Система ограничения доступа к банкомату

PERCo-S-800

Техническое описание

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ 2

1.1. Основные термины и определения 2

2. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ 4

3. НАЗНАЧЕНИЕ И СОСТАВ СИСТЕМЫ 4

3.1. Программное обеспечение 4

3.2. Контроллер управления доступом 5

3.3. Конфигуратор 7

4. ОПИСАНИЕ РАБОТЫ СИСТЕМЫ 7

4.1. Общие принципы работы 7

4.2. Работа с программным обеспечением 7

4.2.1. Алгоритм действий при работе с ПО 8

4.2.2. Редактирование прав пользователей 8

4.2.3. Задание параметров системы 9

4.3. Конфигурирование системы 10

4.4. Работа контроллера управления доступом 10

4.5. Работа контроллера конфигурации 12

1. ВВЕДЕНИЕ

Настоящее техническое описание предназначено для ознакомления с техническими характеристиками, составом и принципами работы системы ограничения доступа к банкомату **PERCo-S-800** (далее — системы) с целью обеспечения правильной ее эксплуатации и наиболее полного использования всех ее возможностей. Документ предназначен для технических специалистов, занимающихся монтажом и обслуживанием системы.

1.1. Основные термины и определения

- **Мастер-карта** — карта, позволяющая сбросить состояние "Тревога" контроллера управления доступом или попасть в зону самообслуживания банкомата при нахождении в ней клиента. Мастер-карта имеет особый номер, задаваемый при проведении конфигурации. Мастер-карта (карты) могут получены двумя способами:
  - В конфигурацию системы заносится номер какой-либо действующей кредитной карты, и в дальнейшем эта карта становится мастер-картой для данной системы,
  - Мастер-карты могут быть выпущены пользователем системы при помощи стандартного оборудования для выпуска кредитных карт путем записи в позиции номера карты кода, указанного в конфигурации системы.
- **Пароль для установления связи с контроллером конфигурации** — последовательность из четырех символов из набора "0123456789ABCDEF", служащая для установления взаимодействия между контроллером конфигурации и контроллером управления доступом или между программным обеспечением и контроллером конфигурации при передаче конфигурации. Связь устанавливается только в том случае, если во все компоненты системы введены одинаковые пароли.
- **Коды платежных систем, обслуживаемых данным банкоматом** — последовательность цифр, как правило в начале номера кредитной карты, характерная для данной платежной системы. При анализе предъявленной кредитной карты не учитываются те позиции ее номера, в которых при создании конфигурации системы при помощи ПО были оставлены знаки "_".
- **Код мастер-карты** — номер специальной магнитной карты, заносимый в контроллер управления доступом банкомата. Магнитная карта с таким номером имеет возможность сбрасывать состояние "Тревога (взлом)" контроллера управления доступом, а также имеет право доступа внутрь кабины банкомата в состоянии "Занято".
- **Разрешенная карта** — кредитная карта любой платежной системы, код которой занесен в конфигурацию контроллера управления доступом, срок действия которой не истек (только при включенной опции контроля срока действия карты).
- **Запрещенная карта** — кредитная карта, не принадлежащая ни к одной из платежных систем, коды которых занесены в конфигурацию контроллера управления доступом, или, при контроле срока действия карты, кредитная карта с истекшим сроком действия.
- **Время разблокировки замка** — время, на которое активизируется релейный выход управления замком. Может принимать значения: 0.2, 1, 2,... 64 с;
- **Предельно допустимое время нахождения двери в открытом состоянии** — время, в течение которого дверь может находиться в открытом состоянии. Может принимать значения: 1, 2, ... 64 секунды;

- **Предельное время нахождения клиента в кабине банкомата** — время, в течение которого клиент может находиться внутри кабины банкомата. Фиксируется по активизации датчика движения. Может принимать значения: 1, 2, … 20 мин;
- **Период опроса датчика нахождения клиента в кабине банкомата** — интервал опроса датчика движения. Величина этого параметра должна быть согласована с циклом работы датчика, фиксирующего наличие человека перед банкоматом. Может принимать значения: 1,2, … 250 секунды;
- **Текущая конфигурация системы** — описание следующих параметров контроллеров управления доступом:
  - пароля для установления связи с контроллером конфигурации, переносным компьютером;
  - кодов платежных систем, обслуживаемых данным банкоматом;
  - кода мастер-карты;
  - времени разблокировки замка;
  - предельно допустимого времени нахождения двери в открытом состоянии;
  - предельного времени нахождения клиента в кабине банкомата и длительности сигнала тревоги;
  - периода опроса датчика нахождения клиента в кабине банкомата;
  - нормального состояния внешних датчиков и кнопки "Выход" (нормально разомкнутые или нормально замкнутые контакты);
  - варианта сброса сигнала "Тревога" при взломе (по истечению времени и по предъявлению мастер-карты — что случится раньше, или только по предъявлению мастер-карты);
  - уровня сигнала, соответствующего зеленому свечению светодиода считывателя.

Примечание: По согласованию с потребителем система может поставляться с заранее оговоренными параметрами.

- **Параметры системы "по умолчанию"** — параметры текущей конфигурации, получаемые контроллером управления доступом при изготовлении.

Могут быть изменены при конфигурировании и восстановлены пользователем (см. «Инструкцию по монтажу»).

Имеют следующие значения:

Коды платежных систем, обслуживаемых данным банкоматом — разрешенной считается карта любой платежной системы, срок действия которой больше даты, считанной из календаря контроллера управления доступом

Код мастер-карты ..... не задан

Текущий пароль на доступ к контроллеру ..... **FFFF**

Время разблокировки замка ..... 4 секунды

Предельно допустимое время нахождения двери в открытом состоянии ..... 10 секунд

Предельное время нахождения клиента в кабине банкомата ..... 1 минута

Период опроса датчика нахождения клиента в кабине банкомата ..... 8 секунд

Нормальное состояние внешних датчиков и кнопки "Выход":

- охранные датчики, датчик двери ..... нормально замкнуты
- кнопка "Выход" ..... нормально разомкнута

Вариант сброса сигнала "Тревога" при взломе ..... по времени, 1 минута

Уровень сигнала, соответствующий зеленому свечению светодиода считывателя ..... равен 0

2. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Напряжение питания контроллера управления доступом, В ..... 12±1,2
Ток потребления контроллера управления доступом (при запитке исполнительных устройств от автономных источников питания), А, не более .. 0,2
Напряжение управления замком, В, не более 36
Ток управления замком при напряжении 12 В, А, не более 3
Напряжение питания контроллера конфигурации, В ..... 1,5…3
Ток потребления контроллера конфигурации, А, не более 0,1
Длина кода платежной системы, десятичных цифр, не более 16
Количество вариантов платежных систем, не более 10
Количество контроллеров управления доступом в системе ..... не ограничено

Минимальные системные требования:

- ОС: MS Windows 95, 98, NT 4.0, 2000;
- Процессор: Intel Pentium 166 и выше;
- ОЗУ: 32 Мб;
- Монитор: 800*600;
- COM-порт.

3. НАЗНАЧЕНИЕ И СОСТАВ СИСТЕМЫ

Система ограничения доступа к банкомату предназначена для предотвращения доступа к банкомату лиц, у которых отсутствует карта любой платежной системы из числа обслуживаемых данным банкоматом или лиц, имеющих кредитную карту с истекшим сроком действия.

- Основным элементом системы ограничения доступа к банкомату является контроллер управления доступом.

Контроллер управления доступом **PERCo-SC-800** — полнофункциональный контроллер, не только обеспечивающий доступ клиента в зону самообслуживания банкомата, но и осуществляющий слежение за шлейфом охранной сигнализации и датчиком наличия клиента в зоне самообслуживания банкомата. Кроме этого, контроллер PERCo-SC-800 имеет выходы для управления замком, индикатором "Занято / Свободно", сигнализатором тревоги и устройством включения видеомагнитофона в режим записи в реальном масштабе времени.

В состав системы может входить любое число контроллеров управления доступом. Другими составными частями системы ограничения доступа к банкомату являются:

- программное обеспечение системы;
- конфигуратор, в качестве которого может выступать переносной компьютер с установленным программным обеспечением или контроллер конфигурации (по желанию потребителя).

3.1. Программное обеспечение

Программное обеспечение состоит из одного модуля, выполняющего следующие функции:

- администрирование прав доступа операторов программного обеспечения;
- настройку параметров конфигурации системы;

- сохранение и восстановление текущей конфигурации контроллера управления доступом;
- обеспечение связи между программным обеспечением и контроллером конфигурации;
- обеспечение связи между программным обеспечением и контроллером управления доступом.

3.2. Контроллер управления доступом

Как уже было сказано, контроллер управления доступом — основной аппаратный элемент системы. Контроллер управления доступом представляет собой микропроцессорное устройство, выполняющее следующие функции:

- анализ состояния внешних датчиков;
- управление работой считывателя карт с магнитной полосой;
- анализ статуса предъявленной карты;
- принятие решения об активизации того или другого исполнительного устройства в зависимости от статуса предъявленной карты и от состояния внешних датчиков;
- установление связи с конфигуратором для изменения текущей конфигурации.

Конструктивно контроллер управления доступом заключен в малогабаритный пластмассовый корпус размером 83x127x22 мм, под декоративной крышкой которого расположены клеммы для подключения источника питания, считывателя, внешних датчиков и исполнительных устройств, а также розетка для подключения конфигуратора.

В верхней части корпуса контроллера расположены клеммы для подключения считывателя магнитных карт и внешних датчиков.

Для подключения считывателя магнитных карт служат клеммы "+5 В", "GND", "RDT", "/RCL", "LED" и "Buzz". При этом:

- клеммы "+5 В" и "GND" предназначены для подачи питания на считыватель;
- клеммы "RDT" и "/RCL" предназначены для подключения линий данных и синхросигналов считывателя соответственно;
- клеммы "LED" и "Buzz" предназначены для подключения светового индикатора считывателя. При этом при использовании считывателя с управлением индикаторным светодиодом по одной линии применяется одна из клемм "LED" или "Buzz", а при использовании считывателя с управлением индикаторным светодиодом по двум линиям применяются обе клеммы, "LED" и "Buzz".

Клеммы для подключения внешних датчиков имеют внутреннюю запитку и рассчитаны на подключение датчиков с выходом типа "сухой контакт".

Для удобства монтажа каждой клемме для подключения внешних датчиков соответствует клемма "GND".

При подключении внешних датчиков следует соблюдать следующие правила:

- кнопка "Выход" подключается между клеммами "Butt" и "GND";
- датчик открытия двери подключается между клеммами "Door" и "GND";
- датчик движения (наличия клиента в кабине банкомата) подключается между клеммами "Vol1" и "GND";
- датчики охранного контура (при их наличии) подключаются между клеммами "Vol2" и "GND" ;
- при наличии в считывателе датчика несанкционированного вскрытия он включается между контактами "Tm-1" и "Tm-2", в противном случае они должны быть замкнуты между собой при помощи перемычки.

Датчиком движения (датчиком наличия клиента в кабине банкомата) для контроллера управления доступом PERCo-SC-800 может служить любой датчик (объёмный, датчик движения и т.п.), фиксирующий присутствие человека непосредственно перед банкоматом.

Датчиками охранного контура для контроллера управления доступом PERCo-SC-800 могут быть любые датчики, фиксирующие наличие в кабине (а не только перед банкоматом) человека или датчики, фиксирующие нарушение целостности кабины.

Если датчиков охранного контура несколько, то соединять их следует в зависимости от нормального состояния контактов:

- нормально замкнутые контакты — соединение последовательное;
- нормально разомкнутые контакты — соединение параллельное.

Клеммы "EL+" и "EL–" предназначены для удобства подключения переключателя перевода контроллера в "дневной" режим в случае использовании нормально разомкнутой кнопки "Выход" и также имеют внутренную запитку. Подробно использование клемм "EL+" и "EL–" описано а подразделе 4.4 настоящего технического описания.

В нижней части корпуса контроллера расположены клеммы для подключения источника питания, исполнительных устройств и калибровочного светодиода.

Для подключения источника питания +12 В служат клеммы "+12 В" и "GND".

Управление исполнительными устройствами осуществляется при помощи реле, для чего на клеммную колодку выведены как нормально замкнутые, так и нормально разомкнутые контакты реле. Контакты всех реле разделены на четыре группы — в соответствии с числом исполнительных устройств, которые могут подключаться к контроллеру.

Для удобства запитки исполнительных устройств от источника питания контроллера здесь же имеются клеммы "+12 В" и "GND", которые можно замыкать с соответствующими контактами реле для обеспечения желаемого коммутирования питания на исполнительные устройства.

Клемма для подключения калибровочного светодиода "LEDK" предназначена для подключения анода светодиода на время настройки зон чувствительности как датчика присутствия человека в кабине банкомата, так и датчиков охранного контура. Катод светодиода при этом необходимо подключить к клемме "GND". В этом случае калибровочный светодиод включается параллельно красной секции индикаторного светодиода контроллера управления доступом и будет светиться при срабатывании датчика присутствия человека в кабине банкомата или датчиков охранного контура.

Клемма "LEDA" является технологической.

Розетка для подключения конфигуратора расположена на левой боковой поверхности корпуса контроллера управления доступом. Во время конфигурирования контроллера управления доступом к этой розетке при помощи специального кабеля подключается конфигуратор (см. также раздел 3 и подраздел 3.3).

Установка текущей даты и времени в контроллере управления доступом производится путем передачи их в файле конфигурации. Следовательно, перед записью файла конфигурации непосредственно в контроллер управления доступом или в контроллер конфигурации, на компьютере с установленным программным обеспечением должны быть установлены действительные дата и время.

3.3. Конфигуратор

В качестве конфигуратора может выступать один из компонентов системы:
- переносной компьютер с установленным программным обеспечением;
- контроллер конфигурации.

Контроллер конфигурации — вспомогательный элемент системы.

С помощью контроллера конфигурации может быть изменена текущая конфигурация каждого контроллера управления доступом из числа входящих в состав данной системы. В ходе работы контроллер конфигурации обменивается информацией с контроллером управления доступом или с компьютером по интерфейсу типа RS-232. Конструктивно контроллер конфигурации выполнен в виде переносного устройства, на лицевой панели которого находится кнопка для инициирования процесса передачи конфигурации в контроллер управления доступом и два индикаторных светодиода, а на боковых стенках — кнопка включения / выключения питания и гнездо для подключения кабеля для связи по интерфейсу типа RS-232.

4. ОПИСАНИЕ РАБОТЫ СИСТЕМЫ

4.1. Общие принципы работы

Основная задача системы — задача ограничения доступа к банкомату решается контроллером управления доступом. Каждый контроллер управления доступом работает совершенно автономно. В том случае, если по каким-либо причинам потребителя не устраивают параметры контроллера управления доступом, принимаемые по умолчанию, необходимо провести конфигурирование контроллера управления доступом. Процесс подготовки конфигурации и ее передачи в контроллер управления доступом более подробно описан в подразделе 4.3.

4.2. Работа с программным обеспечением

Для инсталляция ПО "Конфигуратор системы ограничения доступа к банкомату" (в дальнейшем — ПО) необходимо запустить файл setup.exe и действовать в соответствии с инструкциями, получаемыми в процессе диалога.

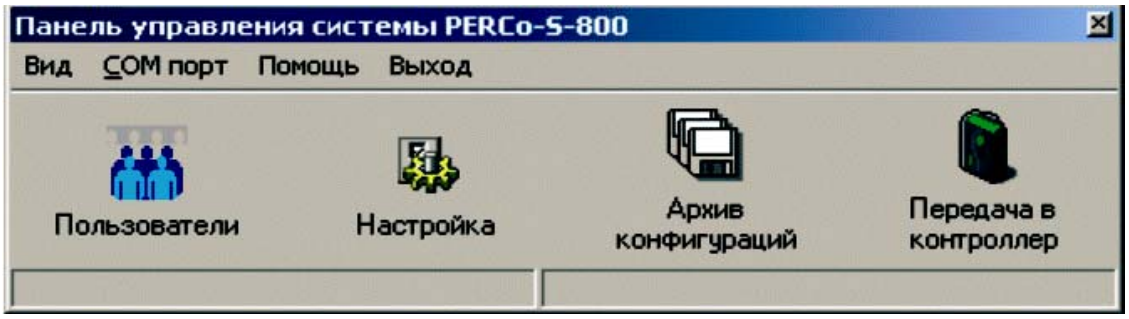
Для входа в ПО необходимо ввести "Имя пользователя" и "Пароль", которые должны быть заданы администратором системы.

При первом запуске ПО на компьютере, имена пользователей и пароли по умолчанию следующие:

user SUPERVISOR; password: <пусто>
user GUEST; password: <пусто>

Не забудьте при первом запуске ПО задать пользователей для работы в системе, задать их права доступа и пароли (форма "Пользователи"). Как только в системе будут введены пользователи, доступ по именам пользователей и паролями по умолчанию работать не будет.

После входа в ПО появляется окно следующего вида:



4.2.1. Алгоритм действий при работе с ПО

1. При первом запуске ПО ввести пользователей, которые будут работать в системе, задать им права доступа и пароли (форма "Пользователи"). Для изменения параметров нажать мышкой на кнопку "Пользователи".
2. Задать параметры системы: параметры контроллера, платежных систем, разрешаемых к допуску, мастер-карты (форма "Настройка"). Для изменения параметров нажать мышкой на кнопку "Настройка".
3. При необходимости сохранить / восстановить конфигурацию на диск. Нажать мышкой на кнопку "Архив конфигураций".
4. Передать информацию в контроллер конфигурации либо непосредственно в контроллер ограничения доступа к банкомату, кнопка: "Передача в контроллер".

4.2.2. Редактирование прав пользователей

В форме "Пользователи" Вы можете добавлять в систему новых пользователей, удалять текущих и изменять их права доступа.

Целесообразно предоставить права доступа пользователям по всем возможным действиям в программе.

При первом запуске программы необходимо задать хотя бы одного пользователя с правами администратора, чтобы иметь доступ к программе, в противном случае доступа не будет.

В левой части формы находится таблица с текущими пользователями, а в правой — описания прав пользователя, выбранного в таблице: имя пользователя, пароль и его права доступа.

4.2.2.1. Добавление пользователя

- Нажмите на кнопку  ;
- В поле для редактирования "Пользователь" введите имя пользователя;
- Задайте права для работы данного пользователя;
- Для сохранения результатов редактирования нажмите на кнопку  ;
- Для отмены нажмите на кнопку  , либо нажмите на клавишу "Esc".

4.2.2.2. Удаление пользователя

- Выберите пользователя, которого Вы хотите удалить;
- Нажмите на кнопку  ;
- Подтвердите удаление пользователя.

4.2.2.3. Редактирование свойств пользователей

- Выберите пользователя, свойства которого Вы хотите изменить;
- Нажмите на кнопку  ;
- Задайте права для работы данного пользователя (аналогично добавлению пользователя);
- Для сохранения результатов редактирования нажмите на кнопку  ;
- Для отмены нажмите на кнопку  .

ВНИМАНИЕ! Не забудьте при первом запуске ПО задать пользователей для работы в системе, задать им права доступа и пароли. Как только в системе будут введены пользователи, доступ по именам пользователей и паролями по умолчанию работать не будет.

4.2.3. Задание параметров системы

При нажатии на кнопку "Настройка" появляется возможность изменять данные в двух формах:

- "Параметры контроллера";
- "Платежные системы + Мастер-карта".

4.2.3.1. Конфигурация параметров контроллера

ВНИМАНИЕ! При получении контроллера в нем предустановлен пароль доступа — **FFFF**.

В данной форме Вы можете изменять параметры контроллеров Системы ограничения доступа к банкомату.

Для изменения паролей на доступ к контроллеру введите новые пароли в нужные поля для редактирования. Символы могут быть следующими: "1234567890ABCDEF" (если включена опция "Скрыть пароли", то вводимые символы в окне будут заменяться символами "*"). При конфигурации контроллера проверяется текущий пароль, и если он не совпадает, конфигурация контроллера не происходит. Если введен "Новый пароль", то он заменит старый при последующей передаче в контроллеры.

Вы можете заменить как текущий пароль, так и новый пароль.

После ввода паролей появится окно для ввода подтверждения.

В него Вы должны ввести тот же пароль.

Для подтверждения изменения паролей нажмите на кнопку "Применить". Пароли будут изменены только в том случае, если совпадут с подтверждением, в противном случае необходимо ввести их заново.

Текущий пароль на доступ к контроллеру при первом подключении должен быть установлен равным **FFFF.**

Также в этом окне требуется ввести следующие параметры системы:

- время разблокировки замка при входе и выходе клиента;
- предельно допустимое время нахождения двери в открытом состоянии;
- нормальные состояния контактов;
- максимальное время присутствия клиента в кабине и длительность сигнала тревоги;
- время опроса датчика присутствия клиента в кабине;
- параметры сброса тревоги;
- возможность контроля срока действия карты.

Для сохранения результатов редактирования нажмите на кнопку "Применить".

Для отмены и выхода из формы нажмите на кнопку "Сбросить".

4.2.3.2. Платежные системы и мастер-карта

В данной форме Вы можете изменять список, содержащий коды платежных систем, обслуживаемых банкоматами, входящими в систему ограничения доступа.

Задайте нужное количество платежных систем, для этого введите цифры, которые будут контролироваться системой, в соответствующие ячейки для каждой из платежных систем, перемещение осуществляется с помощью клавиш управления курсором →, ← и т.д. Символ "_" обозначает, что данный символ проверяться не будет.

Параметры мастер-карты (если это требуется), задаются тем же способом, как и параметры платежных систем, за исключением того, что номер мастер карты не должен содержать символы "_". Т.е. задается только реальный номер магнитной карты, которая будет являтся для системы мастер-картой.

Для сохранения результатов редактирования нажмите на кнопку "Применить".

Для отмены и выхода из формы нажмите на кнопку "Сбросить".

4.3. Конфигурирование системы

Конфигурирование контроллера управления доступом может проводиться двумя способами:

- при помощи переносного компьютера с установленным программным обеспечением;
- при помощи специального контроллера конфигурации.

При проведении конфигурирования при помощи переносного компьютера с установленным программным обеспечением необходимо, после настройки параметров системы, передать эту информацию в контроллер управления доступом, нажав на кнопку "Передача в контроллер". Процесс передачи контролируется по сообщениям программного обеспечения.

При проведении конфигурирования с помощью контроллера конфигурации, в него необходимо записать информацию о конфигурации системы. Для этого нажмите мышью на кнопку "Передача в контроллер". После того, как информация о конфигурации системы будет занесена в контроллер, конфигурацию можно последовательно передавать во все контроллеры управления доступом, по очереди подключая к ним контроллер конфигурации.

Более подробно процедура передачи конфигурации описана в пп. 4.2 и 4.5.

При изменении пароля в контролер посылается файл конфигурации, содержащий как новый пароль, так и старый, после чего контроллер меняет старый пароль на новый, и получить доступ к нему можно, только зная новый пароль (ставший текущим) для данного контроллера.

При отправке файла конфигурации в контроллер ПО проверяет, были ли изменены пароли и в случае изменения запрашивает у пользователя, требуется ли изменить текущий пароль на новый в самом ПО. Если текущий пароль будет заменён на новый, то при следующей передаче файл конфигурации будет содержать только новый пароль.

Во избежании проблем рекомендуется после каждого изменения конфигурации компьютера, сохранять конфигурацию на диск (кнопка "Архив конфигураций").

4.4. Работа контроллера управления доступом

Контроллер управления доступом реализует основную функцию системы — ограничивает доступ в зону самообслуживания банкомата.

Решение о разрешении или запрещении прохода в кабину банкомата контроллер управления доступом принимает на основании сравнения кода платежной системы предъявленной карты со списком разрешенных платежных систем, а также сравнения текущей даты с датой окончания срока действия предъявленной карты (при включенной опции контроля срока действия карты).

Проход в кабину банкомата разрешается только в том случае, если предъявленная карта принадлежит к платежным системам, обслуживаемым данным банкоматом, и срок ее действия не истек. Система перед этим должна находиться в состоянии "Свободно", о чем будет свидетельствовать смена цветов свечения индикатора считывателя с частотой около 0,5 Гц, а также активизация релейного выхода для подключения сигнального табло "Свободно".

При предъявлении разрешенной карты контроллер управления доступом разблокирует замок до момента открытия двери, фиксируемого по срабатыванию датчика двери, либо на время разблокировки замка. Индикатор считывателя при этом перестает мигать и начинает светиться непрерывным зеленым светом до открывания двери или до тех пор, пока не истечет время разблокировки замка.

После открытия двери индикатор считывателя загорается красным светом и контроллер управления доступом выдает управляющий сигнал на включение видеомагнитофона (релейный выход). Этот сигнал, а также красное свечение индикатора считывателя удерживается до возвращения в состояние "Свободно" после выхода клиента.

Время нахождения двери в открытом состоянии контролируется, и при превышении предельного времени нахождения двери в открытом состоянии выдается сигнал "Тревога", который удерживается до закрытия двери.

После закрытия двери контроллер управления доступом в течение периода опроса датчика движения анализирует его состояние и переходит в один из режимов "Занято" или "Свободно" (пока решение не принято — индикатор считывателя светится красным светом, а доступ в зону банкомата извне запрещен, то есть контроллер управления доступом находится в состоянии "Занято").

В режиме "Занято" доступ извне в кабину банкомата по кредитным картам невозможен (исключение делается только для Мастер-карты). Для выхода из кабины банкомата служит кнопка "Выход". При нажатии на эту кнопку контроллер управления доступом открывает замок, позволяя клиенту выйти из кабины.

В контроллере управления доступом предусмотрена возможность перевода его в так называемый "дневной" режим, т.е. в режим постоянной разблокировки замка. Для перехода в "дневной" режим необходимо перевести в активное состояние кнопку "Выход" на время, большее, чем 6 с. Для этого переключатель, переводящий контроллер в "дневной" режим подключается параллельно кнопке "Выход" (при использовании нормально разомкнутой кнопки) или последовательно с кнопкой "Выход" (при использовании нормально замкнутой кнопки). Для удобства параллельного подключения на клеммной колодке имеются контакты "EL+" и "EL–", дублирующих собой контакты "Butt" и "GND" соответственно. При использовании нормально замкнутой кнопки "Выход" контакты "EL+" и "EL–" не используются. Выход из "дневного" режима происходит сразу после перехода в пассивное состояние кнопки "Выход".

В "дневном" режиме, независимо от состояния датчиков, сигнал "Свободно/Занято" индицирует режим "Свободно", а индикатор считывателя светится непрерывным зеленым светом. Встроенный индикатор контроллера управления доступом светится желтым светом, на замок подается разблокирующий сигнал, сигналы "Тревога" и управления видеомагнитофоном пассивны. Переход в "дневной" режим невозможен при действующем сигнале "Тревога" (взлом)".

Примечание: При использовании электромеханических замков, открывающихся при подаче на них импульса управляющего напряжения длительностью до 0,2 секунды, работа в дневном режиме невозможна.

Время нахождения клиента в зоне самообслуживания контролируется, и при превышении времени нахождения клиента в кабине банкомата активизируется сигнал "Тревога". В этом случае система может перейти в режим "Свободно", если в течение периода опроса датчика нахождения клиента в кабине банкомата он будет пассивен. Светодиод считывателя в этом режиме светится красным светом.

Предъявление запрещенной карты в любом режиме индицируется миганием индикатора считывателя с частотой около 5 Гц в течение 1 секунды. Предъявление разрешенной карты в режиме "Занято" так же вызывает мигание индикатора считывателя и кратковременное переключение сигнала "Занято / Свободно" (для привлечения внимания клиента к световому табло "Занято").

В режиме "Свободно" при активизации охранных датчиков, так же, как и при открытии двери без предварительной выдачи команды на разблокировку замка, выдается сигнал "Тревога" (взлом). В этом случае сигнал "Тревога" удерживается либо до предъявления Мастер-карты, либо до предъявления Мастер-карты или в течение предельного времени нахождения клиента в кабине банкомата (вариант действия задается при конфигурировании контроллера управления доступом). Активизация одного или обоих охранных датчиков в любом режиме вызывает свечение встроенного индикатора контроллера управления доступом красным светом.

Сигнал "Тревога" активизируется на 0,5 секунды и при получении контроллером управления доступом кадра конфигурации.

Состояние параметров конфигурации контроллера управления доступом индицируется при помощи индикаторного светодиода считывателя. Если контроллер управления доступом работает с параметрами "по умолчанию", то при включении питания и до перехода в режим ожидания индикатор считывателя будет мигать с частотой около 5 Гц в течение 2 секунд. Если же в контроллере управления доступом есть конфигурация, отличная от конфигурации "по умолчанию", то при включении питания индикаторный светодиод считывателя сразу начинает мигать с частотой около 0,5 Гц.

4.5. Работа контроллера конфигурации

Контроллер конфигурации предназначен для занесения текущей конфигурации в контроллеры управления доступом.

При включении питания контроллера конфигурации его состояние отображается при помощи зеленого и красного индикаторных светодиодов. При этом постоянное горение зеленого светодиода означает готовность его к работе (есть конфигурация в памяти контроллера конфигурации), постоянное свечение красного светодиода означает отсутствие конфигурации в памяти контроллера конфигурации или неисправность часов реального времени, а мигание красного светодиода — разряд элементов питания. Следовательно, если после включения питания загорелся красный светодиод, необходимо передать конфигурацию из компьютера в контроллер конфигурации. Если передача конфигурации системы не приводит к зажиганию зеленого светодиода, контроллер конфигурации подлежит ремонту. Если красный светодиод мигает, необходимо заменить элементы питания контроллера конфигурации.

Конфигурацию в контроллер управления доступом можно передавать только в том случае, если светится зеленый индикаторный светодиод. Для передачи конфигурации в контроллер управления доступом надо нажать кнопку инициирования процесса передачи конфигурации. После начала передачи конфигурации загораются оба индикаторных светодиода. Если процесс передачи конфигурации прошел успешно, гаснет красный светодиод, а зеленый мигает 3 раза и зажигается постоянно. Если во время передачи конфигурации были зафиксированы ошибки (ошибки при передаче, несовпадение паролей), 3 раза мигнет и погаснет красный светодиод.