Руководство программиста UEM SKD Lock

ВНИМАНИЕ! Прежде, чем подключить замок, внимательно ознакомьтесь с настоящим документом.

Оглавление

1 Введение

Настоящий документ является руководством по интеграции для разработчиков программного обеспечения Систем Контроля и Управления Доступом (СКУД). Он описывает особенности реализации протокола **OSDP v2.2** в электромагнитном замке **UEM OSDP Lock**, выступающем в роли Ведомого Устройства (Peripheral Device, PD).

Цель документа — предоставить инженеру ПО контроллера СКУД (Control Panel, CP) всю необходимую информацию для корректного управления замком, опроса его состояния и обработки событий в рамках стандартного протокола OSDP. Документ предполагает, что разработчик знаком со спецификацией OSDP (IEC 60839-11-5) и основами работы с интерфейсом RS-485.

1.1 Назначение устройства в системе

Замок **UEM OSDP Lock** функционирует как интеллектуальный исполнительный механизм в распределённой системе СКУД. Помимо базовой функции дистанционного управления (блокировка/разблокировка), устройство предоставляет контроллеру следующие возможности:

- Контроль положения двери через встроенный датчик «закрыто/открыто».
- Контроль состояния внешних датчиков и устройств (Кнопка, Датчик двери, Пожарный сигнал).
- Управление встроенными световыми (LED) и звуковыми (Зуммер) индикаторами для обратной связи с пользователем.
- Передача событий в реальном времени по защищённому каналу связи.

Для взаимодействия используется **только протокол OSDP**. Устаревшие интерфейсы (типа Wiegand) и проприетарные протоколы не поддерживаются.

Важное отличие: Устройство не содержит встроенного считывателя карт или иных устройств идентификации. Его основная задача — выполнение команд управления от контроллера (CP) и предоставление актуального статуса входов \выходов.

2 Работа с устройством

Устройство **UEM OSDP Lock** поддерживает два режима работы по протоколу OSDP:

- **Обычный режим** — обмен данными происходит в открытом виде (без шифрования).
- **Защищённый режим (Secure Channel)** — весь трафик шифруется с использованием AES-128.

2.1 Инициализация и базовое взаимодействие

Взаимодействие с устройством следует стандартной логике OSDP:

1. Контроллер (CP) периодически отправляет команду *POLL*.
2. Устройство (PD) отвечает *ACK* и ожидает команд. В случае ошибки или невозможности выполнить команду PD отвечает *NAK*.
3. При необходимости, CP выполняет установку защищённого канала (процедура описана в разделе **Использование защищённого режима**).

После установки соединения CP может использовать реализованный набор команд OSDP для управления устройством.

2.2 Поддерживаемые команды OSDP

Устройство реализует следующий набор команд OSDP:

- *COMSET* — настройка параметров связи (скорость, адресация).
- *KEYSET* — установка мастер-ключа для защищённого режима.
- *ISTAT* — запрос состояния входов.
- *OSTAT* — запрос состояния выходов.
- *OUT* — управление выходами (используется для непосредственного управления электромагнитом замка).
- *LED* — управление световой индикацией.
- *BUZ* — управление звуковым сигналом.

Примечание: для запросов статуса и управления устройство использует стандартные структуры данных OSDP. При попытке выполнить неподдерживаемую команду или команду с некорректными данными будет возвращён ответ *NAK*.

2.3 Оповещения об изменении состояния

Устройство активно уведомляет контроллер об изменениях своего состояния:

- При изменении статуса любого входа (например, срабатывание датчика двери) устройство автоматически отвечает соответствующим сообщением на следующую команду *POLL*.
- Аналогично обрабатываются изменения в состоянии выходов.

3 Описание входов/выходов

Устройство предоставляет один цифровой выход для управления электромагнитом и три дискретных цифровых входа для мониторинга состояния. Логика работы соответствует стандартным практикам в системах контроля доступа.

3.1 Выход (OUT)

Устройство имеет **один физический выход**, управляемый командой *OUT* и соответствующий состоянию электромагнита замка.

Логическое состояние выхода	Физическое состояние	Описание
0 (ВЫКЛЮЧЕН)	Электромагнит **ПОДАНО ПИТАНИЕ** (включен)	Замок заблокирован, дверь **ЗАКРЫТА**.
1 (ВКЛЮЧЕН)	Электромагнит **БЕЗ ПИТАНИЯ** (выключен)	Замок разблокирован, дверь **ОТКРЫТА**.

Важно: Команда *OUT* с временными параметрами (таймер) поддерживается. При истечении заданного времени интерфейс автоматически вернет выход в состояние **0** (заблокировано).

3.2 Входы (IN)

Устройство имеет **три физических входа** для мониторинга. Их состояние запрашивается командой *ISTAT* или передается автоматически при изменении. В отчетах используется массив байт, где каждый байт соответствует одному входу. Активным состоянием является логическая **1**.

Байт	Назначение входа	Активное состояние (1)	Неактивное состояние (0)
Байт 1	**Кнопка**	Кнопка ручного открытия **нажата**.	Кнопка **отпущена**.
Байт 2	**Датчик двери**	Магнит датчика деактивирован — дверь **открыта**.	Магнит датчика активирован — дверь **закрыта**.
Байт 3	**Пожарная линия**	Нормально-разомкнутый контакт **замкнут** — сигнал **“Пожар”**.	Контакт разомкнут — нормальный режим.

Состояние входов постоянно мониторится устройством. Любое изменение приводит к тому, что в ответ на следующую команду *POLL* от контроллера будет отправлен соответствующий отчет.

Важно: в целях безопасности, при смене состояния пожарной лини в 1 (пожарная тревога), замок автоматически переводится в режим тревоги. С электромагнита напряжение **снимается**, тем самым, дверь **открывается**.

4 Использование защищённого режима

Устройство поддерживает установку защищённого канала связи (Secure Channel) в соответствии со стандартом OSDP v2.2. Режим обеспечивает шифрование всего трафика между контроллером (CP) и замком (PD) с использованием алгоритма AES-128.

4.1 Процедура установки защищённого режима

Установка защищённого режима выполняется в следующей последовательности:

1. **Передача мастер-ключа (SCBK):**
   - Контроллер должен передать устройству 16-байтовый мастер-ключ (Secure Channel Base Key, SCBK) с помощью команды *KEYSET*.
   - Ключ должен быть уникальным и соответствовать политикам безопасности системы.
2. **Установка защищённого канала:**
   - После перезагрузки устройство будет принимать только команды, защищённые Secure Channel.
   - Контроллер должен выполнить стандартную процедуру OSDP для установки защищённого канала.
   - После успешного завершения процедуры весь последующий обмен данными будет шифроваться.

5 Обновление встроенного программного обеспечения

Процедура обновления встроенного ПО (прошивки) устройства **UEM OSDP Lock** выполняется по стандартному механизму передачи файлов (File Transfer) протокола OSDP. Обновление поддерживается в **любом режиме работы устройства** (как в обычном, так и в защищённом).

5.1 Процедура обновления

1. **Инициация передачи файла:**
   - Контроллер (CP) инициирует передачу файла с помощью команды *FILETRANSFER* стандарта OSDP.
   - В параметрах команды необходимо указать **номер файла (File ID)**, равный **0xAB (171)**, который соответствует образу встроенного ПО устройства.
2. **Передача данных:**
   - Передача файла происходит стандартным для OSDP образом: файл разбивается на блоки, каждый блок передаётся отдельной командой *FILETRANSFER* с соответствующим смещением (offset) и данными.
   - Устройство (PD) подтверждает приём каждого блока.

3. **Завершение и перезагрузка:**
   - После успешной передачи всего файла устройство автоматически начинает процесс обновления:
     - Происходит проверка целостности образа.
     - Если проверка прошла успешно, устройство перезаписывает свою прошивку и перезагружается.
   - Во время процесса обновления устройство **не отвечает на команды**.
   - По окончании обновления устройство автоматически перезагрузится и будет готово к работе с новой версией ПО.

5.2 Критически важные особенности

- **Режим работы:** Обновление возможно в **любом режиме** (обычном или защищённом). Процедура передачи файла через `FILETRANSFER` не зависит от состояния Secure Channel.
- **Риск неисправности:** Загрузка некорректного, повреждённого или несовместимого файла прошивки с высокой вероятностью приведёт к **полному выходу устройства из строя**.
- **Восстановление:** В случае повреждения прошивки в результате обновления устройство **не подлежит восстановлению силами пользователя или интегратора**. Для ремонта потребуется возврат устройства на завод изготовителя.
- **Совместимость:** Используйте **официальные** файлы прошивки, предоставленные производителем для конкретной модели и аппаратной ревизии устройства.

5.3 Рекомендации по безопасности

2. Тщательно проверьте соответствие версии и целостность файла прошивки перед началом передачи.
3. Настоятельно рекомендуется проводить процедуру обновления на этапе предварительной настройки системы, а не в действующей эксплуатации.