

**Технология
«Iron Logic-защищённый»**

Руководство пользователя

Оглавление

| | |
|---|----|
| Что даёт эта защита? | 3 |
| Логика технологии «IronLogic-Защищённый» | 3 |
| Работа с защищённой системой..... | 3 |
| Назначение частей системы..... | 4 |
| Подготовка | 6 |
| Активация Карты Объекта..... | 6 |
| Инициализация настенных считывателей..... | 7 |
| Схемы подключения считывателей Mifare | 8 |
| Добавление ключей доступа..... | 8 |
| 1. Инициализация ключей доступа..... | 8 |
| 2. Запись ключей в контроллеры | 9 |
| Удаление/смена пароля считывателя | 9 |
| Разграничение доступа..... | 10 |
| Пример разграничения доступа..... | 11 |
| Добавление ключей с разграничением доступа..... | 12 |
| Перепрошивка считывателя..... | 12 |
| Запись дополнительных паролей в считыватель | 13 |
| Удаление дополнительных паролей из считывателя..... | 14 |

Что даёт эта защита?

- Ключи доступа защищены от копирования.
- Добавить новый ключ в систему может лишь владелец объекта.
- Предусмотрено удалённое добавление ключей в систему. На объект ключи доставляются готовыми к работе.
- Предусмотрено [разграничение доступа](#) — пользователь того или иного ключа имеет доступ не ко всем дверям объекта, а лишь к разрешённым ему точкам прохода.
- Защитой Iron Logic можно оборудовать уже существующую систему доступа.

Логика технологии «IronLogic-Защищённый»

|  <h3>Уязвимость обычной СКУД</h3> <p>Обычную систему доступа можно сравнить с контрольно-пропускным пунктом, где доступ обеспечивается по личным документам посетителей.</p> |  <h3>Защита Iron Logic</h3> <p>Система доступа «IronLogic-Защищённый» подобна КПП, где у посетителя сперва запрашивают пароль, а уже потом — документы.</p> |
|--|---|
| <p>Если фамилия посетителя содержится в списке допущенных лиц, вахтёр пропускает посетителя на объект.</p>  <p>Если нет — в доступе отказывают.</p>  | <p>Если пароль назван верно, приступают к проверке документов.</p>  <p>Вахтёр сверяет документы посетителя со списком допущенных лиц и принимает окончательное решение о предоставлении доступа.</p> |
| <p>⚠ Уязвимость обычных ключей позволяет легко скопировать «документы», то есть, код ключа.</p>  <p>Это и даёт возможность нарушителю «пройти через КПП».</p>  | <p>Если пароль посетителю неизвестен или назван неверный пароль, до проверки документов даже не доходит.</p>  <p>В доступе сразу отказывают.</p>  |

★ Ключи Mifare1K, применяемые в технологии «IronLogic-Защищённый», лучше защищены от копирования чем обычные ключи — Touch Memory и EM-Marine. Это значительно затрудняет «похищение» пароля. Скопировать пароль «любительскими» методами вовсе не представляется возможным.

★ Для работы с ключами не требуется использование компьютера со всеми его уязвимостями. Для хранения пароля используется физический носитель — Карта Объекта.

★ Предусмотрен упрощённый режим работы, когда решение о предоставлении доступа принимается исключительно на основе пароля — без проверки кода ключа.

Работа с защищённой системой

- Владелец объекта инициализирует считыватели и ключи, записывая в их память один и тот же пароль. Только связанные общим паролем считыватели и ключи способны работать друг с другом.
- Считыватели объекта игнорируют все посторонние ключи. Посторонними считаются все ключи без пароля или с паролем, принадлежащим другому объекту.

Назначение частей системы

Технология защиты заключается в применении совместно с контроллерами доступа связки «считыватели Mifare + ключи Mifare 1K Classic». Эту связку можно применить к уже смонтированным на объекте контроллерам — как к автономным, так и к сетевым.

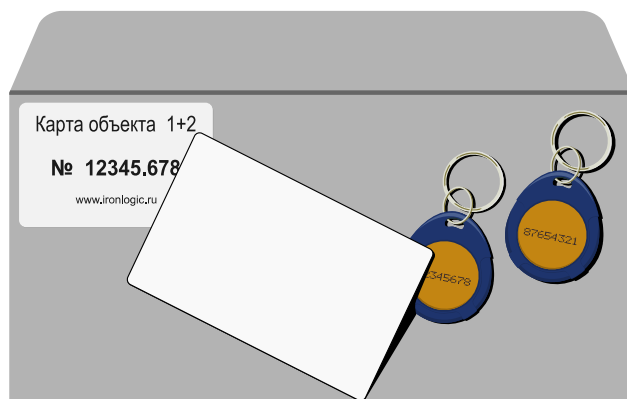


Перечень оборудования

1. **Карта Объекта [Ironlogic 1+2](#)**. Содержит пароль для инициализации считывателей и ключей. Карту Объекта можно создать в сервисе [Smartkey](#) (что дешевле, но работает только с Z-2 (мод. MF) и CP-Z2 (мод. MF-I)) или приобрести готовую «[Карту Объекта Iron Logic 1+2](#)».

Это комплект идентификаторов с записанным в них одинаковым паролем:

- одна карта IL-05M,
- два резервных брелока IL-07M.



Карта и брелоки содержат одинаковый пароль и полностью идентичны. Брелоки являются запасными на случай утери основной карты объекта и для работы с маленькими считывателями (CP-Z-2 (мод MF-I)).



2. Считыватели с индексом MF-I и NFC

| CP-Z-2 (мод. MF-I) накладной | CP-Z-2 (мод. MF-I) врезной | Matrix-II (мод. MF-I) | Matrix-III (мод. MF-I) | Matrix-III (мод. NFC) | Matrix-VI (мод. NFC K Net) |
|---|---|---|---|---|---|
|  |  |  |  |  |  |

3. Идентификаторы (ключи) с индексом M:

Карточки*




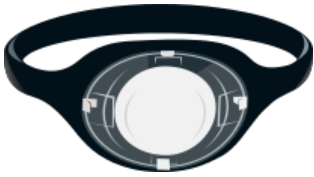




* Допустимо применение карточек с двумя чипами (EM-Marin и Mifare 1K), например [IL-06 E&M](#)

| IL-05M | IL-06M |
|--|---|
|  |  |

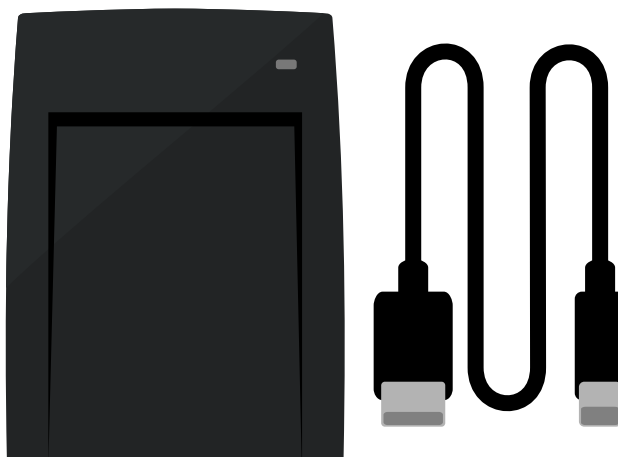
Брелоки

| IL-07M | IL-07MK | IL-08MBTR | IL-70M | IL-71M | IL-74M | IL-75M |
|---|---|---|---|--|---|---|
|  |  |  |  |  |  |  |

Браслеты

| IL-09M | IL-10M | IL-13M | IL-16M |
|---|---|--|---|
|  |  |  |  |
| IL-17M | IL-20M | IL-21M | IL-25M |
|  |  |  |  |

4. Настольные считыватели [Z-2 \(мод. MF\)](#) и [Z-2 \(мод. MF-I\)](#). С их помощью инициализируются ключи доступа.



Подготовка

Активация Карты Объекта

★ Перед началом использования обязательно нужно активировать весь комплект [Карта Объекта Iron Logic 1+2](#) (карту и два брелока) на настольном считывателе с защищенной прошивкой.

• Подключите настольный считыватель Z-2 (мод. MF) или Z-2 (мод. MF-I) к ПК

• Установите драйверы:

для Z-2 (мод. MF) – [drv_z2usb_2.12.26.zip](#);

для Z-2 (мод. MF-I) – [drv_z-2rdall_z-2mfi_v5.1.26.zip](#).

• Прошейте Z-2 (мод. MF) специальной прошивкой [версии 521](#) или [версии 605](#), для этого запустите прошивку от имени администратора;

Z-2 (мод. MF-I) прошивается через утилиту [Z-2 config](#) специальной прошивкой [версии 1.1.8](#).

★ В дальнейшем компьютер не потребуется. Для питания настольного считывателя подходит зарядное устройство для смартфона на 5 вольт.

Готовность к записи пароля в настольный считыватель отражается миганием красного светодиода.

• Приложите Карту Объекта к настольному считывателю.

При успешной записи пароля в настольный считыватель светодиод загорится зелёным цветом.

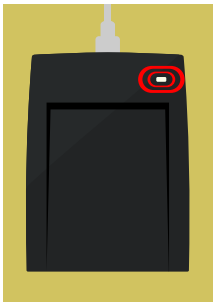



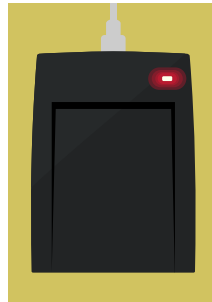

• Уберите карту.

Светодиод загорится красным в постоянном режиме. Настольный считыватель готов к работе.

△ Жёлтый цвет светодиода — приложен идентификатор, не являющийся Картой Объекта.

△ При повторном предъявлении Карты Объекта пароль удаляется из памяти настольного считывателя.

△ Так как пароль хранится в настольном считывателе только пока он запитан, инициализация требуется после каждого отключения питания настольного считывателя.

| Ожидание | Приложите Карту Объекта | Успешно | Уберите Карту | Готов к работе | Это не Карта Объекта! |
|---|---|---|--|---|---|
|  |  |  |  |  |  |

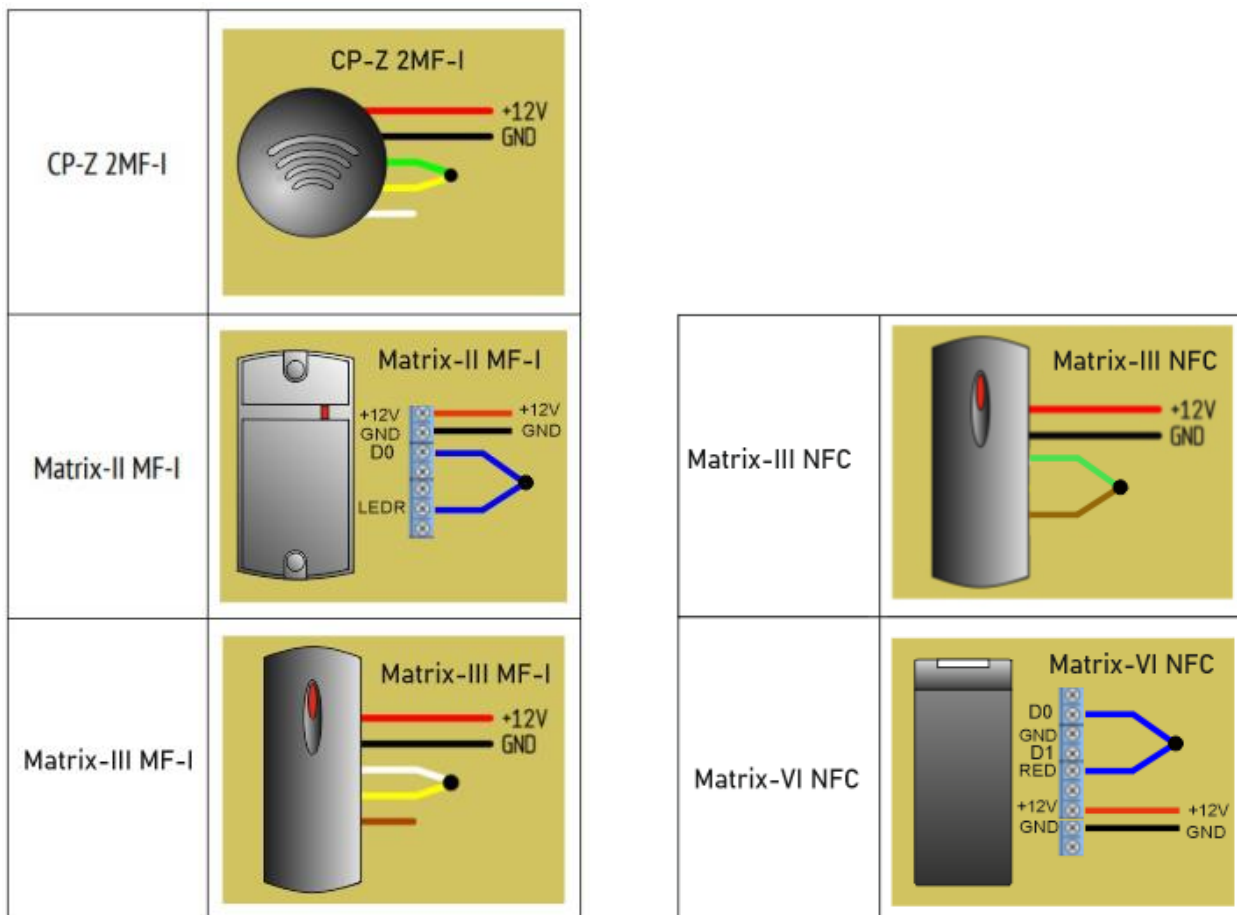
⚠ После успешной активации основной карты объекта необходимо поочередно приложить к настольному считывателю брелоки из комплекта [Карта Объекта Iron Logic 1+2](#) для их активации. Предварительно нужно извлечь предыдущую карту объекта из настольного считывателя, передернув USB шнур считывателя или поднеся повторно записанную ранее в считыватель карту объекта. Перед активацией очередной карты объекта (или брелока) светодиод настольного считывателя должен мигать красным цветом.

Инициализация настенных считывателей

Инициализация — это запись пароля из Карты Объекта в считыватели системы. Пароль **не сбрасывается** при отключении питания считывателя.

Соедините контакты Data 0 и LED-R, подайте питание на считыватель.

⚠ Все остальные провода должны быть изолированы и никуда не подключены.



Свечение красного индикатора говорит о готовности к записи пароля.

• Поднесите Карту Объекта к считывателю.

— При успешной записи пароля в **CP-Z-2 (мод. MF-I)** его светодиод два раза размеренно мигает и загорается в постоянном режиме. Если карту объекта удерживать дольше, то светодиод начнет часто мигать, это свидетельствует о том, что карта объекта уже записана.

— При успешной записи пароля в **Matrix-II/III (мод. MF-I)** его светодиод на 1 секунду загорается зелёным и гаснет.

— При успешной записи пароля в **Matrix-VI (мод. NFC К Net)** его светодиод загорается зелёным и сопровождается звуковым сигналом на 1 секунду.

— При успешной записи пароля в **Matrix-III (мод. NFC)** его светодиод загорается зелёным и сопровождается звуковым сигналом на 1 секунду.

— Если же светодиод считывателя несколько раз часто мигает, значит считыватель уже был инициализирован.

Matrix-II/III (мод. MF-I) при этом выдаёт серию из 5 коротких звуковых сигналов.

Теперь данная Карта Объекта является Мастер-картой для этого считывателя.

• Отключите питание считывателя и подключите его к контроллеру согласно схеме.

Схемы подключения считывателей Mifare

Подключение считывателей к контроллерам выполняется витой парой.

В зависимости от модели контроллера контакт iButton может называться TM, Dallas, Data, RD.

В руководстве по эксплуатации конкретного считывателя вы найдёте полный набор схем.

| | iButton | Wiegand-26 |
|-----------------|---------|------------|
| CP-Z 2MF-I | | |
| Matrix-II MF-I | | |
| Matrix-III MF-I | | |
| Matrix-III NFC | | |
| Matrix-VI NFC | | |

Добавление ключей доступа

1. Инициализация ключей доступа

Инициализация — это запись в ключ доступа пароля из карты объекта с помощью настольного адаптера Z-2 (мод. MF) или Z-2 (мод. MF-I).

⚠ Ключ доступа можно инициализировать лишь единожды. Перезаписать в ключ доступа пароль другой Карты Объекта невозможно.

- Включите настольный считыватель.
- Приложите к настольному считывателю Карту Объекта и уберите.
- Светодиод настольного считывателя станет гореть постоянно красным цветом
- Прикладывайте и убирайте по очереди ключи доступа.

Светодиод настольного считывателя гаснет на две секунды и снова включается.

— Зелёный — инициализация прошла успешно либо ключ уже содержит этот пароль.

— Жёлтый — ключ уже был инициализирован **другим** паролем или ключ с заполненной чем-то памятью; также может быть некачественный ключ.



2. Запись ключей в контроллеры

Запись ключей выполняется по инструкции к конкретной модели контроллера.

⚠ Все ключи участвующие в записи, должны быть заранее инициализированы.

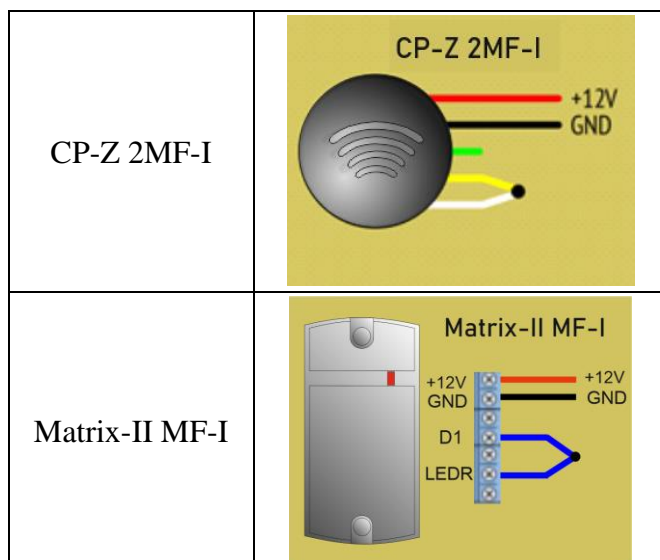
Удаление/смена пароля считывателя

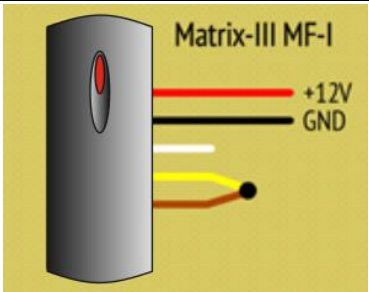
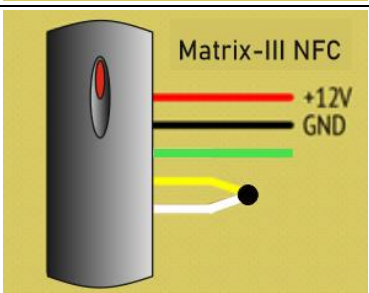
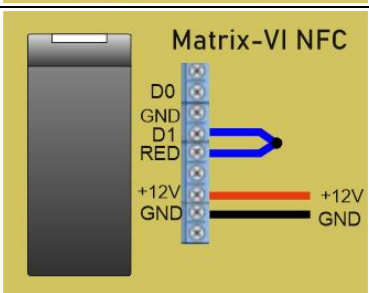
Удаление пароля из считывателя осуществляется его Мастер-ключом — это первая Карта Объекта, которой он был инициализирован.

Удаление пароля переводит считыватель из защищённого в открытый режим. В открытом режиме считыватель работает со всеми ключами Mifare 1K, не разделяя их на свои и чужие.

- Подготовьте Мастер-ключ считывателя.
- Отключите считыватель от контроллера.
- Соедините провода Data 1 и LED-R и подайте питание на считыватель.

⚠ Все остальные провода должны быть изолированы и никуда не подключены.



| | |
|-----------------|--|
| Matrix-III MF-I |  |
| Matrix-III NFC |  |
| Matrix-VI NFC |  |

- Поднесите к считывателю Мастер-ключ.
 - После перехода **CP-Z-2 (мод. MF-I)** в открытый режим светодиод считывателя два раза размеренно мигает и переходит в режим красного свечения.
 - После перехода **Matrix-II/III (мод. MF-I)** в открытый режим светодиод считывателя на 1 секунду загорается зелёным и гаснет.
 - После перехода **Matrix-VI (мод. NFC К Net)** в открытый режим его светодиод загорается зелёным и сопровождается звуковым сигналом на 1 секунду.
 - После перехода **Matrix-III (мод. NFC)** в открытый режим его светодиод загорается зелёным и сопровождается звуковым сигналом на 1 секунду.
 - Если светодиод считывателя несколько раз часто мигает, значит считыватель не был инициализирован.
- Отключите питание считывателя
- При необходимости запишите в считыватель пароль другой Карты Объекта.
- Подключите считыватель по штатной схеме.

Разграничение доступа

★ Контроллеры производства Iron Logic поддерживают режим удалённой подготовки ключей с разграничением доступа. Этот режим служит для ограничения доступа владельцам ключей в определённые помещения объекта.

Особенности режима:

— Процедура добавления ключей в контроллеры упраздняется. Достаточно инициализировать все новые ключи и раздать их пользователям. Ключ записывается в контроллер автоматически — при первом касании к считывателю.

— Все контроллеры необходимо перевести в режим «Асерт». Для этого следует 5 раз кратковременно поднести инициализированный Мастер-ключ **данного контроллера** к каждому считывателю на объекте.

⚠ Важно помнить, что память разных контроллеров Z-5R ограничена его характеристиками. После заполнения памяти доступ по новым ключам прекратится.

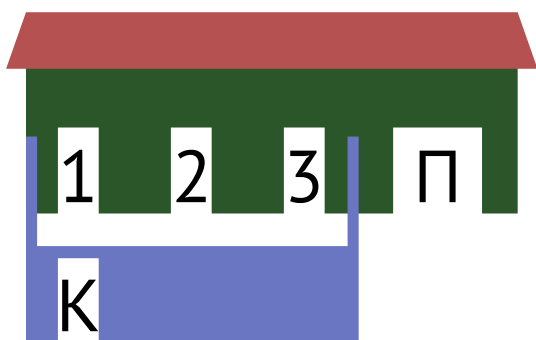
Пример разграничения доступа

В доме три подъезда и паркинг. Доступ на территорию организован через калитку.

Каждому жильцу разрешён доступ через калитку и только в свой подъезд.

Автовладельцам, кроме этого, разрешён доступ в паркинг.

Управляющему разрешён полный доступ — через калитку, во все подъезды и в паркинг.



Таким образом требуется организовать 7 вариантов доступа:

1. Жилец подъезда №1
2. Автовладелец подъезда №1
3. Жилец подъезда №2
4. Автовладелец подъезда №2
5. Жилец подъезда №3
6. Автовладелец подъезда №3
7. Управляющий

Напротив каждого варианта доступа отметим плюсами разрешённые точки прохода ▼

| Точки прохода ► Варианты доступа ▼ | Калитка | Паркинг | Подъезд №1 | Подъезд №2 | Подъезд №3 |
|---------------------------------------|---------|---------|------------|------------|------------|
| Жилец подъезда №1 | + | | + | | |
| Автовладелец подъезда №1 | + | + | + | | |
| Жилец подъезда №2 | + | | | + | |
| Автовладелец подъезда №2 | + | + | | + | |
| Жилец подъезда №3 | + | | | | + |
| Автовладелец подъезда №3 | + | + | | | + |
| Управляющий | + | + | + | + | + |

△ Для каждого варианта доступа следует приобрести отдельную Карту Объекта. В данном примере требуется 7 Карт.

Пароль каждой Карты Объекта следует записать в считыватели тех точек доступа, что помечены плюсом.

Разберём подробно обеспечение доступа для автовладельцев подъезда №2.

Этим жильцам нужен доступ в Калитку, Паркинг и Подъезд №2 (в таблице отмечено зелёным ▼).

Значит в соответствующие считыватели записываем пароль Карты «Автовладелец подъезда №2».

Этой же Картой инициализируем ключи для автовладельцев подъезда №2.

| Точки прохода ► | Калитка | Паркинг | Подъезд №1 | Подъезд №2 | Подъезд №3 |
|--------------------------|---------|---------|------------|------------|------------|
| Автовладелец подъезда №2 | + | + | | + | |

Автовладельцы подъезда №2 не получают доступ в Подъезды №1 и №3 (в таблице отмечено красным ▲), так как пароля Карты «Автовладелец подъезда №2» в этих считывателях нет.

Из таблицы видно, что в каждый считыватель необходимо записать **несколько** паролей. Например, считыватель Паркинга должен содержать 4 пароля ▼

| Варианты доступа ▼ | Паркинг |
|--------------------------|---------|
| Жилец подъезда №1 | |
| Автовладелец подъезда №1 | + |
| Жилец подъезда №2 | |
| Автовладелец подъезда №2 | + |
| Жилец подъезда №3 | |
| Автовладелец подъезда №3 | + |
| Управляющий | + |

▲ Запись нескольких паролей возможна только в считыватель со свежей прошивкой. При необходимости следует перепрошить считыватель.

Свежая прошивка позволяет записать в считыватель до 10 паролей, что соответствует 10 вариантам доступа.

Добавление ключей с разграничением доступа

- Сгруппируйте ключи в соответствии с назначенным им вариантом доступа
- Подготовьте соответствующую Карту Объекта.
- Включите настольный считыватель.
- Приложите к настольному считывателю Карту Объекта и уберите.
- Прикладывайте и убирайте по очереди ключи доступа.

Светодиод адаптера гаснет на две секунды.

- При успешной инициализации светодиод загорается зелёным цветом.
- Если светодиод загорается жёлтым цветом, значит в ключ нельзя записать пароль. Одна из причин — какой-либо пароль уже записан в него.
- Перед инициализацией ключей с другим вариантом доступа удалите пароль из настольного считывателя, обесточив его.

▲ Следует помнить, что записать пароль в ключ доступа можно только один раз. Соответственно, изменить вариант доступа данного ключа будет невозможно.

Перепрошивка считывателя

Перепрошивка не удаляет хранящийся в считывателе пароль.

- Скачайте последнюю прошивку из раздела «Прошивки (Firmware)»:

[CP-Z 2 \(мод. MF-I\)](#)

[Matrix-II \(мод. MF-I\)](#)

[Matrix-III \(мод. MF-I\)](#)

[Matrix-III \(мод. NFC\)](#)

- Прошейте считыватель в программе [Matrix config](#).

Для прошивки потребуется конвертер USB/RS485. Рекомендуется использовать [Z-397](#) или [Z-397 Guard](#). Подключите конвертер к ПК и установите драйверы.

▼ Установите переключатели/джамперы на конвертере и подключите к нему считыватель. Плюс питания пока не подключайте.

| | Z-397 | Z-397 Guard |
|-----------------|-------|-------------|
| CP-Z 2 MF-I | | |
| Matrix-II MF-I | | |
| Matrix-III MF-I | | |
| Matrix-III NFC | | |

- Запустите программу прошивки Matrix config.
- Выберите в окне COM порт, к которому подключен конвертер.
- Нажмите кнопку «Open File» и выберите файл прошивки.
- Установить переключку между клеммами «Вeer» и «Data0». (кроме CP-Z 2 MF-I)
- Подключите плюс питания считывателя.
- В течение 2 секунд нажмите «PGM».

Дождитесь окончания прошивки — сообщение «Transmission OK».

Запись дополнительных паролей в считыватель

⚠ Для добавления пароля дополнительной Карты Объекта в уже инициализированный считыватель **не требуется** соединять провода Data и LED.

Подготовьте Мастер-ключ — ту Карту Объекта, которой он был впервые инициализирован.

- Поднесите к считывателю Мастер-ключ на время 0,5 ... 1 сек. и сразу уберите его.
- В течение 18 секунд, пока мигает светодиод, поднесите к считывателю **дополнительную** Карту Объекта.

— При успешной записи дополнительного пароля в **CP-Z-2 (мод. MF-I)** его светодиод гаснет на 2 секунды.

— При успешной записи дополнительного пароля в **Matrix-II/III (мод. MF-I)** его светодиод на 1 секунду загорается зелёным и гаснет.

— При успешной записи дополнительного пароля в **Matrix-III (мод. NFC)** его светодиод на 1 секунду загорается зелёным и гаснет.

— При успешной записи дополнительного пароля в **Matrix-VI (мод. NFC K Net)** его светодиод на 1 секунду загорается зелёным и гаснет.

- Для выхода из режима поднесите к считывателю Мастер-ключ.

Примерно через 18 сек. бездействия считыватель выйдет из режима самостоятельно.

Удаление дополнительных паролей из считывателя

Для полного удаления паролей из считывателя удалите основной пароль.

В считывателях **CP-Z-2 (мод. MF-I)** предусмотрено выборочное удаление дополнительных паролей:

△ Для удаления пароля дополнительной Карты Объекта из считывателя **не требуется** соединять провода Data и LED.

Подготовьте Мастер-ключ — ту Карту Объекта, которой он был впервые инициализирован.

- Поднесите к считывателю Мастер-ключ на время 0,5 ... 1 сек. и сразу уберите его.

- В течение 18 секунд, пока мигает светодиод, повторно поднесите к считывателю Мастер-ключ на время 0,5 ... 1 сек. и сразу уберите его.

Светодиод переключится на сдвоенное мигание.

Этот режим длится также около 18 секунд.

- В течение 18 секунд, пока мигает светодиод, поднесите к считывателю удаляемую Карту Объекта на время 0,5 ... 1 сек., и сразу уберите её. При успешном удалении дополнительного пароля светодиод гаснет на 2 секунды.

- Для выхода из режима поднесите к считывателю Мастер-ключ.

Примерно через 18 сек. бездействия считыватель выйдет из режима самостоятельно.