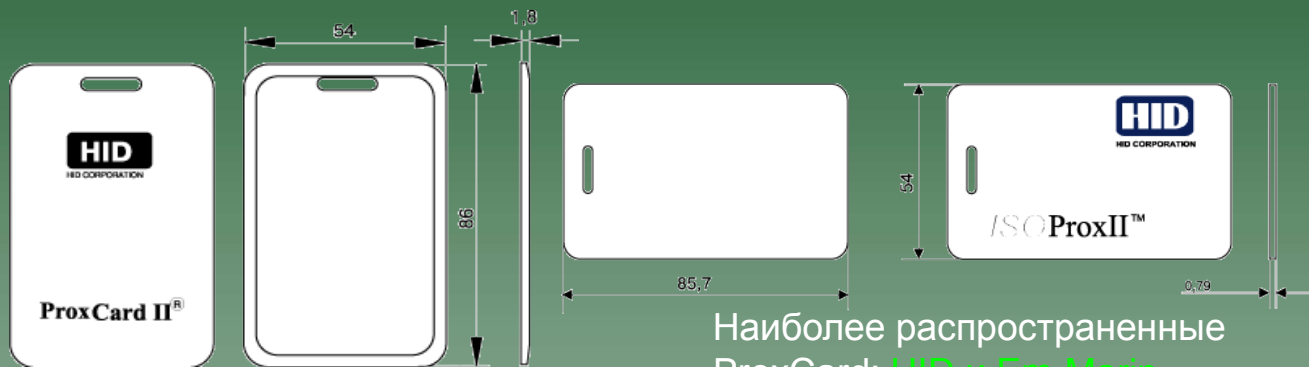
Радиобрелки,
 и др.

Для пассивных систем зависит от: диапазона, мощности, размера антенны.

Для активных систем: + от метода модуляции, ширины спектра.

Идентификаторы

Proximity-карты (RFID). Конструкция, характеристики.



Наиболее распространенные ProxCard: **HID** и **Em-Marin**.



Пассивная проксимити-карта

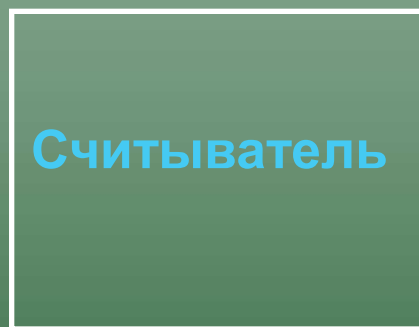
RFID-технология (Radio Frequency Identification Technology)

Достоинства:

- (код до 85 бит = 137 млрд вариантов идентиф. кодов;
- высокая износостойкость (пассивный, без ИП – вечен)
- механическая прочность, устойчивость к изгибам, ударам;
- не боятся влаги и загрязнения.

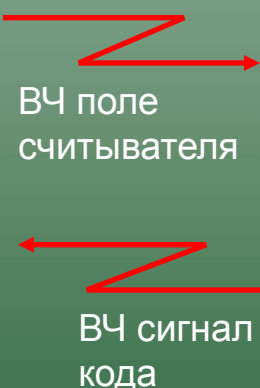
Недостаток: открытый код нет защиты от копирования

Программируются при изготовлении, но есть модели с возможностью перезаписи кода.



Стандарт **HID** использует частотную модуляцию при формировании сигнала, а стандарт **Em-Marin** - AM.

Новинка: Считыватель Антидубь



Идентификаторы

RFID Метки (UHF-диапазон). Характеристики, принцип работы в СКУД

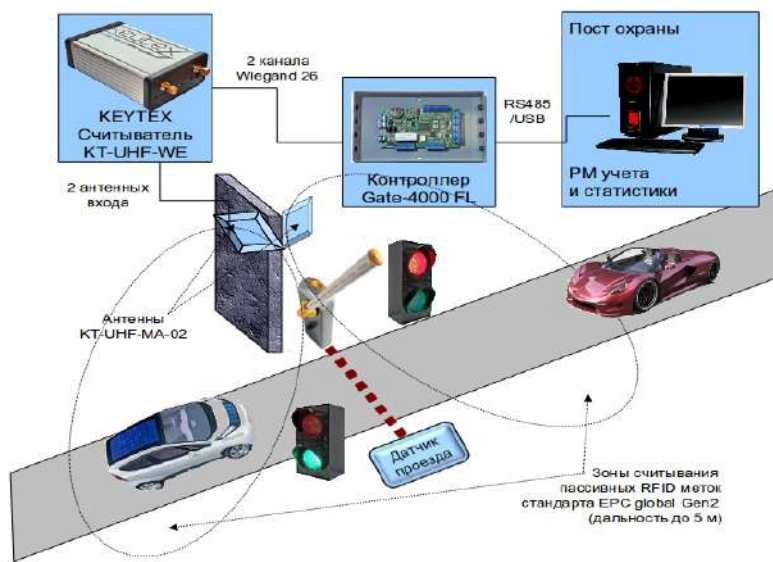


Характеристики системы:

- дальность действия до 8 м ;
- защита от копирования кода
- использование активных и пассивных меток;
- механизм антиколлизии;
- рабочая частота 868 МГц;
- размер антенны 250x250 мм;
- вес считывателя (2 кан)-320 гр;.

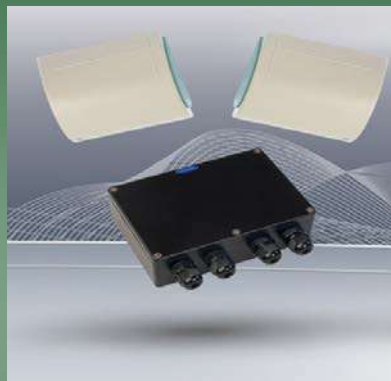
АВТО СКУД

вариант системы на базе типового контроллера Gate-4000
с использованием пассивных RFID карт и считывателя дальнего радиуса действия



3. Идентификаторы

3.1.RFID Метки (SUNF-диапазон). Характеристики, принцип работы в СКУД



Характеристики системы:

- дальность действия 5-60 м ;
- защита от копирования;
- использование активных меток;
- механизм антиколлизии;
- рабочая частота 2,45 Гц;
- размер считывателя (2 кан) – 210x130x60 мм;
- стоимость.



Идентификаторы

Смарт-карты. Конструкция, характеристики.

Смарт-карты это пластиковые карты, которые содержат в себе интегральную схему, обеспечивающие хранение и обработку записанной в ней информации.

Технология смарт (перевод – «внутри») - это микропроцессорная технология (процессор, ОЗУ и ПЗУ).

Контактные смарт-карты



- 1) контактная область 6 или 8 контактов квадратной или овальной формы;
- 2) чип (микропроцессор карты);
- 3) пластиковая основа.

Бесконтактные смарт-карты



Дальность действия:
от 2,5 до 11,5 см.

Радиочастота обмена
закодирована

Достоинства: – возможность перепрограммирования, хранение значительного кол-ва инф-ции;
– высокая степень секретности (шифрование и несколько уровней парольной защиты);
– долговечность эксплуатации (за счет отсутствия ИП)

Хранение информации в карте о доступе, времени работы, платежах, уд/личности обеспечивается за счет 16 отдельных областей памяти, каждая из которых имеет индивидуальную защиту, что гарантирует высокий уровень надежности.

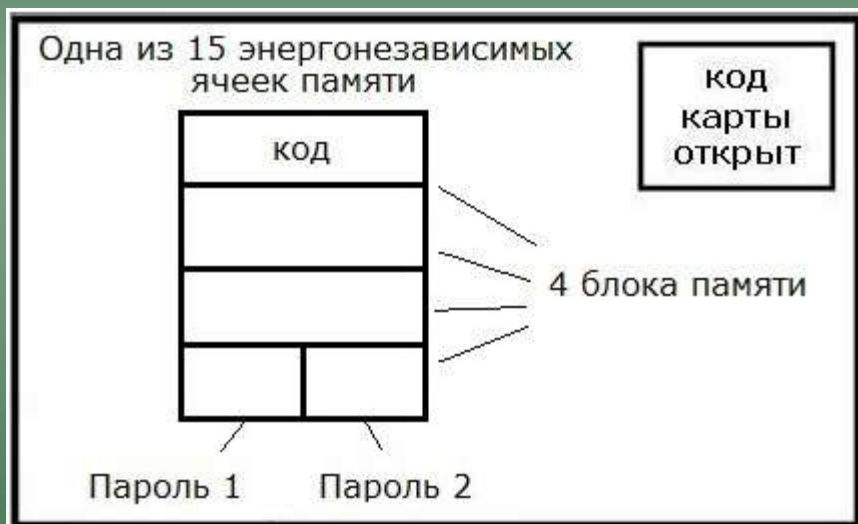
Высокий уровень безопасности объекта, достигается благодаря применению двойной идентификации (ключ карты и считывателя), длиной ключа (48 бит) и специальным алгоритмом.

Недостатки: – значительная стоимость, относительная неустойчивость к механическим повреждениям, относительно низкая пропускная способность в СКУД.

Идентификаторы

Смарт-карты бесконтактные (Mifire, iClass, IClass SE, iClass Seos). *Конструкция, характеристики.*

Смарт-карты обеспечивают принципиально новый уровень защищенности за счет того, что они работают в диалоговом режиме со считывателем, используя механизмы криптозащиты в процессе взаимного обмена информацией.



В смарт-карте есть открытый код карты, однако в системе может использоваться не он, а специальный код, который записывается в одну из криптозащищенных ячеек энергонезависимой памяти карты. Доступ к этой ячейке возможен, только если знать два секретных пароля (ключа доступа к карте). Кроме владельца системы эти пароли никто не знает, а не зная этих двух паролей, подделать специальный код карты невозможно.

Идентификаторы

Смарт-карты бесконтактные (Mifire, iClass, IClass SE, iClass Seos, pivClass). Конструкция, характеристики.

iCLASS® SE – технология повышенной безопасности, конфиденциальности и компактности, поддерживает стандартизованный промышленный протокол Open Supervised Device Protocol (OSDP) для безопасной, двусторонней коммуникации между картой и считывателем.. Связанные идентификационные данные (номер карты, отпечаток пальца на карте) надежно защищены посредством алгоритма SIO. SIO зашифрован стандартными криптографическими алгоритмами (3DES, AES, RSA...), подписан цифровой подписью и закреплен на носителе. SIO может быть помещен на различные носители - карту, USB-токен, NFC-телефон и т.д.



Безопасность – технологии шифрования не зависят от RFID платформы. Много-уровневая защита системы управления ключами.

Оперативная совместимость с технологией мобильного контроля (NFC)
Адаптивность – возможность быстрого обновления.

Совместимость с другими разработками HID Global, Assa Abloy (MIFARE, DESFire, EV1, iCLASS, HID Prox, Indala, EMEMarin)

В-1. Технические средства СКУД

3. Идентификаторы

3.1. Вещественные идентификаторы

3.1.7. Считывание мобильных идентификаторов *Конструкция, характеристики.*


Считыватели PW-mini BLE работают с Mob-ID, а также с ASK и/или FSK идентификаторами.

Параметры работы считывателя, выходной интерфейси типы идентификаторов, с которыми разрешена работа настраиваются с помощью мобильного приложения по интерфейсу BLE (Bluetooth Low Energy). При включении режима персонификации Mob-ID работа с ASK и FSK идентификаторами будет отключена автоматически.

Считывание кода мобильного идентификатора на расстоянии от 0,5 до 5 м.(в зависимости от настройки)



Скачайте и установите мобильное программное обеспечение Mob-ID. С его помощью выполняется получение, хранение и передача кода идентификатора между считывателем и смартфоном по интерфейсу BLE.

Поднесите мобильное устройство к контроллеру и нажмите кнопку  в приложении – будет выполнен обмен данными

Идентификаторы

Биометрические признаки человека

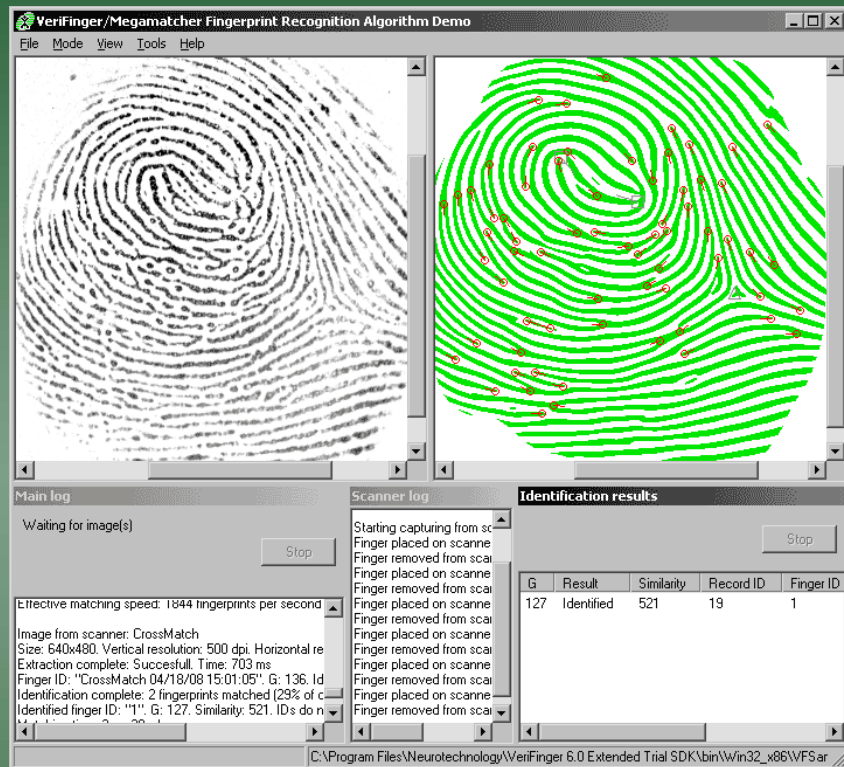
Биометрической характеристикой человека (БХЧ) называется его измеряемая физическая характеристика или персональная поведенческая черта.

Оценка свойств БХЧ

Характеристика	Универсальность	Уникальность	Постоянство	Собираемость
Видеообраз лица	+++	+	++	+++
Термограмма лица	+++	+++	+	+++
Отпечаток пальца	++	+++	+++	++
Геометрия руки	++	++	++	+++
Радужная оболочка глаза	+++	+++	+++	++
Сетчатка	+++	+++	++	+
Подпись	+	+	+	+++
Голос	++	+	+	++
Отпечаток губ	+++	+++	++	+
Особенности ушной раковины	++	++	++	++
Динамика письма	+++	+++	+	+++
Походка	+++	++	+	+

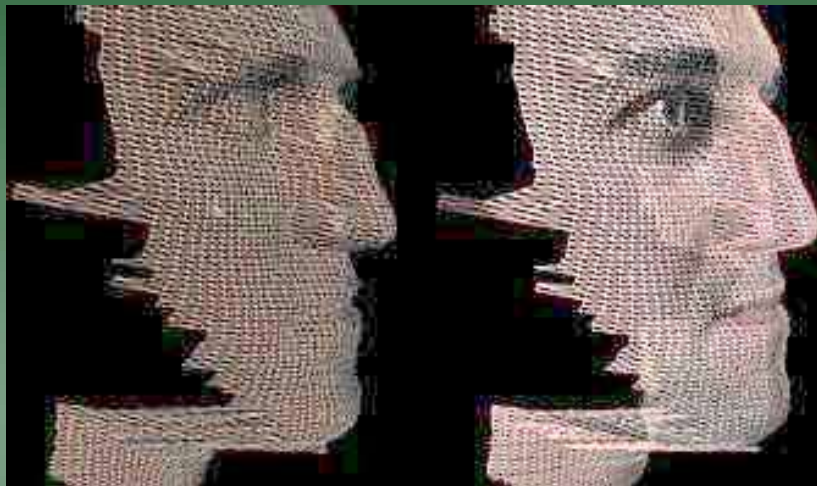
Экспертная оценка свойств БХЧ: +++ - высокая оценка, ++ - средняя, + - низкая.

Идентификация по отпечаткам пальцев



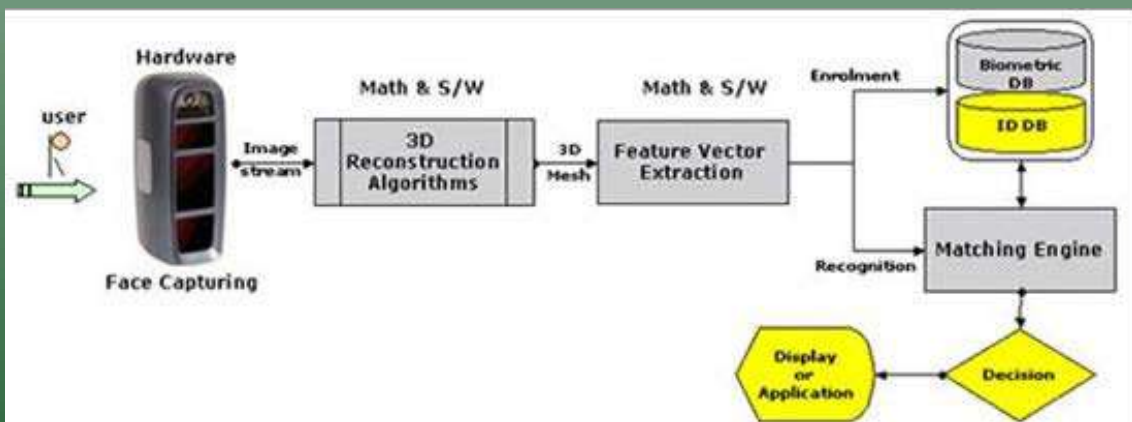
Идентификация по геометрии лица

3-D распознавание

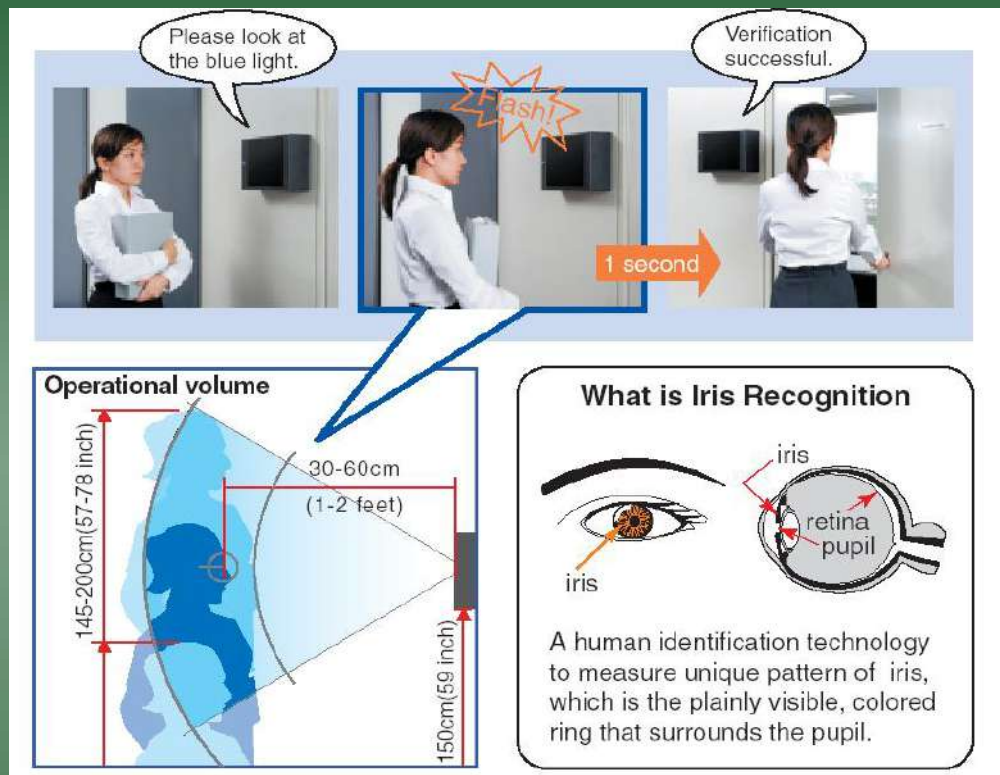


Метод проецирования шаблона:

- на объект (лицо) проецируется сетка;
- камера делает снимки со скоростью десятки кадров в секунду,
- полученные изображения обрабатываются специальной программой и восстанавливается 3D-модель лица,
- производится анализ модели, выделяются антропометрические особенности, которые в итоге и записываются в уникальный код, заносящийся в базу данных.



Идентификация по радужной оболочке глаз



Система контроля доступа путем идентификации личности с автоматическим захватом рисунка радужной оболочки глаза EyeSwipe Nano-TS .



Идентификация по венозному рисунку ладони (пальца)

Система контроля доступа путем идентификации личности по уникальным биометрическим особенностям строения подкожных вен ладоней человека.

В основе работы устройства применяется технология получения изображения ладони в ИК спектре. Обедненная кислородом кровь имеет большой коэффициент поглощения ИК излучения по сравнению с остальной живой тканью ладони.

Полученный рисунок уникален.

Количество пользователей 1 000 000

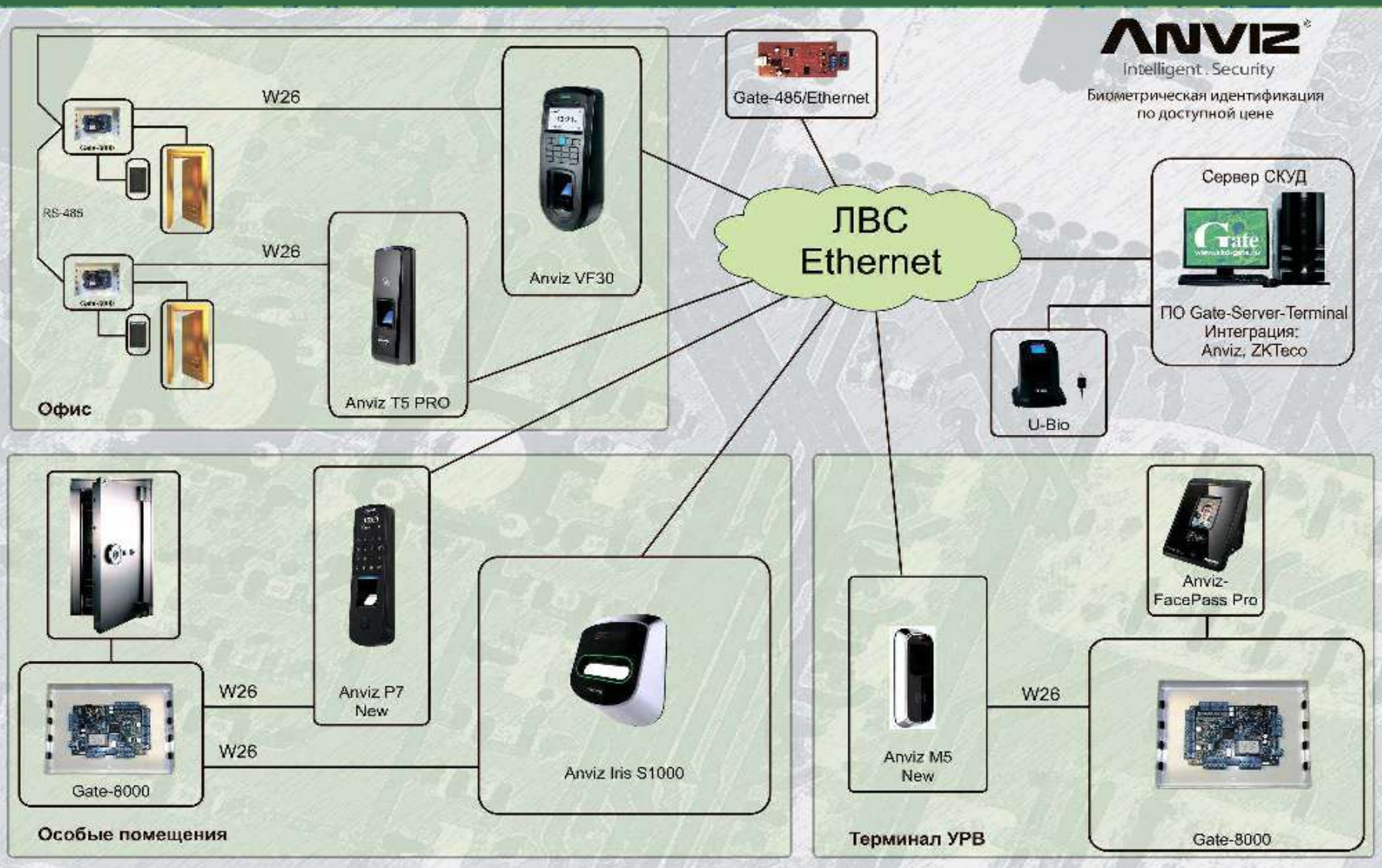
Количество ладоней 300 000

Время идентификации до 2 сек



GATE

СКУД с использованием биометрической идентификации



Программное обеспечение для СКУД

Утилиты



Полнофункциональное сетевое ПО



Интеграция с системами безопасности управления



Программное обеспечение управления точкой доступа

Функции программного обеспечения СКУД

Мониторинг и управление

- мониторинг;
- фотоидентификация;
- слежение за перемещением;
- отчеты по событиям;
- учет рабочего времени;
- интеграция с системами; видеонаблюдения, охранной и пожарной сигнализации.

Работа с пропусками

- выдача и удаление пропусков;
- ввод номера карт со считывателя;
- ведение базы данных пропусков;
- отчеты по пропускам;
- печать пропусков;
- работа с несколькими контроллерами;
- документооборот;
- интеграция с системами планирования и учета ресурсов предприятия;
- смена PIN-кода.

Конфигурирование

- конфигурирование контроллеров;
- многопользовательская работа;
- восстановление после сбоев.

Расширение технических возможностей контроллеров

- сложные алгоритмы прохода;
- изъятие разовых пропусков;
- контроль времени первого предъявления пропуска;
- автоматическое задержание пропуска;
- проход с сопровождающим
- глобальный контроль повторного прохода;
- преобразование номеров карт.

Основные точки прохода:

- КПП (людовой проход, транспортный проезд);
- запасной выход/выезд;
- дверь, калитка;
- ворота.

Технические устройства в точках прохода:

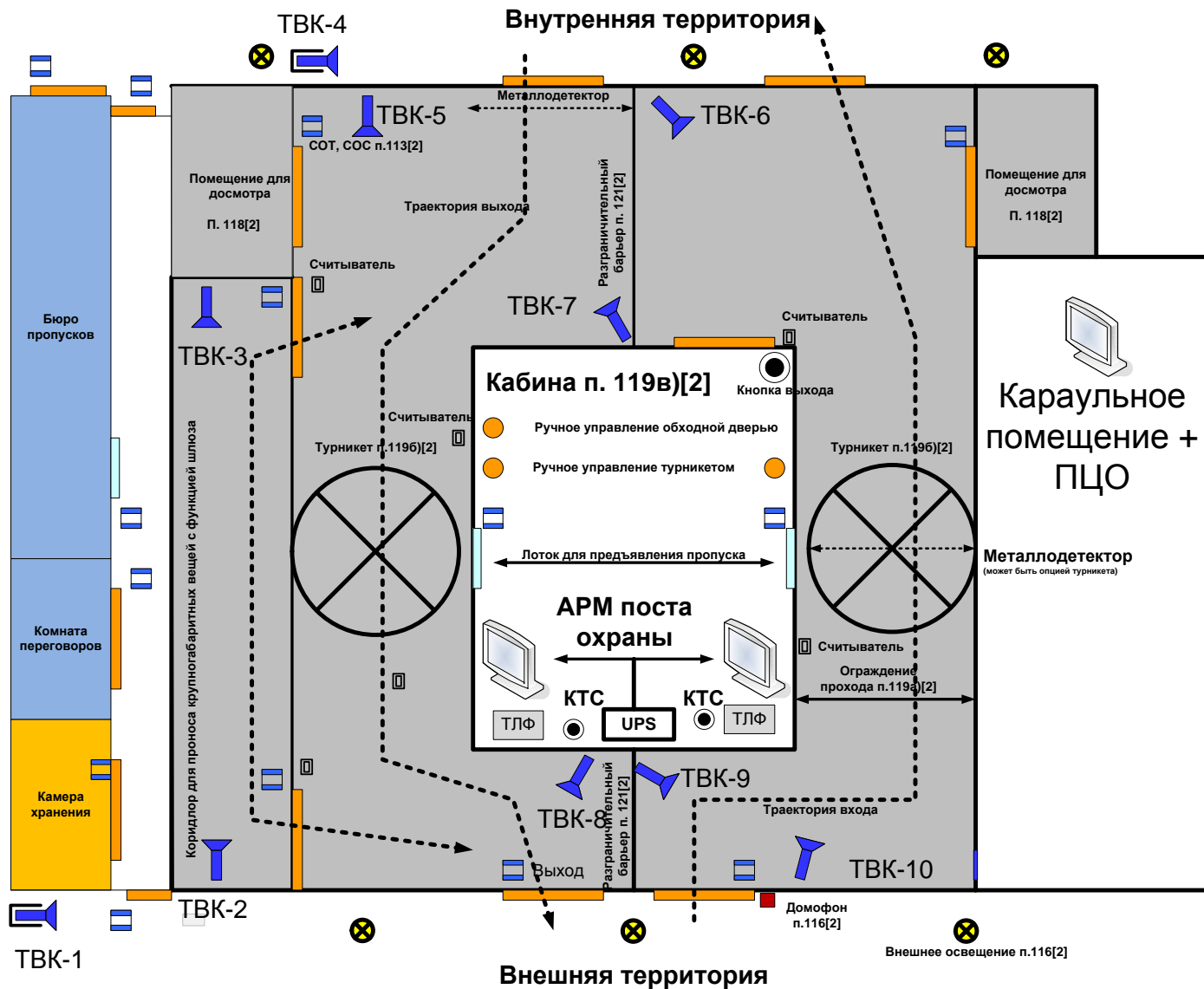
- замок;
- турникет;
- шлагбаум;
- противотаранное устройство;
- устройство снижения скорости;

Информационное обеспечение точек прохода

- светофор;
- дорожный знак;
- запрещающий знак;
- объявление
- телекамера;
- охранный извещатель.

Сущность проектирования состоит в том, чтобы выбрать техническую базу (ИТСЗ, ТСО и информационное обеспечение) и разработать схему размещения и электрические соединения для точек доступа. Выбор технической базы проводится в зависимости от набора систем безопасности (приложение 1[2]).

Типовое оборудование пешеходного КПП п.п. 109 – 127 ПП 458



Организация досмотра автотранспорта



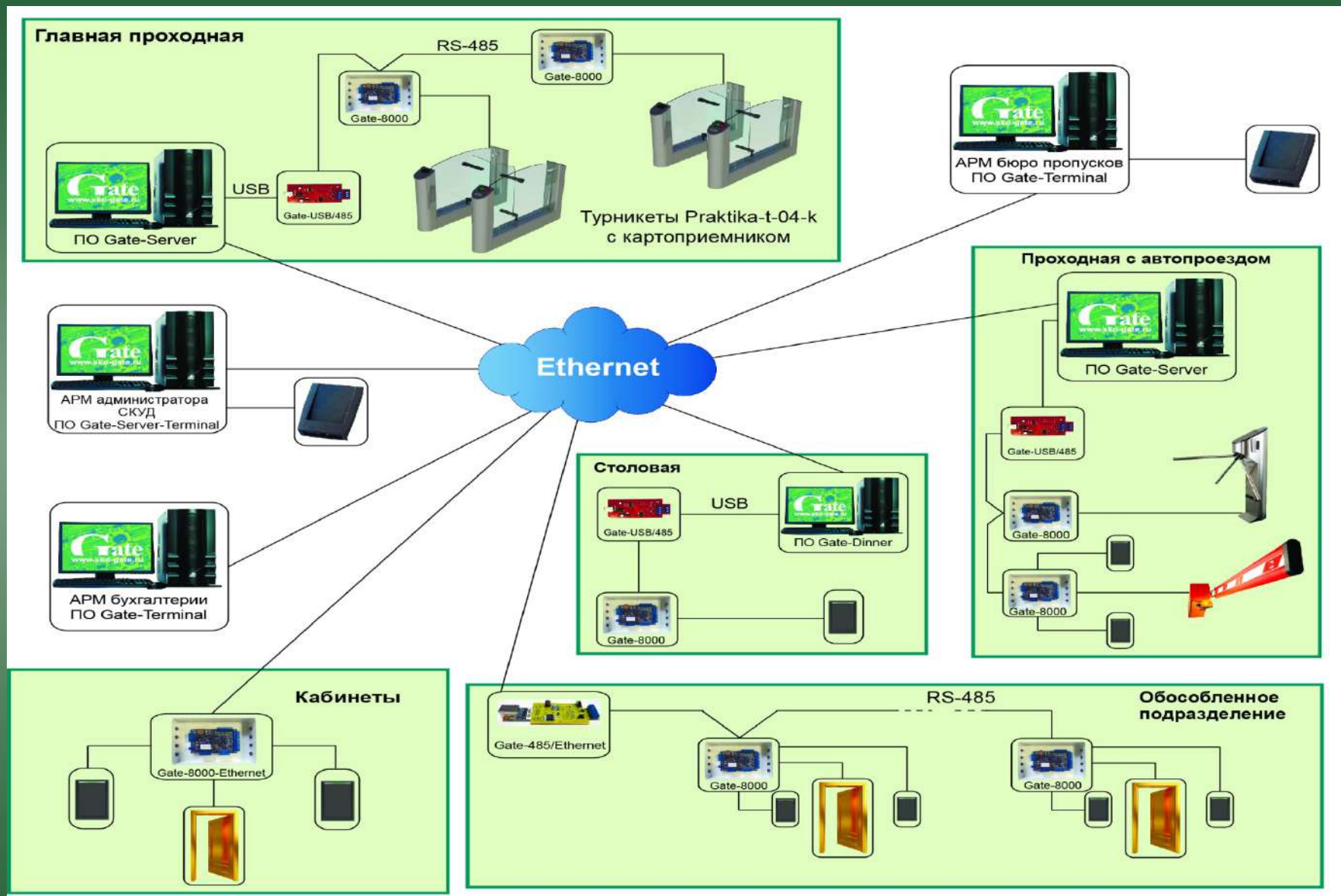
Цель: формирование единой базы данных включающей:

- дату и время досмотра
- информацию о транспортном средстве (номер, тип ..)
- информацию о грузе, водителе, перевозчике
- данные накладной
- фото груза
- видеозапись досмотра

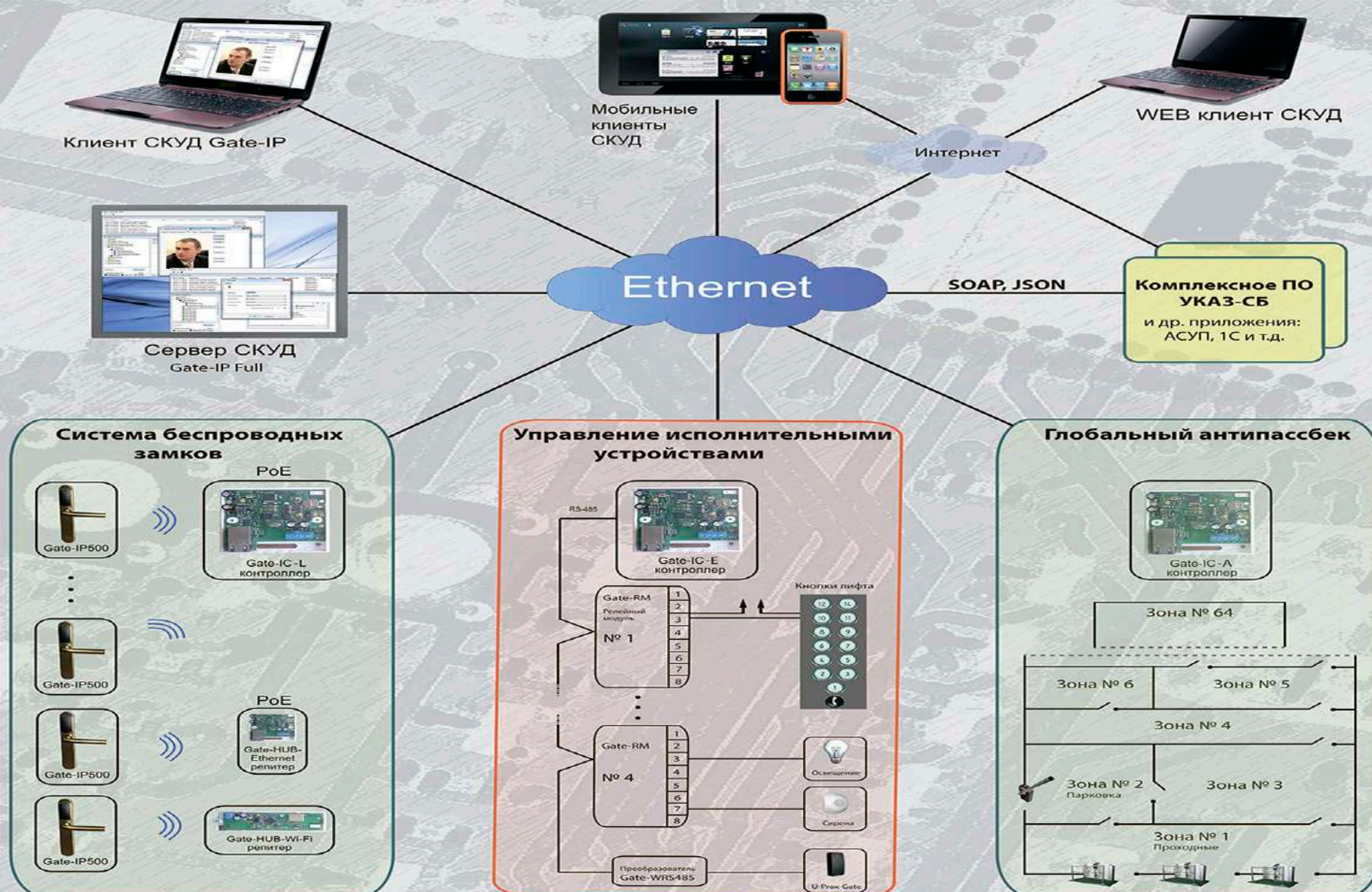
- Аудит (видеофиксация) груза, контроль документов (на транспортное средство, водителя, груз), информирование диспетчера

Идентификация транспортного средства, получение разрешения на въезд от охранника, включение видеозаписи событий

Пример построенияСКУД Gate



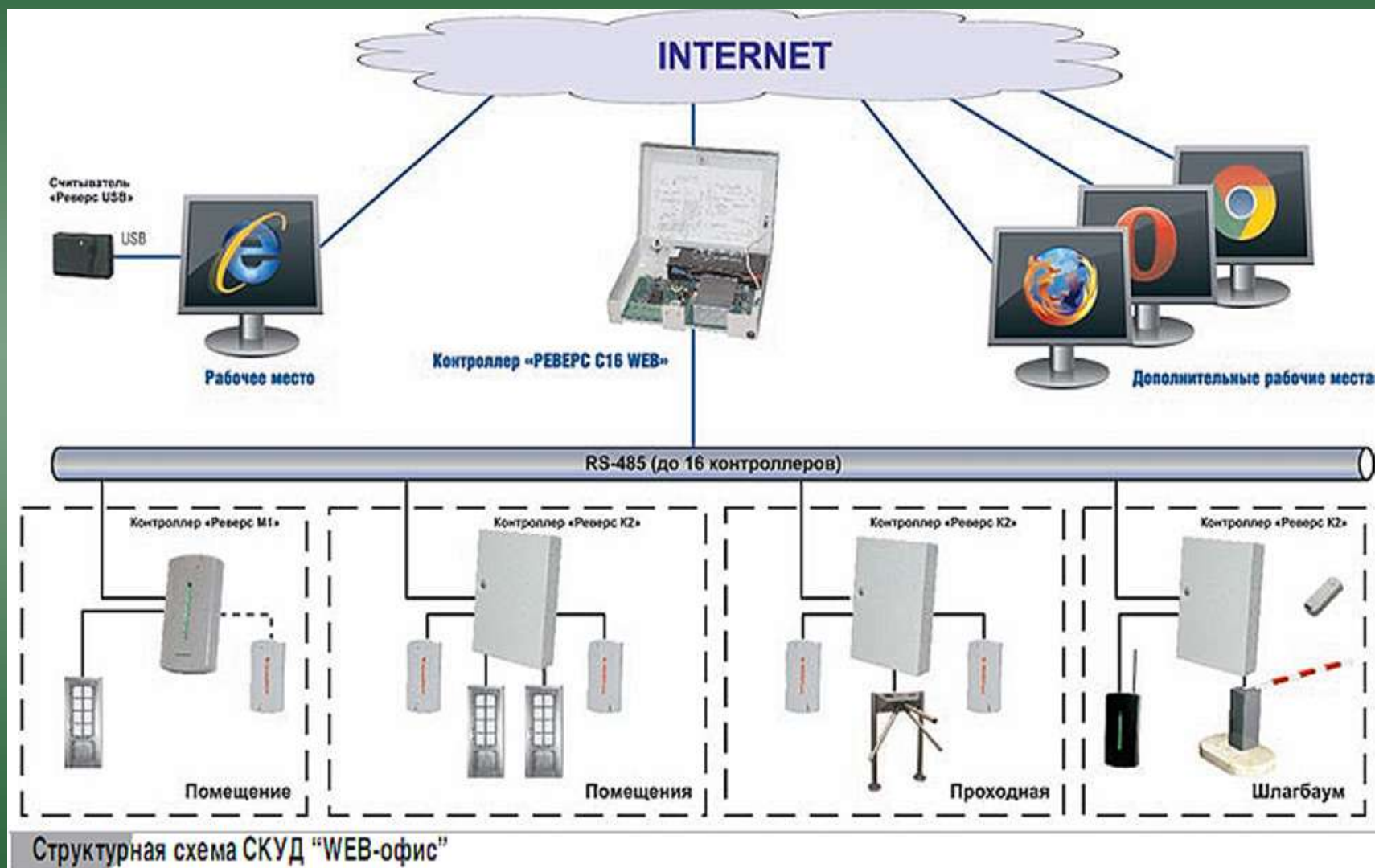
Вариант решения сетевой СКУД на оборудовании Gate-IP



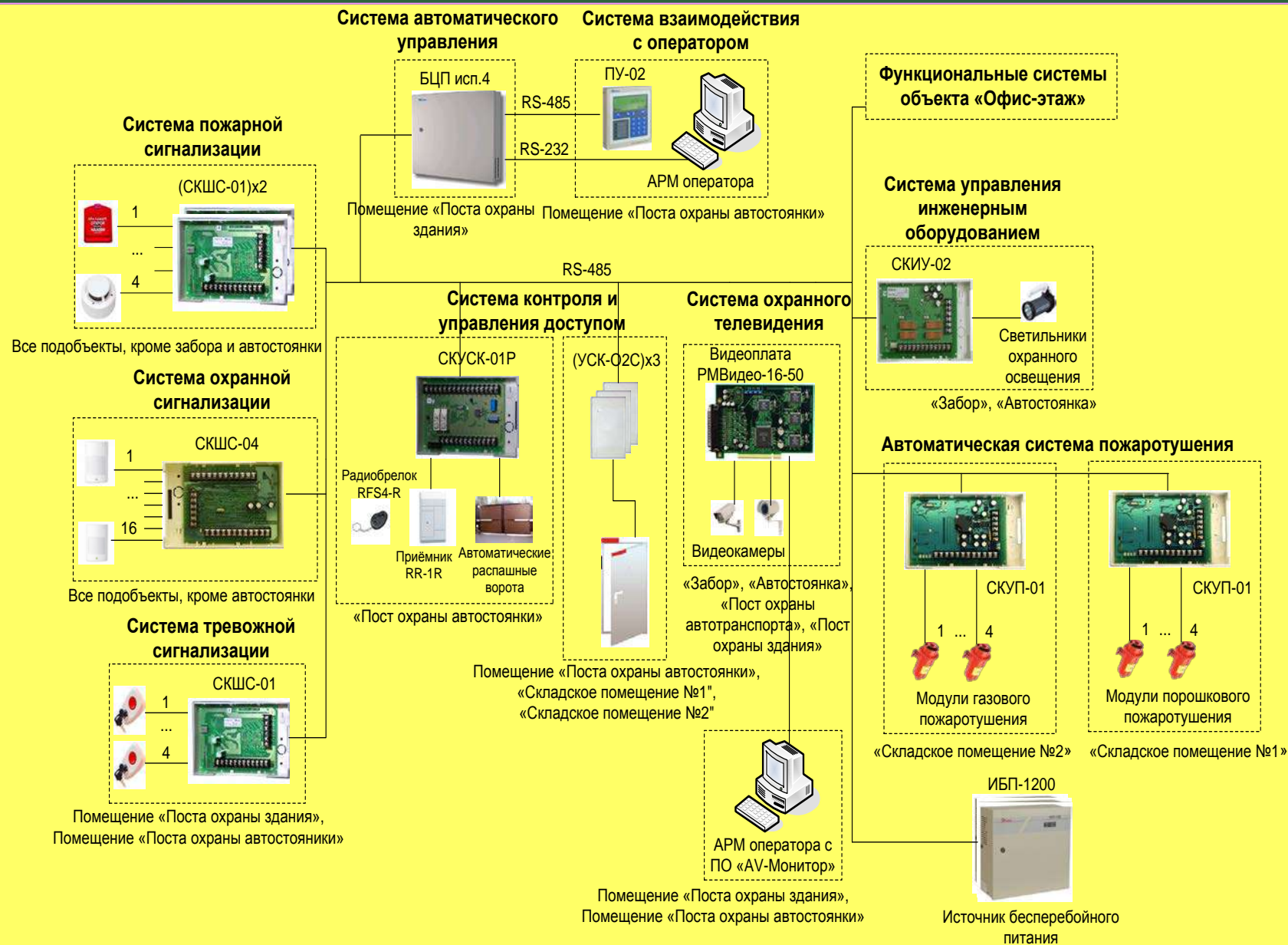
Особенности передачи данных в IP-СКУД:

- Нотификационная схема работы коммутатора.
- Постоянный контроль каналов связи.
- Защита протоколов передачи данных.
- Резервирование путей передачи данных.
- Использование преимуществ сетевых протоколов (DHCP, DNS).

Вариант решения сетевой СКУД на оборудовании Реверс (Кронверк)



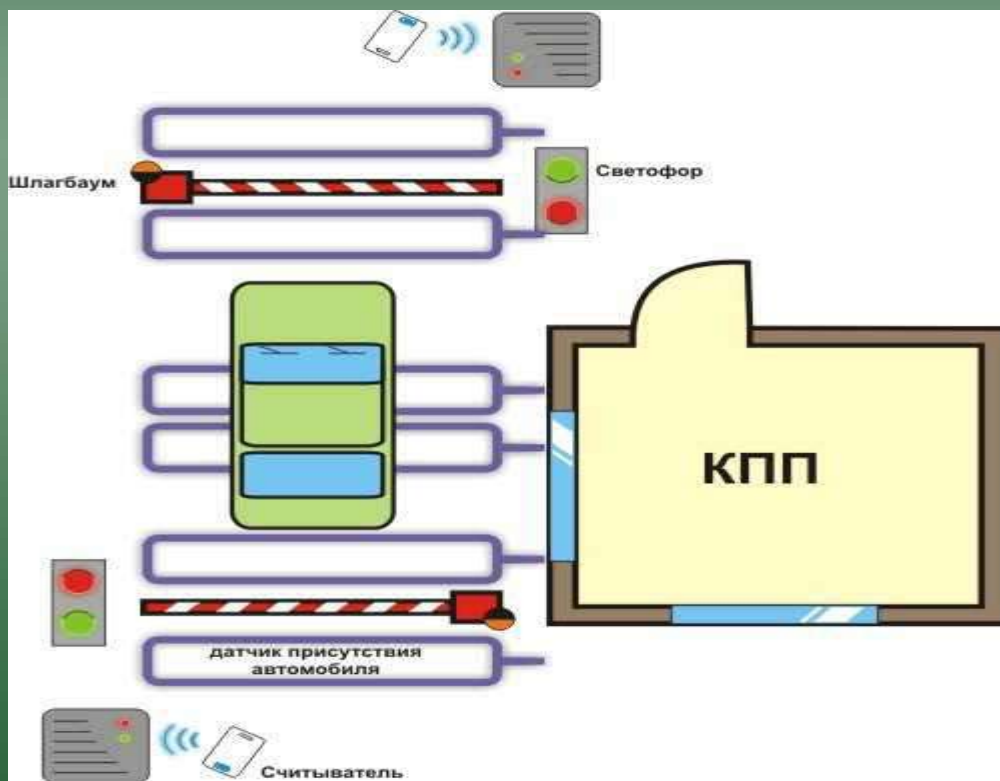
Решение СКУД ИСБ РУБЕЖ



Аппаратные и программные средства ИСБ «Рубеж»

Автоматизированная система проезда (транспортный шлюз)

предназначен для осуществления автоматического доступа (въезда и выезда на автомобиле) на охраняемую территорию. Строится на базе программного обеспечения Рубеж-08 и аппаратных модулей БЦП Рубеж-08 исп.5 и контроллера СК-01.



Алгоритм работы следующий:

1. Автомобиль становится на линию въезда/выезда
2. Водитель подносит карточку к считывателю
3. При наличии допуска и состояния шлюза "Свободен", система зажигает светофор на противоположной стороне красным и открывает шлагбаум на въезд.
4. Если система детектирует наличие автомобиля в шлюзе и отсутствие препятствий для закрывания въездного шлагбаума (автомобиль полностью въехал и за ним следом не следует другой автомобиль), то он закрывается, и въездной светофор переходит в режим въезд запрещен.
5. После закрывания въездного шлагбаума открывается шлагбаум на выезд, и система ждет, пока автомобиль полностью покинет шлюз.



Успехов в работе!

