КАФЕДРА ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ СИСТЕМ

Тема 5. Технические решения и проектирование подсистем автоматического управления в ЭСБ различного функционального назначения (Часть 4)

Дисциплина:
«АВТОМАТИКА В ЭЛЕКТРОННЫХ СИСТЕМАХ БЕЗОПАСНОСТИ»

Технические решения системы автоматического пропуска людей и транспорта в СКУД: идентификаторы пользователя

Идентификатор пользователя **–** это предмет, в который (на который) с помощью специальной технологии занесена кодовая информация, подтверждающая полномочность прав его владельца, и служащий для управления доступом в охраняемую зону. Для идентификации применяются *атрибутные* и *биометрические идентификаторы*. В качестве ***атрибутных идентификаторов*** используют автономные носители признаков допуска: магнитные карточки, бесконтактные проксимити-карточки, ключи «тач-мемори», различные радиобрелки.

В качестве ***биометрических идентификаторов*** используют изображение радужной оболочки глаза, отпечаток пальца, отпечаток ладони, черты лица и другие физические признаки. Каждый идентификатор характеризуется определенным уникальным двоичным кодом. В СКУД каждому коду ставится в соответствие информация о правах и привилегиях владельца идентификатора.

В качестве идентификаторов применяются магнитные карточки, карточки Виганда, карточки со штриховым кодом (бар-кодом), карточки с искусственным интеллектом (смарт-карты), бесконтактные карточки (проксимити-карты), электронные ключи (тач-мемори) и др.

Идентификаторы (пропуска) пользователей СКУД могут иметь различный статус. Для обеспечения большинства необходимых в повседневной жизни требований, необходимо как минимум, чтобы контроллеры поддерживали следующие типы карточек:

- постоянная – для сотрудников предприятия;
- временная – с ограничением срока действия;
- n-разовая – автоматически аннулируемая после исчерпания определенного числа проходов;
- одноразовая – частный случай n-разовой карточки.

Магнитные карточки. Представляют собой карточку с магнитной полосой, на которой записан код. При желании код, записанный на дорожках магнитной полосы, может быть легко перепрограммирован, а при утере карточки можно быстро, дешево и без проблем закодировать новую карточку. Код с карточки считывается магнитным считывателем, принцип работы которого аналогичен считывателю обычного магнитофона: информация считывается при перемещении карточки между магнитными головками считывателя.

Карточки с магнитной полосой являются дешевыми, но не очень надежными, так как существует достаточно высокая вероятность их подделки. К их недостаткам можно также отнести наличие механического контакта при считывании с головками считывателя, что сокращает срок службы (средний срок службы 1 год), и необходимость бережного обращения, связанного с возможностью искажения или уничтожения записанной информации в относительно слабых магнитных полях и при температуре окружающего воздуха свыше 80 °С. Для повышения степени защищенности карточек, наряду с обычной информацией о владельце, может наноситься, например, специальный защитный код, описывающий структуру материала, из которого они изготовлены.

Карточки с магнитной барий-ферритовой прослойкой. В таких карточках магнитный слой является серединой «сэндвича» из несущей основы (с фотографией и личными данными владельца) и пластикового покрытия. Расположение в нем и полярность зарядов барий-ферритовых частиц образуют код. Достоинством таких карточек является самая низкая стоимость по сравнению со всеми другими видами карточек и повышенная защищенность от копирования. Однако они не обеспечивают надежной защиты от случайного или умышленного стирания или изменения встроенного кода. Кроме того, они недостаточно износоустойчивы. Область их применения ограничена теми сферами, где не требуется высокий уровень безопасности при контроле доступа.

Карточки Виганда. Карточки названы по имени ученого, открывшего магнитный сплав, обладающий прямоугольной петлей гистерезиса. В основу таких карточек встраиваются небольшие отрезки тонкой ферромагнитной проволоки, расположенные в строго определенной порядке, представляющем собой кодовую комбинацию, которая и содержат информацию о ее владельце. При вложении карточки в считыватель «проволочки Виганда» вызывают изменение магнитного потока, которое фиксируется соответствующим датчиком, преобразующим импульсы в двоичный код. Технология кодирования Виганда обеспечивает достаточно высокую степень защиты идентификационной карточки от случайного и умышленного стирания, фальсификации кода и изготовления дубликата.

Карточки со штриховым кодом (бар-кодом). На поверхность таких карточек наносятся полосы иного цвета, чем цвет остальной поверхности, ширина и расстояние между которыми представляют собой кодовую последовательность. Кодовая последовательность наносится на карточку при ее изготовлении (обычно она определяется генератором случайных чисел) и в дальнейшем не может быть изменена. Код считывается оптическим считывателем (инфракрасным или лазерным).

Карточки со скрытым штриховым кодом. В таких карточках невидимый штриховой код впечатывается в основу карточки и считывается с помощью излучения в инфракрасном спектре. Код образуется за счет конфигурации теней при прохождении ИК-излучения через карточку и обладает высокой степенью защищенности от подделки. Однако эта технология довольно дорого стоит, хотя стоимость таких карточек и ниже, чем стоимость карточек Виганда.

Карточки с оптической памятью. Кодирование информации на таких карточках осуществляется примерно так же, как при записи данных на оптические диски. Считывание производится лазером. Современная технология обеспечивает очень высокую плотность записи, поэтому емкость памяти таких карточек исчисляется мегабайтами. Это позволяет хранить не только буквенно-цифровые данные, но и изображения и звуковую информацию. Карточки такого типа имеют низкую стоимость и высокую степень защищенности от несанкционированного копирования. Однако высокая плотность хранения информации требует достаточно бережного отношения к карточкам и сложных считывающих терминалов.

Технические решения системы автоматического пропуска людей и транспорта в СКУД: турникеты, шлагбаумы и т.д.

Принцип действия всех турникетов примерно одинаков. Если карточка пользователя действительна, турникет разблокируется. Турникет проворачивается вручную (если нет встроенного двигателя), и пользователь, пройдя между створок, оказывается на охраняемой территории. Одновременно можно пройти только одному человеку и только в одном направлении.

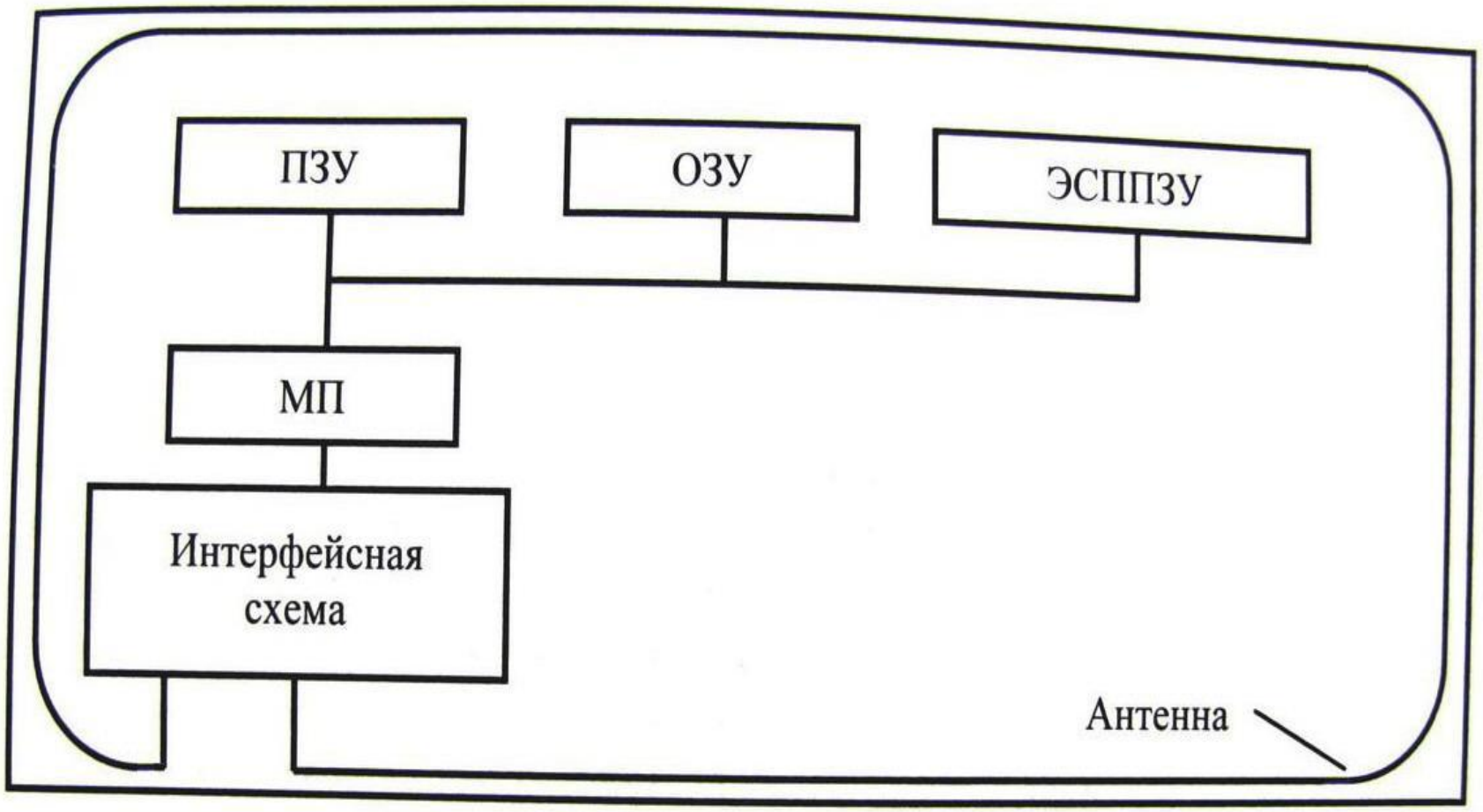
Голографические карточки. На поверхность таких карточек наносятся трехмерные голограммы, которые формируются на основе интерференции двух или нескольких когерентных волновых полей. Применение голограммы наряду с повышенной защитой документов от фальсификации обеспечивает высокую плотность записи информации. Повышенная защищенность карточки обусловлена тем, что техническая реализация методов голографии отличается достаточной сложностью и требует применения специальной аппаратуры.

Наносимые на документ с помощью голограммы данные могут представлять собой как отдельные буквенно-цифровые знаки, так и сложную комбинацию буквенно-цифровых, графических и фотографических символов.

При необходимости, голограммы могут применяться и для хранения биометрических данных (например, отпечатков пальцев). Для обеспечения надежной защиты от подделки или копирования идентификационных карточек может применяться еще и шифрование данных.

Голографические методы защиты информации на документах, наряду с высокой надежностью, обладают и рядом недостатков. К ним относятся, например, высокая сложность аппаратуры автоматизации процесса контроля, достаточно жесткие требования к сохранности документа.

Карточки с искусственным интеллектом (смарт-карты). Такие карточки содержат вмонтированные в основу миниатюрные интегральные микросхемы – запоминающие устройства и микропроцессор. Одним из преимуществ карточек такого типа является возможность регистрации значительного объема идентификационных данных. Они обладают достаточно высокой степенью защищенности записанной в них информации от фальсификации и различного рода злоупотреблений. В литературе встречаются и другие названия таких карточек – «разумные» или «интеллектуальные». Они могут быть контактные и бесконтактные .


ПЗУ
ОЗУ
ЭСППЗУ
МП
Интерфейсная схема
Антенна

Вычислительный микроблок такой карточки содержит три типа запоминающих устройств (ЗУ). Для хранения программного обеспечения предназначена память типа ПЗУ (постоянное ЗУ), в которую информация заносится фирмой-изготовителем на этапе выпуска карточки в обращение и которая не допускает внесения каких-либо изменений в хранящиеся инструкции. Для хранения промежуточных результатов вычислений и других данных временного характера применяется память типа ОЗУ (оперативное ЗУ). Она управляется встроенным микропроцессором (МП), который осуществляет контроль за процессом взаимодействия со считывателем. После отключения электрического питания информация здесь не сохраняется.

Память третьего типа ЭСППЗУ (электрически стираемое программируемое постоянное запоминающее устройство) предоставляется пользователю для записи персональной информации. Она также находится под управлением встроенного микропроцессора, то есть только по его команде в эту память могут вноситься какие-либо изменения. Записанная в этой памяти информация не стирается при отключении электрического питания. В памяти этого типа, как правило, выделены три зоны: открытого доступа, рабочая и секретная.

В ***открытой зоне*** может храниться, например, персональная информация пользователя (имя, адрес и т. п.), считывание которой допускается посторонним терминалом соответствующего типа. Однако какие-либо изменения в записях могут производиться только с разрешения пользователя и с помощью специальной аппаратуры.

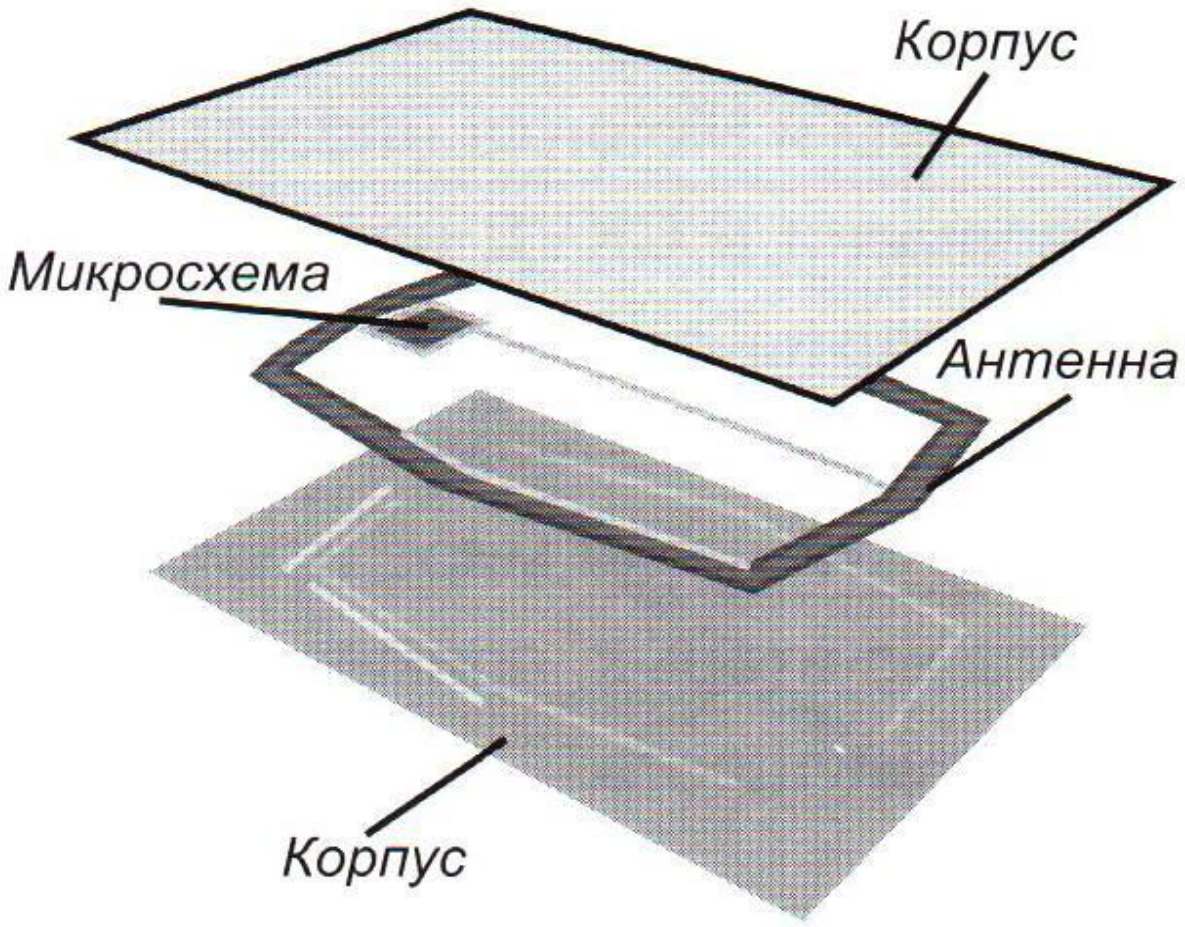
Рабочая зона предназначена для занесения специфической информации, изменение и считывание которой допускается только по команде пользователя и при наличии соответствующих технических средств.

В ***секретной зоне*** записывается идентифицирующая информация, например, личный номер или код-пароль. Кроме того, здесь же обычно хранятся временные и территориальные полномочия пользователя по доступу к охраняемым объектам и помещениям.

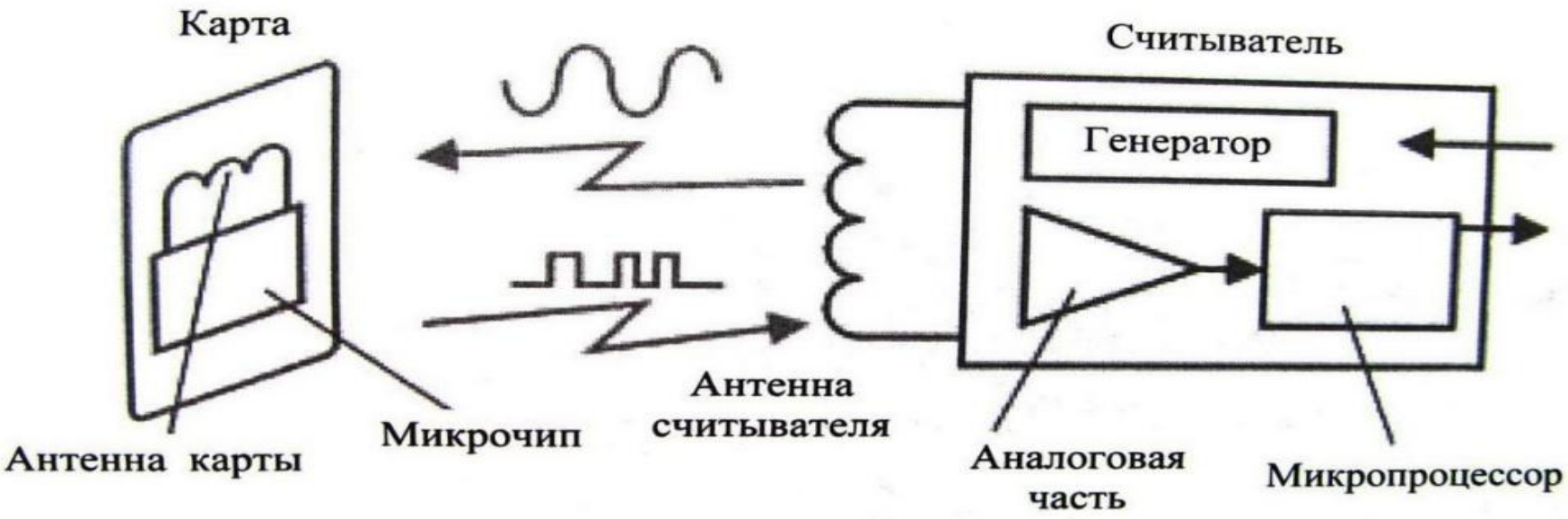
Некоторые интеллектуальные карточки позволяют хранить цифровые образы биометрических характеристик пользователя (динамику росписи, отпечатка пальца, ладони, геометрических параметров кисти, рисунка глазного дна, портретного изображения). В целях защиты от несанкционированного использования идентификационных карточек, применяемых пользователями таких систем, электронный «портрет» хранится в памяти в цифровом зашифрованном виде, что значительно затрудняет восстановление записанной информации и ее подделку злоумышленником.

Бесконтактные карточки (проксимити-карты).
Современные проксимити-идентификаторы представляют собой электронные пропуска в виде пластиковых карточек или брелков и широко используются в системах контроля доступа. Они обеспечивают бесконтактное дистанционное распознавание (идентификацию) персонального кода владельца электронными считывателями. В переводе на русский язык proximity (проксимити) означает «близость». Однако эта близость довольно условна, поскольку расстояние между проксимити-идентификатором и считывателем в зависимости от мощности считывателя и типа идентификатора может варьироваться от нескольких сантиметров до нескольких метров.

Типовая конструкция проксимити - карты



Считыватель генерирует электромагнитное излучение определенной частоты и при внесении карты в зону действия считывателя это излучение через встроенную в карте антенну запитывает микросхему карты. Получив необходимую энергию для работы, карта пересылает на считыватель свой идентификационный номер с помощью электромагнитного импульса определенной формы и частоты .



Бесконтактные карточки делятся на пассивные и активные. В **пассивных** карточках информация записывается один раз на все время действия карточки, а в **активных** существует возможность изменения информации в микросхеме.

Пассивные электронные метки. Работают на основе переизлучения электромагнитной энергии от микроволнового радиопередатчика терминала. Переизлученный сигнал принимается радиоприемником терминала, после чего подается соответствующая команда на механизм отпирания двери.

Полуактивные электронные метки. Содержат миниатюрную батарею, которая является источником электропитания для приемопередатчика. Сам приемопередатчик находится обычно в режиме ожидания и при попадании в зону действия микроволнового излучателя поста контроля выдает сигнал определенной частоты, принимаемый терминалом системы.

Активные электронные метки. Представляют собой микроволновый передатчик-радиомаяк, непрерывно передающий сигнал определенной частоты (для некоторых моделей – кодированный).

Электронные ключи (тач-мемори). Электронные ключи могут использоваться во всех рассмотренных выше способах кодирования. Их отличие заключается в конструктивном способе отпирания, внешне напоминающем способ отпирания обычного механического замка – вставление ключа в скважину, проверку доступа и индикацию владельцу ключа разрешения на открытие замка (поворот ключа).

Запись, добавление или стирание информации осуществляется мастер-ключом из контроллера. Считывание информации происходит при касании ключом считывателя. Принцип проверки основан на сравнении вводимого пользователем номера с номером, хранящимся в памяти ключа, который считывается терминалом при его вставлении в прорезь.

. В память ключа обычно заносится следующая информация:

- системный идентификационный номер (уникален для каждой системы и предоставляется фирмой-изготовителем при ее заказе);
- пользовательский идентификационный номер (определяется покупателем при выпуске и программировании ключа);
- уровни доступа;
- дни недели;
- временные зоны;
- параметры кодонаборной панели.

Кодонаборные устройства (кнопочные клавиатуры). Принцип действия кнопочных клавиатур достаточно прост: если набранный на клавиатуре код доступа верен, то проход на защищаемую территорию разрешен. Кодонаборные устройства могут совмещаются со считывателем карточек, в этом случае код служит для подтверждения факта санкционированного использования карты.

Клавиатуры СКУД можно считать «псевдобиометрическими» устройствами СКУД, так как носителем ПИН-кода является память человека.

Более широкие возможности предоставляют не кнопочные клавиатуры с нанесенными цифрами, а с сенсорным кодонаборным устройством. В этом случае для защиты от подсматривания вводимого ПИН-кода могут быть применены поляризационные фильтры, ограничивающие угол обзора, при котором можно различить отображаемые на клавиатуре цифры. Еще одним преимуществом подобных кодонаборных устройств является то, что отображаемые на клавиатуре цифры не привязаны к определенному местоположению (кнопке). Используя возможность перестановки цифр, можно добиться того, что при каждом использовании клавиатуры цифры будут располагаться в новом, случайном порядке. А если цифры будут загораться только при активации клавиатуры пользователем и гаснуть сразу после ввода.