МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
УНИВЕРСИТЕТ ИТМО

В. В. Волхонский

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Учебное пособие

Санкт-Петербург
2015

Волхонский В.В. Системы контроля и управления доступом. – СПб: Университет ИТМО, 2015. – 105 с. Рис. 96. Библ. 6.

Рассматриваются системы контроля и управления доступом. Анализируются особенности функционирования, основные характеристики и параметры, которые целесообразно учитывать при проектировании системы, выборе алгоритма ее работы и конкретной аппаратуры для реализации.

Учебное пособие построено как конспект лекций в форме презентаций, в нем приводятся все необходимые иллюстрации (схемы, графики, диаграммы и т.п. материал). В распечатанном виде позволяет конспектировать только текстовые комментарии для сокращения потерь времени на копирование иллюстративного материала во время прослушивания лекций.

Учебное пособие предназначено для обучения магистров по направлению 16.04.01 «Техническая физика» в рамках магистерской программы «Оптоэлектронные системы безопасности». Может быть рекомендовано слушателям курсов повышения квалификации и техническим специалистам, занимающимся проектированием и эксплуатацией систем ТВ-наблюдения.

Рекомендовано к печати Ученым советом инженерно-физического факультета, протокол № 3 от 10.03.2015 .

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Предисловие

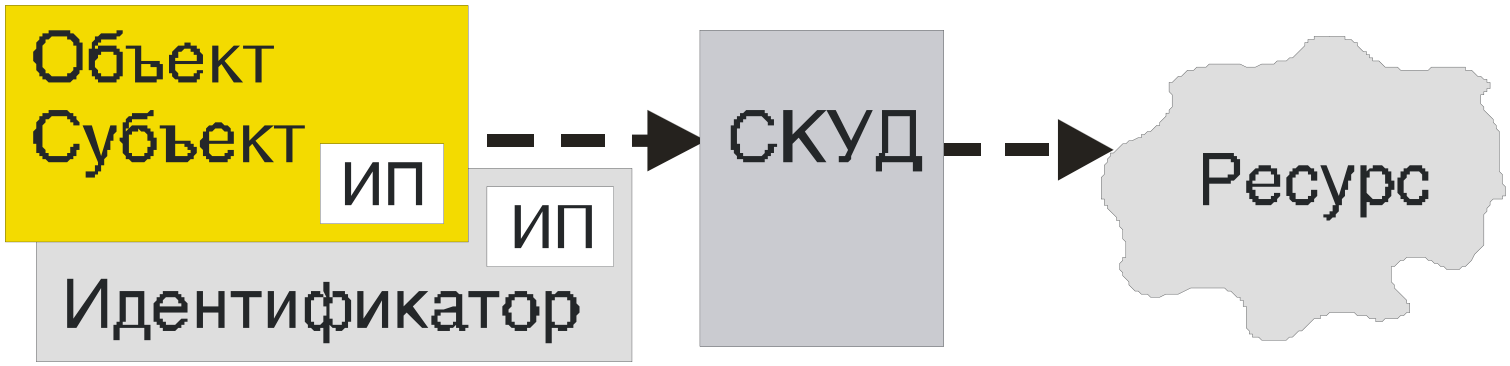
Одной из важнейших задач обеспечения безопасности жизнедеятельности человека является контроль и управление перемещением людей или предметов по определенным маршрутам и зонам. Как примеры можно привести контроль допуска служащих на предприятие; людей в подъезды дома, в котором они живут; обнаружение выноса неоплаченных товаров из магазина или проноса неразрешенных к провозу в самолете предметов и т. д. Все это может решаться системами контроля и управления доступом.

В основу пособия положены материалы лекций, которые автор читает Национальном исследовательском университете информационных технологий, механики и оптики, а также материалы статей, опубликованных в изданиях по безопасности.

Учебное пособие построено как конспект лекций в форме презентаций, в нем приводятся все необходимые иллюстрации (схемы, графики, диаграммы и т.п. материал). Электронная версия может быть распечатана так, что позволяет конспектировать только текстовые комментарии для сокращения потерь времени на копирование иллюстративного материала во время прослушивания лекций.

Пособие предназначено, прежде всего, для обучения студентов, но может быть полезно техническим специалистам, связанным с разработкой и эксплуатацией систем охранной сигнализации, а также с подготовкой и переподготовкой таких специалистов в различных учебных заведениях.

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ



Что должна выполнить СКУД?

- Обнаружение некоего субъекта или объекта, претендующего на право доступа к некоторому ресурсу .
- Опознавание этого субъекта или объекта по определенным отличительным признакам.
- Проверку законности владения им этими признаками.
- Проверку правомочности попытки доступа.
- Разрешение или отказ в доступа.

Государственный стандарт ГОСТ Р 51241-2008.
Средства и системы контроля и управления доступом.

- *Доступ* – перемещение субъекта или объекта в(из) некоторую зону или получение возможности взаимодействия с определенным материальным или информационным ресурсом.
- *Субъект доступа* (СД) или *объект доступа* (ОД) – человек, живое существо, предмет или физический процесс претендующий на право доступа.
- *Зона* – часть контролируемого объекта, ресурса (помещение, здания, территория, канал связи, область на носителе информации,…).

- *Идентификация* – процедура опознавания субъекта или объекта по присущему ему или присвоенному ему некоторому носителю идентификационным признакам.

- *Аутентификация* - проверка принадлежности субъекту доступа предъявленного им идентификатора (процедура проверки правомочности владения субъектом или объектом предъявленным идентификационным признаком).

- *Контроль и управление доступом (КУД)* – идентификация, аутентификация, контроль санкционированности и управление доступом в контролируемую зону.

Для опознавания СД он должен обладать идентификационными характеристиками.

Идентификационные характеристики в свою очередь характеризуются идентификационными параметрами или признаками.

- *Идентификационные признаки (ИП)* – набор параметров, содержащих информацию, достаточную для решения задач идентификации и(или) аутентификации.
- *Идентификатор* – носитель идентификационных признаков или параметров:
  - предмет, принадлежащий субъекту или объекту доступа
  - сам субъект или объект доступа:
    - физические признаки;
    - знания субъекта доступа.

Идентификаторы:

- индивидуальные;
- групповые.

- *Действительный идентификатор* – идентификатор с идентификационными признаками, допускающий перемещение СД через данную точку доступа (ТД) в данный временной и календарный период.

- *СКУД* – совокупность методов и средств контроля и управления доступом, функционирующих и взаимодействующих по определённым правилам.

Зоны, в которые должен контролироваться доступ, могут обладать различными особенностями.

- *Зона контролируемого доступа* – зона, доступ в которую контролируется СКУД.

- *Зона разрешенного (санкционированного) доступа* – зона, доступ в которую определенному субъекту или объекту разрешен только в определенные временные и календарные интервалы.

- *Зона неразрешенного (несанкционированного) доступа* – зона, доступ в которую определенному субъекту или объекту запрещен в определенные временные и календарные интервалы.

- *Зона свободного (неконтролируемого) доступа* – зона, доступ в которую не ограничивается.

- *Зона ограниченного по времени доступа* – зона, доступ в которую ограничивается только временными и календарными интервалами.

- *Зона ограниченного доступа объектов* – зона, доступ в которую ограничивается правилами запрета перемещения определенных объектов, предметов.

- *Санкционированный доступ* – доступ, не нарушающий правила управления доступом (доступ СД, имеющего соответствующий уровень доступа).
- *Несанкционированный доступ* – доступ, нарушающий правила управления доступом (доступ СД, не имеющего права доступа).
- *Разграничение доступа* – разрешение перемещения по одним маршрутам и запрет перемещения по другим.
- *Точка доступа* – часть объекта, оборудованная соответствующими средствами, в которой осуществляется контроль и управление доступом.

Уровень доступа – это совокупность разрешенных точек доступа и соответствующих им разрешенных временных и календарных интервалов.

- Составляющие уровня доступа:
  - пространственная (то есть маршруты перемещения или перечень разрешенных зон доступа);
  - временная (временные и календарные интервалы);
  - специальные.
- Уровень доступа включает в себя:

1. Перечень разрешенных зон контролируемого доступа
2. Совокупность разрешенных точек доступа в эти зоны.
3. Допустимые временные и календарные интервалы доступа в эти зоны
4. Уровень угрозы

$$У(d_1, d_2, \ldots, d_N, \Delta t_1, \Delta t_2, \ldots, \Delta t_M, \Delta T_1, \Delta T_2, \ldots, \Delta T_J, L)$$

$У(d_1, d_2, \ldots, d_N, \Delta t_1, \Delta t_2, \ldots, \Delta t_M, \Delta T_1, \Delta T_2, \ldots, \Delta T_J, L)$

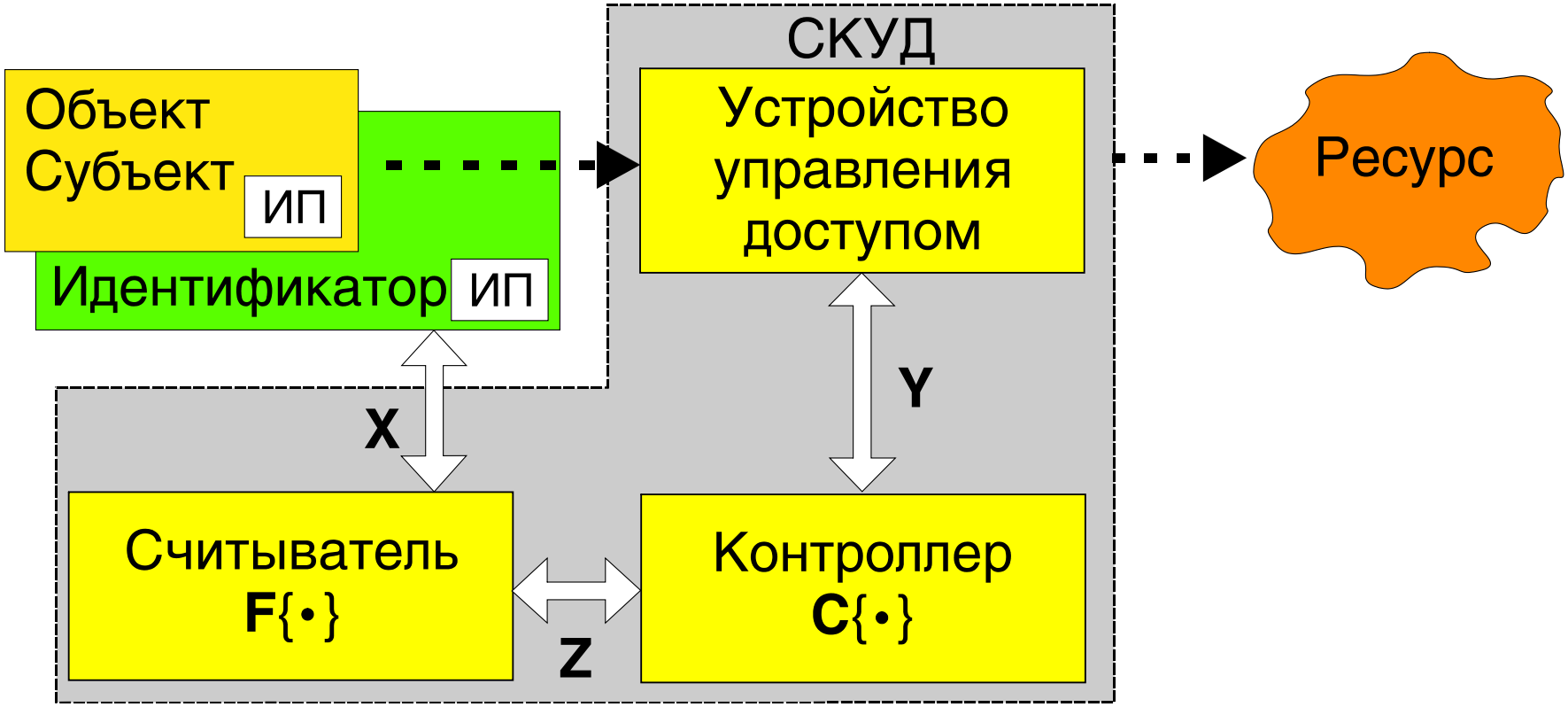
$У(d_1, d_2, \ldots, d_N)$

$У(d_1);\ У(d_2)$

$У(d_1);\ У(d_1, d_2);\ У(d_1, d_2, d_3)$

- СКУД должна выполнить следующие основные процедуры:
  - идентификацию субъекта или объекта;
  - аутентификацию;
  - проверку санкционированности доступа;
  - разрешение или запрет доступа;
  - протоколирование событий.

- Основные элементы:
  - устройство считывания идентификационных признаков - считыватель(и) ;
  - устройство анализа ИП и принятия решения – контроллер;
  - устройство управления доступом .


СКУД
Объект
Субъект
ИП
Идентификатор
ИП
Устройство управления доступом
Ресурс
X
Y
Считыватель
F{•}
Z
Контроллер
C{•}

Для решения задач контроля и управления доступом система должна включать в себя три основных элемента:

- устройство считывания идентификационных признаков (считыватель);
- устройство анализа ИП и принятия решения (контроллер);
- устройство управления доступом.

Устройство управления доступом включает в себя:

- преграждающее управляемое устройство (дверь, турникет и т.п. устройства и конструкции);
- исполнительное устройство для управления состоянием преграждающего устройства (например, электромагнитный замок);
- элементы контроля состояния преграждающего устройства (к примеру, магнитоконтактный датчик);
- элементы неконтролируемого управления состоянием преграждающего устройства.

Идентификационные характеристики преобразуются в набор идентификационных параметров

$$\mathbf{X} = \begin{bmatrix} x_{11} & x_{21} & \cdots & x_{K1} \\ x_{12} & \cdots & \cdots & x_{K2} \\ \cdots & x_{km} & \cdots & \cdots \\ x_{1M} & \cdots & \cdots & x_{KM} \end{bmatrix}$$

$$\mathbf{Z} = \mathrm{F}\{\mathbf{X}\}$$

$$\mathbf{Z} = \begin{bmatrix} z_{11} & z_{21} & \cdots & z_{K1} \\ z_{12} & \cdots & \cdots & z_{K2} \\ \cdots & z_{km} & \cdots & \cdots \\ z_{1M} & \cdots & \cdots & z_{KM} \end{bmatrix}$$

$$\mathbf{Y}_i = \mathbf{C}\left\{\mathbf{Z}, \mathbf{Z}_i^0\right\}\Big|_{i=1\ldots\mathrm{I}} \qquad \mathbf{Z} - \mathbf{Z}_{i0} = \mathbf{0}$$

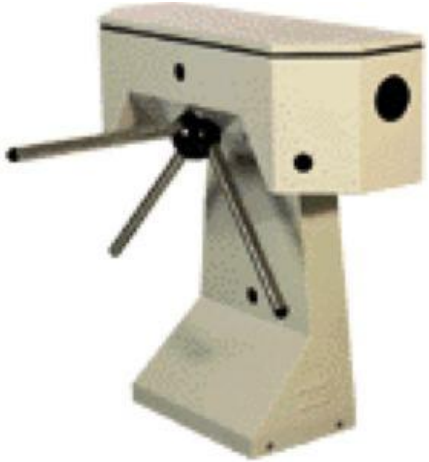
Примеры элементов СКУД

Клавиатура

Считыватель бесконтактных карт

Контроллер СКУД

Преграждающее устройство – турникет



- Устройство управления доступом включает в себя:
  - преграждающее устройство (дверь, турникет, шлагбаум, шлюзовая кабина, …);
  - исполнительное устройство для управления состоянием преграждающего устройства (э/м замок, …);
  - элементы возврата преграждающего устройства в исходное состояние;
  - элементы контроля состояния преграждающего устройства;
  - элементы неконтролируемого управления состоянием преграждающего устройства.

Устройства преграждающие управляемые (УПУ):

Устройства, обеспечивающие физическое препятствие доступу и оборудованные исполнительными устройствами для управления их состоянием (турникеты, шлюзы, проходные кабины, двери и ворота, оборудованные исполнительными устройствами СКУД, а также другие подобные устройства).

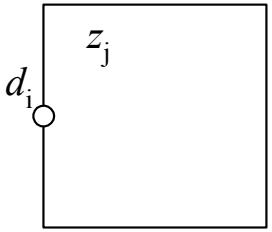
Устройства исполнительные (УИ):

Устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние УПУ (электромеханические, электромагнитные замки, электромагнитные защелки, механизмы привода шлюзов, ворот, турникетов и другие подобные устройства).

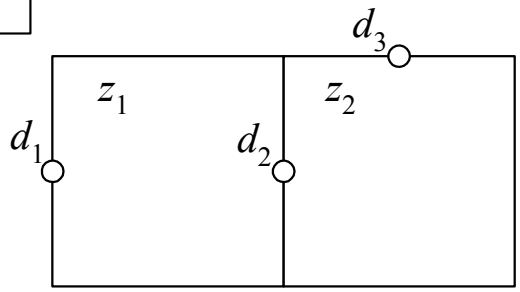
Устройство считывающее (УС), считыватель:

Устройство, предназначенное для считывания (ввода) идентификационных признаков.

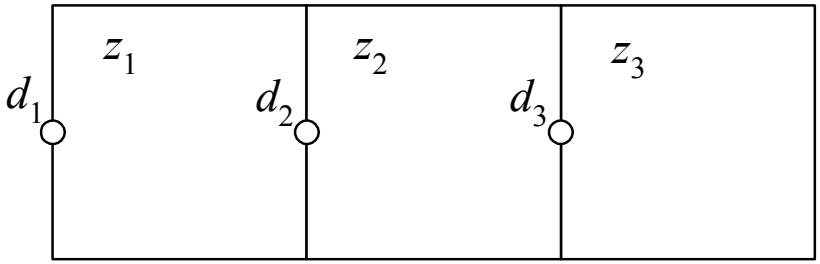
Одиночная зона



Связанные зоны (перемещение в одну возможно через другие)

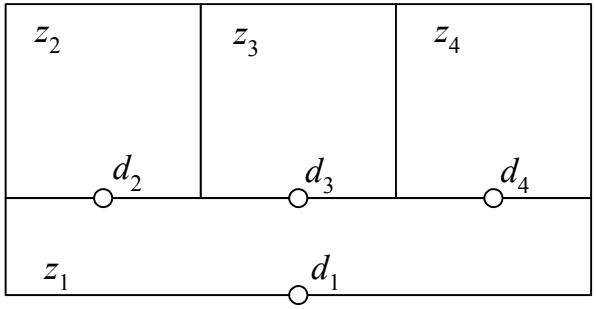


- Последовательно связанные зоны

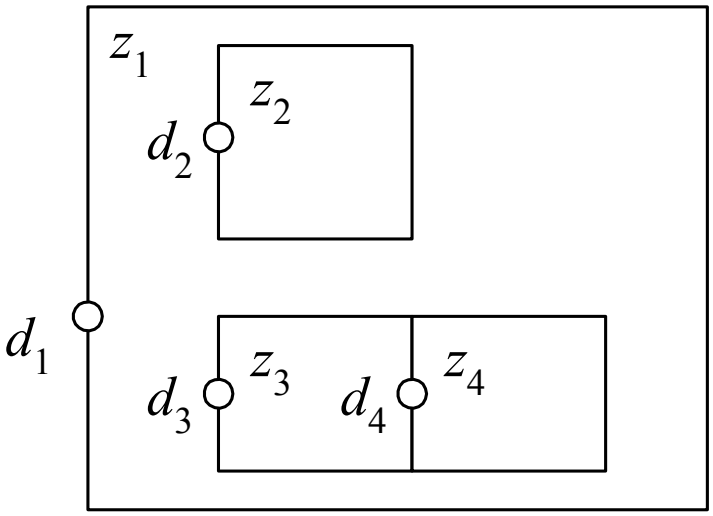


- Параллельно связанные

- Произвольно связанные



Вложенные зоны

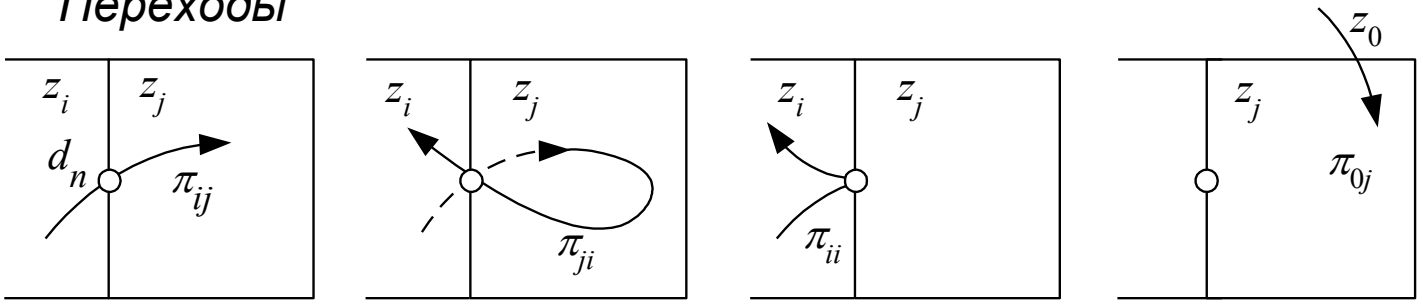


Уровень вложения зон

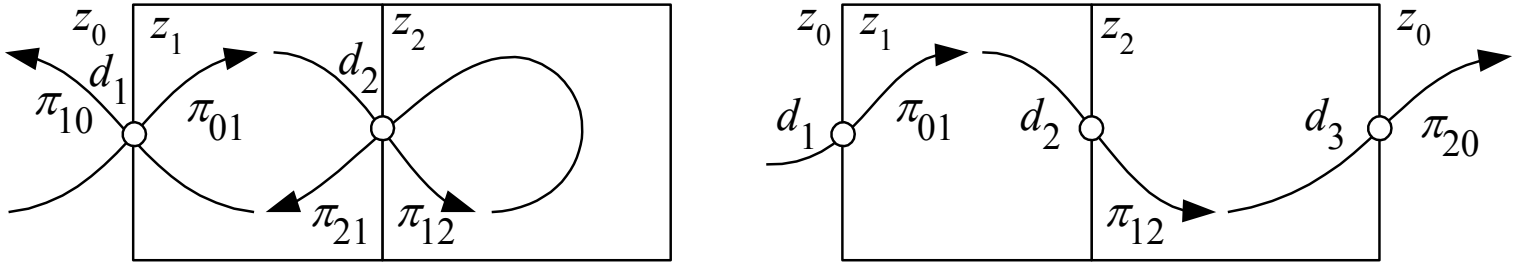
Внешние зоны контролируемого доступа – зоны, доступ в которые возможен из зон свободного доступа.

Внутренние зоны контролируемого доступа – зоны, доступ в которые возможен только из других зон контролируемого доступа.

Переходы



Маршрут субъекта доступа – это конечная последовательность переходов, выполненных им.



Зоны, с которых начинается и которыми заканчивается маршрут, называются *концевыми*. Остальные являются *внутренними*.

Замкнутый маршрут начинается и заканчивается в одной и той же зоне доступа. В противном случае маршрут называется *открытым*.

Полный маршрут начинается и оканчивается на внешних концевых зонах свободного доступа и включает в себя все переходы, выполненные в зонах контролируемого доступа на объекте.

Полный замкнутый маршрут начинается и заканчивается в одной и той же внешней концевой зоне свободного доступа.

Маршрут может быть *квазизамкнутым*, когда субъект доступа перемещается в контролируемую зону из зоны свободного доступа через одну точку доступа, а выходит также в ЗСД, но через другую внешнюю ТД .

1. ***Санкционированность*** – любые действия в СКУД должны подтверждаться соответствующим уровнем доступа.
2. ***Неповторяемость*** – прохождение одной и той же точки доступа не может быть выполнено дважды подряд в одном и том же направлении без прохождения других ТД или этой же ТД в обратном направлении.
3. ***Непрерывность*** – санкционированное перемещение через точки доступа по маршруту должно осуществляться только с последовательным прохождением подряд всех связанных зон и соответствующих этим зонам точек доступа без пропуска на данном маршруте.
4. ***Замкнутость*** – маршрут перемещения субъекта доступа должен быть замкнутым (квазизамкнутым) в пределах установленных уровнем доступа временных и календарных интервалов.
5. ***Монотонность*** – требуемый уровень доступа для каждой из следующих последовательно связанных зон должен быть выше, иначе нет необходимости в соответствующих точках доступа и зоны могут быть объединены.

Точка доступа – это часть объекта, оборудованная соответствующими средствами, в которой осуществляется контроль и управление доступом.

К числу этих средств, в первую очередь, относятся:

- считыватели;
- контроллер;
- устройства неконтролируемого управления (к примеру, кнопка управления выходом);
- управляемое преграждающее устройство (турникет, дверь и тому подобные конструкции);
- исполнительное устройство (например, электромагнитный замок).

По расположению на контролируемом объекте.

- Внешние, через которые осуществляется перемещение из ЗСД в зоны контролируемого доступа или выход из ЗКД в ЗСД.
- Внутренние, при прохождении которых СД не покидает пределов зон контролируемого или ограниченного по времени доступа.

По характеру взаимодействия точек доступа друг с другом.

- Связанные – алгоритм работы которых зависит от алгоритма других ТД.
- Не связанные – ТД, функционирующие независимо от других.

По направлению перемещения.

- Однонаправленные, движение через которые осуществляется только в одном направлении.
- Ненаправленные, движение через которые может осуществляться в обоих направлениях.

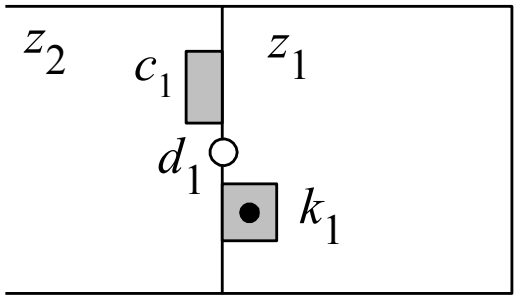
По способу контроля направления перемещения.

- С односторонним контролем доступа, в которых контроль доступа осуществляется только в одном направлении.
- С двухсторонним контролем доступа.

Точка доступа с односторонним контролем

Точка доступа, в которой контролируется и фиксируется только факт прохода, без определения направления. Т.е. используется, к примеру, один и тот же считыватель для контроля и управления проходом в обоих направлениях.

Пройти в прямом, направлении может только обладатель действительного идентификатора. В обратном - любой, находящийся в зоне доступа.



Недостатки:

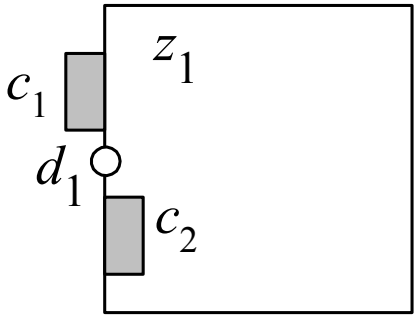
- Неизвестно, где находится субъект/объект доступа – в контролируемой зоне или вне). Причина – выход не контролируется, и система не может фиксировать факт выхода субъекта, вошедшего на объект.

- Вследствие неконтролируемого выхода возникает возможность использования одного и того же идентификатора для многократного, повторного прохода через эту точку доступа.

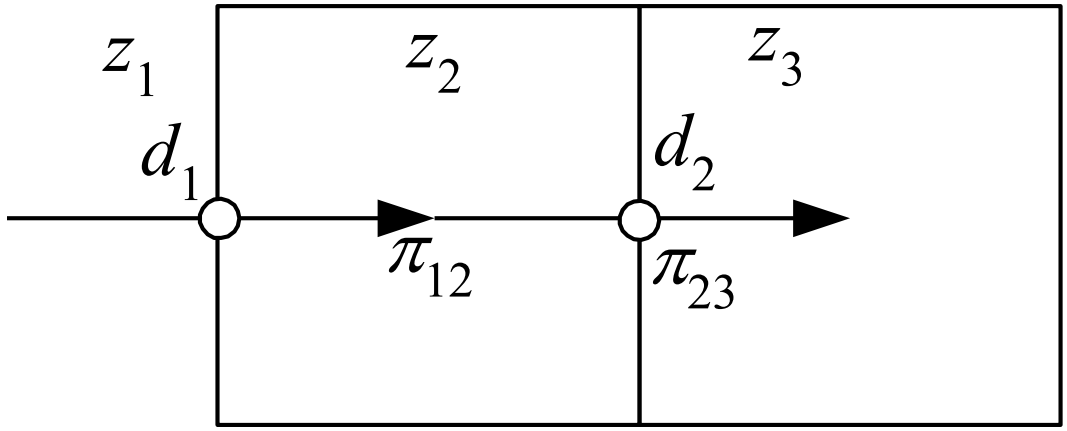
Эти рассуждения справедливы для СКУД, в которых не используется аутентификация – то есть проверка правомочности владения субъектом предъявляемого идентификатора.

Точка доступа с двухсторонним контролем

Точка доступа, в которой контролируется и фиксируется также и направление перемещения. Для этого обычно используются отдельные считыватели для контроля и управления дверью при проходе с каждой стороны.



Связанные ТД – алгоритм работы которых зависит от алгоритма работы других точек доступа



- *Наблюдение* - действия, производимые с устройствами СКУД, без прямого доступа к ним, с целью получения действующего кода.
- *Съем информации о СКУД* – действия направленные на получение информации об идентификационных характеристиках и параметрах СКУД.
- *Манипулирование* – действия, производимые с устройствами контроля доступа, находящимися в рабочем режиме, с целью получения действующего идентификатора или приведению в открытое состояния устройства управления доступом. Манипулирование включает также несанкционированные действия над программным обеспечением и по съему информации с каналов связи и интерфейсов устройств доступа. .

- *Копирование* – действия, производимые с идентификаторами, целью которых является получение копии идентификатора с действующим кодом.
- *Принуждение* – насильственные действия по отношению к лицу, имеющему право доступа, с целью несанкционированного проникновения через устройства управления доступом.
- *Повреждение* – воздействие, приводящее к механическому или электрическому повреждению устройств СКУД.
- *Кража* – незаконное завладение идентификатором.

Методы идентификации

Идентификатор – носитель идентификационных признаков

Методы идентификации основаны на том, что:

- имеет ОД или СД;
- СД знает;
- принадлежит ОД или СД.

Существуют разные способы реализации методов .

Материальный носитель, предмет (то, что пользователь имеет):

- ключ;
- карта;
- номерной знак автомобиля ;
- … .

Знания субъекта (то, что пользователь знает):

- пароль;
- … .

[12345]

Сам субъект или его индивидуальные особенности

- биометрические признаки, то, что характеризует пользователя как индивидуума):
  - отпечаток пальца;
  - радужная оболочка глаза;
  - геометрия лица;
  - … .

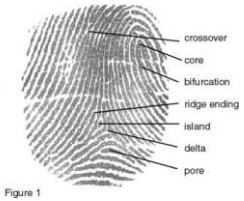


Figure 1

- Скрытность его использования.
- Устойчивость к несанкционированным действиям.
- Сложность съема информации об идентификационных признаках и их параметрах и использования тем или иным способом этой информации.
- Сложность использования самого идентификатора для несанкционированных действий в СКУД.

Основа метода идентификации	Защищенность от НСД						Возможность аутентификации
	Кража	Съем информации	Манипулирование	Копирование	Принуждение	Повреждение	
То, что пользователь имеет	Н	В	В	Н…В	Н	Н…В	Н
То, что пользователь знает	В	Н	С…В	В	Н	Н…В	Н
То, что характеризует пользователя	В	В	В	П…В	Н	Н…В	В

Основной способ улучшение защищенности:

совмещение нескольких методов идентификации

По способу взаимодействия идентификатора и считывателя:

- безконтакные (дистанционного действия);
- контакные (с непосредственным взаимодействием).

По наличию источника питания в идентификаторе:

- с пассивными идентификаторами;
- с активными идентификаторами.

По количеству объектов или субъектов идентификации:

- индивидуальные (персональные);
- групповые.

По возможности аутентификации:

- с возможностью;
- без возможности.

По количеству одновременно используемых идентификационных характеристик:

- с одной;
- с несколькими.

По принадлежности СОД:

- неотъемлемо принадлежащие СОД;
- зафиксированные с принципиальной возможностью удаления (перемещения) без повреждения объекта;
- свободно перемещаемые.

По защищенности от съема информации:

- с закрытой от свободного считывания информацией;
- с открытой для считывания информацией.

По защищенности от копирования:

- с защитой;
- без защиты.

По возможности модификации информации:

- с возможностью;
- без возможности.

Физический способ записи/считывания ИП:

- магнитный;
- графический / оптический (в том числе ИК);
- радиочастотный;
- электромагнитный;
- эффект Виганда;
- механический;
- электронный;
- биометрический;
- другие.

Требования к идентификационным характеристикам и признакам

Неповторяемость

Идентификационные признаки не должны повторяться у любых субъектов или объектов доступа.

Достаточность

Должна быть возможность принятия однозначного решения об идентификации данного объекта или субъекта доступа.

Стабильность

ИП должны оставаться неизменными во времени.

Защищенность

Должна обеспечиваться защищенность ИП от съема информации о них и копирования, от воздействия естественных и искусственных факторов приводящих к нарушению целостности ИХ и ИП, к их частичной или полной потере.

Принадлежность

Должна обеспечиваться однозначная принадлежность идентификатора или ИП субъекту или объекту доступа, не допускающей использование этого идентификатора или ИП другим СД или ОД.

Требования к идентификационным характеристикам и признакам

Считываемость

Должна обеспечиваться возможность считывания этих признаков современными техническими средствами.

Доступность

Это возможность получения этих признаков без каких-либо юридических, этических, моральных и других норм и правил.

Наличие

Признаки должны присутствовать у всех СОД

Присваиваемость

Возможность присвоения идентификатора определенному субъекту

Приемлемость

Согласие субъекта или объекта доступа на присвоения определенного идентификационного признака.

Законность

Соответствие законам и правилам страны и территории.

С точки зрения решения задачи идентификации или аутентификации:

- предъявлен действующий идентификатор;
- предъявлен не действующий идентификатор.

С точки зрения решения задачи верификации:

- предъявленный идентификатор принадлежит субъекту или объекту доступа;
- предъявленный идентификатор не принадлежит субъекту или объекту доступа.

Система принимает решение:

- разрешение доступа;
- запрет доступа.

- Вероятность разрешения доступа при предъявлении действующего идентификатора характеризуется *вероятностью правильного предоставления доступа* $P_{п.р.}$
- Запрет доступа при предъявлении действующего идентификатора называется ложным отказом в доступе и характеризуется *вероятностью ложного отказа в доступе* $P_{л.о.}$

Эти два события образуют полную группу, т.е.

$$P_{п.р.} + P_{л.о.} = 1.$$

- Вероятность разрешения доступа при предъявлении не действующего идентификатора характеризует *вероятность несанкционированного доступа* $P_{н.д}$
- Вероятность запрета доступа при предъявлении не действующего идентификатора называется *вероятностью правильного отказа в доступе* $P_{п.о.}$

Эти два события образуют полную группу

$$P_{н.д.} + P_{п.о.} = 1.$$

Гипотеза	Решение системы идентификации			
	Разрешение доступа		Запрет доступа	
Предъявлен действующий идентификатор	Правильное разрешение доступа	$P_{\text{п.р}}$	Ложный отказ в доступе	$P_{\text{л.о}}$
Предъявлен недействующий идентификатор	Несанкциониро-ванный доступ	$P_{\text{н.д}}$	Правильный отказ в доступе	$P_{\text{о.д}}$

$P_{\text{н.д}}$ обозначаются как FAR (False Acceptance Rate) или FMR (False Match Rate).

$P_{\text{л.о}}$ – как FRR (False Rejection Rate) или FNMR (False Non-Match Rate).

Ложный отказ в доступе и несанкционированное разрешение доступа называются ошибками первого и второго рода соответственно.

Структура систем контроля и управления доступом

Параметры системы обычно определяются параметрами контроллера *СКУД*

- Количество точек доступа.
- Тип точек доступа.
- Количество пользователей.
- Уровни доступа.
- Состав и структура системы.
- Каналы связи между элементами системы.
- Каналы передачи информации о состоянии системы.
- Возможность взаимодействия с другими подсистемами (интеграция).
- Возможность и объем протокола событий.
- Наличие специальных функций (контроль повторного прохода, учет рабочего времени, …).
- Наличие функций других подсистем безопасности (охранная сигнализация, …).
- Возможность управления различным оборудованием (лифты, освещение, …).
- ….

Основные элементы СКУД

- Идентификаторы.
- Считыватели.
- Контроллеры.
- Интерфейсные модули.
  - Модули считывателей.
  - Модули входов (датчиков контроля состояния двери,…).
  - Модули выходов (управления замками, …).
  - Комбинированные.
- Центральная ССОИ .
- Вспомогательные элементы.
- …

Каналы связи:

- Выделенные линии (обмен данными с конкретным устройством).
- Шины данных (обмен данными с группой устройств).
- Выделенные сетевые системы связи.
- Сетевые системы связи общего применения (компьютерные, телефонные,…) .
- ….

Ресурсы – возможности СКУД по обработке информации и управлению, позволяющие выполнять основные функции.

1. *По сбору и обработке данных*.

- Вычислительные.
- Базы данных.
- …

2. *По взаимодействию с другими элементами системы* (преобразованию и передаче сигналов без изменения информативности).

- Интерфейсы
  - Сигнальные (RS232, RS485, Ethernet, …).
  - Приема информации (шлейфы сигнализации, …).
  - Управляющие (замками, лифтами, …).
  - ….

Архитектура - это состав и способ соединения и взаимодействия элементов системы.

- Централизованная архитектура:

  Выполнение основных функций СКУД (работа со считывателями, замками, …) осуществляется центральным устройством (контроллером) через промежуточные.

- Децентрализованная архитектура:

  Выполнение основных функций СКУД осуществляется непосредственно локальными контроллерами.

- Смешанная (комбинированная) архитектура:

  Сочетание предыдущих.

СКУД с сосредоточенными ресурсами радиальной структуры.

Без интерфейсов связи или с неиспользуемыми интерфейсами.

Возможно конструктивное совмещение контроллера со считывателем.

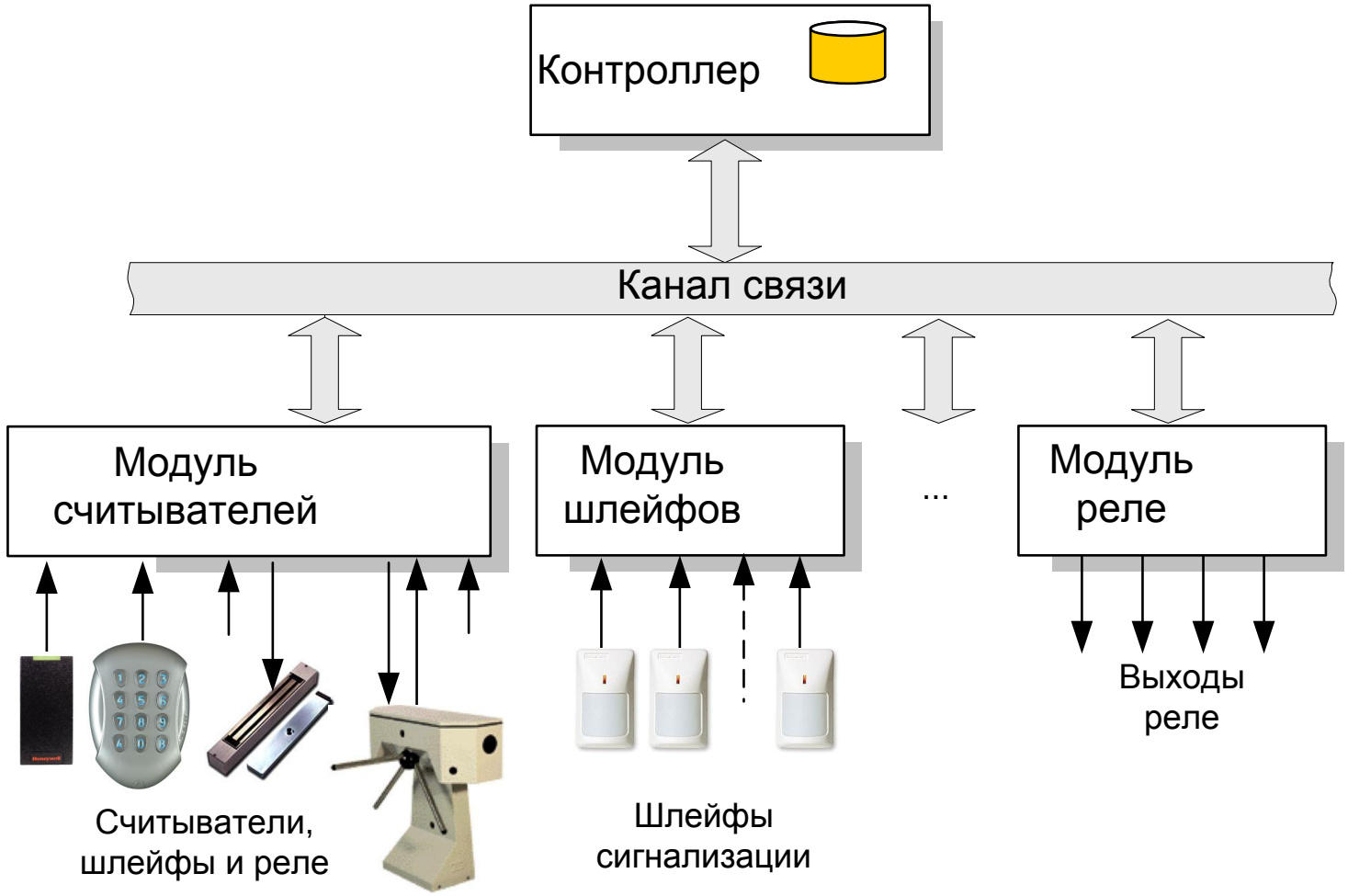
Выходы для управления:

- устройствами управления доступом (электромагнитные замки, электромеханические замки и защелки, турникеты, ..);
- оповещателями (сиренами);
- освещением;
- вентиляцией;
- лифтовым оборудованием;
- …

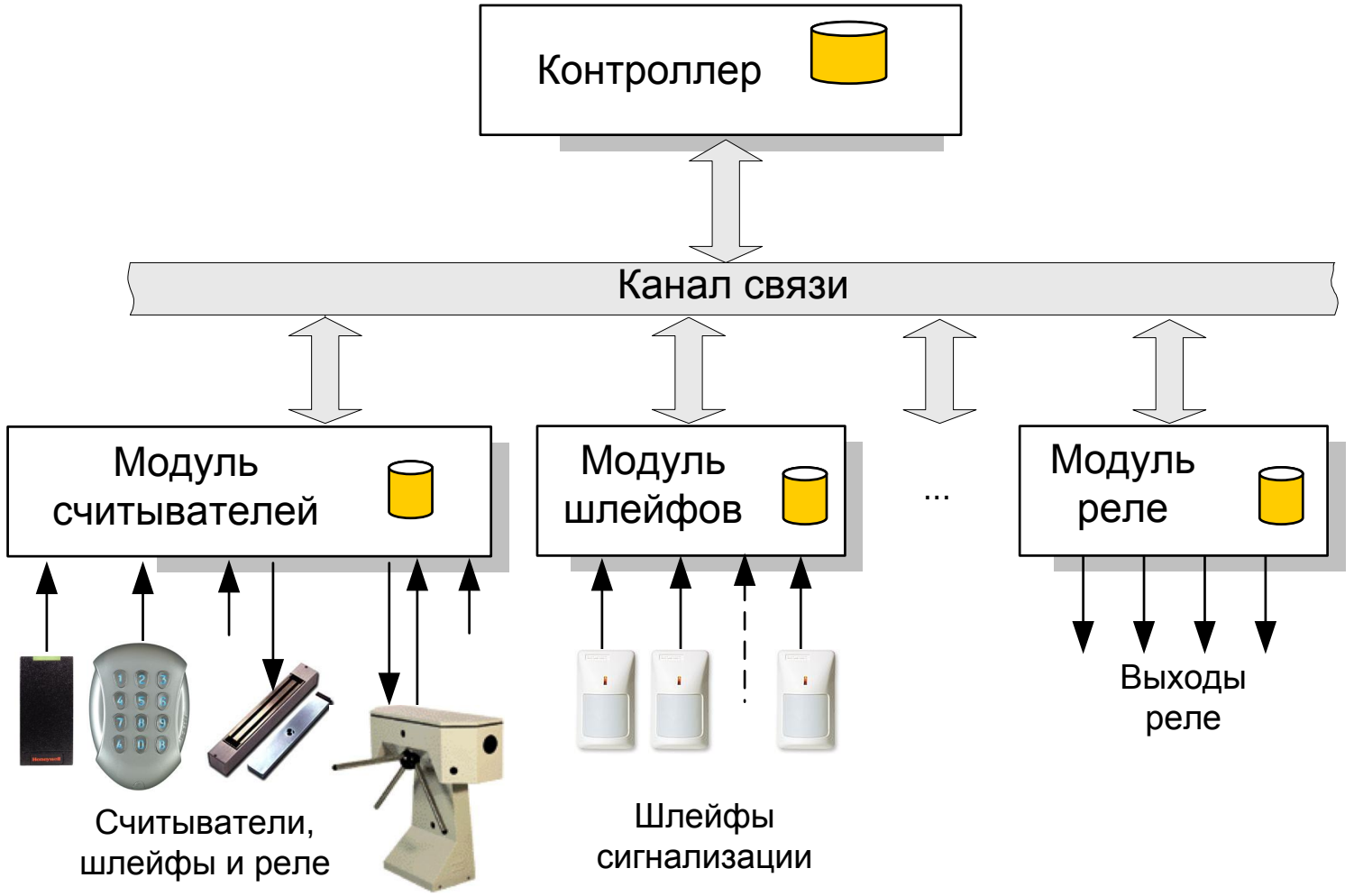
Входы шлейфов контроллера

- Контроль за состоянием устройствами управления доступом.
- Шлейфы охранной сигнализации.
- Подключение кнопок запроса на выход.
- …

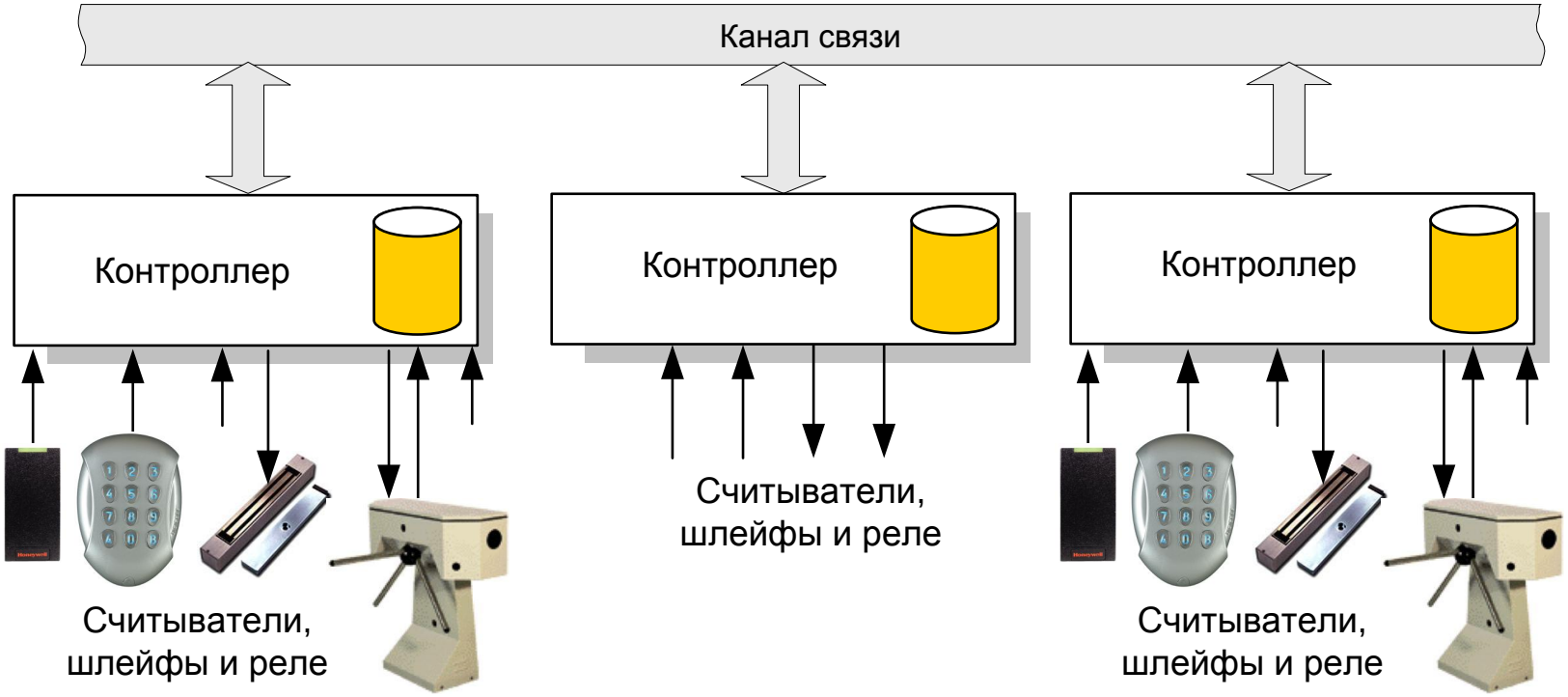
СКУД с централизованной архитектурой



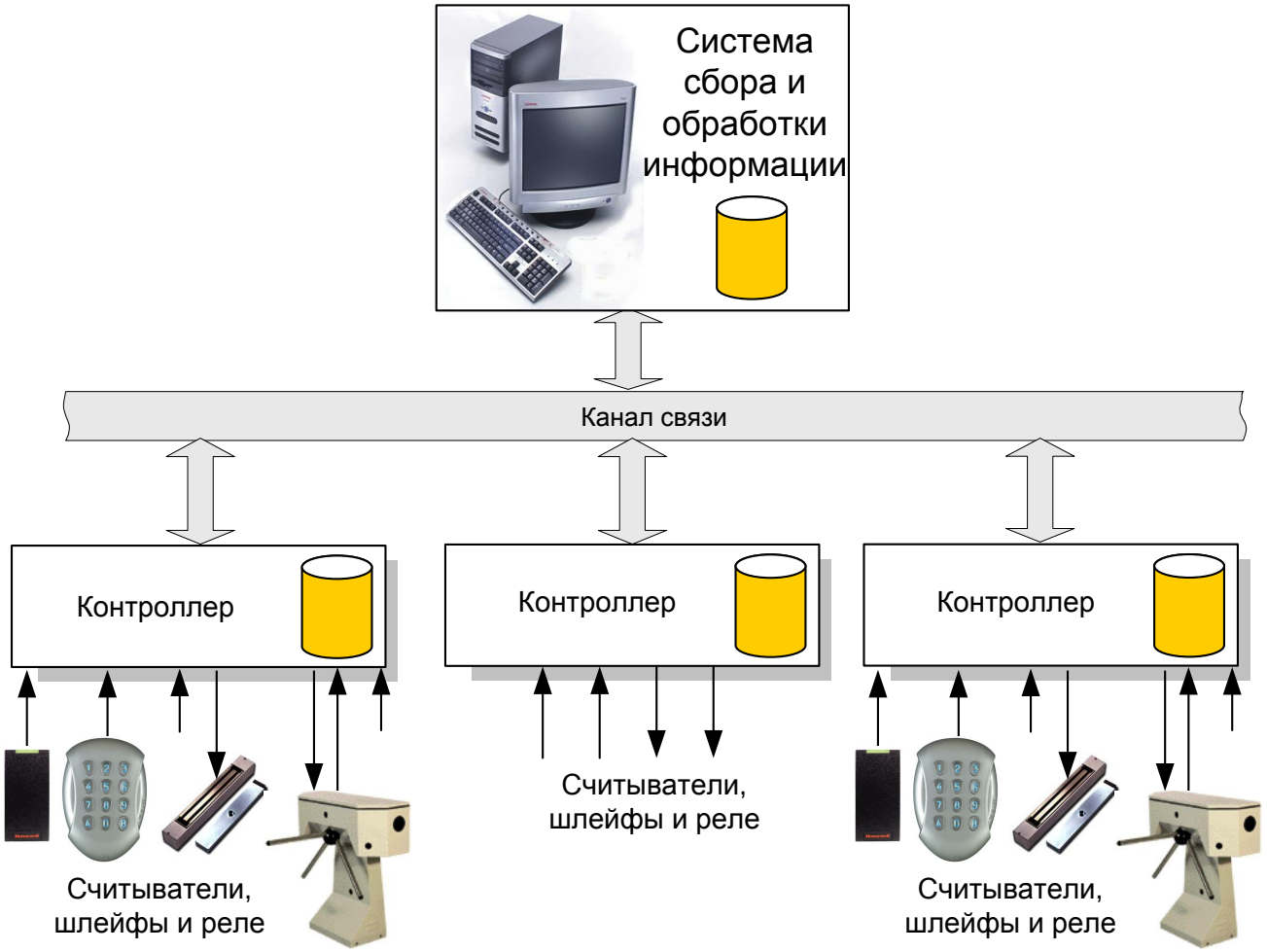
СКУД с централизованной архитектурой



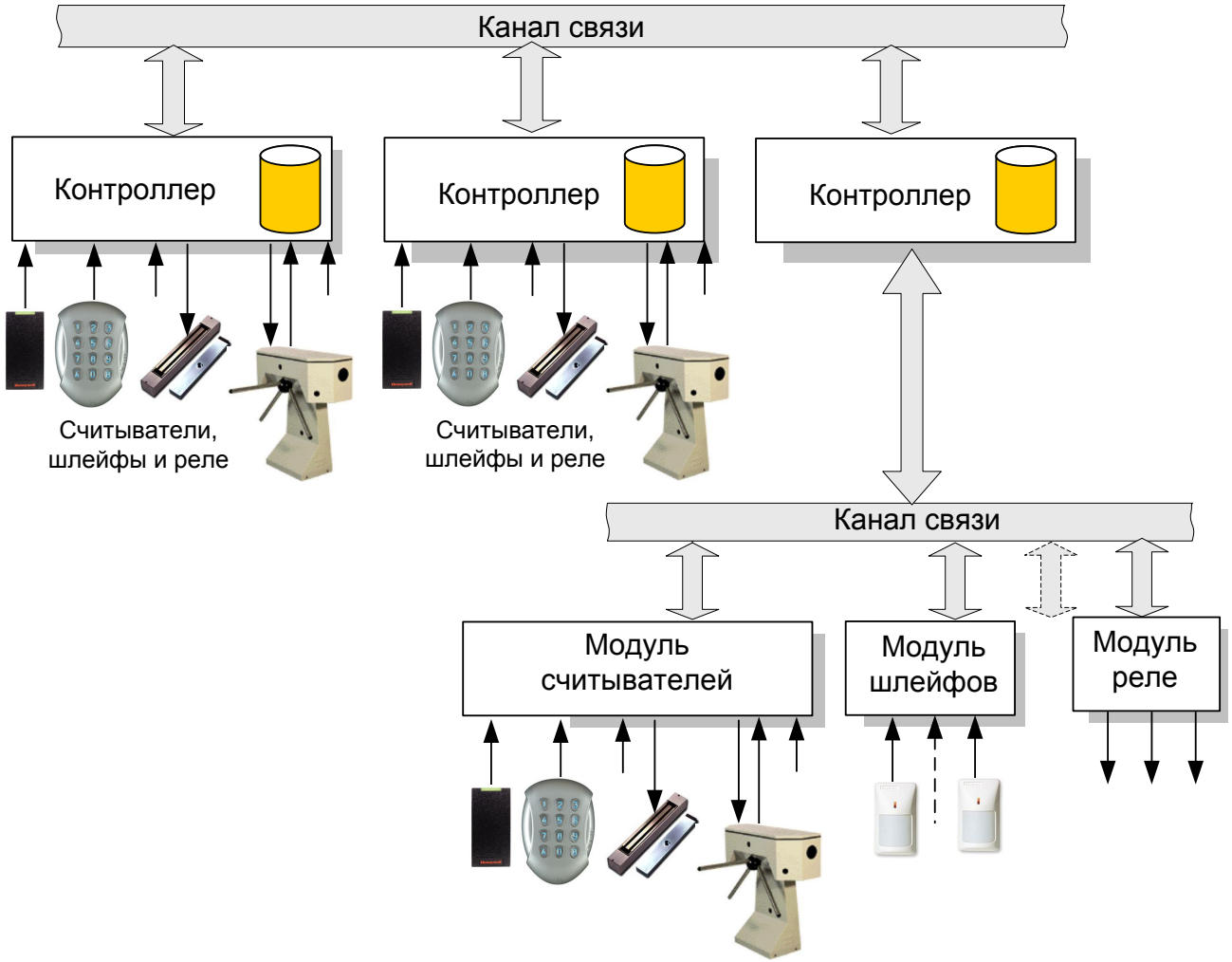
СКУД с децентрализованной архитектурой



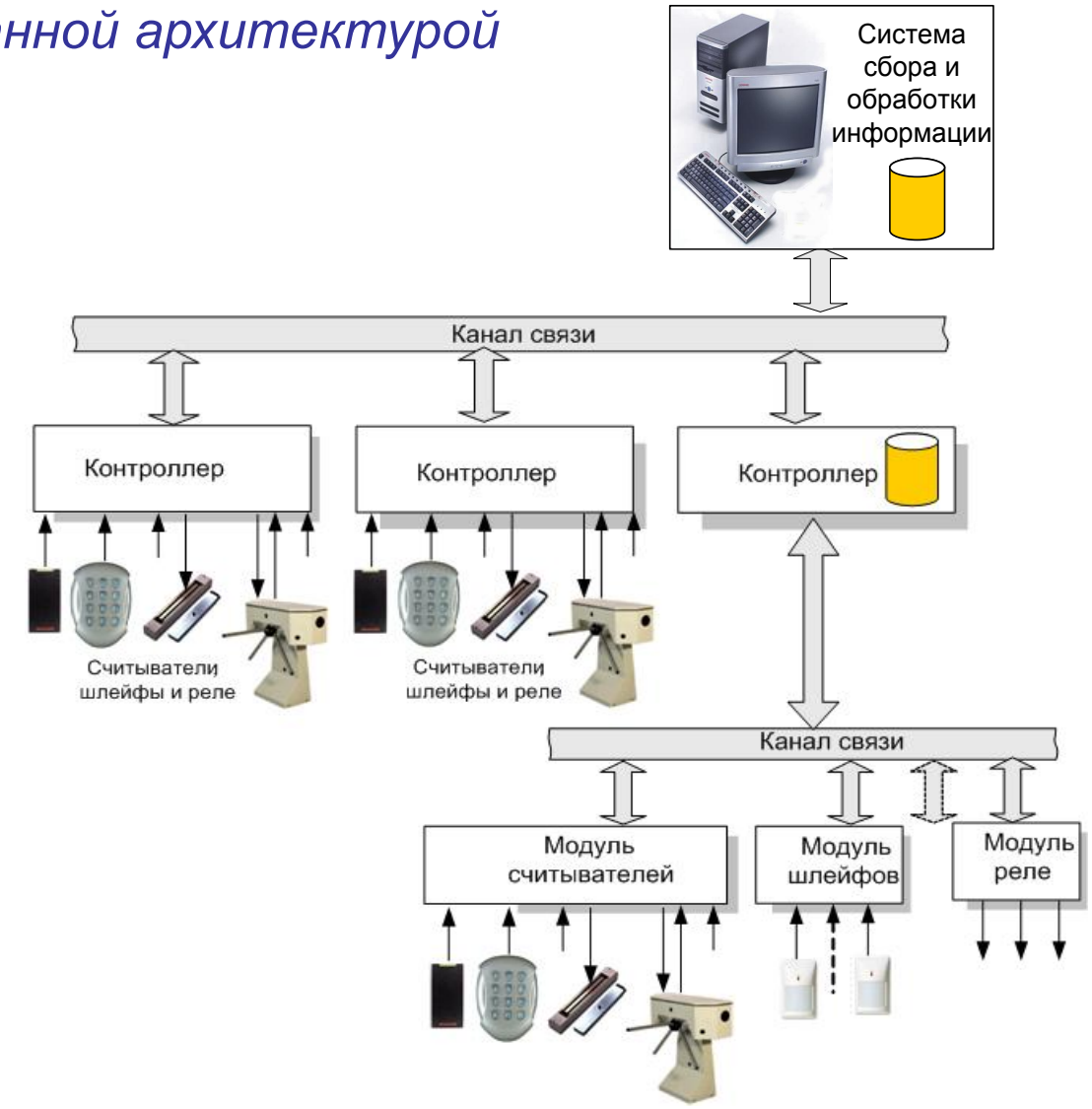
СКУД с централизованной архитектурой



СКУД со смешанной архитектурой



СКУД со смешанной архитектурой



Сетевая СКУД

Домофоны

- Небольшие здания (одна квартира).
- Небольшие здания с обособленной территорией с контролируемым дистанционно доступом.
- Комплексы небольших зданий на обособленной территории с контролем доступа на отдельные объекты и на территорию.
- Отдельные многоэтажные жилые здания.
- Отдельные административные здания.
- Жилые комплексы из нескольких зданий с обособленной контролируемой территорией.

- Домофон – может быть и «бытовое» оборудование, и система безопасности.
- Возможности современного оборудования значительно шире, чем только дистанционное открывание дверей.

Поэтому:

- Можно создать многофункциональную интегрированную систему безопасности.
- Можно использовать современные инновационные технологии.
- Можно использовать эффективные IP каналы связи.

- С позиций современных требований и возможностей домофонная система может быть *интегрированной системой безопасности интеллектуального здания*

  - с контролем доступа:
    - на территорию;
    - в подъезды;
    - в квартиры;
    - в общие объекты комплекса.

  и с функциями:

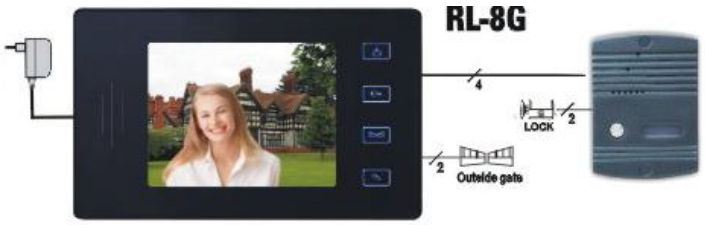
    - энергосбережения,;
    - управления освещением и домашним оборудованием;
    - охранной и пожарной сигнализации;
    - контроля утечки газа;
    - и др.

- Разнообразие пользовательских панелей – на любой вкус.
- Многофункциональность - с дополнительными функциями:
  - ✓ часы и календарь,
  - ✓ охранная и пожарная сигнализация,
  - ✓ контроль утечки газа,
  - ✓ управление светом,
  - ✓ ...
- Разные способы управления
  - ✓ клавиатуры,
  - ✓ сенсорные экраны,
  - ✓ громкая связь ,
  - ✓ «свободные руки,
  - ✓ …

- Разнообразие вызывных устройств.
- Разные способы управления

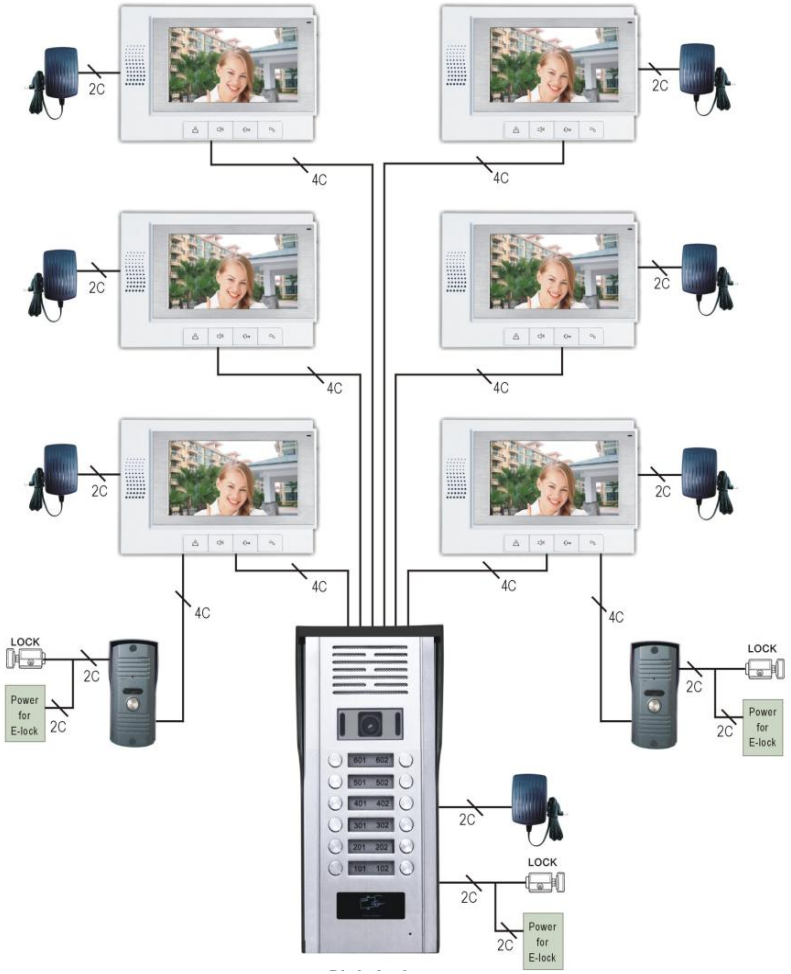
  (клавиатуры, карты, брелоки, электронные «таблетки»,…).
- Формирование и автоматическая запись видеоизображения посетителей при любой освещенности.

- «Один пользователь – один вход».
- «Один пользователь – несколько входов».
- «Несколько пользователей – один вход».

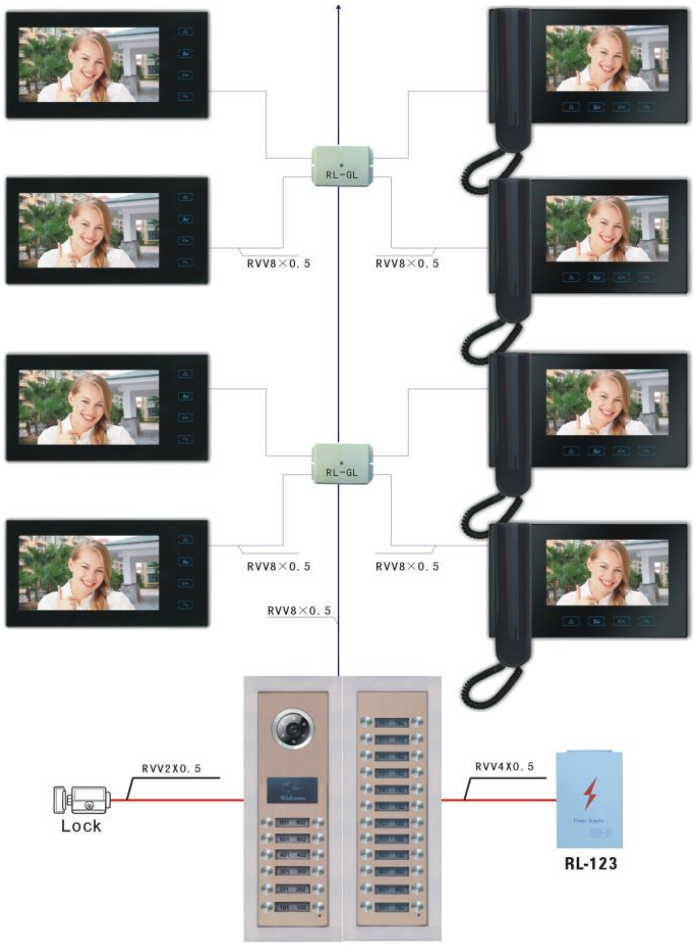


Возможные решения для многопользовательских систем

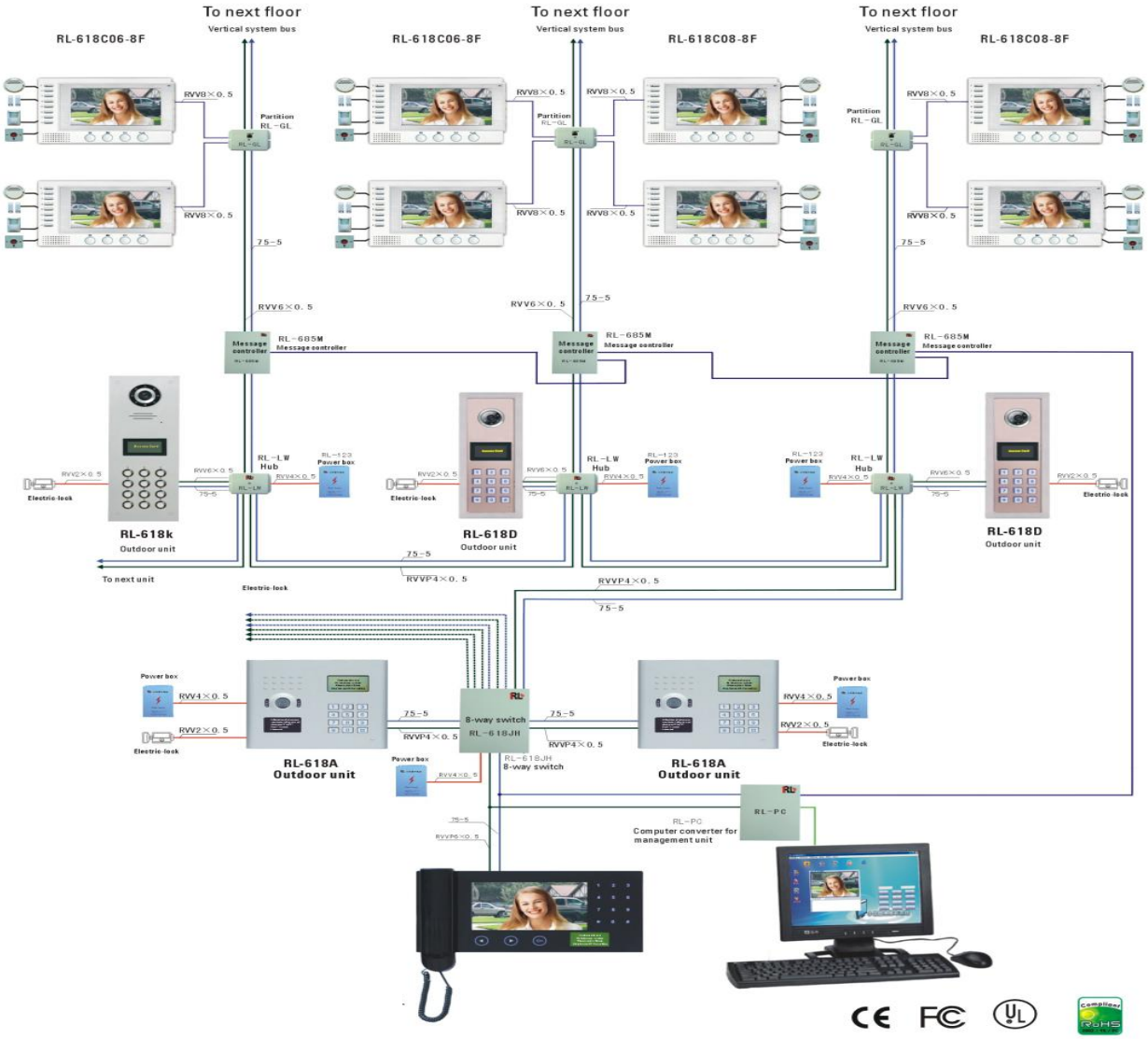
- Радиальная структура



- Древовидная структура (шина данных)



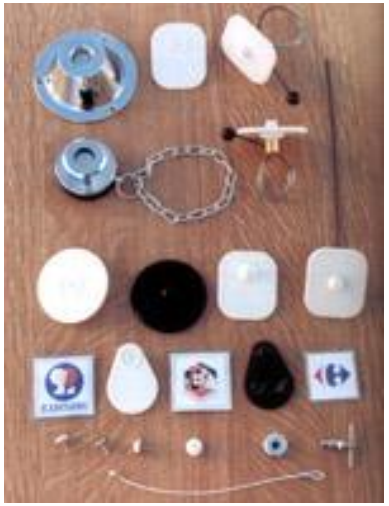
Домофоны
Возможные решения



Домофоны
Возможные решения – сетевые системы

Антикражевые системы

- Зарубежный термин – EAS (Electronic Article Surveillance).
- Задача обратная – при наличии действующего идентификатора - отказ в доступе.
- С недействующим идентификатором (или без идентификатора - санкционированное перемещение.
- Групповой идентификатор – одинаковый для группы объектов (товаров).
- Различать объекты доступа не требуется (только обнаружение).
- Используют однобитовый идентификатор, прикрепляемый к контролируемому товару.

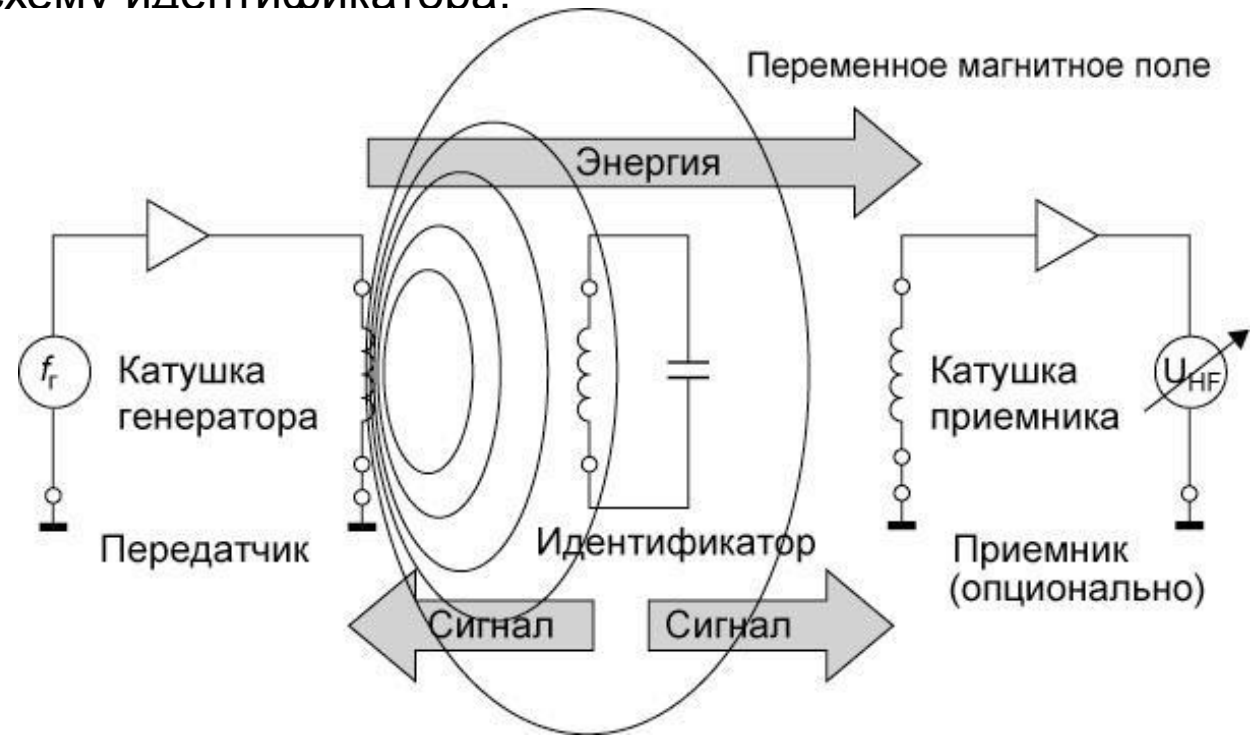


- *Два состояния*:
  - действующий идентификатор находится в зоне действия считывателя;
  - идентификатора нет (или он деактивирован).
- *Управление доступом* в таких системах обычно осуществляется не техническими элементами системы, а сотрудниками службы безопасности и продавцами.

Резонансные явления в LC-цепи

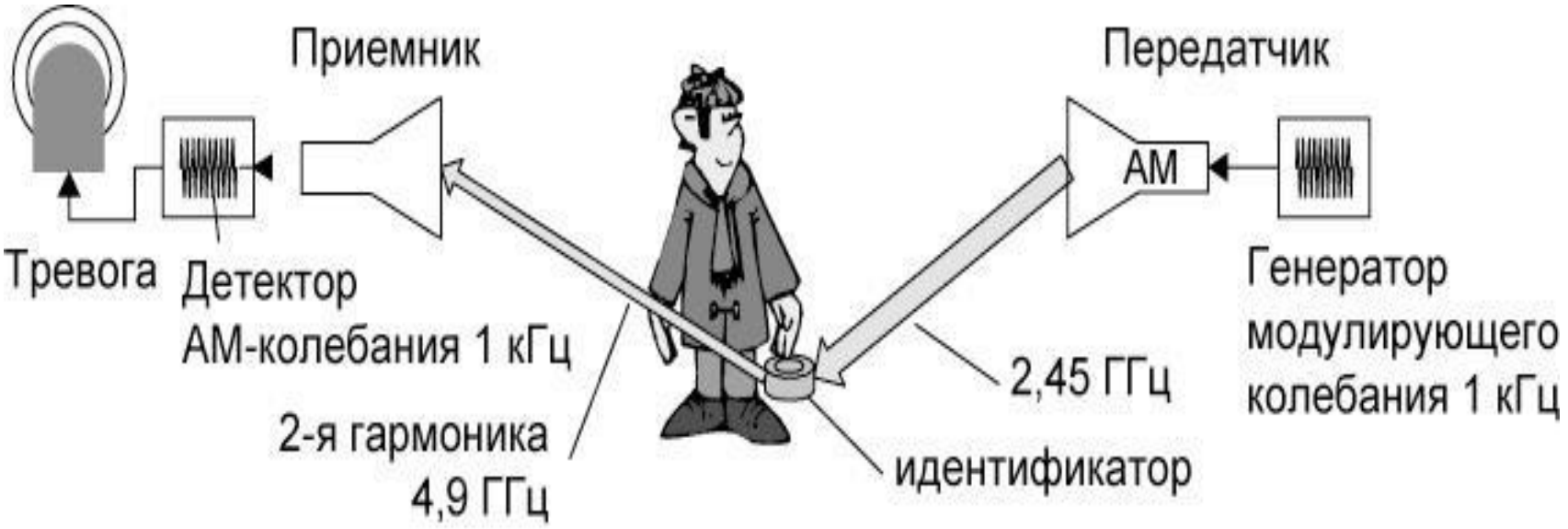
- Идентификатор – резонансная LC-цепь, настроенная на определенную частоту f_p.
- Передатчик считывателя генерирует переменное магнитное поле f_e. Если $f_p = f_e$, возникает резонанс.
- Изменение напряжения, вызванное появлением идентификатора очень мало, поэтому в реальных системах частота генерируемого поля изменяется (8,2 МГц ± 10%).

- Расстояние между антеннами считывателя до 2 м.
- Вероятность обнаружения – около 70% (влияет материал).
- Для деактивации применяется источник сильного магнитного поля, разрушающего схему идентификатора.



- Используется элемент с нелинейной характеристикой для формирования гармоник несущей частоты (2*f*, 3*f*, 4*f*, ...).
- Для умножения частоты используются емкостные диоды, а в качестве антенны – диполь.

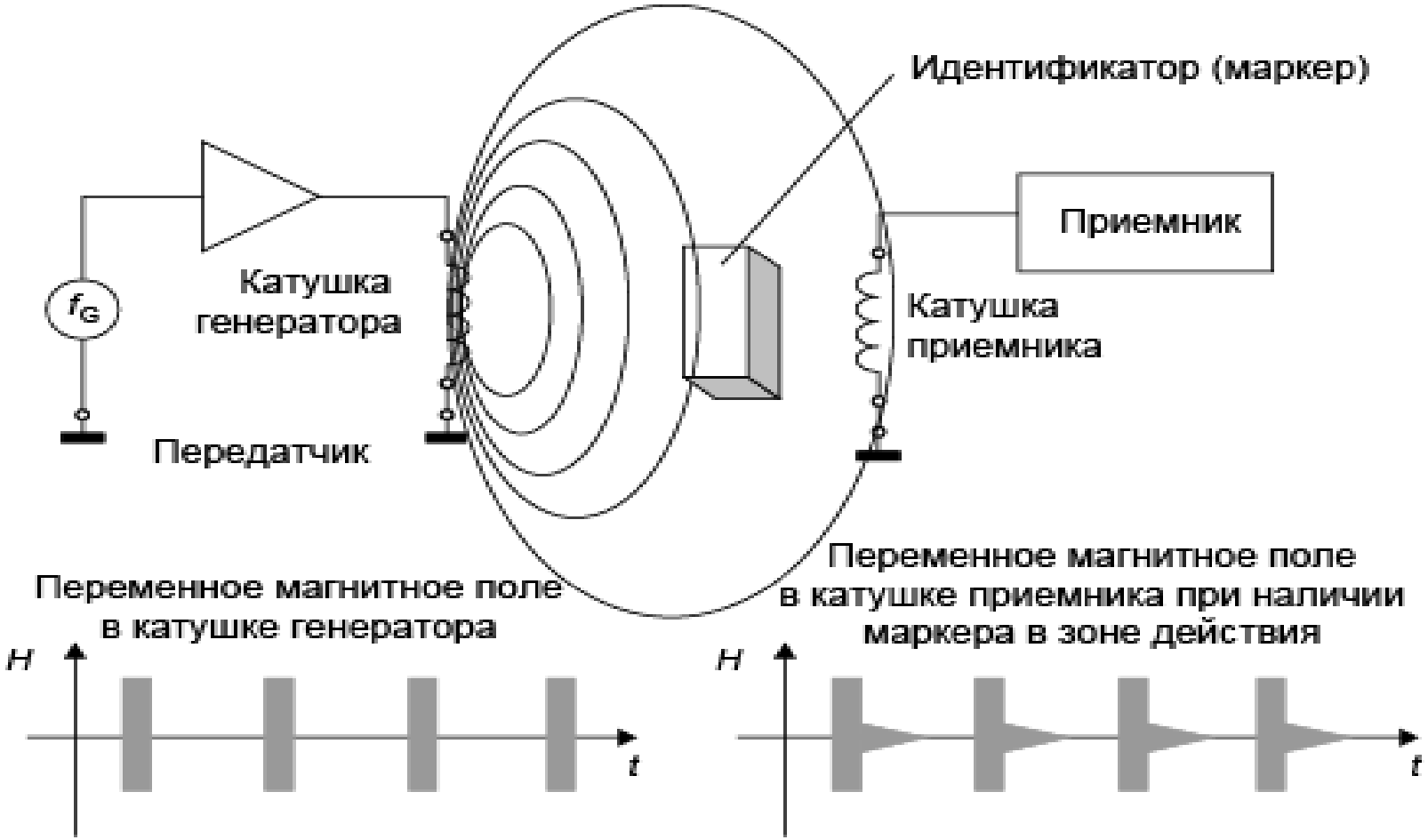
- Если идентификатор находится в зоне действия передатчика (f=2,45 ГГц), то генерируется и излучается через диполь вторая гармоника несущего колебания (4,9 ГГц). Эта частота обнаруживается приемником.
- Для снижения влияния помех несущее колебание подвергают АМ (тогда все гармоники также будут модулированными).



- Маркер содержит фиксированную полоску из магнитотвердого материала и перемещающуюся полоску из ферромагнитного материала.

- В магнитном поле ферромагнитные материалы изменяют размеры (*магнитострикция* – изменение межатомного расстояния при намагничивании).

- В переменном магнитном поле полоска вибрирует в продольном направлении (особенно сильно на акустической частот
- Магнитострикционный эффект обратим, т.е. вибрирующая полоска создает переменное магнитное поле после снятия поля.
- Для деактивации надо размагнитить фиксированную полоску.
- Преимущества:
- Высокая вероятность обнаружения (т.к. поле выключается на время отклика).
- Сложно размагнитить полоску (требуется переменное магнитное поле с медленно затухающей напряженностью).


Идентификатор (маркер)
Приемник
Катушка генератора
Катушка приемника
f_G
Передатчик
Переменное магнитное поле в катушке генератора
Переменное магнитное поле в катушке приемника при наличии маркера в зоне действия
H
t
H
t

- Маркер содержит полоску из магнитомягкого материала с нелинейной петлей гистерезиса и ферромагнитного элемента из магнитотвердого материала.
- Используется низкочастотный диапазон 10-1000 Гц.
- Нелинейные свойства материала полоски приводят к появлению сигналов с суммарными и разностными частотами.
- Для деактивации необходимо намагнитить магнитотвердый элемент.

Преимущества:

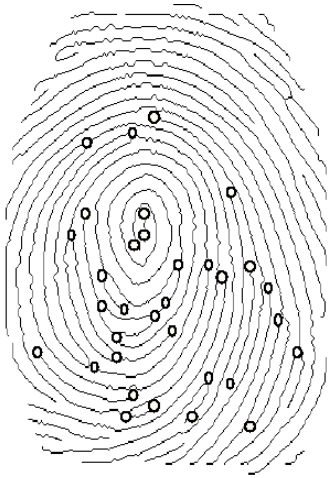
- Возможна повторная активизация маркеров
- Низкая стоимость маркеров
- Возможность использования на товарах, содержащих металл
- Удобно для магазинов книг, библиотек и т.п.

Недостатки:

- Вероятность обнаружения до 70%, зависимость от положения.

МЕТОДЫ
И УСТРОЙСТВА ИДЕНТИФИКАЦИИ

Биометрические методы идентификации



- Активно развиваются в последнее время.
- Основаны на исследовании уникальных физиологических особенностей или поведенческих характеристик человека.
- Важное преимущество: с высокой степенью вероятности одновременно решаются задачи *идентификации* и *аутентификации.*

Две группы систем:

Квазистатические	***Квазидинамические***
Мало меняющиеся во времени	Достаточно сильно изменяющиеся во времени

При внедрении системы нужно учитывать требования:

- этические, т. е. приемлемость субъектом;
- юридические, т.е. соответствие законодательству;
- **.....**

Квазистатические признаки:

- отпечаток пальца;
- форма кисти руки;
- геометрия лица;
- рисунок сетчатки глаза;
- рисунок радужной оболочки глаза;
- код ДНК;
- подпись;
- запах;
- и др.

Квазидинамические признаки:

- параметры речи;
- параметры пульса;
- клавиатурный почерк;
- динамика воспроизведения подписи;
- и др.

Для успешной идентификации необходимо, чтобы возможный разброс параметров идентификационных признаков, принадлежащих одному человеку, был значительно меньше различия между аналогичными признаками, принадлежащими другим людям.

Перед анализом выбранных биометрических признаков, нужно удостовериться, что предъявленные характеристики принадлежат живому существу (не муляж или муляж + живое существо).

Если это не выполняется, существуют угрозы для такой системы:

1. Несанкционированного доступа, при предъявлении муляжа, являющегося копией биометрического признака уполномоченного пользователя.
2. Добавления муляжа при занесении эталонных биометрических признаков в систему.
3. Отказ действующего пользователя от получения им доступа, если носитель биометрических признаков может быть подделан.

Этапы считывания биометрических признаков:

1. Поиск и обнаружение биометрических характеристик.
2. Считывание биометрических характеристик признаков.
3. Проверка соответствия предъявленных характеристик живому человеку.
4. Преобразование считанной характеристики в набор идентификационных параметров.
5. Проверка достаточности считанной информации для успешной идентификации.
6. Сравнение считанных идентификационных параметров с эталонными и принятие решения или занесение образца в память системы.

- Существуют две гипотезы, которые проверяет биометрическая система идентификации:
  - Предъявленный биометрический идентификатор принадлежит уполномоченному пользователю.
  - Предъявленный биометрический идентификатор не принадлежит уполномоченному пользователю.
- Система принимает решение о разрешении или запрете доступа

Гипотеза	Решение системы идентификации			
	Разрешение доступа		Запрет доступа	
Предъявлен действующий идентификатор	Правильное разрешение доступа	$P_{\text{п.р}}$	Ложный отказ в доступе	$P_{\text{л.о}}$
Предъявлен недействующий идентификатор	Несанкциониро-ванный доступ	$P_{\text{н.д}}$	Правильный отказ в доступе	$P_{\text{о.д}}$

- В любой системе важно иметь вероятности $P_{н.д}$ и $P_{л.о}$ как можно меньшими, но на практике эта задача оказывается противоречивой
- В некоторых системах есть возможность настройки характеристик для соответствия решаемой задаче.
- Ещё одна характеристика систем биометрической идентификации – вероятность отказа в регистрации пользователя в системе (если при занесении эталонного образца характеристик недостаточно)

Требования к биометрическим идентификационным признакам

1. Неповторяемость
2. Достаточность
3. Стабильность
4. Защищенность
5. Считываемость
6. Принадлежность
7. Доступность
8. Наличие
9. Присваиваемость
10. Приемлемость
11. Законность

Требования:

1. Низкая вероятность ложного отказа в доступе (I).
2. Низкая вероятность несанкционированного доступа (II).
3. Высокая вероятность правильного предоставления доступа.
4. Высокая вероятность правильного отказа в доступе.
5. Низкая вероятность отказа в регистрации в системе.
6. Высокая пропускная способность (например, число человек в минуту).
7. Данные от пользователей (опрос).

…

Требования оказываются сложно связанными между собой, а зачастую и взаимно противоречивыми.

Требования зависят от области применения.

Идентификационная характеристика - папиллярные узоры, образованные валиками и бороздками верхнего слоя кожи на внутренней поверхности ладоней, пальцев рук, подошвах стоп и пальцах ног человека.

Два типа признаков - глобальные и локальные.

Глобальные признаки - те, которые можно увидеть невооружённым глазом.

Все папиллярные узоры делятся на три основных типа:

- петлевые (частота встречаемости примерно 65%);
- завитковые (30%);
- дуговые (5%).

Идентификация по отпечатку пальца
Типы папиллярных узоров

1 – 4 – узоры типа «петля» (левая, правая, центральная, двойная),

5 и 6 – узоры типа «дельта» или «дуга» (простая и острая),

7 и 8 – узоры типа «спираль» (центральная и смешанная).

Локальные признаки называют минуциями - уникальные для каждого отпечатка признаки, определяющие:

- тип изменения структуры папиллярных линий в определенных точках (окончание, раздвоение, разрыв и т.д.);
- координаты этих точек;
- ориентация папиллярных линий этих точках.

- Каждый отпечаток содержит до 70 минуций.
- Отпечатки пальцев разных людей могут иметь одинаковые глобальные признаки, но практически невозможно наличие одинаковых микроузоров минуций.
- Поэтому глобальные признаки используют для разделения базы данных на классы.
- На втором этапе используют уже локальные признаки.

- Координаты обнаруженных минуций и их углы ориентации записываются в виде вектора:

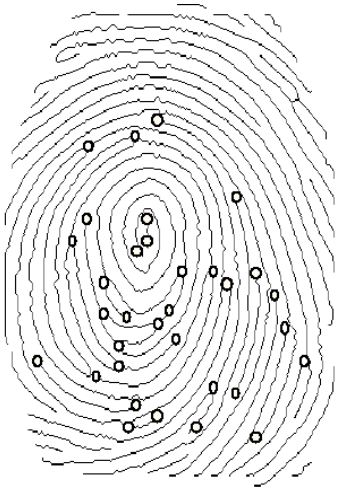
$$W(N)=[(x_1, y_1, \varphi_1, T_1), (x_2, y_2, \varphi_2, T_2)\ldots(x_N, y_N, \varphi_N, T_N)] ,$$

где N — число минуций.

- При регистрации пользователей этот вектор считается эталоном и записывается в базу данных.
- При идентификации этот вектор определяет текущий отпечаток.

Идентификация по отпечатку пальца
Локальные признаки

Пересечение линий
Соединение линий
Разветвление линий
Окончание линии
Островок
Дельта
Пора



- Разрешение считывателя - 500 dpi (элемент 50x50 мкм).
- Считывание рисунка с 256 или 64 градациями серого.
- Считанное изображение 2x3 см занимает около 240 Кбайт памяти.
- После сжатия – размер 10-50 Кбайт.
- После выделения характерных точек – размер 40…2500 байт.

Улучшение качества исходного изображения отпечатка, увеличивается резкость границ папиллярных линий.

1. Бинаризация - приведение к чёрно-белому изображению.
2. Утончение линий изображения отпечатка, производится до тех пор, пока линии не будут шириной 1 пиксель.
3. Выделение минуций - изображение разбивается на блоки 9x9 пикселей. Подсчитывается число чёрных (ненулевых) пикселей, находящихся вокруг центра. Пиксель в центре считается минуцией, если он сам ненулевой и соседних ненулевых пикселей один (минуция «окончание») или два (минуция «раздвоение).
4. Координаты минуций и их углы ориентации записываются как вектор.
5. Сопоставление минуций:
   - поиск пар соответствующих минуций (перебор углов поворота, сдвига и масштаба);
   - оценка соответствия отпечатков.
7. Принятие решения.

Методы обмана :

- Муляжи.
- Использование предыдущего отпечатка.
- Принуждение.

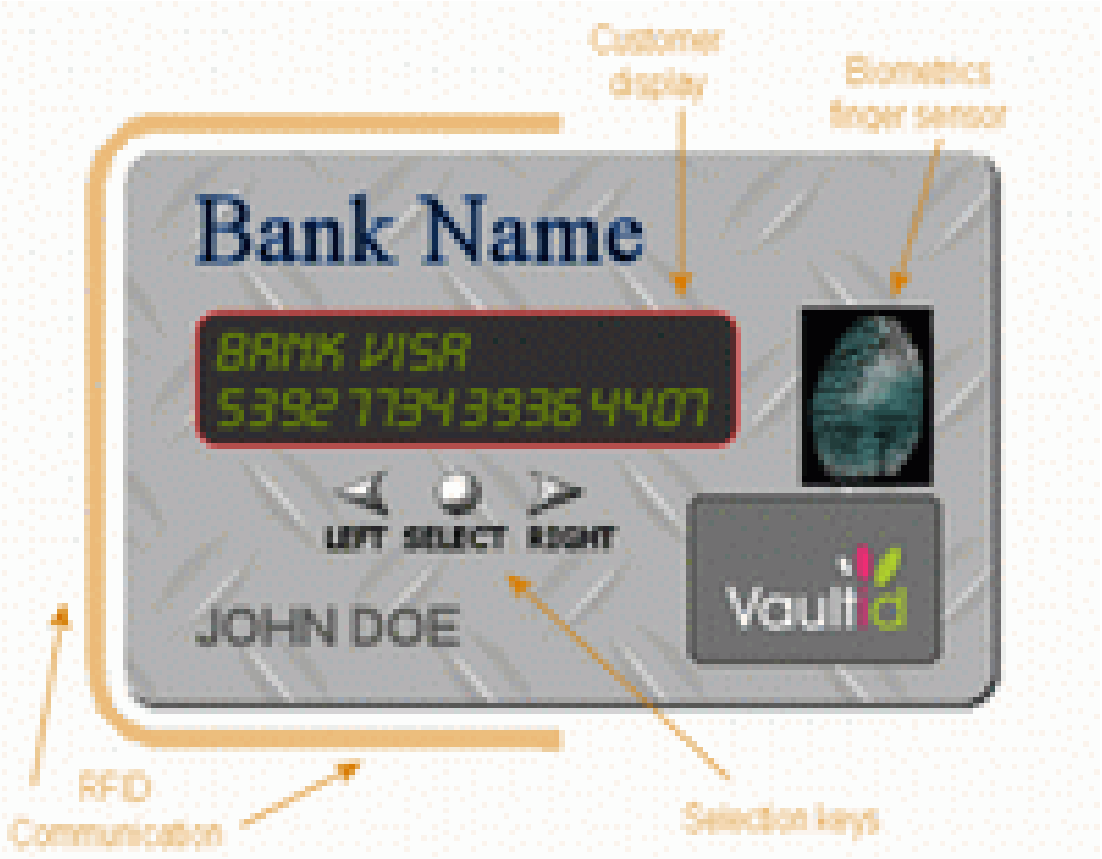
Недостатки :

- Пользователи считают, что их отпечатки пальцев могут использоваться в криминалистике.
- В случае сильного ожога или множественных порезов, идентификация пользователя становится невозможной.
- Зависимость от чистоты пальца.
- Зависимость от состояния кожи.

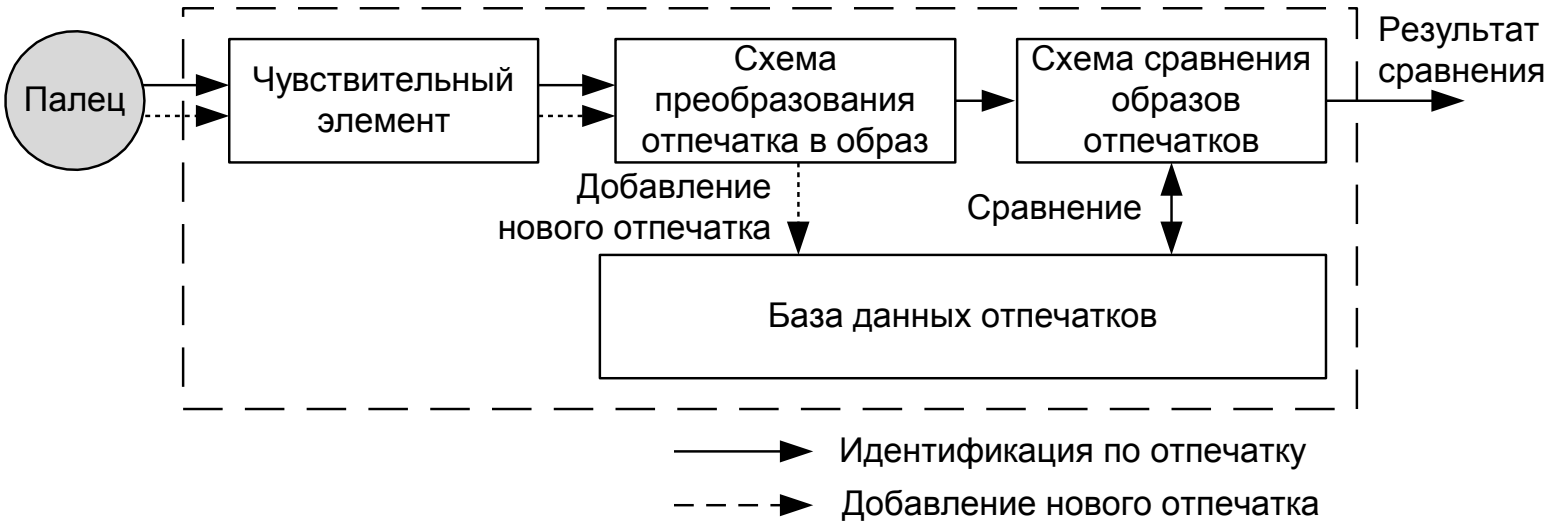
Достоинства:

- Пользователю не нужно запоминать или иметь с собой что-либо.
- Хорошее соотношение цена/надёжность.
- Малые размеры сканеров (можно сделать размером 1x10мм и меньше).

Биометрическая идентификация для владельцев платежных карт



Алгоритм 1:N



- Сравнение образа считанного отпечатка со всеми образцами, хранящимися в памяти. Если такой образец не найден, принимается решение об отказе в доступе.
- Достоинством является возможность работы только по отпечатку пальца без использования дополнительных идентификаторов.

Алгоритм 1:1

- Сравнение образа считанного отпечатка с одним конкретным образцом. В этом случае биометрический считыватель до анализа образа считанного отпечатка пальца должен иметь априорную информацию о пользователе.
- Достигается это за счет совмещения считывателя отпечатка пальца с клавиатурой или считывателем с другим физическим принципом действия. Два варианта:
  - Образ отпечатка хранится в идентификаторе.
  - Образ отпечатка хранится в базе данных СКУД, а считывается только номер.

Преимущества алгоритма 1:1

- Возможность использования одновременно двух различных методов идентификации (повышение защищенности).
- Более высокое быстродействие, поскольку осуществляется сравнение считанного образа только с одним эталонным, а не перебор всех возможных образцов.
- Возможность хранения в базе данных информации о большем количестве пользователей.

Для считывания надо выделить различия в некотором физическом параметре для валиков и бороздок папиллярного узора.

Классификация:

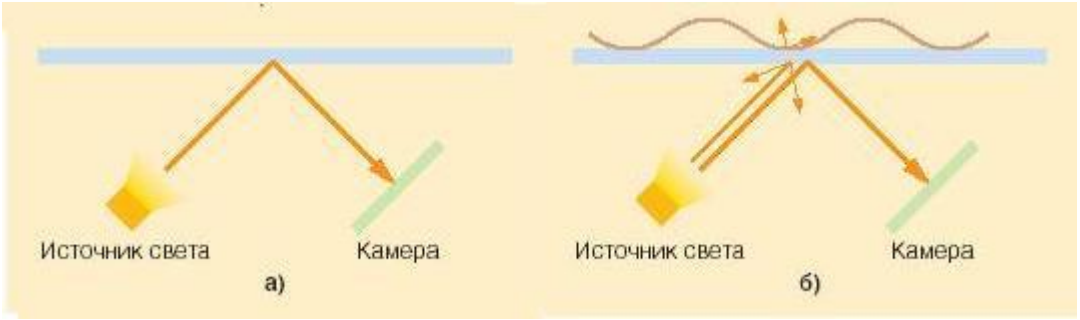
по принципу физическому действия:

- оптические;
- емкостные;
- температурные;
- полупроводниковые;
- ультразвуковые;
- давления;
- др.

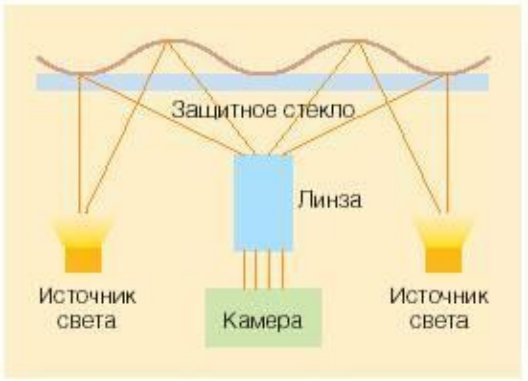
по способу формирования изображения:

- сканирующие (формирующие изображение последовательно по строкам);
- формирующие полное изображение.

- Использование эффекта нарушения полного внутреннего отражения.

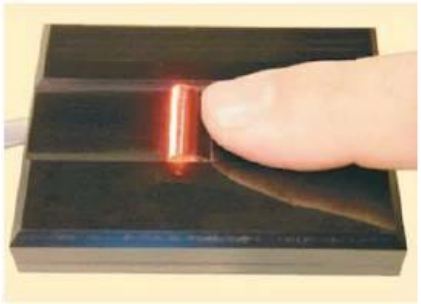


- Непосредственно получение изображения отпечатка пальца.

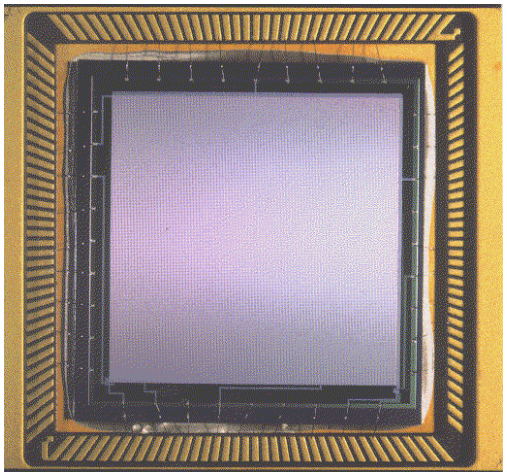


- Оптические протяжные и роликовые сканеры

  Важно обеспечить равномерность сканирования по обеим координатам, иначе появляются искажения.



- Используется эффект изменения емкости pn-перехода полупроводникового прибора при соприкосновении гребня папиллярного узора с элементом матрицы.
- Каждый полупроводниковый элемент в матрице сканера выступает в роли одной пластины конденсатора, а палец — в роли другой. Матрица этих емкостей преобразуется в изображение отпечатка пальца.



Идентификация по радужной оболочке глаза

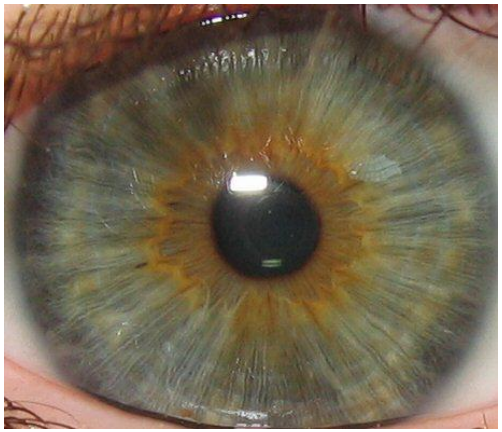
- Рисунок стабилен на протяжении жизни человека.
- Рисунок защищен от повреждения.
- Изображение практически плоское (удобно для электронной идентификации).
- Бесконтактное считывание возможно при наличии очков или контактных линз.
- Вероятность совпадения 10^{-78}.
- Дальность считывания может достигать 1 м.
- В современных считывателях для успешной идентификации достаточно, чтобы было доступным 40% площади радужной оболочки.

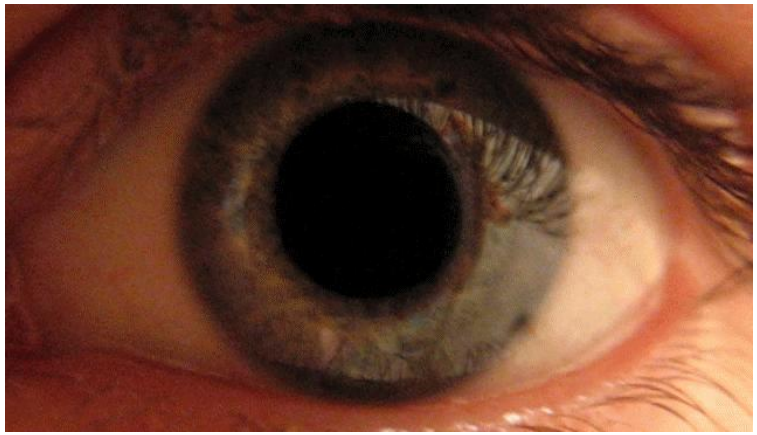
Защищенность идентификации по радужной оболочке глаза

Принадлежность изображения глазу живого человека?

Как защититься от предъявления муляжа глаза?

- Контроль процедуры оператором.
- Эффект изменения диаметра зрачка при изменении освещенности.
- Анализ характеристик перемещения глаза (например, при чтении).
- Эффект «красных глаз» - анализ частотной характеристики двумерного изображения радужной оболочки.
- Использование нескольких камер для получения стереоизображения.





Состав системы

- Оптический считыватель (обнаружение и считывание изображения и передача его в специализированный контроллер). В считывателе обычно находится монохромная камера с датчиком расстояния и ИК-подсветкой.

- Специализированный контроллер, работающий с одним или несколькими считывателями. В памяти контроллера хранятся индивидуальные образцы радужных оболочек для каждого пользователя (1:N). Контроллер выполняет функцию сравнения считанного образа со всеми образцами из памяти. Или нужен дополнительный считыватель для режима 1:1.

- Персональный компьютер с ПО для добавления новых пользователей в систему.

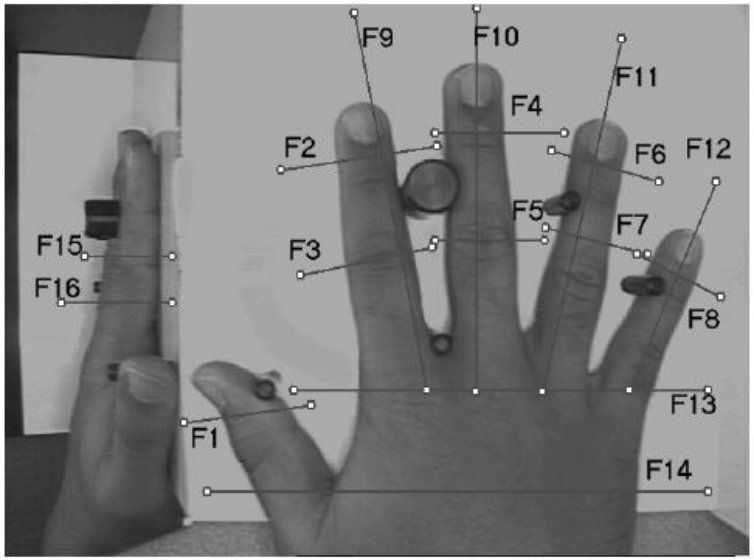
Идентификация по радужной оболочке глаза

Структура системы

- Одно из наиболее быстро развивающихся направлений биометрической идентификации.
- Удобство метода для пользователей (наиболее естественный).
- Возможность использования на объектах с повышенными требованиями безопасности, где с помощью других методов невозможно ограничить доступ людей, но требуется выявлять определённый круг лиц (на вокзалах, в аэропортах и т.п.).
- Возможность вести скрытую идентификацию.
- Высокая пропускная способность.
- Возможность взаимодействия такой СКУД с системой телевизионного наблюдения.

Идентификация по форме кисти руки

- Метод основан на анализе двух- или трехмерного изображения кисти руки.
- Один из наиболее удобных способов идентификации для пользователей.
- Для идентификации надо по изображению сформировать набор параметров.
- При формировании изображения – минимизировать разброс этих параметров (обеспечить инвариантность относительно положения руки).
- Для получения изображения кисти может использоваться ч/б телекамера с ИК-подсветкой.
- Информативными могут быть два изображения: виды сверху и сбоку.
- Формируется набор параметров,
- Которые преобразуются в образ (например, 96 параметров, 9 байт).
- Режим сравнения обычно "1:1" (пароль или карта).

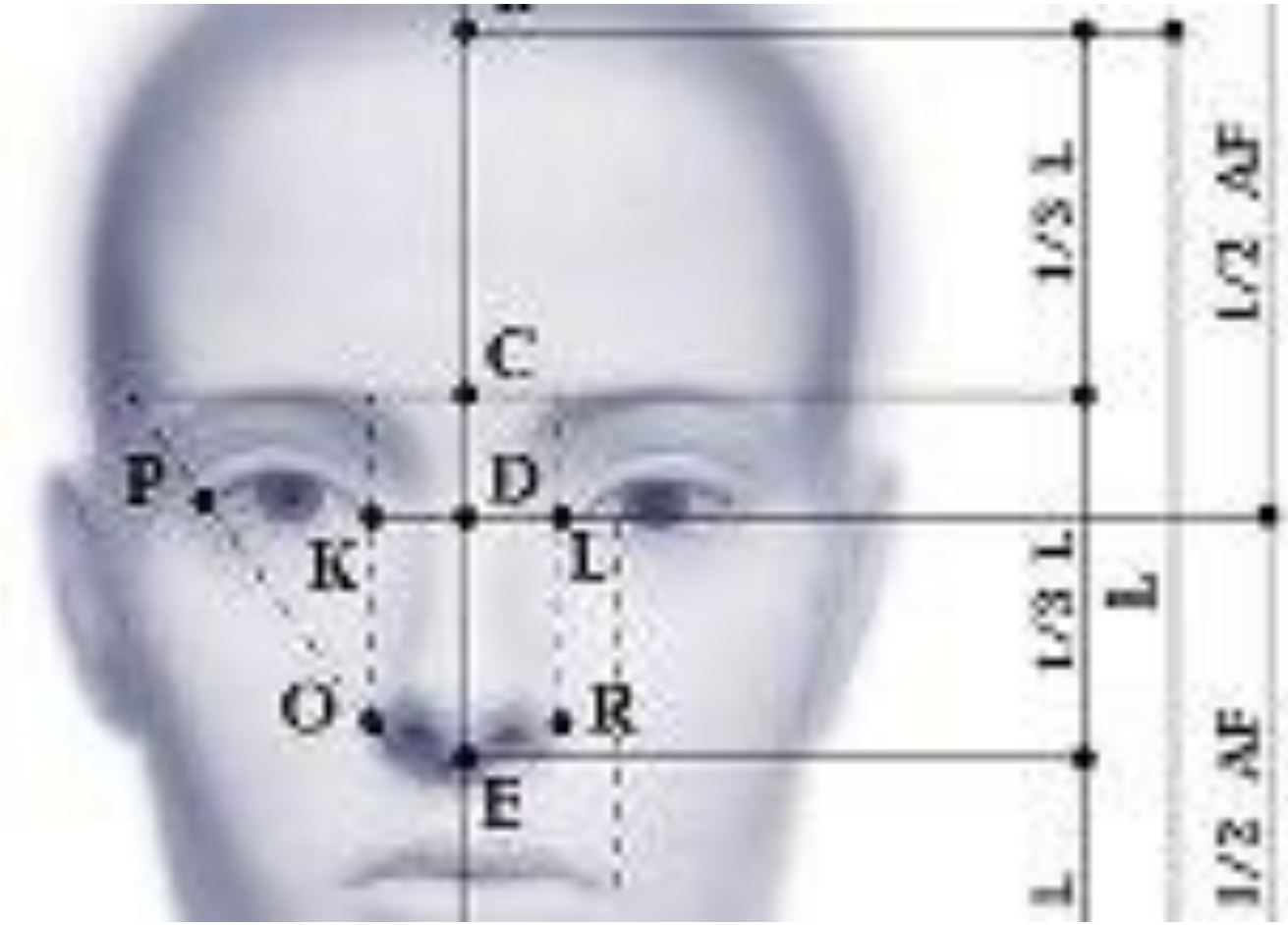


- Один из производителей считывателей – Schlage Recognition Systems (США)

- Особенности считывателя HK-2:
  - Работа в автономном режиме или передача данных на контроллер
  - Время идентификации менее 1 с
  - Число пользователей: 512 - 32512
  - Интерфейсы: RS-232, RS-485, Виганда, Ethernet (опция)
  - Пароль (1-10 цифр) или вход данных по интерфейсу Виганда

- Для успешной идентификации разных людей необходимо, чтобы разброс считанных идентификационных признаков, принадлежащих одному человеку, был значительно меньше чем, принадлежащими разным людям.
- Лицо не является стационарным объектом и может существенно изменяться за небольшой промежуток времени.
- Лицо является трёхмерным объектом, изображение которого зависит от угла зрения, яркости и спектральных составляющих падающего света.
- Изображение лица существенно зависит от угла наклона и поворота головы и от угла наблюдения.

  Поэтому большинство применяемых алгоритмов используют характерные ключевые точки (контуры глаз, скул, носа, подбородка) и взаимные расстояния между ними.


C
P
D
K
L
O
R
E
1/3 L
L
1/2 AF
1/2 AF

Защищенность идентификации по изображению лица

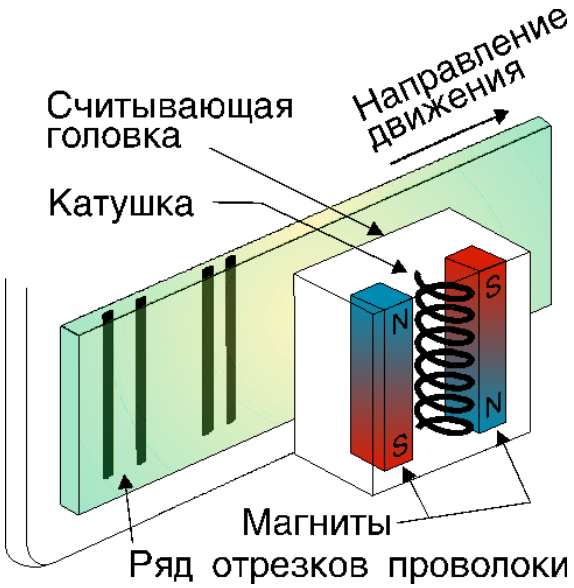
- Правильный выбор параметров, по возможности, инвариантных к мимике и гриму.
- Правильный выбор параметров, по возможности, инвариантных к наклону и повороту изображения.
- Обеспечение правильного взаимного положения считывателя и идентифицируемого.
- Использование методов анализа принадлежности живому человеку.

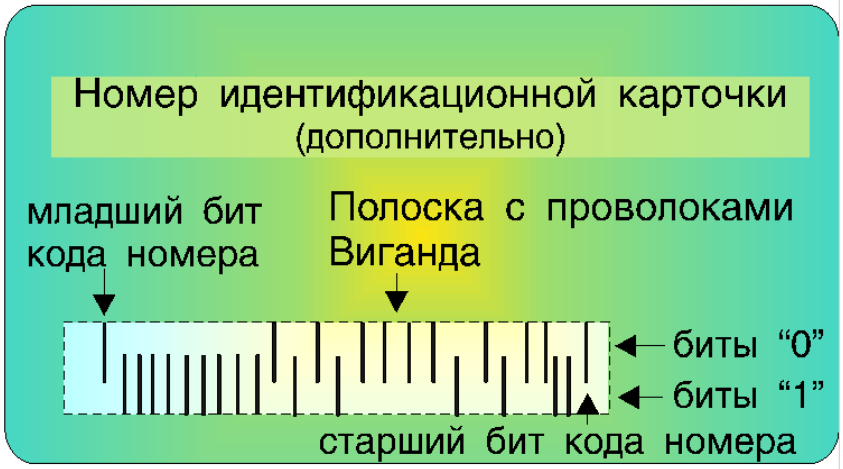
  Например, при наблюдении в дальнем ИК-диапазоне волн. При этом осуществляется термография – выявление расположения кровеносных сосудов на лице.

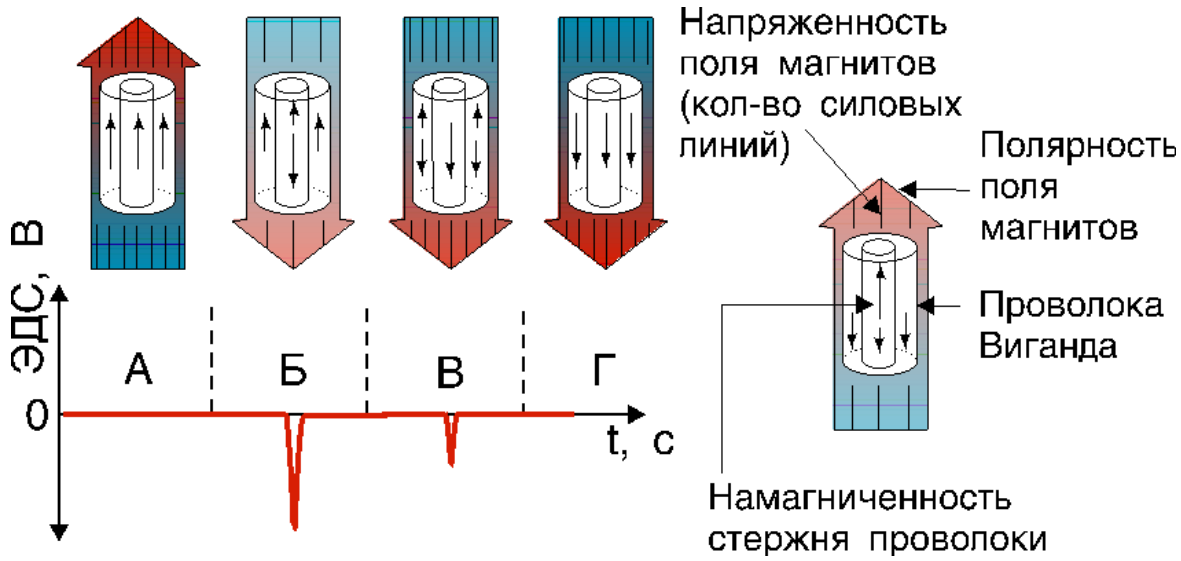
  Преимущества термографии:
  - не требуется подсветка (лицо – это источник ИК-излучения);
  - не влияют процессы старения, пластических операций;
  - возможно различение близнецов.
- Техническая реализация различна.

Считыватели карт Виганда и интерфейс Виганда

- *Эффект Виганда* - быстрое изменение магнитных полей с помощью специально обработанных ферримагнитных проводников малого диаметра.
- *Проволока Виганда* – сплав кобальта, железа ванадия (викаллой), диаметр около 0,2 мм, имеет магнитомягкую сердцевину и поверхность с высокой коэрцитивной силой.

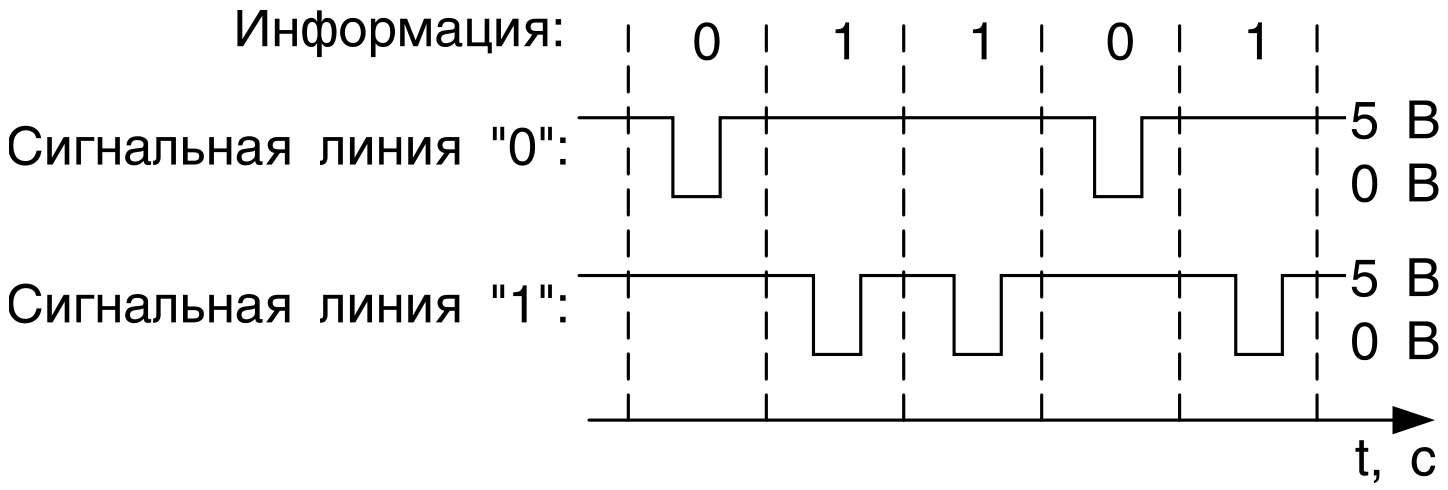






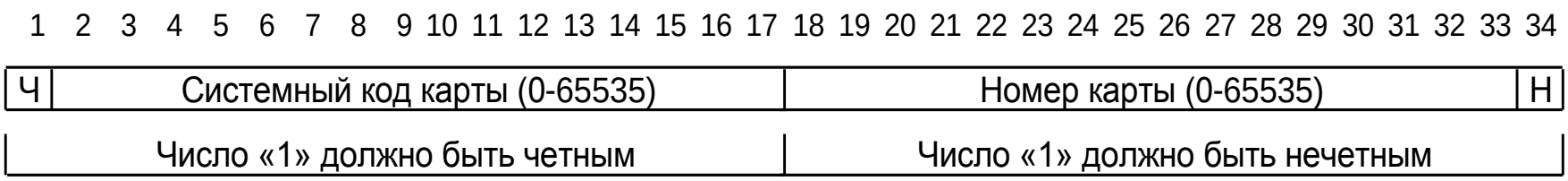
- Отсутствие внешнего источника питания.
- Нет механического износа деталей считывателя.
- Высокая надежность.
- Высокая устойчивость карт к внешним воздействиям, в том числе, электрическим и магнитным.
- Невозможность изготовления карт вне заводских условий.
- Использование в других отраслях (различные датчики).

- Интерфейс передачи данных от считывателя на контроллер СКУД. (стандартный интерфейс среди большинства производителей СКУД)
- Обмен данными через буфер для согласования скоростей.
- Используется разных типах считывателей различных производителей (проксимити, биометрических, кодонаборных устройствах и т.п.).
- Использует две сигнальные линии, по одной из которых передаются, соответствующие «0» двоичного кода, по другой – «1».



- Формат Виганда 26 бит

- Открытый формат (можно заказать любому).
- Для исключения повтора – свои форматы.
- Например, HID: 26, 34, Long (до 84).
- Пример:



Радиочастотная идентификации

Принцип действия основан на связи двух электрических цепей через магнитное поле (трансформаторная связь).

- Работают на частотах от 100 кГц и выше.
- Области применения:
  - контроль доступа людей на объекте;
  - платёжные системы (метро, железная дорога, автостоянки, …);
  - контроль за перемещением предметов (склады, производство, магазины, …).

Преимущества:

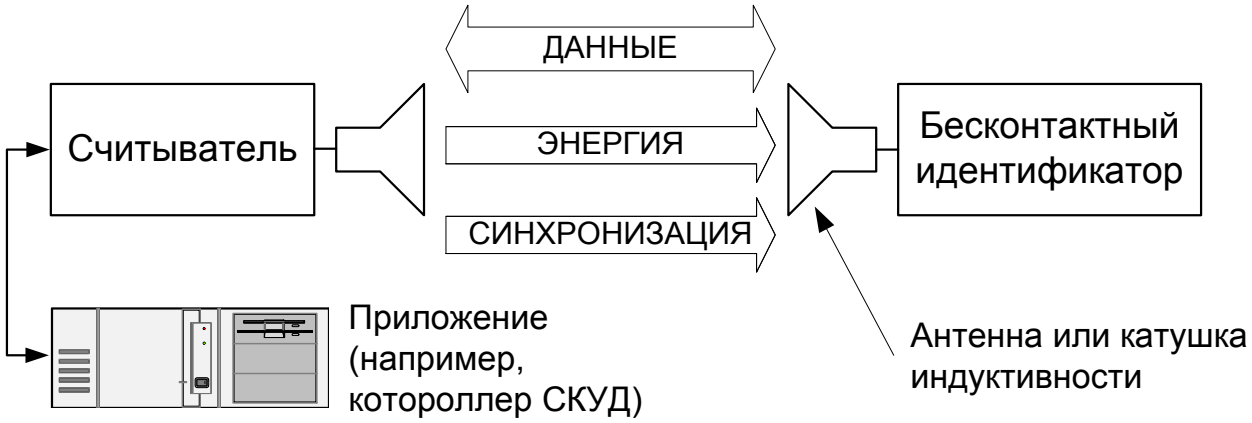
- высокая надежность системы за счет отсутствия механического износа деталей считывателя и идентификатора;
- бесконтактное считывание данных, в том числе на большом расстоянии;
- высокая скорость считывания (пропускная способность системы);
- возможность защиты идентификационных данных от несанкционированных действий;
- возможность считывания данных с нескольких идентификаторов, находящихся в зоне действия считывателя.

1. Рабочая частота считывателя (от 100 кГц до 5,8 ГГц).
2. Дальность действия (от нескольких мм до десятков метров).
3. Физическая связь между считывателем и идентификатором (магнитное или электромагнитное поле).
4. Объем памяти идентификатора (от 1 бита до десятков килобайт).
5. Способ обеспечения энергией идентификатора (активные / пассивные)
6. Возможность записи данных в идентификатор

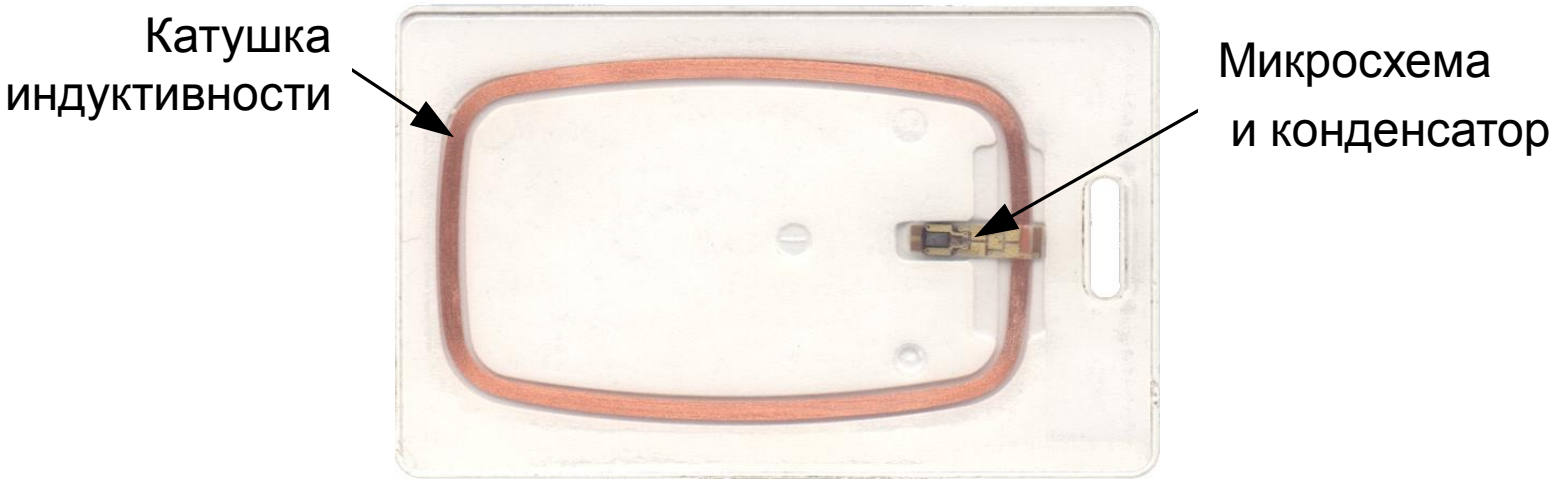
   (только чтение / однократная запись / многократной записи).
7. Тип взаимодействия считывателя и идентификатора

   (дуплекс / полудуплекс / симплекс).
8. Функции по обработки информации в идентификаторе.

Функциональная схема радиочастотного устройства идентификации



- Принцип действия пассивных идентификаторов:
  1. Передатчик считывателя через антенну формирует поле определенной частоты.
  2. Попавший в зону действия поля идентификатор обнаруживает его и отвечает собственным сигналом, содержащим полезную информацию на той же самой или другой частоте.
  3. Сигнал улавливается антенной считывателя, данные декодируются и передаются для обработки.

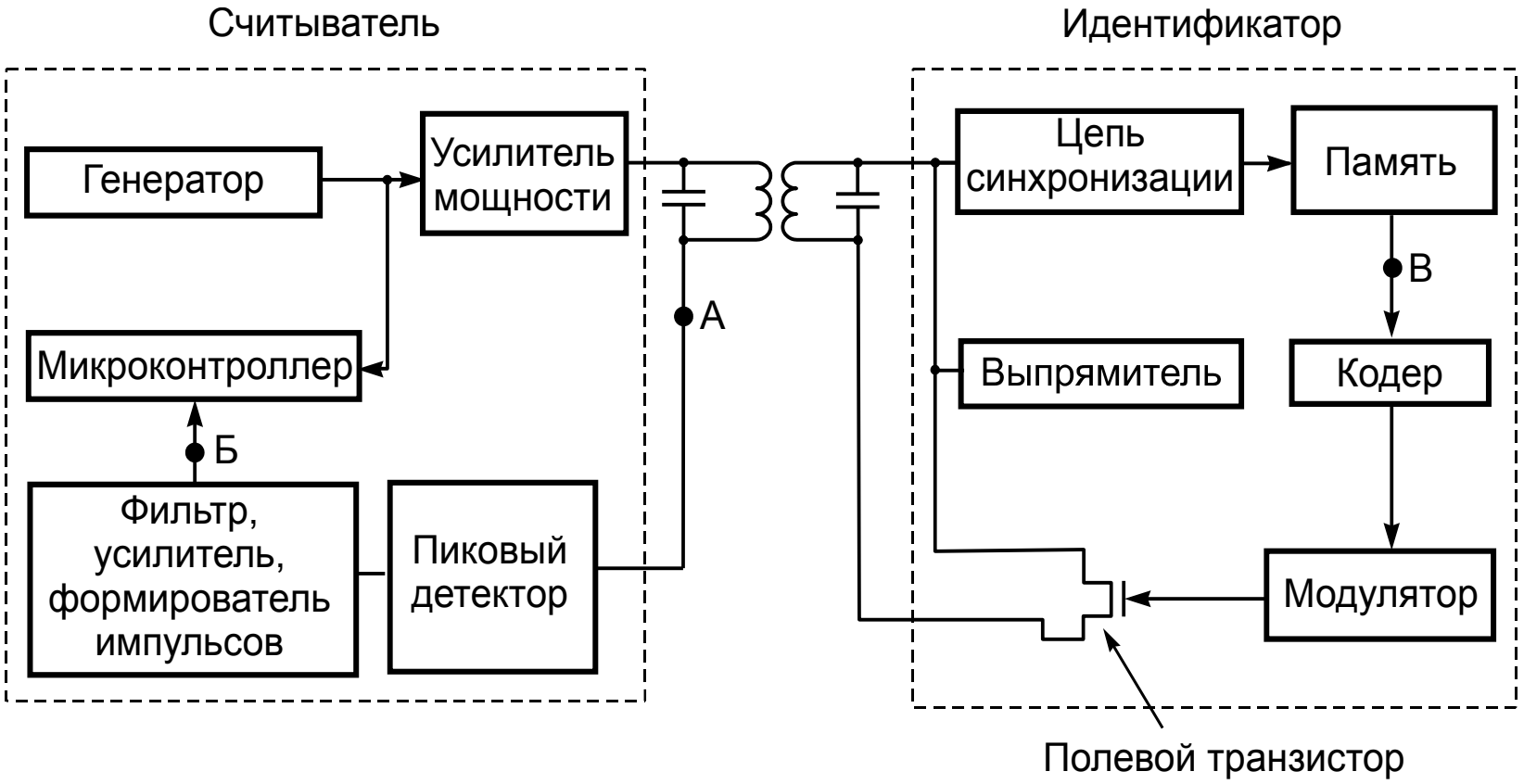


- Катушка может быть реализована в виде катушки из проводников или печатных проводников.
- В диапазоне частот порядка сотен килогерц необходима индуктивность в несколько миллигенри, на частоте 13,56 МГц, достаточно катушки с индуктивностью в несколько микрогенри.
- В литературе обычно катушку индуктивности называют антенной, хотя реально таковой она может не являться.

- Когда идентификатор оказывается вблизи считывателя, два контура (идентификатора и считывателя) оказываются индуктивно связанными.
- Контур считывателя можно рассматривать как первичный, а идентификатора – как вторичный.
- Индуктивная связь катушек приводит к появлению взаимной индуктивности.
- Следовательно, появление в магнитном поле первичного контура катушки индуктивности вторичного приводит к изменению параметров первичного контура считывателя, которые могут регистрироваться.
- Т. о., изменяя параметры вторичного контура, можно организовать информационный обмен между считывателем и идентификатором.
- Для изменения параметров вторичного контура идентификатора (т. е. для модуляции), используется специальная микросхема.

Диапазоны частот

- Длинноволновый диапазон (125-400 кГц)
  - Связь – индуктивная. Катушка (>100 витков) и конденсатор.
  - Только чтение информации с идентификаторов.
  - Наиболее широко используемая частота – 125 кГц.
  - Типичная дальность считывания 5-60 см.
- Диапазон коротких волн (3-30 МГц)
  - Связь – индуктивная.
  - Катушка (<100 витков) и конденсатор.
  - Чтение и запись информации на идентификаторы (бесконтактные смарт-карты).
  - Наиболее широко используемая частота – 13,56 МГц.
  - Выше скорость обмена информацией.
  - Возможность хранить на карте больший объем информации и двухстороннего обмена данными.
- СВЧ-диапазон (>900 МГц)
  - Системы с электромагнитной связью.
  - Антенна идентификатора – диполь (отрезок проводника).
  - Большая дальность считывания (0,5-12 м).
  - Сильное влияние окружающих условий на дальность считывания.


Считыватель
Идентификатор
Генератор
Усилитель мощности
Микроконтроллер
Б
Фильтр, усилитель, формирователь импульсов
Пиковый детектор
А
Цепь синхронизации
Память
В
Выпрямитель
Кодер
Модулятор
Полевой транзистор

Сеанс связи между считывателем и картой:

1. Считыватель формирует колебания несущей частоты, контролируя наличие модуляции в сигнале. Модуляция будет означать обнаружение карты в зоне действия считывателя.
2. Карта попадает в поле считывателя. После накопления энергии, достаточной для работы микросхемы и синхронизации, начинается управление транзистором, шунтирующим контур (модуляция).
3. Модуляция производится в соответствии с информационным кодом, записанным в памяти микросхемы карты. Это приводит к изменению параметров несущего колебания в контуре считывателя.
4. Считыватель осуществляет детектирование амплитудно-модулированного сигнала и декодирование информации.

Факторы, влияющие на дальность считывания

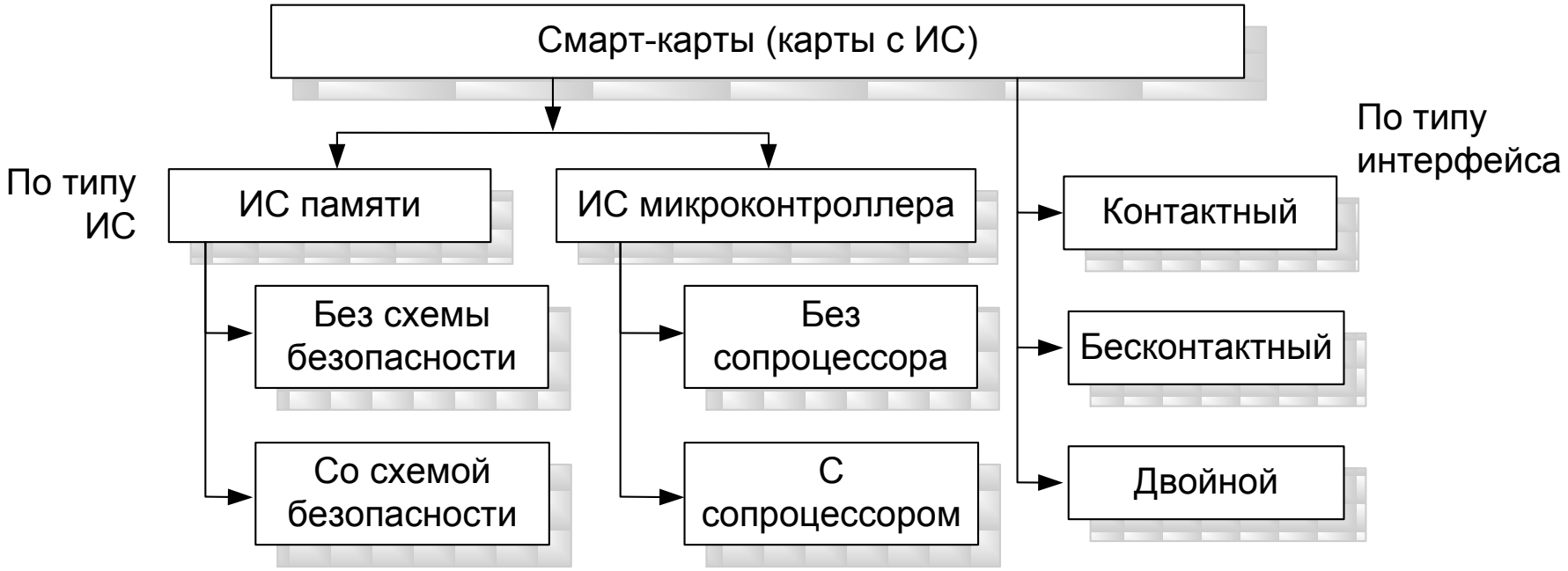
- Рабочая частота.
- Конструкция антенны считывателя.
- Добротность контура антенны считывателя.
- Конструкция антенны идентификатора.
- Добротность контура антенны идентификатора.
- Взаимная ориентация антенн считывателя и идентификатора в пространстве.
- Величина тока и напряжения в катушке считывателя.
- Чувствительность приемника считывателя.
- Используемый способ модуляции сигнала.
- Окружающие условия (наличие близкорасположенных металлических предметов, электромагнитных помех и т. п.).
- и др.

- Возможность считывания нескольких карт, находящихся в зоне действия считывателя.
- Для этого - антиколлизионные методы мультидоступа:
  - пространственное разделение;
  - частотное разделение;
  - временное разделение;
  - кодовое разделение.
- Практически неограниченный срок службы карт.
- Высокая пропускная способность СКУД.
- Сравнительно невысокая защищенность от копирования.
- Нет единого стандарта (карты и считыватели разных производителей не всегда совместимы друг с другом).

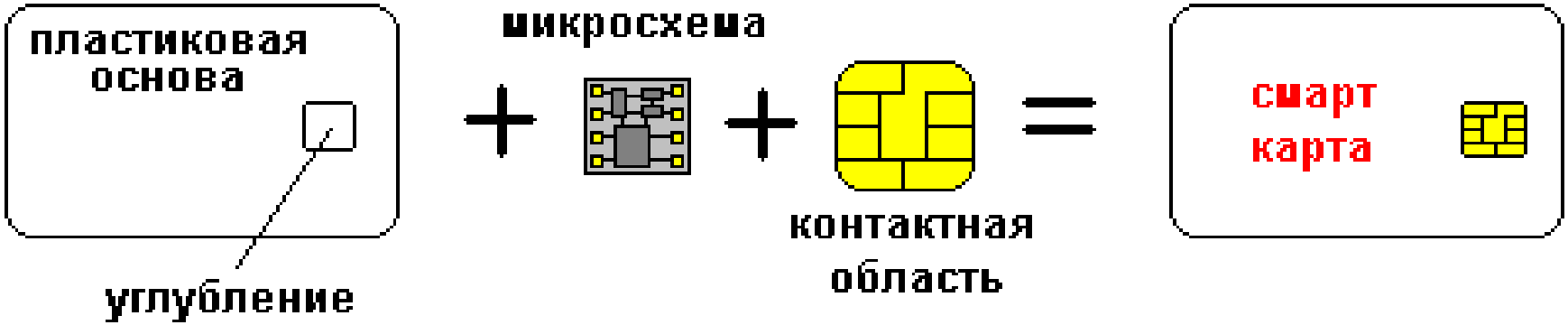
Смарт-карты

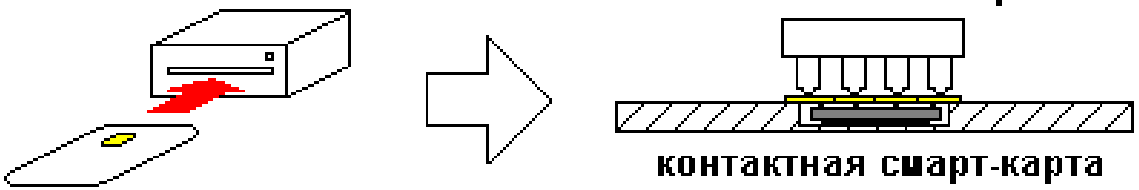
- Smartcard – «интеллектуальная» карта.
- Области применения:
  - платёжные системы (кредитные карты, транспортные карты, …);
  - СКУД;
  - доступ к компьютерам и программному обеспечению;
  - телефония (SIM-карты, таксофонные карты);

  и др.
- Преимущества по сравнению с другими типами карт:
  - Большой объем памяти (например, на 32 Кбит).
  - Высокая скорость обмена данными со считывателем (до 115,2 кбит/с для контактных смарт-карт и 7,8 кбит/с для бесконтактных).
  - Высокая безопасность хранения данных и защита от копирования.
  - Возможность использования алгоритмов шифрования данных при обмене информацией со считывателем.
- Смарт-карты классифицируются:
  - по типу микросхем памяти и микроконтроллера;
  - по способу считывания (контактный, бесконтактный, двойной интерфейс).


Смарт-карты (карты с ИС)
По типу ИС
ИС памяти
ИС микроконтроллера
Без схемы безопасности
Со схемой безопасности
Без сопроцессора
С сопроцессором
По типу интерфейса
Контактный
Бесконтактный
Двойной

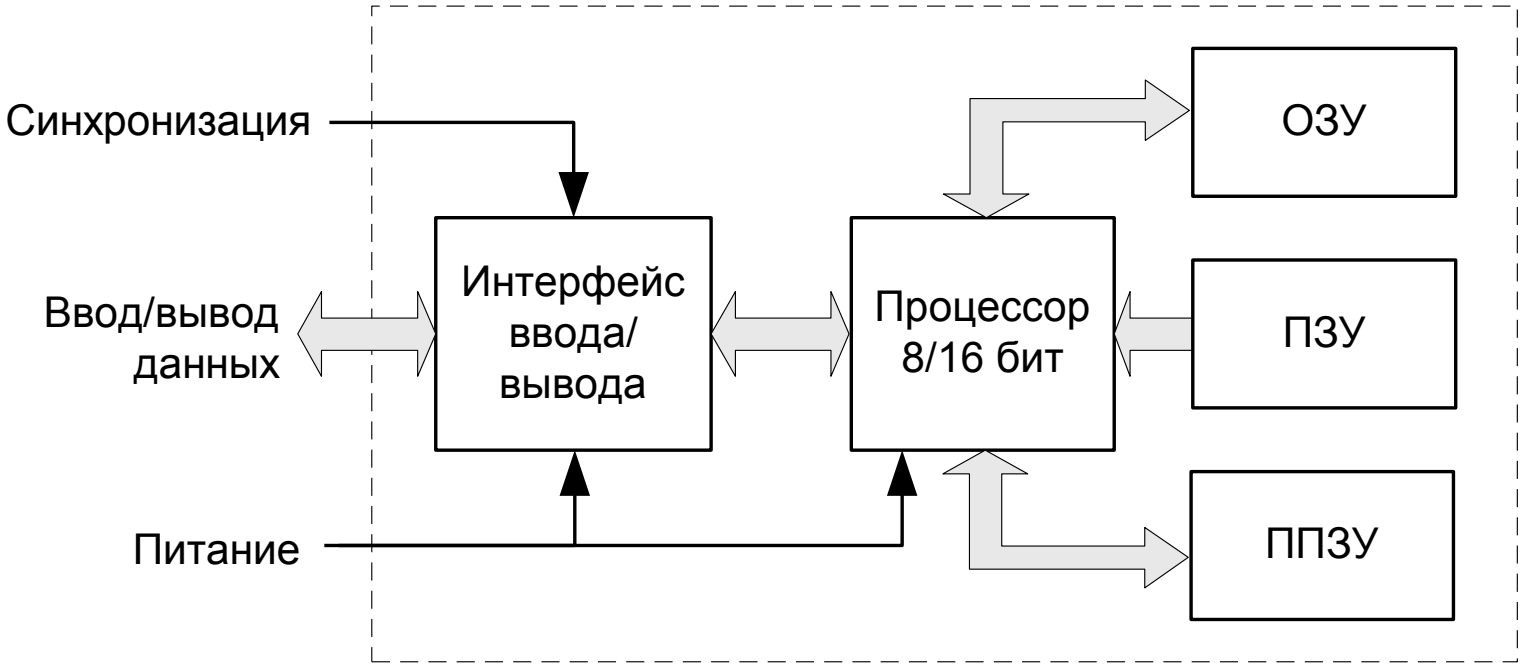
Конструкция контактных карт





VCC	GND
RST	VPP
CLK	I/O
RFU	RFU

Функциональная схема контактной карты



- Сочетают достоинства бесконтактных проксимити-карт и смарт-карт.
- Преимущества по сравнению с проксимити-картами:
  - Возможность многократной перезаписи информации на карте.
  - Шифрование данных при обмене информацией со считывателем.
  - Безопасное хранение данных на карте.
  - Хранение данных в нескольких независимых областях памяти для различных применений.
  - Единые стандарты ISO на бесконтактные смарт-карты.

- Применение:
  - контроль доступа людей в помещения;
  - платёжные системы ;
  - общественный транспорт ;
  - платные парковки ;
  - доступ к компьютерам;
  - биометрические системы.

- Наиболее известные стандарты:
  - ISO / IEC 14443 – рабочее расстояние до 10 см ;
  - ISO / IEC 15693 – рабочее расстояние до 1 м.

- Характеристики:
  - рабочая частота 13,56 МГц;
  - скорость обмена данными со считывателем 26 / 106 кбит/с ;
  - стандартный объём памяти на карте 2–16 кбит ;
  - продолжительность сеанса связи со считывателем 100 мс.

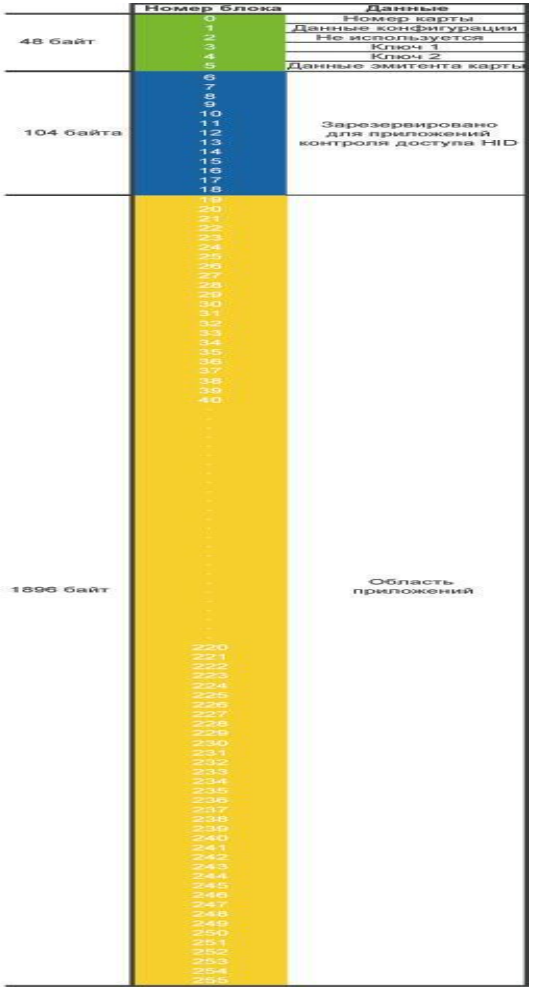
Смарт карты
Пример объёма информации

Тип данных	Размер (бит)	Размер (байт)	Карта 2 кбит (256 байт)	Карта 16 кбит (2 кбайт)
Двоичные данные (“1”/”0”)	1	1/8	832	15168
Символ ASCII-кода	8	1	104	1896
Значение от 0 до 65535	16	2	52	948
Образ геометрии ладони (RSI)	72	9	11	210
Образ отпечатка пальца (Bioscrypt)	2784	348	0	5
Образ радужной оболочки глаза (LG)	4096	512	0	3
Шаблон голоса	10000	1250	0	1
Фотография с низким разрешением	12000	1500	0	1

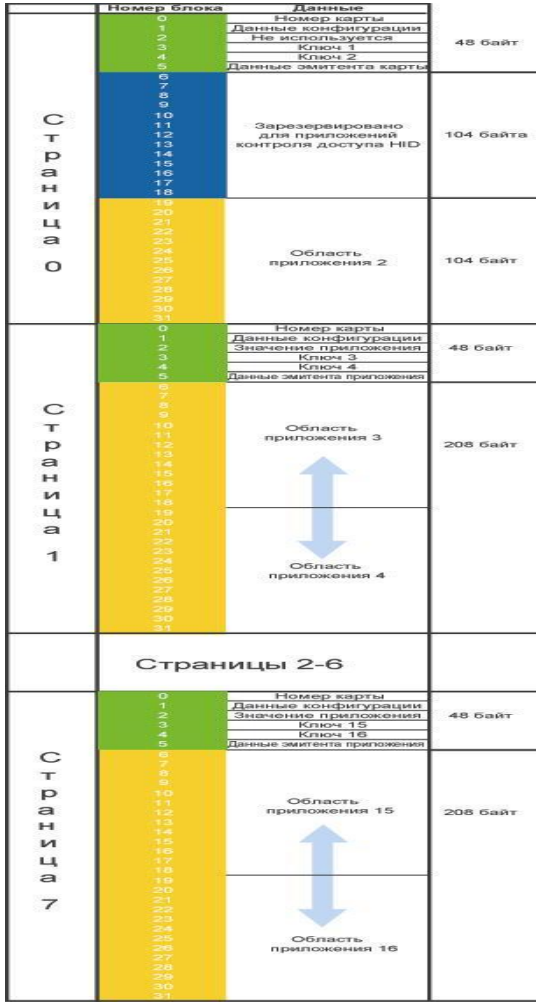
2 кбит / 2 приложения

	Номер блока	Данные
48 байт	0	Номер карты
	1	Данные конфигурации
	2	Не используется
	3	Ключ 1
	4	Ключ 2
	5	Данные эмитента карты
104 байта	6	Зарезервировано для приложений контроля доступа HID
	7	
	8	
	9	
	10	
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
104 байта	19	Область приложений
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
	28	
	29	
	30	
	31	

16 кбит / 2 приложения

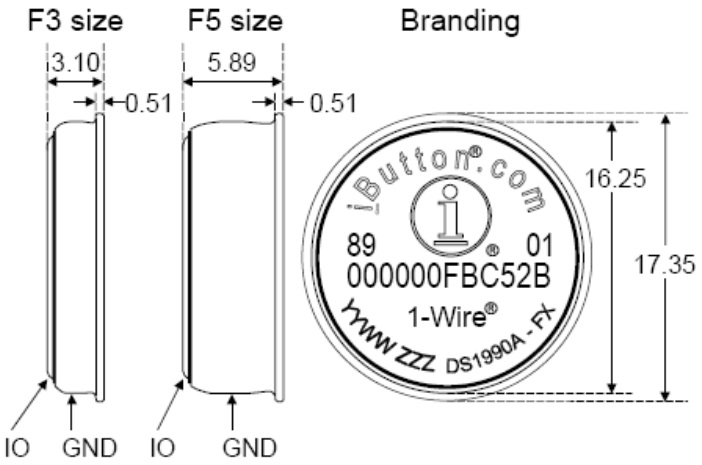


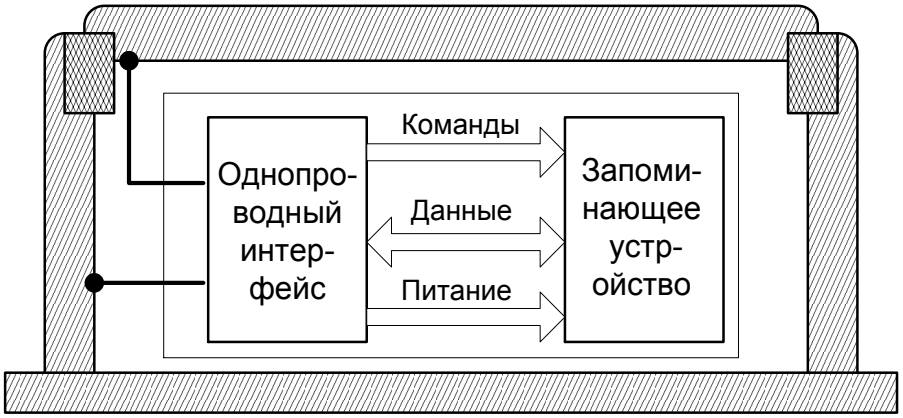
16 кбит / 16 приложений



Контактная память (электронные ключи)

- Электронные ключи
- Контактная память
- Электронные таблетки
- Touch-memory
- iBotton

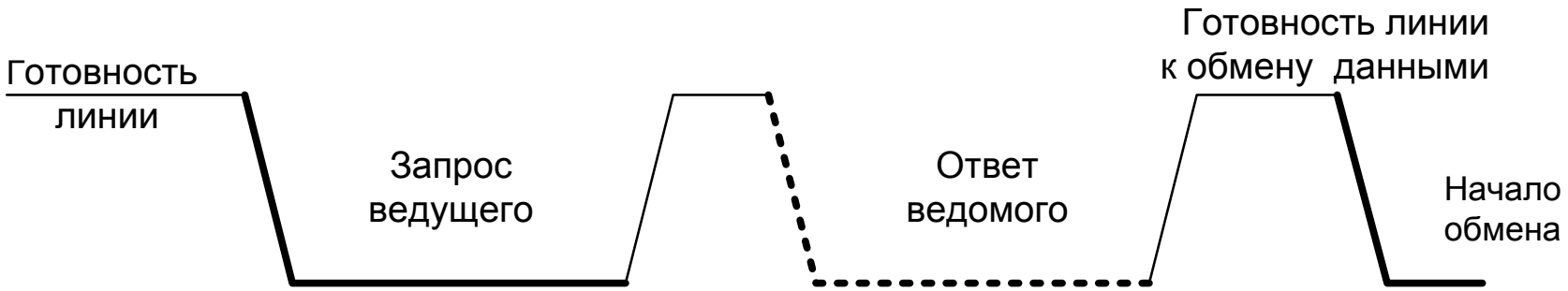


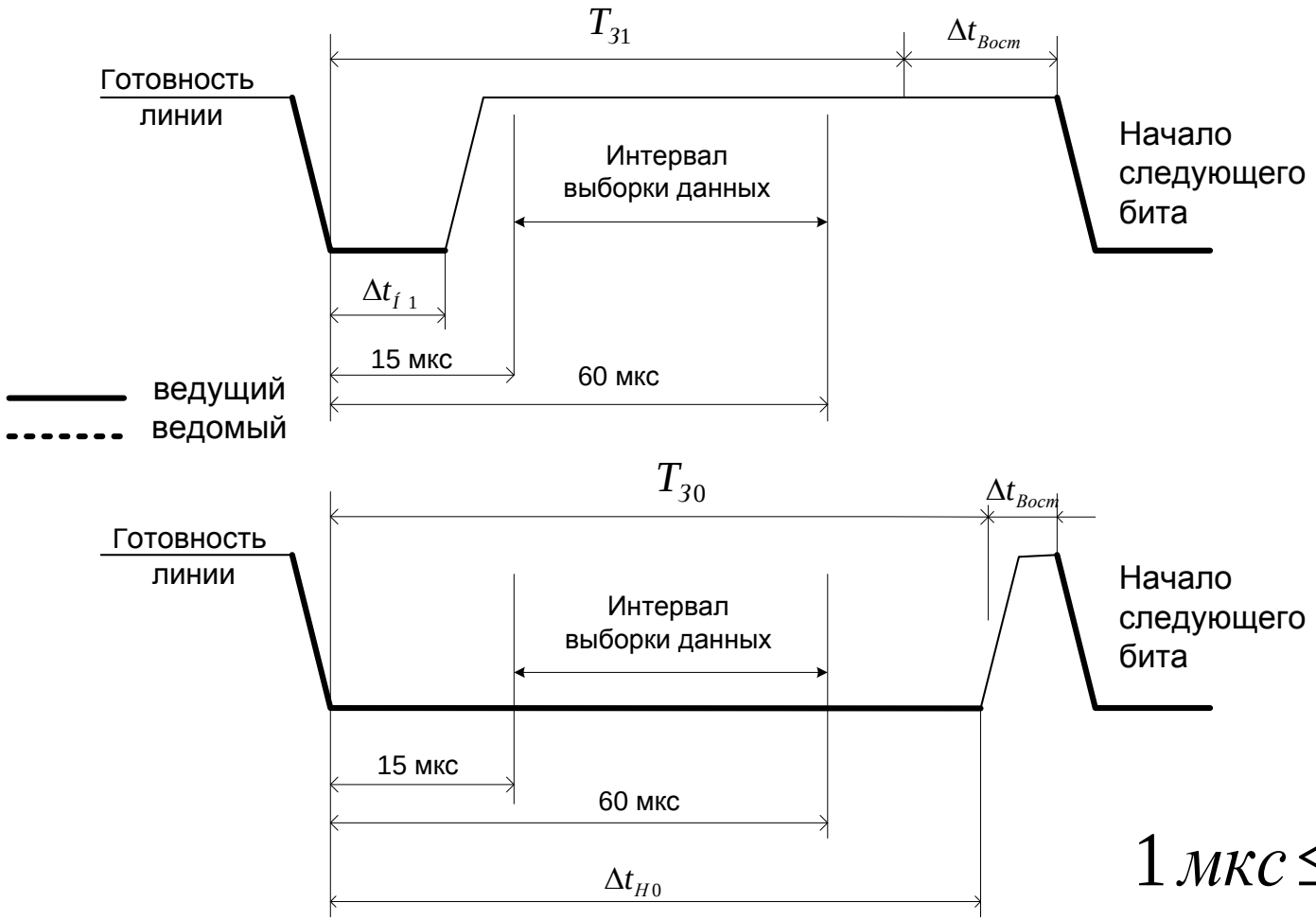


Основные особенности

- Однопроводной интерфейс .
- Принцип взаимодействия - «ведомый-ведущий», ведущим всегда является считыватель, а электронный ключ всегда ведомый.
- Считыватель инициирует передачу каждого бита.
- Передача или прием информации в полудуплексном режиме по битам.
- Тактовые интервалы независимые. Поэтому в любой момент может быть сделано прерывание (задержка) в процессе обмена.

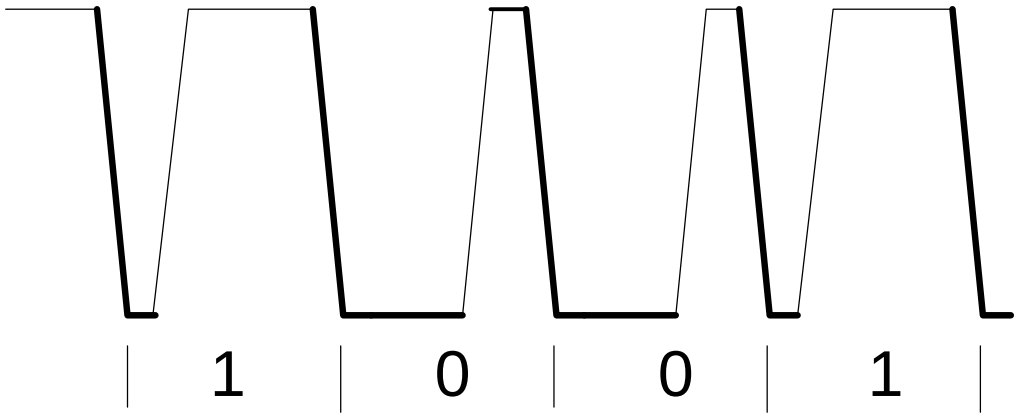
- Исходное высокое (логическая единица) состояние линии связи свидетельствует о готовности считывателя.
- Начало временного сегмента (такта считывания или записи) осуществляется переходом линии в низкое состояние логического нуля, что эквивалентно запросу от ведущего устройства.
- Затем считыватель освобождает линию и переходит в режим приема. Линия при этом возвращается в высокое состояние.
- Ведомое устройство обнаруживает сигнал ведущего и формирует сигнал опознавания – переход в низкое состояние
- Затем освобождение линии с возвратом в высокое состояние.



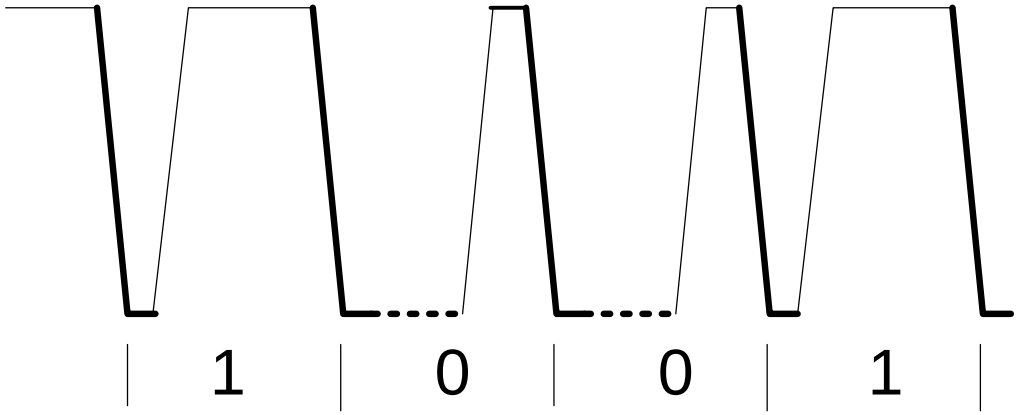


$$1\,мкс \le \Delta t_{Вост} < \infty$$

Запись



Чтение



- Постоянное запоминающее устройство (ПЗУ), данные в которое записываются при изготовлении и не могут быть изменены в процессе эксплуатации.
- Интерфейс для приема и передачи информации с функциями контроля целостности данных.
- Пассивный источник питания.
- Энергонезависимое перепрограммируемое запоминающее устройство (ППЗУ).
- Встроенный источник питания для ППЗУ.
- Буферная память для защиты от возможного нарушения контакта во время процесса записи/считывания.
- Схема синхронизации и часы.
- Датчик температуры и влажности.

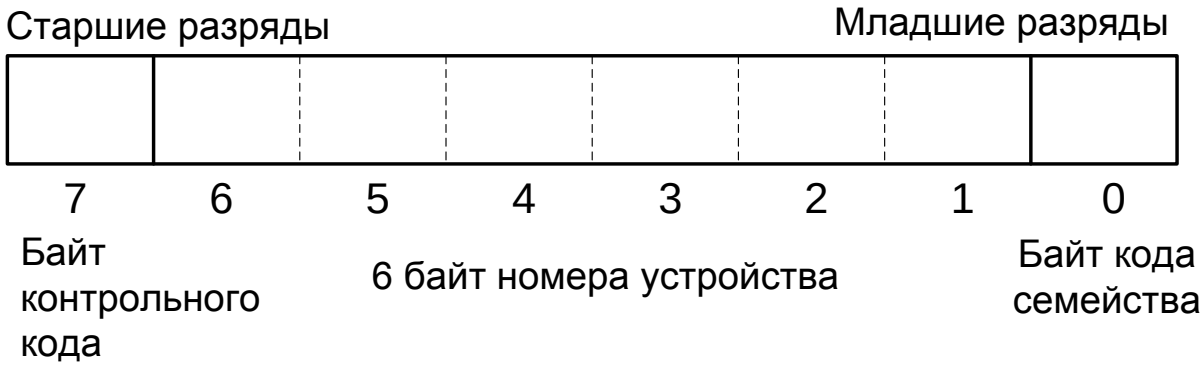
Первые три элемента присутствует во всех устройствах.

- Питание микросхемы и обмен данными осуществляется в период касания идентификатора и считывателя. Таким образом, питание, прием и передача данных осуществляется по одной паре проводников.
- Поскольку как для питания, так и для обмена информацией могут использоваться только два контакта, необходимо разделение постоянного (питание) и переменного (информация) токов, что достаточно просто реализуется технически.
- Следует учитывать возможность нестабильного контакта при работе. Этим обусловлена необходимость в буферной памяти для идентификаторов, имеющих перепрограммируемые запоминающие устройства.

Постоянное запоминающее устройство

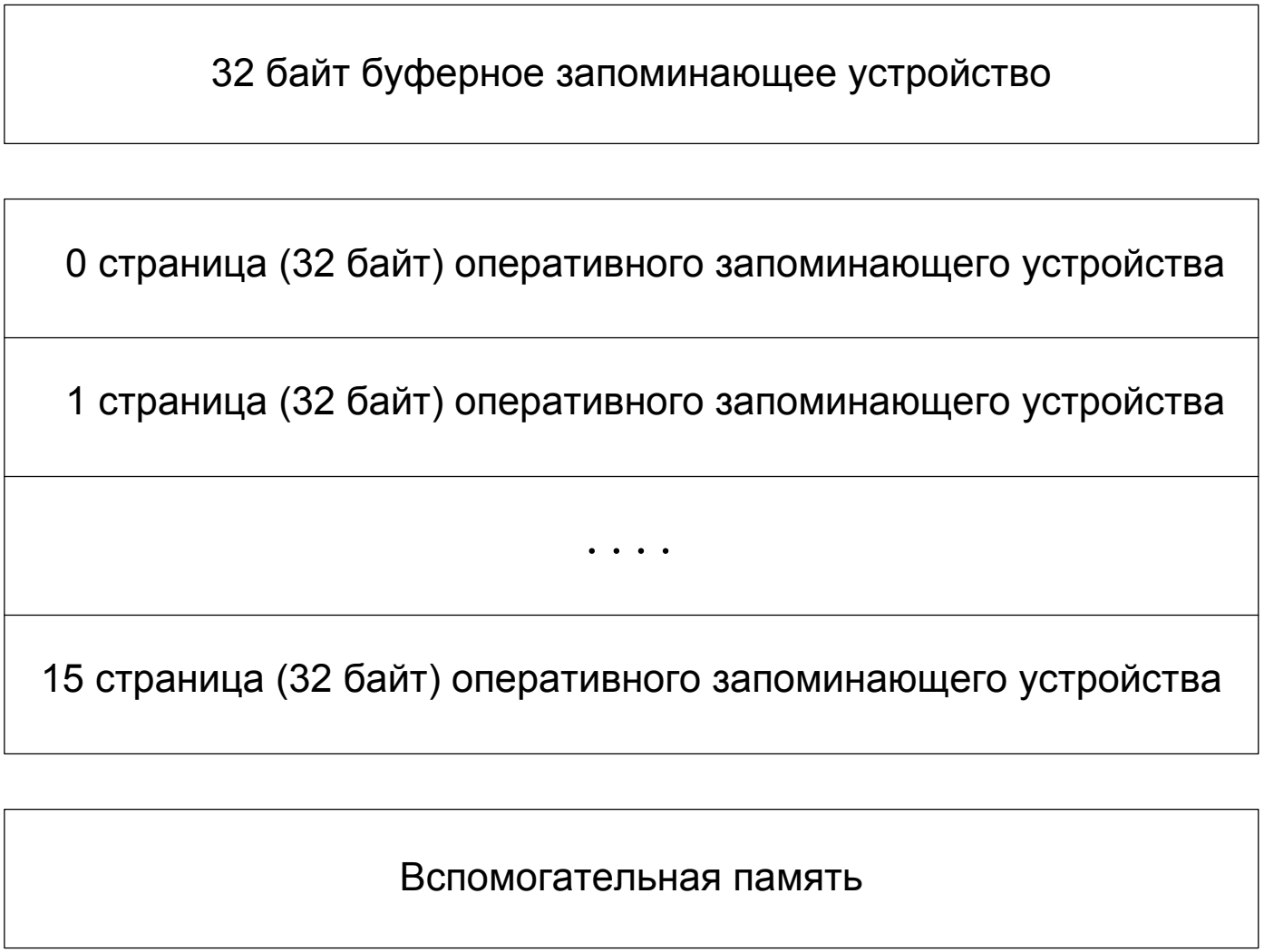
- ПЗУ – это элемент, присутствующий во всех типах электронных ключей. В постоянное запоминающее устройство при изготовлении лазером записывается 64-разрядный код, который состоит из следующих компонентов:
- 8-разрядного кода семейства;
- 48-разрядного уникального серийного номера устройства;
- 8-разрядного контрольного кода.

Структура ПЗУ



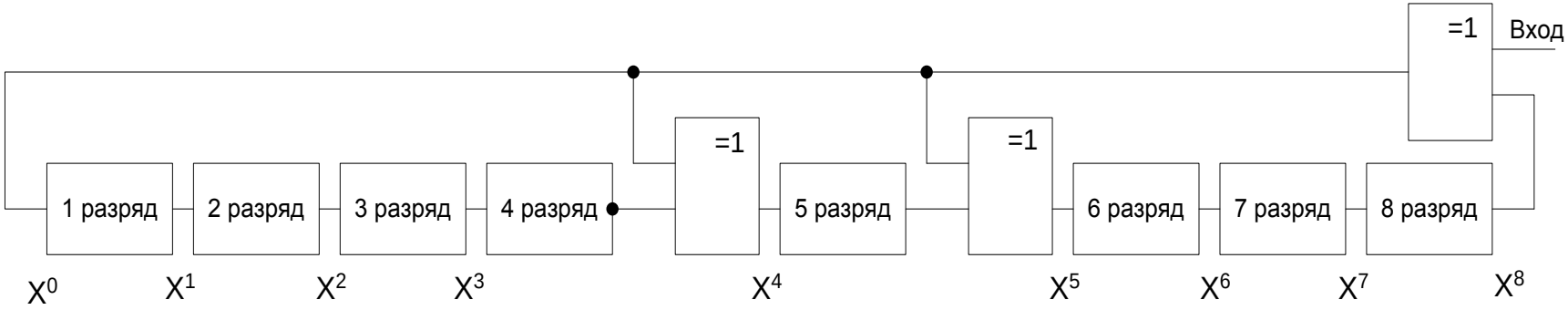
- Все электронные ключи, кроме простейшего, имеют составе статическую оперативную память с неограниченным числом циклов записи/чтения. Питание памяти обеспечивается миниатюрной литиевой батарейкой, срок службы которой составляет не менее 10 лет.

- Для обеспечения целостности информации в процессе обмена информацией кроме ОЗУ электронные ключи имеют буферную память от 1 до 32 байт.


32 байт буферное запоминающее устройство
0 страница (32 байт) оперативного запоминающего устройства
1 страница (32 байт) оперативного запоминающего устройства
. . . .
15 страница (32 байт) оперативного запоминающего устройства
Вспомогательная память

Контактная память
Структурная схема простейшего устройства

Проверка правильности считывания данных осуществляется с помощью циклически избыточного кода (CRC).



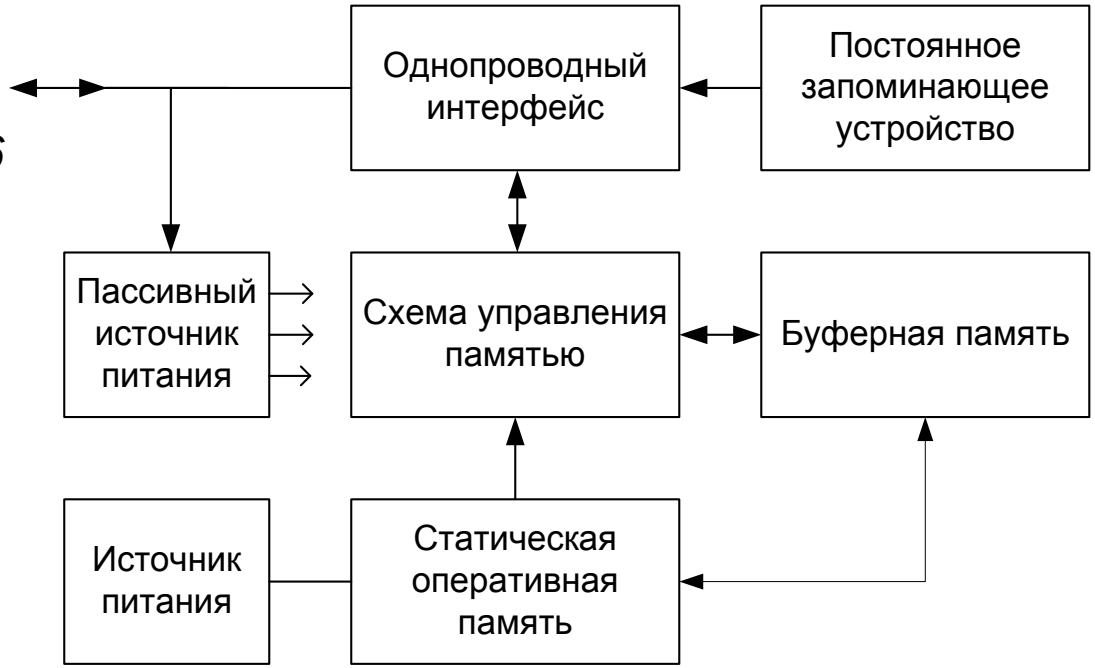
Такой алгоритм контроля правильности данных позволяет выявлять:

- любое нечетное число ошибок в пределах 64-битового кода;
- любые двойные битовые ошибки в пределах 64-битового кода;
- любые кластеры ошибок, которые могут содержаться в пределах 8-битовых окон;
- самые большие кластеры ошибок.

DS1992-1996 имеют статическое ОЗУ идентичной структуры с объемом памяти от 4 (1024 бит) до 256 (65536 бит) страниц.

- ОЗУ доступно как для чтения, так и для записи.
- Чтение осуществляется напрямую через схему управления памятью.
- Запись – через 32 бит буферную память.
- Вспомогательная память статуса памяти на 8 бит.

Структурная схема *DS1996*



Устройства типа *DS1991* и *DS 1977* обеспечивают защиту памяти от несанкционированной записи/чтения.

0 страница (48 байт) оперативного запоминающего устройства	Пароль 8 байт	Идентификатор 8 байт
1 страница (48 байт) оперативного запоминающего устройства	Пароль 8 байт	Идентификатор 8 байт
2 страница (48 байт) оперативного запоминающего устройства	Пароль 8 байт	Идентификатор 8 байт
3 страница - 64 байта буферное запоминающее устройство		

- Три независимых страницы памяти, защищенных паролями.
- Открытый идентификатор записывается и считывается.
- Закрытый пароль может быть только записан и не может быть считан.
- При обращении к памяти необходим пароль для доступа как для чтения, так и для записи.
- Если был введен неправильный пароль, то будут считываться случайные числа.
- Для записи нового пароля необходим открытый идентификатор.
  При программировании нового пароля все данные стираются.

DS1982-1986 имеют однократно записываемое запоминающее устройство.

- Нет встроенного источника питания.
- Есть схема контроля напряжения питания.
- Запись данных осуществляется через 1-байтную буферную память.
- При записи проверяются команды, адрес и сами данные с использованием 8 разрядного циклического кода.
- Каждая страница может быть индивидуально защищена от повторной записи. Для этого имеется регистр 8 байт статуса памяти.

Электронный ключ *DS1994* содержит встроенные часы.

Они содержат кварцевый генератор тактовой частоты 32.768 кГц, интервальный счетчик и счетчик циклов с возможностью формирования сигнала от этих счетчиков.

Датчик температуры *DS1920* 9 (в диапазоне -40^{0}C …+85^{0}C).

Позволяет считывать данные из одной точки с нескольких устройств. Различные проблемно ориентированные модификаций устройств. Например, для измерения температуры тела.

Штриховые коды

- Штриховый код – группа полос (прямоугольников) различной ширины (формы) и цвета, наносимых на поверхность идентификатора.
- Способ кодирования (нанесения) информации графический. Каждый символ кодируется определенным количеством штрихов и пробелов.
- Способ считывания - оптический.
- Информационными параметрами в штриховом коде являются определенная комбинация штрихов и их параметров - соотношение ширины темных полос (штрихов) и ширины светлых полос (пробелов между штрихами). Это соответствует широтно-импульсной модуляции.
- Отведенное для каждой цифры кода место называется знаком и является основной единицей информации в штриховом коде.
- Код в общем случае может содержать как цифры, так и буквы.
- Основное преимущество – низкая стоимость – около $0,005 (для сравнения – радиочастотный идентификатор стоит $0,07-0,3)

По длительности (количеству символов)
- непрерывные;
- фиксированной длины.

По способу кодирования (нанесения) информации
- Одномерные (линейные);
- Двумерные.

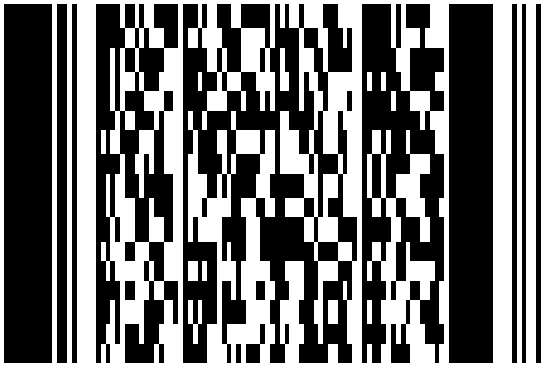
По виду кодируемых знаков
- Кодирование цифр.
- Кодирование цифр, букв и специальных символов

По длительности кода символов
- С постоянной длиной кода
- С переменной длиной кода

По способу нанесения информации на носитель
- С дублирование кодов символами
- Без дублирования

По способу контроля правильности считывания кода
- С контролем
- Без контроля

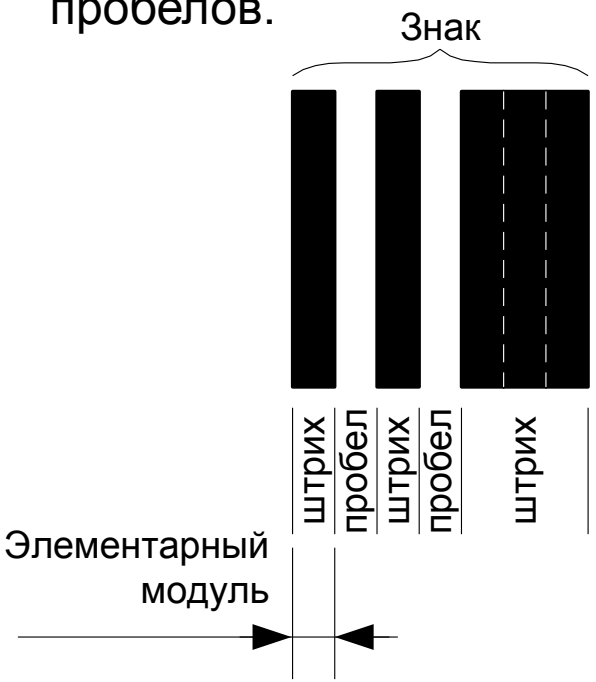
Примеры штриховых кодов



- Линейными (одномерными) - штриховые коды, читаемые в одном направлении (поперек штрихов).
- Это собой группа вертикальных полос различной ширины, наносимых на поверхность идентификатора.

Основные принципы формирования:

- Символы кодируются определенными последовательностями штрихов и промежутков.
- Ширина графического элемента кода обычно кратна значению ширины элементарного модуля.
- Элементарный модуль – это самый узкий элемент – штрих или пробел.
- Фиксированный набор используемых значений ширины штрихов и пробелов.



1010111

11113

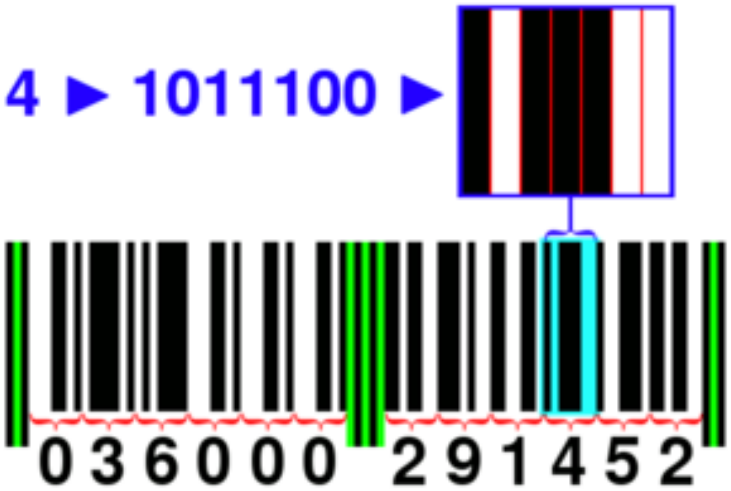

UPC-A
1 23456 78910 4
0 123456 789104 >
Контрольное число
EAN-13

Универсальный код товара

Основные требования:

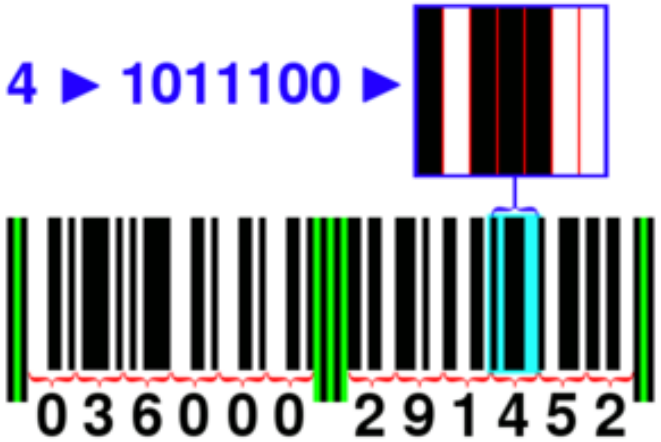
- симметричности кода – он должен читаться правильно в любом направлении – прямом и обратном, то есть при любой ориентации (перевороте);
- инвариантности к сочетанию цвета или тона – черные штрихи/белые промежутки и наоборот;
- простота нанесения/считывания;
- дешевизна;
- высокая надежность правильности считывания.

Структура штрихового кода UPC



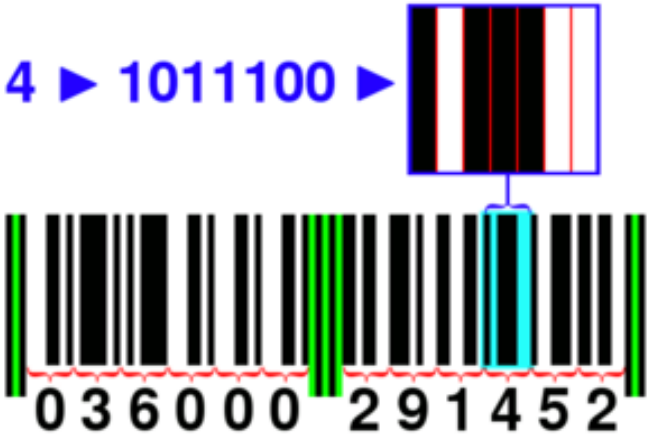
- Код состоит из 2 групп цифр, по 6 цифр в каждой группе — левой и правой.
- Группы цифр разделяются так называемыми защитными шаблонами. Эти шаблоны содержат штрихи единичной ширины, которые служат для синхронизации сканеров штрихового кода.
- Левые и правые защитные шаблоны состоят из 3 штрихов единичной ширины — двух тёмных и одного светлого межу ними.
- Средний защитный шаблон состоит из 5 штрихов — трех светлых и двух темных. Всё остальное – цифры кода.

Особенности штрихового кода UPC



- Каждая цифра представляется последовательностью из 7 бит.
- Каждая цифра кодируется с помощью четырёх штрихов: двух светлых и двух тёмных.
- Каждый штрих может иметь относительную ширину в одну, две, три или четыре единицы.
- Общая ширина штрихов для одной цифры всегда составляет семь единиц.
- Максимальная длина тёмного или светлого участка кода не может превышать четырёх единиц. То есть переход с одного символа на другой – со сменой цвета
- Общая ширина всего кода всегда равна 95 единицам.
- В любом коде 29 светлых и 30 тёмных штрихов.

Кодировка цифр штрихового кода UPC



Защитные шаблоны

101

01010

Цифра	Левый код	Правый код	Ширина линий
0	0001101	1110010	3-2-1-1
1	0011001	1100110	2-2-2-1
2	0010011	1101100	2-1-2-2
3	0111101	1000010	1-4-1-1
4	0100011	1011100	1-1-3-2
5	0110001	1001110	1-2-3-1
6	0101111	1010000	1-1-1-4
7	0111011	1000100	1-3-1-2
8	0110111	1001000	1-2-1-3
9	0001011	1110100	3-1-1-2

Отличительные особенности:

- постоянная длина кода;
- высокая помехозащищённость;
- максимальное отличие битового представления цифр;
- переход с одной цифры на другую – обязательно со сменной штриха
  на пробел или наоборот;
- наличие «разделителей» или синхронизационных полей;
- равное количество штрихов в правой и левой частях кода.

Расчет контрольного числа (последняя 12 цифра)

1. Суммируются все цифры на нечётных позициях (первая, третья, пятая, и т. д.) и результат умножается на три.
2. Суммируются все цифры на чётных позициях (вторая, четвёртая, шестая, и т. д.)
3. Обе суммы складываются, и от полученного результата оставляется только последняя цифра.
4. Эту цифру вычитают из 10.
   Конечный результат этих вычислений - контрольная цифра (десятке соответствует цифра 0).

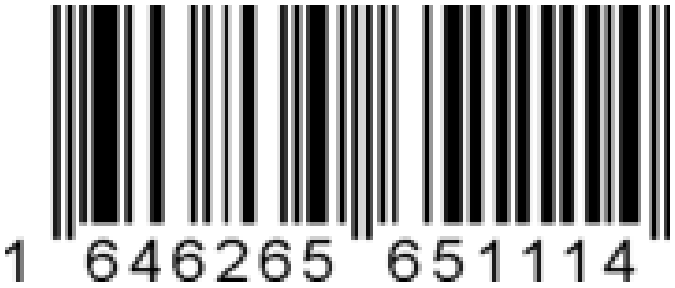
Проверка правильность считывания кода:

1. суммируются все нечётные цифры и умножаются на 3
2. суммируются все четные цифры, включая контрольную цифру
3. эти суммы складываются и оставляется последняя цифра от результата.

Если эта цифра ноль, то принимается решение, что код считан правильно, если любая другая, то код однозначно считан неверно.

Основные требования :

- максимальная совместимость с кодировкой UPC;
- расширение диапазона кодов для европейских производителей;
- чтение американских кодов.



Структура кода

Дополнительная 13-я цифра (первая по счёту) обычно указывается арабской цифрой слева от штрихового кода и кодируется с помощью 12 основных цифр кода.

Код EAN-13 условно можно разделить на 5 зон:

- Префикс национальной организации GS1(3 цифры).
- Регистрационный номер производителя или продавца товара(4-6 цифр).
- Код товара (3-5 цифр).
- Контрольное число (1 цифра).

Код для дополнительной цифры

Структура кода EAN-13		
Первая цифра	Первая (левая) группа из 6 цифр	Вторая (правая) группа из 6 цифр
0	LLLLLL	RRRRRR
1	LLGLGG	RRRRRR
2	LLGGLG	RRRRRR
3	LLGGGL	RRRRRR
4	LGLLGG	RRRRRR
5	LGGLLG	RRRRRR
6	LGGGLL	RRRRRR
7	LGLGLG	RRRRRR
8	LGLGGL	RRRRRR
9	LGGLGL	RRRRRR

Кодирование цифр			
Цифра	L-код	G-код	R-код
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110
6	0101111	0000101	1010000
7	0111011	0010001	1000100
8	0110111	0001001	1001000
9	0001011	0010111	1110100

Расчет контрольной цифры

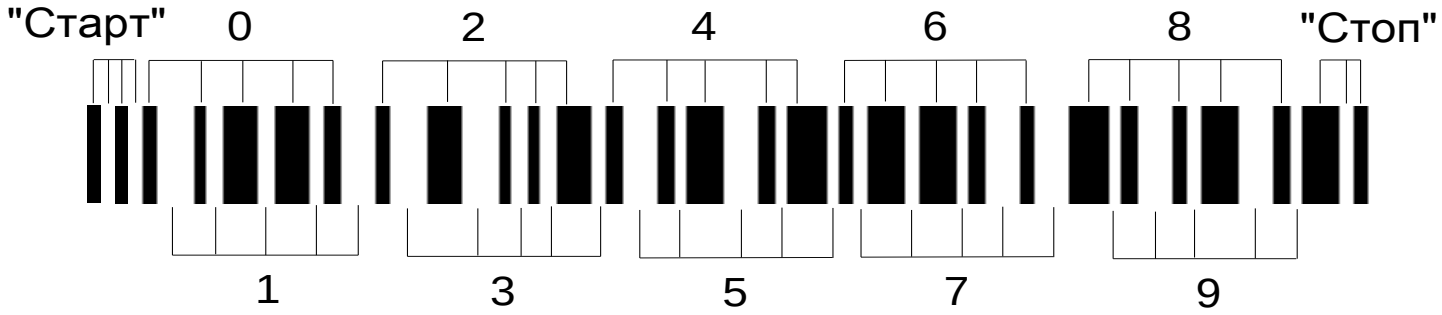
1. Сложить цифры, стоящие на четных местах.
2. Полученную сумму умножить на 3.
3. Сложить цифры, стоящие на нечетных местах, без контрольной цифры.
4. Сложить числа, указанные в пунктах 2 и 3.
5. Отбросить десятки.
6. Из 10 вычесть полученное в пункте 5.

Особенности:

- Код переменной длины
- кодирование 43 символов A-Z, 0-9 и спец. символов
- Каждый символ начинается и заканчивается темным штрихом
- Каждый символ состоит из 5 темных и 4 светлых штрихов
- знак состоит из 9 элементов, 3 элемента – широкие, 6 – узкие
- Отношение ширины узкого и широкого штриха может составлять от 2,2:1 до 3:1.
- нет контрольной цифры, но сам код обеспечивает коррекцию ошибок
- высокая достоверность (вероятность ошибки $3{,}3 \cdot 10^{-7}$).

- Этот непрерывный штриховой код переменной длины
- Позволяет кодировать цифры от 0 до 9.
- Цифры записываются парами с разным цветом штрихов
- Штрихи одной цифры пары являются разделителями для другой
- Относится к кодам с высокой плотностью записи и позволяет записывать до 18 цифр на дюйм при ширине элементарного модуля 0,19 мм. Высокая плотность достигается за счет исключения пробелов, разделяющих соседние знаки.

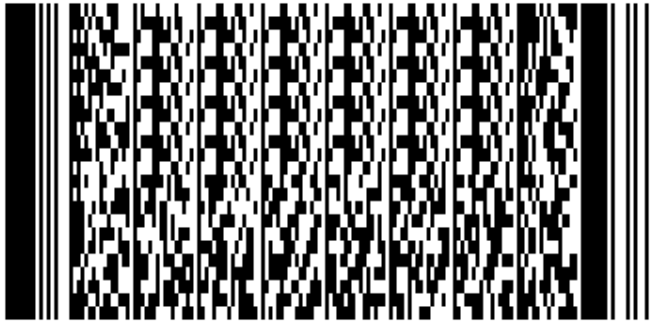
Структура штрихового кода Interleaved 2 of 5



- Имеет пять элементов в знаке, два из которых являются широкими.
- Представление пар цифр в знаках штрихового кода с помощью пяти штрихов и пяти промежутков.
- При этом используется чередование цифр: на нечетных позициях (считая слева направо) знаки изображаются штрихами, а на четных – пробелами. От этого произошло название кода – Interleaved - чередующийся).
- При кодировании данных с нечетным количеством знаков впереди записывается «0».
- В двоичном изображении широкий штрих или широкий промежуток идентичен «1», узкий штрих или узкий промежуток – «0»

Кодировка символов штрихового кода Interleaved 2 of 5

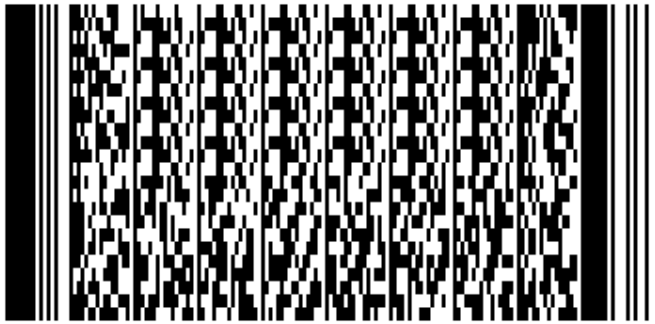
Знак	Комбинация широких (1) и узких (0) элементов
0	00110
1	10001
2	01001
3	11000
4	00101
5	10100
6	01100
7	00011
8	10010
9	01010
"Старт"	0000
"Стоп"	100



Два основных вида двумерных кодов: стековые и матричные.

Стековые представляют собой множество одномерных (линейных) штрих-кодов небольшой высоты, расположенных один над другим.

Матричные основаны на расположении черных элементов внутри матрицы. Каждый черный элемент имеет определенный размер и его позиция кодирует данные.



Что должно быть в коде:

- элементы обнаружения кода;
- элементы ориентации кода;
- элементы синхронизации данных;
- данные.

Двумерный штриховой код Aztec

Два основных формата символа Aztec Code:

- Компактный с мишенью из двух квадратов
- Полный с мишенью из трех квадратов.

Эти два формата образуют 33 различных вариантов размеров, которые могут эффективно кодировать как малые, так и большие сообщения.

В общем случае символы Aztec Code:

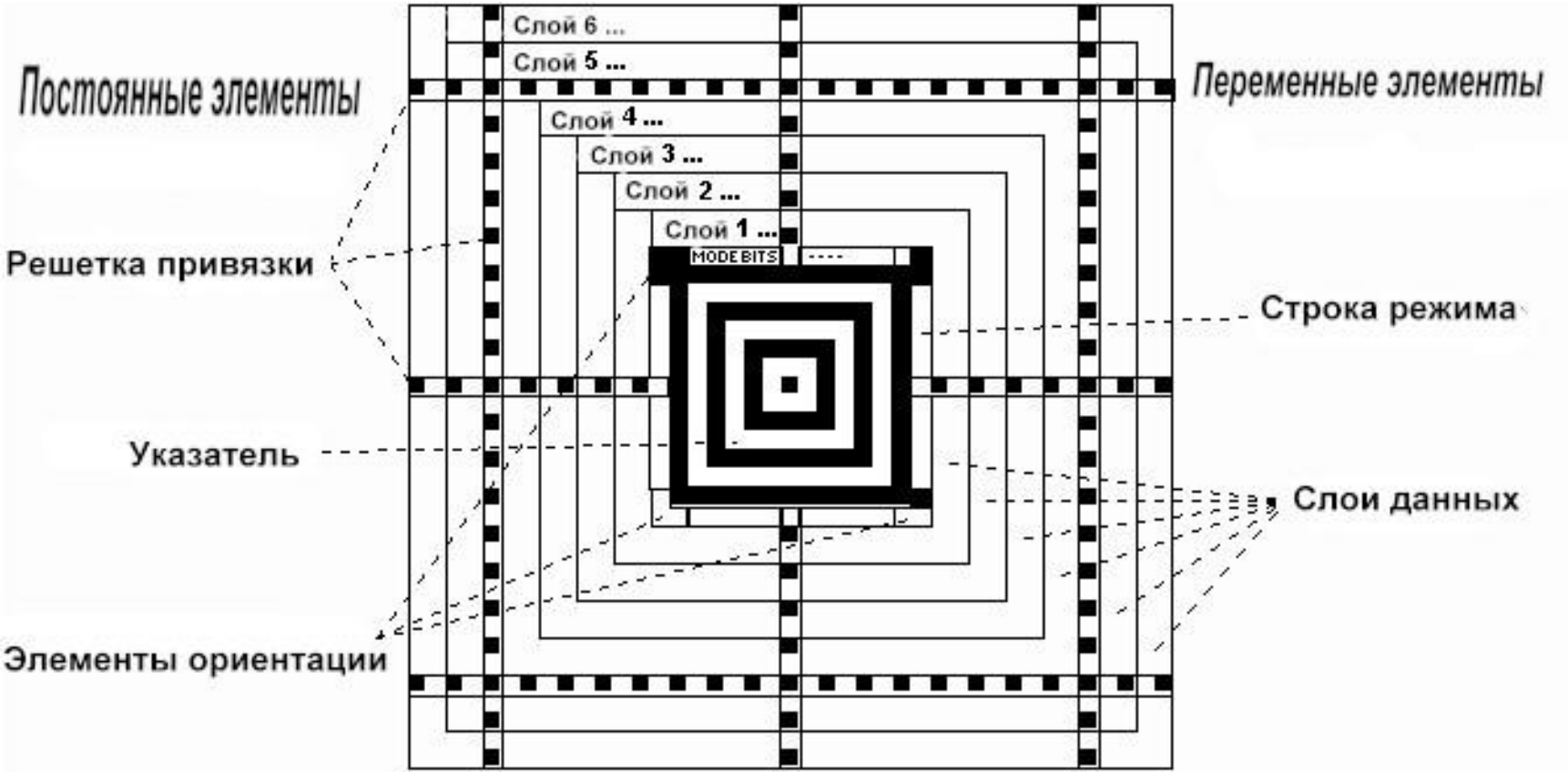
- могут кодировать любую байтовую последовательность;
- всегда квадратной формы (размером от 15x15 модулей -12 ASCII-символов до 151x151 модулей 3750 ASCII-символов);
- обнаружение и коррекция ошибок (избыточность 5-95%);
- свободной зоны вокруг кода не требуется.

# of Data Layers	Symbol Size (H x W, in X)	Symbol Data Capacities		
		Digits	Text	Bytes
1 *	15 x 15	13	12	6
4 *	27 x 27	110	89	53
7	45 x 45	294	236	145
11	61 x 61	601	482	298
15	79 x 79	1008	808	502
20	101 x 101	1653	1324	824
26	125 x 125	2632	2107	1314
32 **	151 x 151	3832	3067	1914

* indicates Compact symbols; the rest are Full-Range.

** exceeds the resolution capability of current readers.

Структура двумерного штрихового кода Aztec



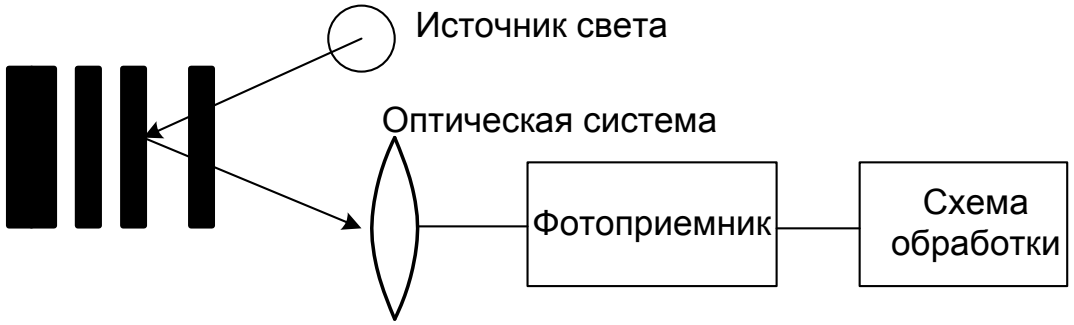
Упрощенный алгоритм чтения кода

1. Поиск и обнаружение мишени, соответствующее обнаружению символа кода Aztec. Алгоритм поиска, инвариантен относительно ориентации кода и угла сканирования.
2. После обнаружения мишени, оцениваются параметры элементов ориентации и строки режима.
3. Начиная от центра места по направлению к краям символа обрабатываются слои данных.

В общем случае в штриховом коде должны быть следующие элементы:

- опознавания (обнаружения) кода;
- ориентации для определения взаимного положения кода и считывателя;
- синхронизации для определения порядка считывания информации;
- информация.

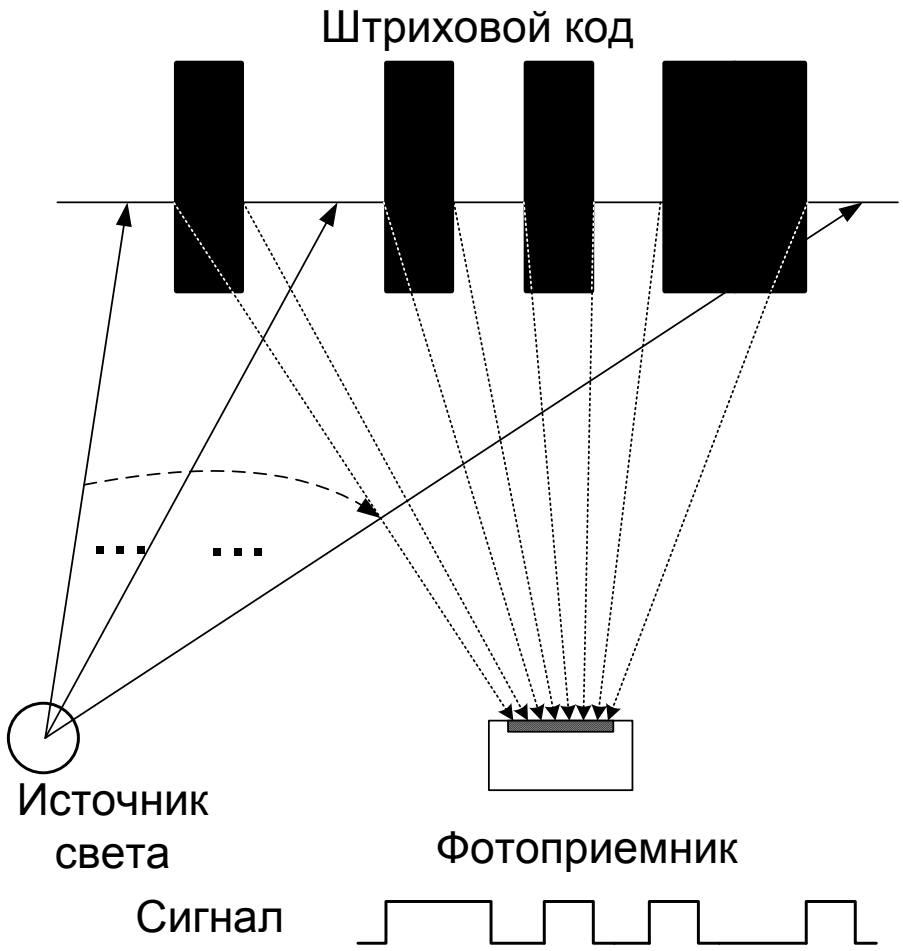
Функции некоторых из этих элементов могут объединены.



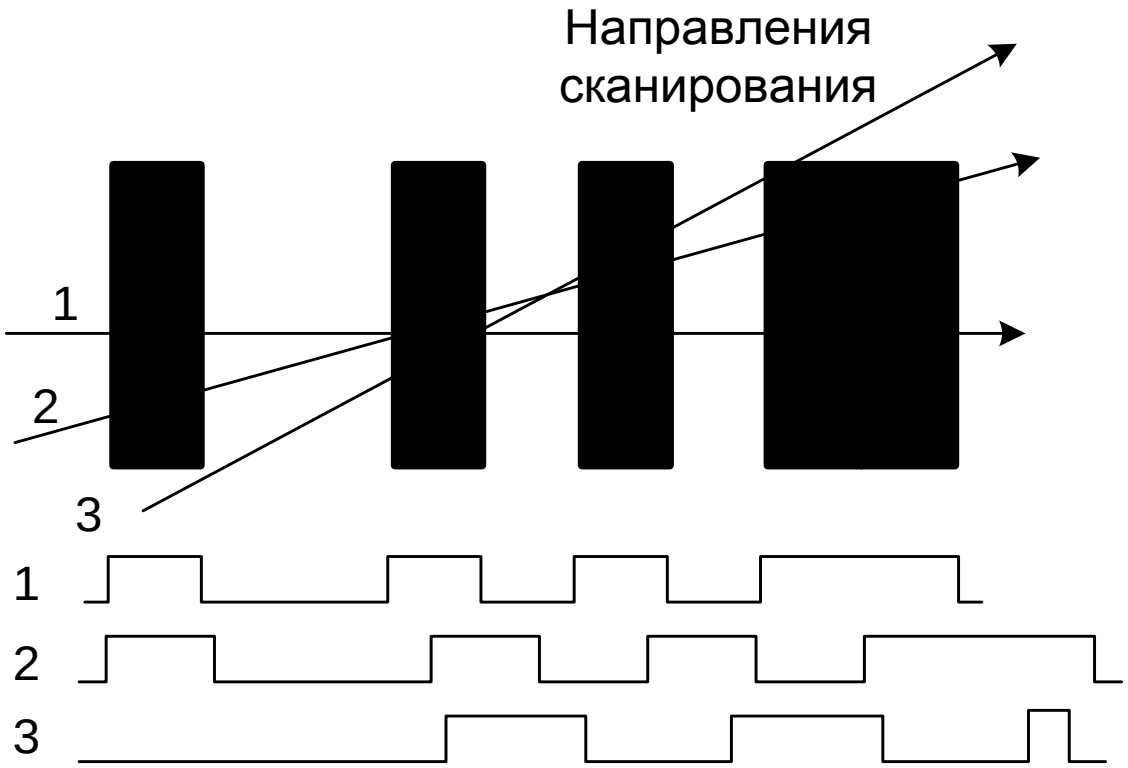
По способу считывания информации считыватели могут быть сканирующие и формирующие изображение кода. Последнее может быть одномерное (линейное) или двумерное (матричное).

Считыватели штриховых кодов

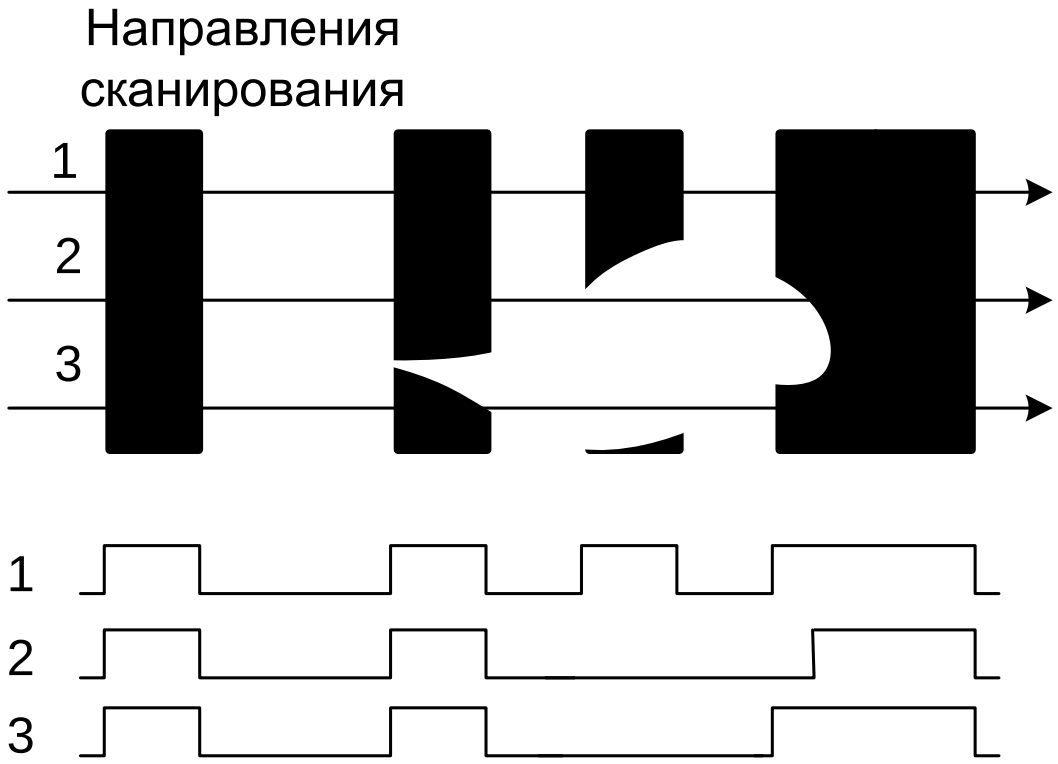
Принцип работы последовательного сканера



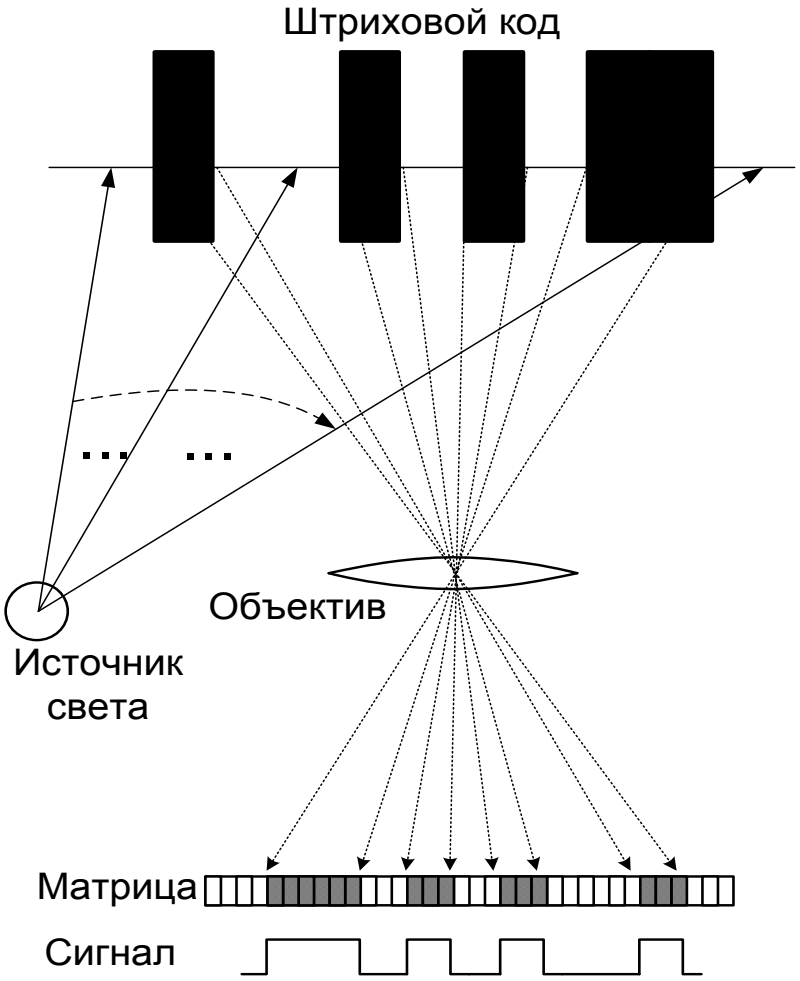
Влияние взаимного положения считывателя и кода



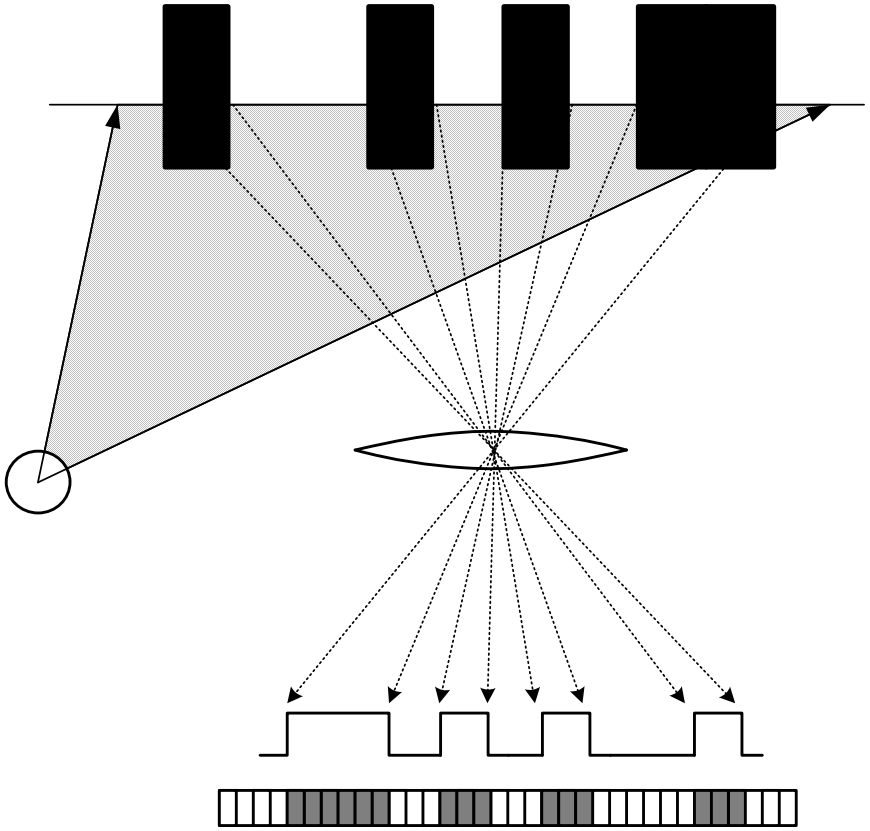
Считывание при повреждении кода



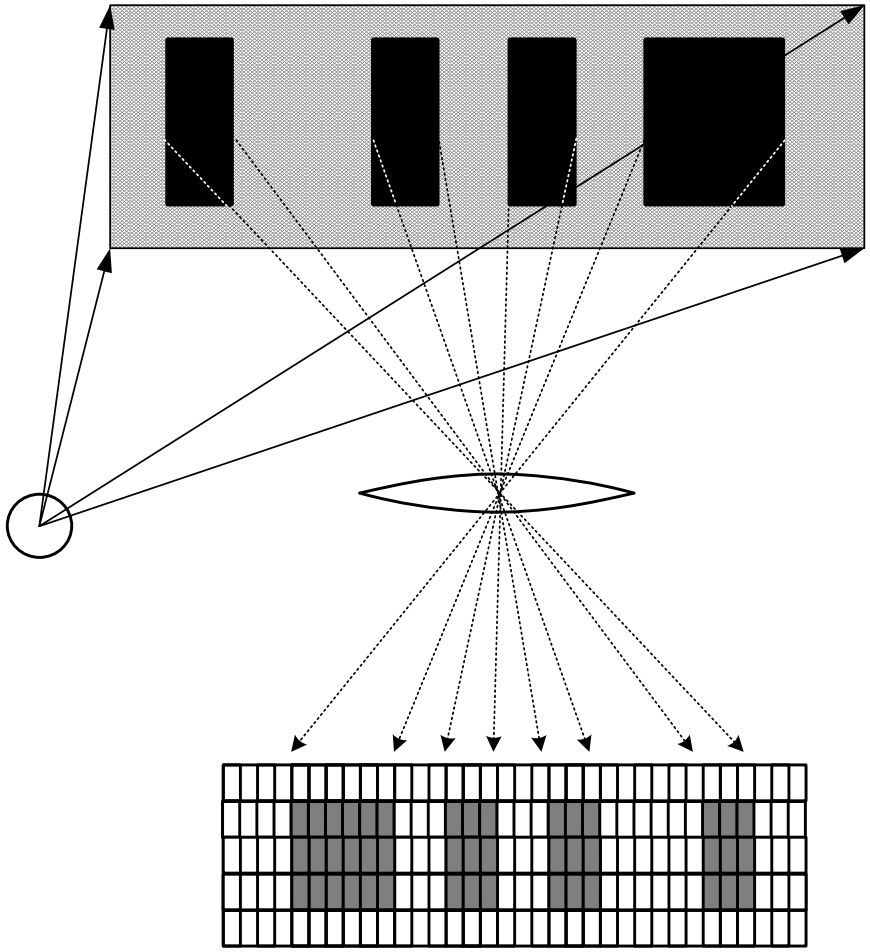
Принцип работы линейного сканирующего считывателя



Принцип работы линейного матричного считывателя



Формирование изображения кода матричным считывателем



Заключение

Рассмотренные в учебном пособии материалы охватывают основные типы устройств, используемые в настоящее время. Конечно, разнообразие оборудования постоянно увеличивается и пособие включает не все возможные вопросы построения и эксплуатации СКУД. Однако общие принципы построение систем контроля и управления доступом, выбора идентификаторов для таких систем, рассмотрение физических принципов действия различных устройств с общетеоретической точки зрения, приведенные в учебном пособии, позволяют подходить к проблеме разработки СКУД с общих позиций, заранее учесть различные аспекты и потенциальные проблемы и, тем самым, построить эффективную систему наиболее полно отвечающую сформулированным требованиям.

Литература

1. Волковицкий В. Д., Волхонский В. В. Системы контроля и управления доступом. – СПб.: Экополис и культура, 2003. – 165 с.
2. Волхонский В.В. Штриховые коды. – СПб: Университет ИТМО, 2015. – 53 с.
3. Руководство по созданию комплексной унифицированной системы обеспечения безопасности музейных учреждений, защиты и сохранности музейных предметов/ А. В. Богданов, В. В. Волхонский, И. Г. Кузнецова и др. Ч. II. – СПб.: Инфо-да, 2014. – 264 с.
4. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. – Введ. 2008-12-17. – М.: Стандартинформ. – 34 с.
5. Петраков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита современного предприятия. – М.: – Энергоатомиздат. – 1999. – 568 с.
6. Петраков А. В. Защита и охрана личности, собственности, информации: Справ. пособие. – М.: Радио и связь. – 1997. – 318 с.

Содержание

УНИВЕРСИТЕТ ИТМО

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА ТВЕРДОТЕЛЬНОЙ ОПТОЭЛЕКТРОНИКИ

Кафедра входит в состав инженерно-физического факультета НИУ ИТМО и была организована в 1983 году в период выделения оптоэлектроники в самостоятельную область науки и производства. На кафедре работают высококвалифицированные специалисты, являющиеся ведущими экспертами в отраслях науки и техники. В состав кафедры входят шесть научно-учебных лабораторий, оснащенных современным оборудованием, позволяющим вести подготовку учащихся студентов на высоком современном уровне. Кафедра ведет подготовку бакалавров и магистров по направлениям «Техническая физика» и «Лазерная техника и лазерные технологии», а также аспирантов по специальности «Оптические и оптико-электронные приборы и комплексы».

Кафедрой руководит заслуженный деятель науки Российской Федерации, профессор, доктор технических наук Прокопенко Виктор Трофимович.

Волхонский Владимир Владимирович

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Учебное пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж экз.
Отпечатано на ризографе

Редакционно-издательский отдел

Университета ИТМО

197101, Санкт-Петербург, Кронверкский пр., 49