

Принцип работы карт HID

Давайте ознакомимся с тем, как работает карта HID, и что нужно для того, чтобы данные с карты дошли до контроллера и открыли дверь. Эта информация применима как к картам Proximity 125 кГц, так и к продукции iClass 13,56 мГц.

Любая система контроля карт доступа состоит из 4-х простых элементов. В зависимости от размера и того, где и как будет использоваться система, могут выделяться многие другие дополнительные виды устройств, но эти 4 являются основными.

1. карты;
2. считыватели (возможно, оснащённые кейпадами);
3. панель контроля доступа (контроллеры);
4. терминал или компьютер-хост.

Карта

Каждая карта доступа содержит в себе бинарные числа (единицы и нули), которые используются для идентификации владельца карты. HID производит карты, которые могут совмещать в себе следующие типы данных:

- Магнитные полосы (ленты);
- [Wiegand](#);
- [Prox 125 кГц](#);
- бесконтактные [смарт-карты Mifare](#);
- [iClass 13,56 мГц](#) бесконтактные смарт-карты.

Нужно отметить, что HID производит много карт, которые являются комбинацией двух и более технологий. Самая известная комбинация — 13,56 мГц IClass / 125 кГц Prox / магнитные ленты.

В зависимости от используемой технологии, данные шифруются и передаются с карты на считыватель по-разному. Впрочем, независимо от формата, данные на карте — это набор бинарных чисел определенной конфигурации и размера.

В большинстве случаев, данные карты содержат лишь информацию о формате, который, в последствии, будет передан на контроллер.

В крайне редких случаях карта содержит дополнительный код, который является как бы указателем для той или иной группы считывателей. Этот id-код будет удален считывателем, и только информация о формате будет послана на контроллер.

Считыватель

Компания HID производит [считыватели](#), которые совместимы с каждым из пяти вышеперечисленных типов карт. Каждый считыватель может «понимать» только

<http://www.hid.su> – системы контроля доступа (СКД, СКУД), бесконтактные карты, считыватели и программное обеспечение.

тот тип карт, с которым он совместим, так как все технологии являются уникальными.

Важно отметить, что каждый вид считывателя использует свою собственную технологию для считывания данных с карты. Все считыватели способны конвертировать данные в формат Wiegand для дальнейшей их передачи на контроллер (некоторые считыватели могут также общаться с контроллером посредством технологий RS 232 или Clock&Data).

Все стандартные считыватели, использующие описанную технологию, просто конвертируют бинарные данные карты в формат Wiegand и посылают его без изменений на контроллер.

Некоторые специально изготовленные считыватели получают id-код с соответствующих карт, затем удаляют его и посылают на контроллер только оставшиеся бинарные данные.

Сам считыватель не знает ни о формате данных карт, ни о возможных особых привилегиях владельца карты. Данная информация находится только на контроллере и возможно на компьютере-хосте.

Панель контроля доступа (контроллер)

Когда [контроллер](#) получает данные со считывателя, специальная программа решает — позволить доступ или нет.

Обычно процесс принятия решения состоит из следующих стадий.

Совпадает ли длина формата данных с контроллером? Некоторые контроллеры приспособлены принимать только данные с определенной длиной (например, 34 бита). Если данные не совпадают с «ожиданиями» контроллера, то он просто проигнорирует их полностью. Некоторые контроллеры могут иметь специальный запрет доступа для не соответствующих форматов.

Как соотносится структура формата с контроллером? Если длина формата принята, то контроллер разбивает бинарную цепочку на несколько компонентов. Это могут быть:

- фасилити-код;
- код сетевого узла;
- номер карты.

Соответствующий ли фасилити-код? Контроллер проверит данные, чтобы убедиться, что фасилити-код совпадает с кодом запрограммированным в сам контроллер. Некоторые контроллеры поддерживают несколько различных фасилити-кодов.

Если фасилити-код не совпадает, то в доступе будет отказно и будет сгенерировано сообщение в логе.

<http://www.hid.su> – системы контроля доступа (СКД, СКУД), бесконтактные карты, считыватели и программное обеспечение.

Совпадает ли код узла? Если формат содержит код узла или иной идентификатор, то с ним будет проведена аналогичная с фасилити-кодом операция.

Находится ли номер карты в нужном пределе? Если нет, то в доступе будет отказано и сгенерировано сообщение в логе.

Есть ли в памяти номер карты? Если да, то процесс идентификации продолжится, в противном случае в логе появится сообщение “card not in memoгу”.

Является ли эта карта действительной в настоящее время? Если да, то доступ будет получен и замок сработает. Если нет, то в логе появится сообщение с причиной отказа.

Контроллеры — это единственное устройство в системе контроля доступа, в котором бинарные данные карты могут быть расшифрованы или преобразованы.

Разные бренды контроллеров по-разному реагируют на неправильные форматы данных карты. Некоторые из них ведут разные логи в зависимости от вида ошибок. Простые контроллеры могут вести только один общий лог, а некоторые модели могут вообще полностью проигнорировать несовместимый формат, никак на него не отреагировав.

Вы должны четко представлять возможности контроллера для более полного устранения всех возможных ошибок связанных с картами и считывателями.

Терминал

Каждая система контроля доступа должна иметь некоторую форму пульта управления или пользовательского терминала, то есть места, где оператор или администратор мог бы:

- добавлять или удалять держателей карт;
- давать, изменять или удалять привилегии доступа;
- создавать, изменять расписания, списки выходных и т. д.;
- конфигурировать оборудования для дверей, точек сигнализации;
- наблюдать за системой в реальном времени;
- вести отчет системных ресурсов.

Только в крайне редких случаях, в огромных, комплексных системах хост может принимать решение о контроле доступа. В 99,9% существующих систем за данную операцию отвечает контроллер.

Подводя итог, скажем — работа с картами HID удобна и доступна. При правильной эксплуатации и понимании их принципов работы, вы получите надежный инструмент безопасности инфраструктуры.

<http://www.hid.su> – системы контроля доступа (СКД, СКУД), бесконтактные карты, считыватели и программное обеспечение.