Контроллер доступа

Руководство пользователя

Правовая информация

О руководстве

Руководство содержит инструкции для использования и управления продуктом. Изображения, графики и вся другая информация предназначены только для ознакомления. Этот документ может быть изменен без уведомления, в связи с обновлением прошивки и по другим причинам. Последнюю версию настоящего документа можно найти на веб-сайте (***https:// www.hikvision.com/***).
Используйте этот документ под руководством профессионалов, обученных работе с продуктом.

Торговые марки

HIKVISION и другие торговые марки Hikvision и логотипы являются интеллектуальной собственностью Hikvision в различных юрисдикциях.
Другие торговые марки и логотипы, содержащиеся в руководстве, являются собственностью их владельцев.

Правовая информация

ДО МАКСИМАЛЬНО ДОПУСТИМОЙ СТЕПЕНИ, РАЗРЕШЕННОЙ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ДАННОЕ РУКОВОДСТВО, ПРОДУКТ, АППАРАТУРА, ПРОГРАММНОЕ И АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ», СО ВСЕМИ ОШИБКАМИ И НЕТОЧНОСТЯМИ. HIKVISION НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, КАСАТЕЛЬНО УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ СООТВЕТСТВИЯ УКАЗАННЫМ ЦЕЛЯМ. ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА НЕСЕТ ПОЛЬЗОВАТЕЛЬ. HIKVISION НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ПЕРЕД ПОТРЕБИТЕЛЕМ ЗА КАКОЙ-ЛИБО СЛУЧАЙНЫЙ ИЛИ КОСВЕННЫЙ УЩЕРБ, ВКЛЮЧАЯ УБЫТКИ ИЗ-ЗА ПОТЕРИ ПРИБЫЛИ, ПЕРЕРЫВА В ДЕЯТЕЛЬНОСТИ ИЛИ ПОТЕРИ ДАННЫХ ИЛИ ДОКУМЕНТАЦИИ, ПО ПРИЧИНЕ НАРУШЕНИЯ УСЛОВИЙ КОНТРАКТА, ТРЕБОВАНИЙ (ВКЛЮЧАЯ ХАЛАТНОСТЬ), УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ ИНОГО, В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ HIKVISION БЫЛО ИЗВЕСТНО О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.
ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА С ДОСТУПОМ В ИНТЕРНЕТ НЕСЕТ ПОЛЬЗОВАТЕЛЬ; HIKVISION НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА НЕНОРМАЛЬНУЮ РАБОТУ ОБОРУДОВАНИЯ, ПОТЕРЮ ИНФОРМАЦИИ И ДРУГИЕ ПОСЛЕДСТВИЯ, ВЫЗВАННЫЕ КИБЕР АТАКАМИ, ВИРУСАМИ ИЛИ ДРУГИМИ ИНТЕРНЕТ РИСКАМИ; ОДНАКО, HIKVISION ОБЕСПЕЧИВАЕТ СВОЕВРЕМЕННУЮ ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ, ЕСЛИ ЭТО НЕОБХОДИМО.
ВЫ ОБЯЗУЕТЕСЬ ИСПОЛЬЗОВАТЬ ЭТОТ ПРОДУКТ В СООТВЕТСТВИИ С ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, А ТАКЖЕ НЕСЕТЕ ПОЛНУЮ ОТВЕТСТВЕННОСТЬ ЗА ЕГО СОБЛЮДЕНИЕ. В ЧАСТНОСТИ, ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ДАННОГО ПРОДУКТА ТАКИМ ОБРАЗОМ, ЧТОБЫ НЕ НАРУШАТЬ ПРАВА ТРЕТЬИХ ЛИЦ, ВКЛЮЧАЯ ПРАВА НА ПУБЛИЧНОСТЬ, ПРАВА НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ, ЗАЩИТУ ДАННЫХ И ДРУГИЕ ПРАВА КАСАТЕЛЬНО НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ.

ВЫ ОБЯЗУЕТЕСЬ НЕ ИСПОЛЬЗОВАТЬ ЭТОТ ПРОДУКТ В ЗАПРЕЩЕННЫХ ЦЕЛЯХ, ВКЛЮЧАЯ РАЗРАБОТКУ ИЛИ ПРОИЗВОДСТВО ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ, РАЗРАБОТКУ ИЛИ ПРОИЗВОДСТВО ХИМИЧЕСКОГО ИЛИ БИОЛОГИЧЕСКОГО ОРУЖИЯ, ЛЮБУЮ ДЕЯТЕЛЬНОСТЬ, СВЯЗАННУЮ С ЯДЕРНЫМИ ВЗРЫВЧАТЫМИ ВЕЩЕСТВАМИ, НЕБЕЗОПАСНЫМ ЯДЕРНЫМ ТОПЛИВНЫМ ЦИКЛОМ ИЛИ НАРУШАЮЩУЮ ПРАВА ЧЕЛОВЕКА.
В СЛУЧАЕ КАКИХ-ЛИБО КОНФЛИКТОВ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ И ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПОСЛЕДНЕЕ ПРЕВАЛИРУЕТ.

Защита данных

Во время использования устройства личные данные будут собираться, храниться и обрабатываться. При разработке устройств Hikvision соблюдаются принципы конфиденциальности в целях защиты данных. Например, устройства с функциями распознавания лиц разработаны таким образом, что сохраняемые биометрические данные защищены шифрованием; в устройствах с функцией идентификации по отпечатку пальца будут сохранены только шаблоны отпечатка пальца и, таким образом, изображение отпечатка пальца не подлежит реконструкции.
Поскольку данные находятся под вашим контролем, сбор, хранение, обработку и передачу данных необходимо выполнять в соответствии с применимыми законами и требованиями по защите данных. Также необходимо выполнять действия по безопасности для защиты личных данных, такие как разумный административный и физический контроль безопасности, периодические обзоры и оценки эффективности мер безопасности.

Доступные модели

Наименование	Модель
Контроллер доступа	Контроллер доступа серии DS-K2601T
	Контроллер доступа серии DS-K2602T
	Контроллер доступа серии DS-K2604T
	Контроллер доступа серии DS-K2601-G
	Контроллер доступа серии DS-K2602-G
	Контроллер доступа серии DS-K2604-G

Регулирующая информация

Информация о FCC

Обратите внимание, что изменения или модификации, не одобренные явно стороной, ответственной за соответствие, могут привести к аннулированию полномочий пользователя по работе с данным оборудованием.
Соответствие FCC: это оборудование прошло испытания и соответствует регламенту для цифрового устройства класса B, применительно к части 15 Правил FCC. Данный регламент разработан для того, чтобы обеспечить достаточную защиту от вредных помех, возникающих при использовании оборудования в коммерческой среде. Это оборудование генерирует, использует и может излучать радиоволны на разных частотах и, если устройство установлено и используется не в соответствии с инструкцией, оно может создавать помехи для радиосигналов. Тем не менее, нет никакой гарантии, что помехи не возникнут в каких-либо конкретных случаях установки. Если оборудование создает вредные помехи для приема радио- или телевизионных сигналов, что может быть определено путем включения и выключения оборудования, пользователю рекомендуется попытаться устранить помехи одним или несколькими способами, а именно:
— изменить ориентацию или местоположение приемной антенны;
— увеличить расстояние между оборудованием и приемником;
— подключить оборудование к розетке в цепи, отличной от той, к которой подключен приемник;
— обратиться к дилеру или опытному радио / телемастеру.
Данное оборудование следует устанавливать и использовать на расстоянии не менее 20 см между источником излучения и пользователем.
Условия FCC
Это устройство соответствует регламенту для цифрового устройства применительно к части 15 Правил FCC. Эксплуатация допускается при соблюдении следующих двух условий:
1. Данное устройство не должно создавать вредных помех.
2. Устройство должно выдерживать возможные излучения, включая и те, которые могут привести к выполнению нежелательных операций.

Соответствие стандартам ЕС

CE

Данный продукт и (если применимо) поставляемые принадлежности отмечены знаком «CE» и, следовательно, согласованы с европейскими стандартами, перечисленными под директивой 2014/30/EC EMC, директивой 2014/53/EC RE, директивой 2011/65/EC RoHS.

2012/19/EC (директива WEEE). Продукты, отмеченные данным знаком, запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Для надлежащей переработки верните этот продукт своему местному поставщику при покупке эквивалентного нового оборудования или утилизируйте его в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: www.recyclethis.info

2006/66/EC (директива о батареях). Данный продукт содержит батарею, которую запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Подробная информация о батарее изложена в документации продукта. Батарея отмечена значком, который может включать наименования, обозначающие содержание кадмия (Cd), свинца (Pb) или ртути (Hg). Для надлежащей утилизации возвратите батарею своему поставщику либо избавьтесь от нее в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: www.recyclethis.info

Инструкция по технике безопасности

Эта инструкция предназначена для того, чтобы пользователь мог использовать продукт правильно и избежать опасности или причинения вреда имуществу.

Меры предосторожности разделены на «Предупреждения» и «Предостережения».

Предупреждение: игнорирование предупреждений может привести к тяжелым травмам или смерти.

Предостережение: игнорирование любого из предостережений может привести к травмам или порче оборудования.

⚠	⚠
Предупреждение: следуйте данным правилам для предотвращения серьезных травм и смертельных случаев.	**Предостережение:** следуйте мерам предосторожности, чтобы предотвратить возможные повреждения или материальный ущерб.

⚠ Предупреждение:

- В рамках установки необходимо предусмотреть разъединитель.

  Примечание

  Внешние разъединители не входят в комплект поставки.
- Эксплуатация электронных устройств должна строго соответствовать правилам электробезопасности, противопожарной защиты и другим соответствующим нормам в регионе эксплуатации.
- Используйте адаптер питания соответствующей компании. Потребляемая мощность не может быть меньше требуемого значения.
- Не подключайте несколько устройств к одному блоку питания, перегрузка адаптера может привести к перегреву или возгоранию.
- Прежде чем подключать, устанавливать или разбирать устройство, убедитесь, что питание отключено.
- Если устройство устанавливается на потолок или стену, убедитесь, что оно надежно закреплено.
- Если из устройства идет дым или доносится шум — отключите питание, извлеките кабель и свяжитесь с сервисным центром.
- Избегайте проглатывания батареи, существует опасность химического ожога.
  Данное устройство оснащено батареей таблеточного типа. Проглатывание батареи таблеточного типа может вызвать серьезные внутренние ожоги всего за 2 часа и привести к смерти.
  Храните новые и использованные батареи в недоступном для детей месте. Если отсек для батареи закрывается ненадежно, прекратите использование продукта и храните его в недоступном для детей месте. В случае проглатывания батареи немедленно обратитесь за медицинской помощью.
- Если продукт не работает должным образом, необходимо обратиться к дилеру или в ближайший сервисный центр. Не пытайтесь самостоятельно разобрать устройство. (Компания не несет ответственность за проблемы, вызванные несанкционированным ремонтом или техническим обслуживанием.)

⚠ Предостережение:

- Не бросайте устройство и не подвергайте его ударам или воздействию сильных электромагнитных помех. Избегайте установки устройства на вибрирующую поверхность или в местах, подверженных ударам (пренебрежение этим предостережением может привести к повреждению устройства).
- Запрещено размещать устройство в местах с чрезвычайно высокой или низкой температурой окружающей среды (подробная информация о рабочей температуре представлена в спецификации устройства), в пыльной или влажной среде, запрещено подвергать устройство воздействию сильных электромагнитных помех.
- Не подвергайте крышку устройства, предназначенного для использования внутри помещения, воздействию дождя или влаги.
- Не подвергайте устройство воздействию прямых солнечных лучей, не устанавливайте в местах с плохой вентиляцией или рядом с источником тепла таким, как обогреватель или радиатор (пренебрежение этим предостережением может привести к пожару).
- Запрещено направлять устройство на солнце или очень яркие источники света. Яркий свет может вызвать размытие или потерю четкости изображения (что не является признаком неисправности), а также повлиять на срок службы матрицы.
- Используйте прилагаемую перчатку во время демонтажа крышки устройства, избегайте прямого контакта с крышкой устройства, так как пот и жир с пальцев могут стать причиной разрушения защитного покрытия на поверхности устройства.
- Для очистки внутренних и внешних поверхностей крышки устройства используйте мягкую и сухую ткань, не используйте щелочные моющие средства.
- Сохраните упаковку после распаковки для использования в будущем. В случае сбоя работы устройство необходимо вернуть на завод (с оригинальной упаковкой). Транспортировка без оригинальной упаковки может привести к повреждению устройства и к дополнительным расходам.
- Неправильное использование или замена батареи может привести к опасности взрыва. Проводите замену на такие же батареи или аналогичные. Утилизируйте использованные батареи в соответствии с инструкциями, предоставленными производителем батарей.

Содержание

Раздел 1 Профилактические меры и предостерегающие рекомендации

Перед подключением и эксплуатацией устройства, обратите внимание на следующие моменты:

- Убедитесь, что устройство установлено в хорошо проветриваемом, непыльном помещении.
- Не допускайте попадания жидкостей в устройство.
- Убедитесь, что условия окружающей среды соответствуют спецификациям производителя.
- Убедитесь, что устройство надежно закреплено на стойке или полке. Сильные удары или толчки устройства, полученные в результате падения, могут привести к повреждению чувствительной электроники устройства.
- Если позволяют условия, рекомендуется использовать устройство в комбинации с ИБП.
- Перед подключением и отключением аксессуаров и периферийных устройств необходимо отключить питание устройства.
- Для этого устройства следует использовать рекомендованный производителем жесткий диск.
- Неправильное использование или замена батареи может привести к опасности взрыва. Проводите замену на такие же батареи или аналогичные. Утилизируйте использованные батареи в соответствии с инструкциями, предоставленными производителем.

Раздел 2. Описание устройства

- Оснащен 32-битным высокоскоростным процессором.
- Поддержка TCP / IP, EHome 5.0, протокола ISAPI и OSDP. Специальное шифрование данных связи для предотвращения утечки конфиденциальной информации.
- Поддержка распознавания и хранения номера карт с максимальной длиной 20 символов.
- Поддержка до 100,000 карт и 300,000 записей выдачи карт.
- Поддержка функций: блокировка нескольких дверей, запрет двойного прохода, множественная аутентификация, открытие двери первой картой, суперкарта и суперпароль, шифрование M1-карты, онлайн обновление и дистанционное управление дверьми.
- Тревога тампера для считывателя карт, тревога незакрытой двери, тревога принудительного открытия двери, тревога превышения времени ожидания при открытии двери, тревога использования принудительной карты и пароля принуждения, тревога черного списка и тревога превышения попыток считывания недействительной карты.
- Тревога короткого замыкания и тревога разомкнутой цепи.
- Обнаружение конфликта IP-адресов.
- Функция запрета двойного прохода в обоих направлениях (для реализации функции запрета двойного прохода в обоих направлениях на основе карты необходимо подключить считыватель карт к RS-485. Для реализации функции запрета двойного прохода в обоих направлениях на основе сети убедитесь, что сервер и устройство правильно взаимодействуют друг с другом. На выбранном сервере может быть сохранено до 5000 записей, функция запрета двойного прохода в обоих направлениях на внутреннем устройстве.
- Поддержка RS-485 и интерфейса Wiegand для доступа к считывателю карт. Интерфейс Wiegand поддерживает W26, W34 и совместим со сторонним считывателем карт с интерфейсом Wiegand.
- Поддержка добавления различных типов пользователей: обычный пользователь, посетитель и пользователь из черного списка.
- Поддержка различных типов карт: обычная / отключенная / в черном списке / патрульная / гостевая / принудительная / суперкарта и т.д.
- Устройство оснащено различными индикаторами для отображения различных состояний.
- Поддержка автоматической и ручной синхронизации времени.
- Поддержка функции хранения записей, когда устройство находится офлайн, и функции тревоги при недостаточном пространстве для хранения.
- Резервный аккумулятор, функция сторожевого таймера и защиты от несанкционированного доступа.
- После выключения контроллера доступа данные хранятся бессрочно.
- Поддержка привязки интерфейса входа / выхода и привязки событий.
- Поддержка протокола EHome для подключения к сети общего доступа.
- 500 групп паролей в режиме аутентификации карты или пароля.
- Поддержка настройки часовых поясов.

Раздел 3. Описание основной платы управления

3.1 Описание основной платы управления контроллера доступа на 1 дверь

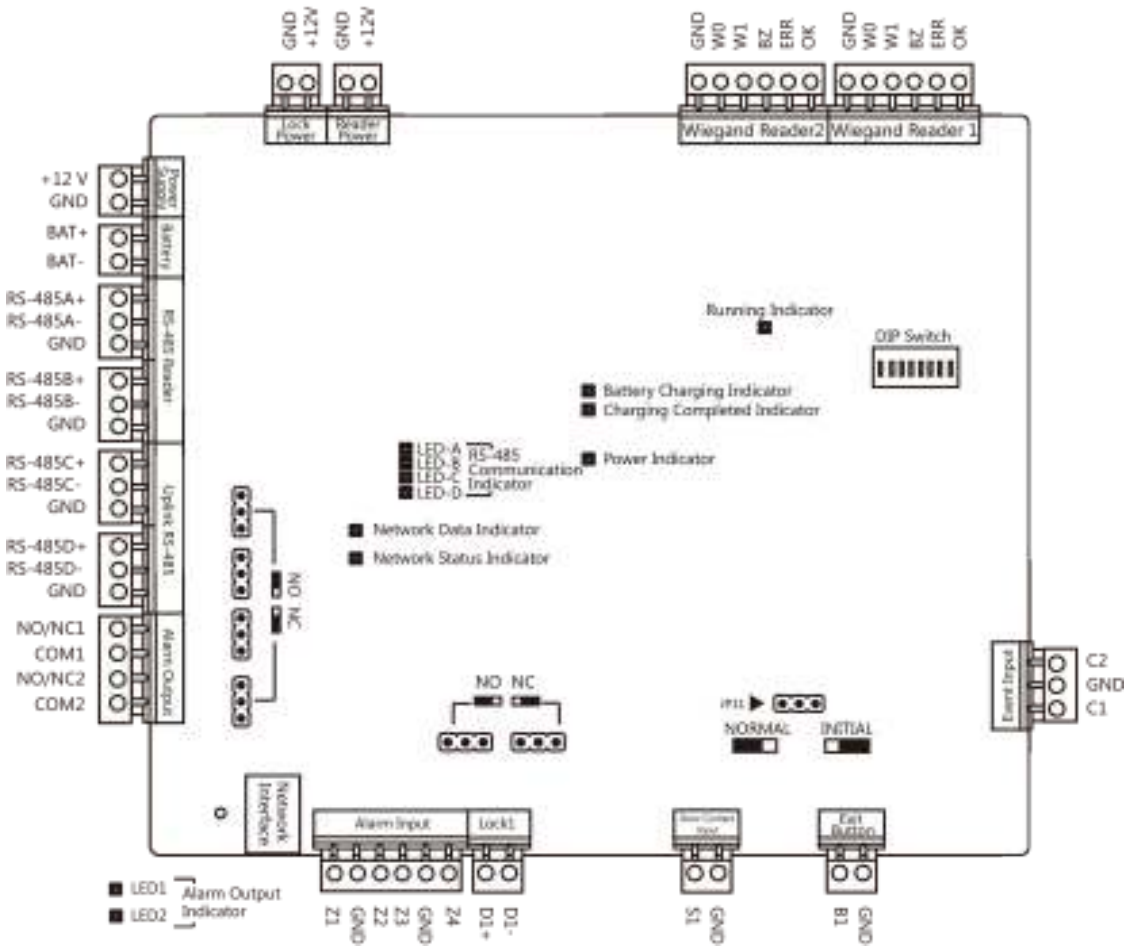


Рисунок 3-1. Основная плата управления контроллера доступа на 1 дверь

Английский язык	**Русский язык**
Lock Power	Питание замка
Reader Power	Питание считывателя
Wiegand Reader	Считыватель с Wiegand
Event Input	Вход событий
Exit Button	Кнопка выхода
Door Contact Input	Вход дверного контакта
Lock	Замок
Alarm Input	Тревожный вход
Network Interface	Сетевой интерфейс
Alarm Output	Тревожный выход
Uplink RS-485	Восходящий канал RS-485
RS-485 Reader	Считыватель с RS-485
Battery	Батарея
Power Supply	Питание
NO	Нормально разомкнутый контакт
NC	Нормально замкнутый контакт
Network Data Indicator	Индикатор сетевых данных
Network Status Indicator	Индикатор состояния сети
RS-485 Communication Indicator	Индикатор связи RS-485
Power Indicator	Индикатор питания
Battery Charging Indicator	Индикатор заряда батареи
Charging Completed Indicator	Индикатор завершения зарядки
Running Indicator	Индикатор режима работы
DIP Switch	DIP-переключатель
Normal	Нормальное положение
Initial	Исходное положение
Alarm Output Indicator	Индикатор тревожного выхода

3.2 Описание основной платы управления контроллера доступа на 2 двери

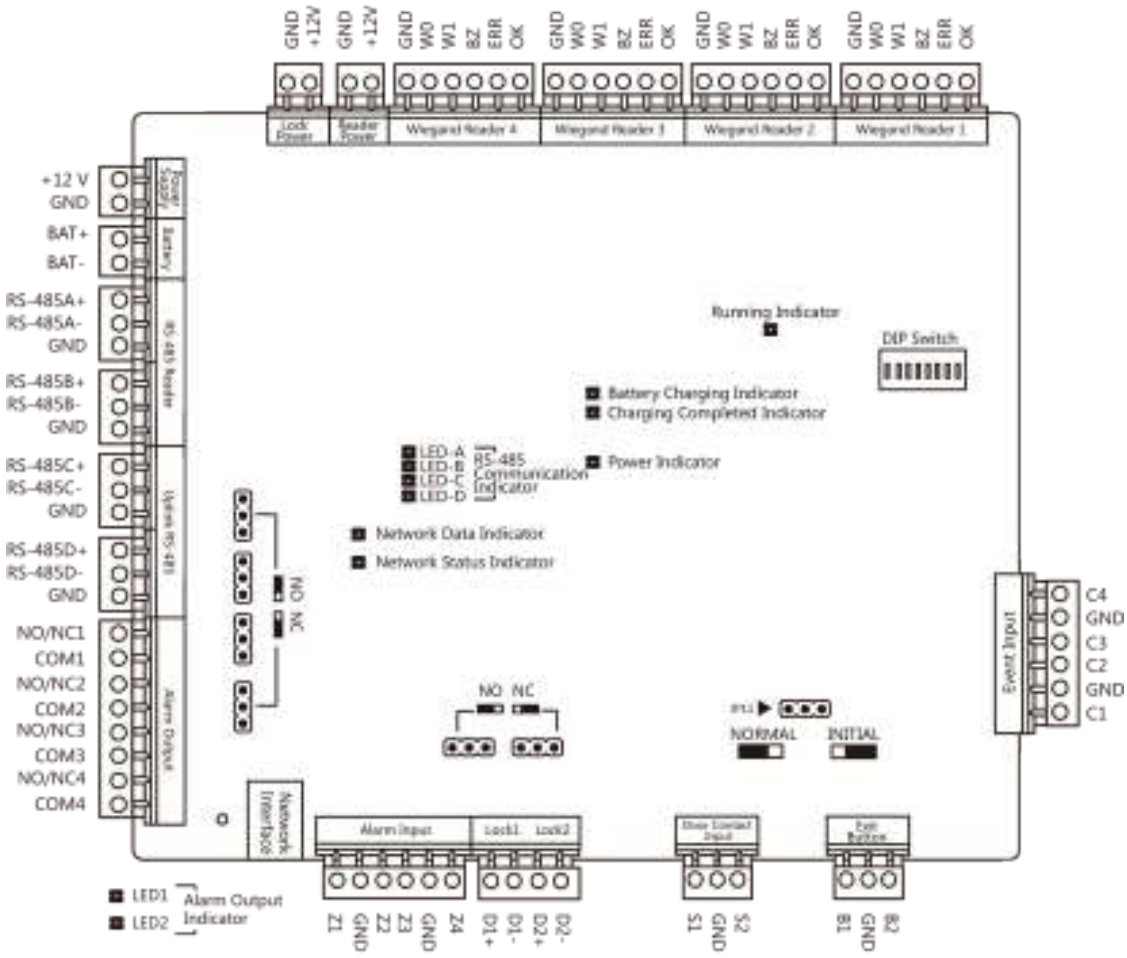


Рисунок 3-2. Основная плата управления контроллера доступа на 2 двери

Английский язык	**Русский язык**
Lock Power	Питание замка
Reader Power	Питание считывателя
Wiegand Reader	Считыватель с Wiegand
Event Input	Вход событий
Exit Button	Кнопка выхода
Door Contact Input	Вход дверного контакта
Lock	Замок
Alarm Input	Тревожный вход
Network Interface	Сетевой интерфейс
Alarm Output	Тревожный выход
Uplink RS-485	Восходящий канал RS-485
RS-485 Reader	Считыватель с RS-485
Battery	Батарея
Power Supply	Питание
NO	Нормально разомкнутый контакт
NC	Нормально замкнутый контакт
Network Data Indicator	Индикатор сетевых данных
Network Status Indicator	Индикатор состояния сети
RS-485 Communication Indicator	Индикатор связи RS-485
Power Indicator	Индикатор питания
Battery Charging Indicator	Индикатор заряда батареи
Charging Completed Indicator	Индикатор завершения зарядки
Running Indicator	Индикатор режима работы
DIP Switch	DIP-переключатель
Normal	Нормальное положение
Initial	Исходное положение
Alarm Output Indicator	Индикатор тревожного выхода

3.3 Описание основной платы управления контроллера доступа на 4 двери

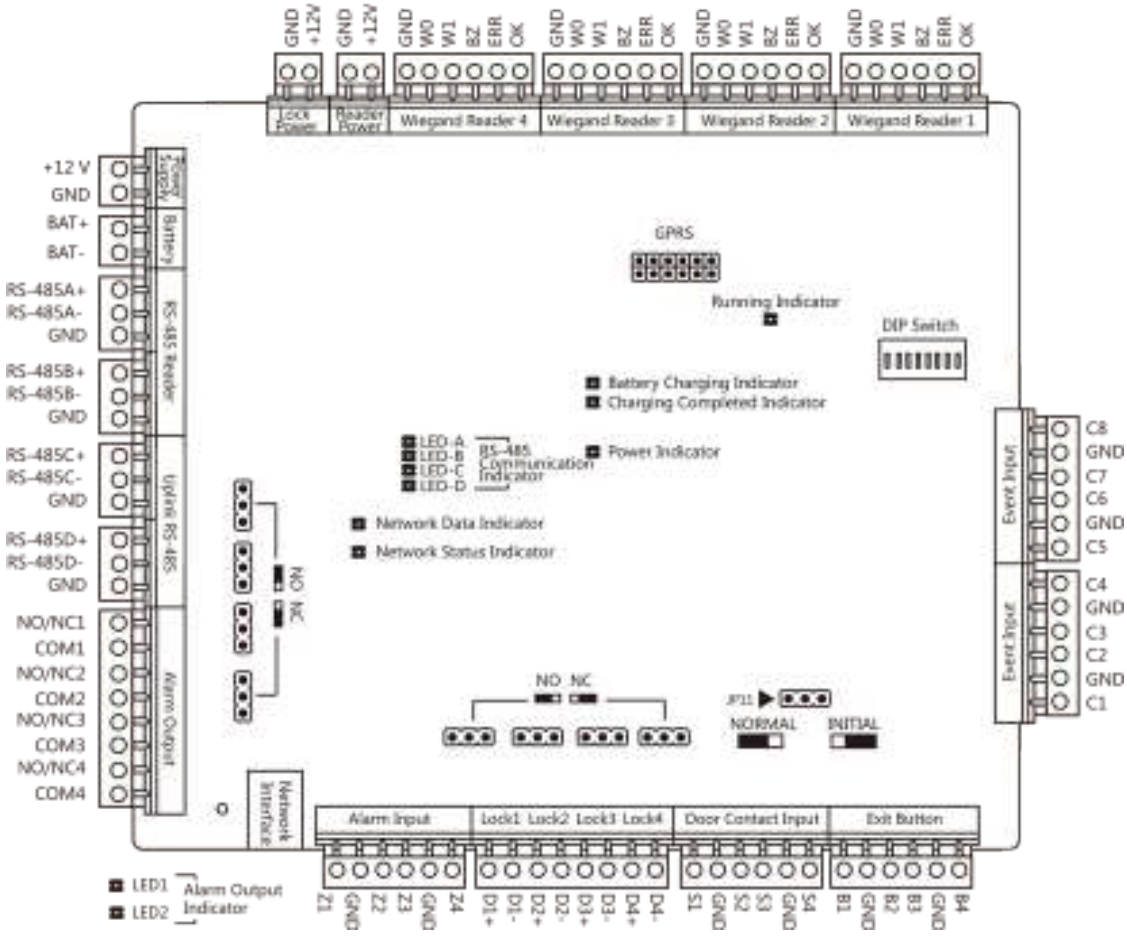


Рисунок 3-3. Основная плата управления контроллера доступа на 4 двери

Английский язык	**Русский язык**
Lock Power	Питание замка
Reader Power	Питание считывателя
Wiegand Reader	Считыватель с Wiegand
Event Input	Вход событий
Exit Button	Кнопка выхода
Door Contact Input	Вход дверного контакта
Lock	Замок
Alarm Input	Тревожный вход
Network Interface	Сетевой интерфейс
Alarm Output	Тревожный выход
Uplink RS-485	Восходящий канал RS-485
RS-485 Reader	Считыватель с RS-485
Battery	Батарея

Английский язык	**Русский язык**
Power Supply	Питание
NO	Нормально разомкнутый контакт
NC	Нормально замкнутый контакт
Network Data Indicator	Индикатор сетевых данных
Network Status Indicator	Индикатор состояния сети
RS-485 Communication Indicator	Индикатор связи RS-485
Power Indicator	Индикатор питания
Battery Charging Indicator	Индикатор заряда батареи
Charging Completed Indicator	Индикатор завершения зарядки
Running Indicator	Индикатор режима работы
DIP Switch	DIP-переключатель
Normal	Нормальное положение
Initial	Исходное положение
Alarm Output Indicator	Индикатор тревожного выхода
GPRS	GPRS

3.4 Описание компонентов

В данном документе представлены компоненты устройства с описаниями.

В качестве примера далее представлена схема компонентов контроллера доступа на 4 двери.

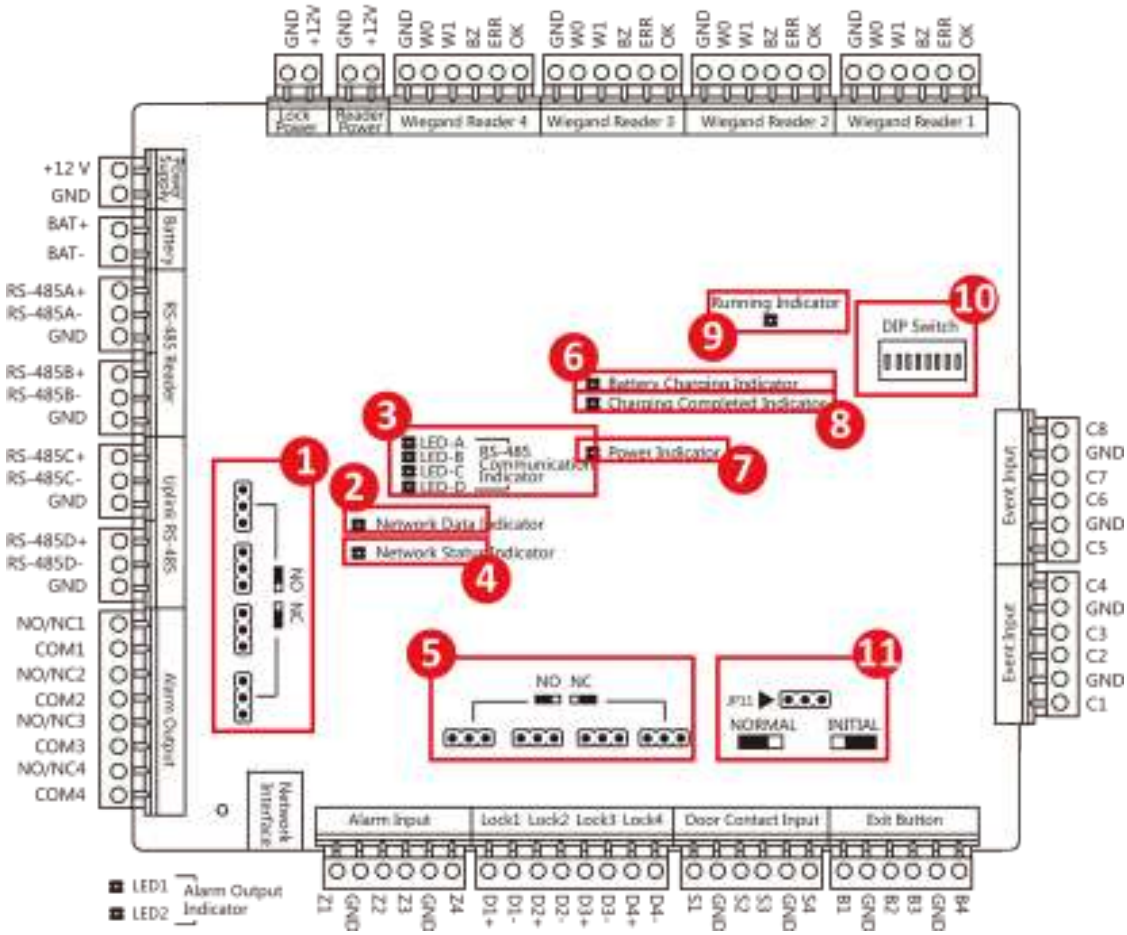


Рисунок 3-4. Схема компонентов контроллера доступа на 4 двери

Английский язык	**Русский язык**
Lock Power	Питание замка
Reader Power	Питание считывателя
Wiegand Reader	Считыватель с Wiegand
Event Input	Вход событий
Exit Button	Кнопка выхода
Door Contact Input	Вход дверного контакта
Lock	Замок
Alarm Input	Тревожный вход
Network Interface	Сетевой интерфейс
Alarm Output	Тревожный выход
Uplink RS-485	Восходящий канал RS-485

Английский язык	**Русский язык**
RS-485 Reader	Считыватель с RS-485
Battery	Батарея
Power Supply	Питание
NO	Нормально разомкнутый контакт
NC	Нормально замкнутый контакт
Network Data Indicator	Индикатор сетевых данных
Network Status Indicator	Индикатор состояния сети
RS-485 Communication Indicator	Индикатор связи RS-485
Power Indicator	Индикатор питания
Battery Charging Indicator	Индикатор заряда батареи
Charging Completed Indicator	Индикатор завершения зарядки
Running Indicator	Индикатор режима работы
DIP Switch	DIP-переключатель
Normal	Нормальное положение
Initial	Исходное положение
Alarm Output Indicator	Индикатор тревожного выхода
GPRS	GPRS

Таблица 3-1. Описание компонентов контроллера доступа на 4 двери

№	Описание компонентов		
	Контроллер доступа на 1 дверь	Контроллер доступа на 2 двери	Контроллер доступа на 4 двери
1	Состояние тревожного релейного выхода (NC / NO)		
2	Индикатор сетевых данных		
3	Индикатор связи RS-485		
4	Индикатор состояния сети		
5	Выбор состояния тревожного релейного выхода (NC / NO)		
6	Индикатор заряда батареи		

№	Описание компонентов		
	Контроллер доступа на 1 дверь	Контроллер доступа на 2 двери	Контроллер доступа на 4 двери
7	Индикатор питания		
8	Индикатор завершения зарядки		
9	Индикатор режима работы		
10	DIP-переключатель основной платы Задайте положение DIP-переключателей для контроллера доступа. Доступный диапазон: от 1 до 63. Пример: если значение DIP-переключателя равно 24, установите бит 4 и бит 5 в положение ВКЛ. **Примечание** • Настройки станут действительны после перезагрузки устройства. • Подробная информация о настройке DIP-переключателей представлена в *Приложении А. Описание DIP-переключателей*.		
11	Инициализация оборудования и выбор стандартного режима работы		

Раздел 4. Описание разъемов

Примечание

- Серия 2602 и 2604: номинальная мощность для дверного замка 12 В / 2 А, для питания считывателя карт 12 В / 0.67 А.
- Серия 2601: номинальная мощность для дверного замка 12 В / 0.5 А, для питания считывателя карт 12 В / 0.3 А.

4.1 Описание разъемов контроллера доступа на 1 дверь

Далее представлено описание разъемов контроллера доступа на 1 дверь.

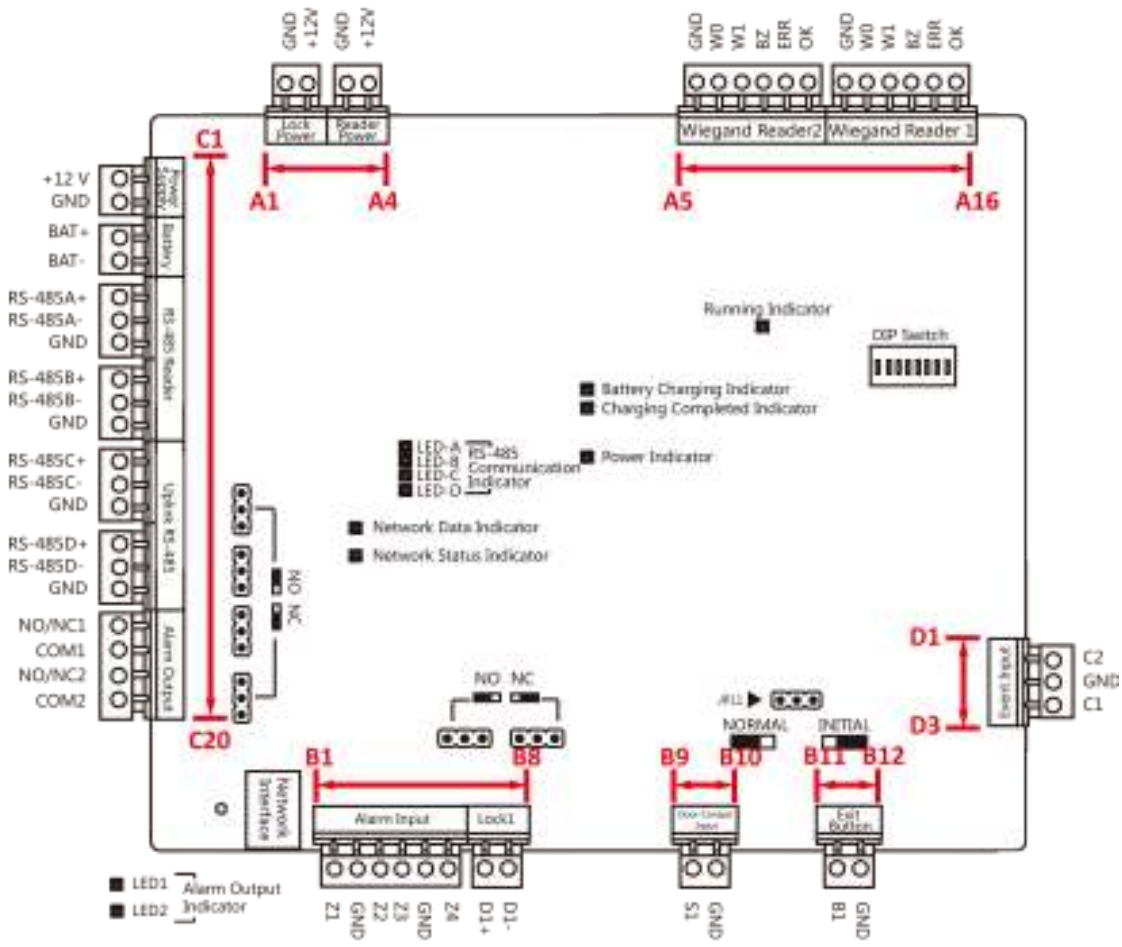


Рисунок 4-1. Основная плата управления контроллера доступа на 1 дверь

Английский язык	**Русский язык**
Lock Power	Питание замка
Reader Power	Питание считывателя
Wiegand Reader	Считыватель с Wiegand
Event Input	Вход событий
Exit Button	Кнопка выхода
Door Contact Input	Вход дверного контакта
Lock	Замок
Alarm Input	Тревожный вход
Network Interface	Сетевой интерфейс
Alarm Output	Тревожный выход
Uplink RS-485	Восходящий канал RS-485
RS-485 Reader	Считыватель с RS-485
Battery	Батарея
Power Supply	Питание
NO	Нормально разомкнутый контакт
NC	Нормально замкнутый контакт
Network Data Indicator	Индикатор сетевых данных
Network Status Indicator	Индикатор состояния сети
RS-485 Communication Indicator	Индикатор связи RS-485
Power Indicator	Индикатор питания
Battery Charging Indicator	Индикатор заряда батареи
Charging Completed Indicator	Индикатор завершения зарядки
Running Indicator	Индикатор режима работы
DIP Switch	DIP-переключатель
Normal	Нормальное положение
Initial	Исходное положение
Alarm Output Indicator	Индикатор тревожного выхода
GPRS	GPRS

Таблица 4-1. Описание разъемов контроллера доступа на 1 дверь

	Контроллер доступа на 1 дверь		
A1	Питание электронного замка	GND	Заземление
A2		12 В	Питание выхода электронного замка
A3	Питание считывателя карт	GND	Заземление
A4		12 В	Питание выхода считывателя карт
A5	Считыватель карт Wiegand 2	GND	Заземление
A6		W0	Интерфейс чтения входных данных Wiegand 0
A7		W1	Интерфейс чтения входных данных Wiegand 1
A8	Считыватель карт Wiegand 2	BZ	Вывод управления бипером считывателя карт
A9		ERR	Индикатор управления выводом считывателя карт (отказ карты)
A10		OK	Индикатор управления выводом считывателя карт (прием карты)
A11	Считыватель карт Wiegand 1	GND	Заземление
A12		W0	Интерфейс чтения входных данных Wiegand 0
A13		W1	Интерфейс чтения входных данных Wiegand 1
A14		BZ	Вывод управления бипером считывателя карт
A15		ERR	Индикатор управления выводом считывателя карт (отказ карты)
A16		OK	Индикатор управления выводом считывателя карт (прием карты)

	Контроллер доступа на 1 дверь		
B1	Вход датчика постановки области на охрану	Z1	Терминал доступа 1 для постановки области на охрану
B2		GND	Заземление
B3		Z2	Терминал доступа 2 для постановки области на охрану
B4		Z3	Терминал доступа 3 для постановки области на охрану
B5		GND	Заземление
B6		Z4	Терминал доступа 4 для постановки области на охрану
B7	Электронный замок	D1+	Релейный вход двери 1 (сухой контакт)
B8		D1-	
B9	Вход дверного контакта	S1	Вход датчика дверного контакта двери 1
B10		GND	Заземление
B11	Кнопка открытия двери	B1	Вход кнопки открытия двери 1
B12		GND	Заземление
C1	Питание	12 В	Катод DC 12 В
C2		GND	Заземление
C3	Батарея	BAT+	Катод батареи DC 12 В
C4		BAT-	Анод батареи DC 12 В
C5	Интерфейс RS-485 считывателя карт	RS485A+	Доступ к считывателю карт RS485A+
C6		RS485A-	Доступ к считывателю карт RS485A-
C7		GND	Заземление
C8		RS485B+	Считыватель карт RS485B+
C9		RS485B-	Считыватель карт RS485B-
C10		GND	Заземление

	Контроллер доступа на 1 дверь		
C11	Интерфейс RS485 контроллера доступа	RS485C+	Связь по восходящей линии связи RS485+
C12		RS485C-	Связь по восходящей линии связи RS485-
C13		GND	Заземление
C14		RS 485D+	Зарезервировано
C15		RS 485D-	
C16		GND	
C17	Тревожный выход	NO / NC1	Тревожный релейный выход 1 (сухой контакт)
C18		COM1	
C19		NO / NC2	Тревожный релейный выход 2 (сухой контакт)
C20		COM2	
D1	Вход событий	C2	Тревожный вход событий 2
D2		GND	Заземление
D3		C1	Тревожный вход событий 1

Примечание

- Аппаратный интерфейс тревожного входа нормально разомкнут по умолчанию. Поэтому допускается только нормально открытый сигнал. Он может быть связан с бипером считывателя карт и контроллером доступа, релейным выходом тревоги и релейным выходом двери.
- Привязка тревожного входа при постановке области на охрану выполняется только к тревожному релейному выходу.
- Идентификатор считывателя карт RS-485 должен быть в диапазоне от 1 до 2. В приведенной ниже таблице показана связь номера двери и идентификатора.

Номер двери	Идентификатор считывателя карт (RS-485)	Описание
Дверь 1	1	Вход
	2	Выход

- Для контроллера доступа на 1 дверь связь считывателя карт Wiegand и дверью следующая.

Номер двери	Считыватель карт Wiegand	Описание
Дверь 1	1	Вход
	2	Выход

4.2 Описание разъемов контроллера доступа на 2 двери

Далее представлено описание разъемов контроллера доступа на 2 двери.

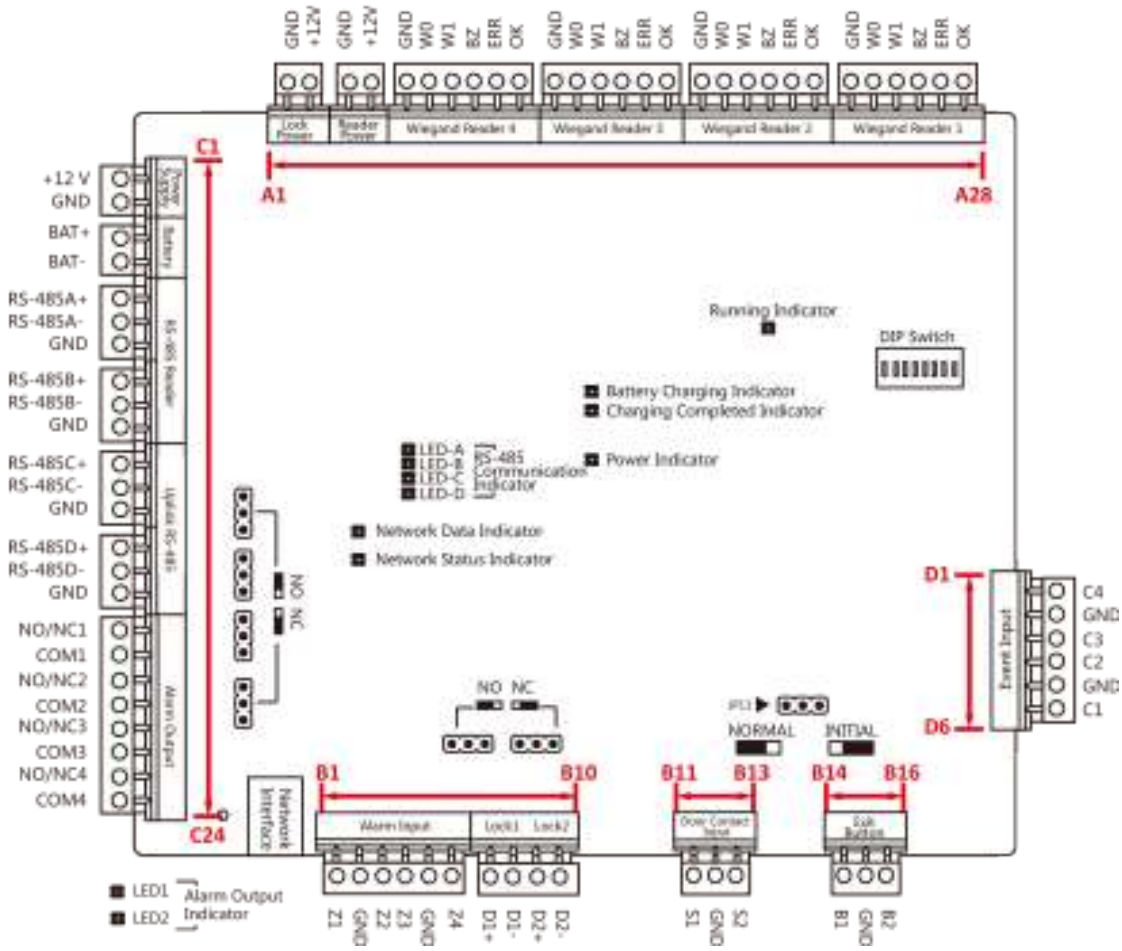


Рисунок 4-2. Основная плата управления контроллера доступа на 2 двери

Английский язык	**Русский язык**
Lock Power	Питание замка
Reader Power	Питание считывателя
Wiegand Reader	Считыватель с Wiegand
Event Input	Вход событий
Exit Button	Кнопка выхода
Door Contact Input	Вход дверного контакта
Lock	Замок
Alarm Input	Тревожный вход
Network Interface	Сетевой интерфейс
Alarm Output	Тревожный выход
Uplink RS-485	Восходящий канал RS-485
RS-485 Reader	Считыватель с RS-485
Battery	Батарея
Power Supply	Питание
NO	Нормально разомкнутый контакт
NC	Нормально замкнутый контакт
Network Data Indicator	Индикатор сетевых данных
Network Status Indicator	Индикатор состояния сети
RS-485 Communication Indicator	Индикатор связи RS-485
Power Indicator	Индикатор питания
Battery Charging Indicator	Индикатор заряда батареи
Charging Completed Indicator	Индикатор завершения зарядки
Running Indicator	Индикатор режима работы
DIP Switch	DIP-переключатель
Normal	Нормальное положение
Initial	Исходное положение
Alarm Output Indicator	Индикатор тревожного выхода
GPRS	GPRS

Таблица 4-2. Описание разъемов контроллера доступа на 2 двери

№	Контроллер доступа на 2 двери		
A1	Питание электронного замка	GND	Заземление
A2		12 В	Питание выхода электронного замка
A3	Питание считывателя карт	GND	Заземление
A4		12 В	Питание выхода считывателя карт
A5	Считыватель карт Wiegand 4	GND	Заземление
A6		W0	Интерфейс чтения входных данных Wiegand 0
A7		W1	Интерфейс чтения входных данных Wiegand 1
A8		BZ	Вывод управления бипером считывателя карт
A9		ERR	Индикатор управления выводом считывателя карт (отказ карты)
A10		OK	Индикатор управления выводом считывателя карт (прием карты)
A11	Считыватель карт Wiegand 3	GND	Заземление
A12		W0	Интерфейс чтения входных данных Wiegand 0
A13		W1	Интерфейс чтения входных данных Wiegand 1
A14		BZ	Вывод управления бипером считывателя карт
A15		ERR	Индикатор управления выводом считывателя карт (отказ карты)
A16		OK	Индикатор управления выводом считывателя карт (прием карты)

№	Контроллер доступа на 2 двери		
A17	Считыватель карт Wiegand 2	GND	Заземление
A18		W0	Интерфейс чтения входных данных Wiegand 0
A19		W1	Интерфейс чтения входных данных Wiegand 1
A20		BZ	Вывод управления бипером считывателя карт
A21		ERR	Индикатор управления выводом считывателя карт (отказ карты)
A22		OK	Индикатор управления выводом считывателя карт (прием карты)
A23	Считыватель карт Wiegand 1	GND	Заземление
A24		W0	Интерфейс чтения входных данных Wiegand 0
A25		W1	Интерфейс чтения входных данных Wiegand 1
A26		BZ	Вывод управления бипером считывателя карт
A27		ERR	Индикатор управления выводом считывателя карт (отказ карты)
A28		OK	Индикатор управления выводом считывателя карт (прием карты)
B1	Вход датчика постановки области на охрану	Z1	Терминал доступа 1 для постановки области на охрану
B2		GND	Заземление
B3		Z2	Терминал доступа 2 для постановки области на охрану
B4		Z3	Терминал доступа 3 для постановки области на охрану

№	Контроллер доступа на 2 двери		
B5	Вход датчика постановки области на охрану	GND	Заземление
B6		Z4	Терминал доступа 4 для постановки области на охрану
B7	Электронный замок 1	D1+	Релейный вход двери 1 (сухой контакт)
B8		D1-	
B9	Электронный замок 2	D2+	Релейный вход двери 2 (сухой контакт)
B10		D2-	
B11	Магнитоконтактный датчик	S1	Вход магнитоконтактного датчика двери 1
B12		GND	Заземление
B13		S2	Вход магнитоконтактного датчика двери 2
B14	Кнопка открытия двери	B1	Вход кнопки открытия двери 1
B15		GND	Заземление
B16		B2	Вход кнопки открытия двери 2
C1	Питание	12 В	Катод DC 12 В
C2		GND	Заземление
C3	Батарея	BAT+	Катод батареи DC 12 В
C4		BAT-	Анод батареи DC 12 В
C5	Интерфейс RS-485 считывателя карт	RS485A+	Доступ к считывателю карт RS485A+
C6		RS485A-	Доступ к считывателю карт RS485A-
C7		GND	Заземление
C8		RS485B+	Считыватель карт RS485B+
C9		RS485B-	Считыватель карт RS485B-
C10		GND	Заземление

№	Контроллер доступа на 2 двери		
C11	Интерфейс RS485 контроллера доступа	RS485C+	Связь по восходящей линии связи RS485+
C12		RS485C-	Связь по восходящей линии связи RS485-
C13		GND	Заземление
C14		RS 485D+	Зарезервировано
C15		RS 485D-	
C16		GND	
C17	Тревожный выход	NO / NC1	Тревожный релейный выход 1 (сухой контакт)
C18		COM1	
C19		NO / NC2	Тревожный релейный выход 2 (сухой контакт)
C20		COM2	
C21		NO / NC3	Тревожный релейный выход 3 (сухой контакт)
C22		COM3	
C23		NO / NC4	Тревожный релейный выход 4 (сухой контакт)
C24		COM4	
D1	Вход событий	C4	Тревожный вход событий 4
D2		GND	Заземление
D3		C3	Тревожный вход событий 3
D4		C2	Тревожный вход событий 2
D5		GND	Заземление
D6		C1	Тревожный вход событий 1

Примечание

- Аппаратный интерфейс тревожного входа нормально разомкнут по умолчанию. Поэтому допускается только нормально открытый сигнал. Он может быть связан с бипером считывателя карт и контроллером доступа, релейным выходом тревоги и релейным выходом двери.
- Привязка тревожного входа при постановке области на охрану выполняется только к тревожному релейному выходу.
- Идентификатор считывателя карт RS-485 должен быть в диапазоне от 1 до 8.

Номер двери	Идентификатор считывателя карт (RS-485)	Описание
Дверь 1	1	Вход
	2	Выход
Дверь 2	3	Вход
	4	Выход

- Для контроллера доступа на 2 двери связь считывателя карт Wiegand и дверью следующая.

Номер двери	Считыватель карт Wiegand	Описание
Дверь 1	1	Вход
	2	Выход
Дверь 2	3	Вход
	4	Выход

4.3 Описание разъемов контроллера доступа на 4 двери

Далее представлено описание разъемов контроллера доступа на 4 двери.

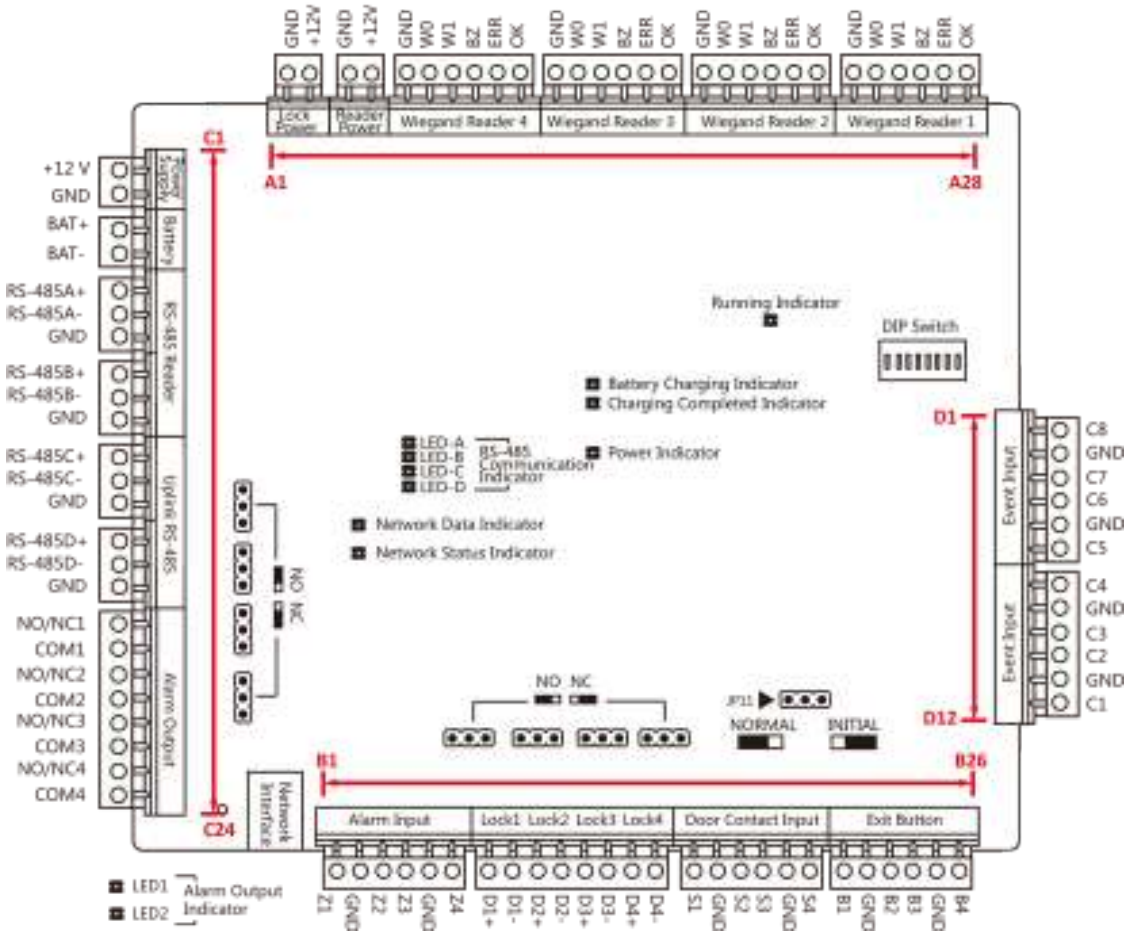


Рисунок 4-3. Основная плата управления контроллера доступа на 4 двери

Английский язык	**Русский язык**
Lock Power	Питание замка
Reader Power	Питание считывателя
Wiegand Reader	Считыватель с Wiegand
Event Input	Вход событий
Exit Button	Кнопка выхода
Door Contact Input	Вход дверного контакта
Lock	Замок
Alarm Input	Тревожный вход
Network Interface	Сетевой интерфейс
Alarm Output	Тревожный выход
Uplink RS-485	Восходящий канал RS-485

Английский язык	**Русский язык**
RS-485 Reader	Считыватель с RS-485
Battery	Батарея
Power Supply	Питание
NO	Нормально разомкнутый контакт
NC	Нормально замкнутый контакт
Network Data Indicator	Индикатор сетевых данных
Network Status Indicator	Индикатор состояния сети
RS-485 Communication Indicator	Индикатор связи RS-485
Power Indicator	Индикатор питания
Battery Charging Indicator	Индикатор заряда батареи
Charging Completed Indicator	Индикатор завершения зарядки
Running Indicator	Индикатор режима работы
DIP Switch	DIP-переключатель
Normal	Нормальное положение
Initial	Исходное положение
Alarm Output Indicator	Индикатор тревожного выхода
GPRS	GPRS

Таблица 4-3. Описание разъемов контроллера доступа на 4 двери

№	**Контроллер доступа на 4 двери**		
A1	Питание электронного замка	GND	Заземление
A2		12 В	Питание выхода электронного замка
A3	Питание считывателя карт	GND	Заземление
A4		12 В	Питание выхода считывателя карт
A5	Считыватель карт Wiegand 4	GND	Заземление
A6		W0	Интерфейс чтения входных данных Wiegand 0

№	Контроллер доступа на 4 двери		
A7		W1	Интерфейс чтения входных данных Wiegand 1
A8		BZ	Вывод управления бипером считывателя карт
A9		ERR	Индикатор управления выводом считывателя карт (отказ карты)
A10		OK	Индикатор управления выводом считывателя карт (прием карты)
A11	Считыватель карт Wiegand 3	GND	Заземление
A12		W0	Интерфейс чтения входных данных Wiegand 0
A13		W1	Интерфейс чтения входных данных Wiegand 1
A14		BZ	Вывод управления бипером считывателя карт
A15		ERR	Индикатор управления выводом считывателя карт (отказ карты)
A16		OK	Индикатор управления выводом считывателя карт (прием карты)
A17	Считыватель карт Wiegand 2	GND	Заземление
A18		W0	Интерфейс чтения входных данных Wiegand 0
A19		W1	Интерфейс чтения входных данных Wiegand 1
A20		BZ	Вывод управления бипером считывателя карт
A21		ERR	Индикатор управления выводом считывателя карт (отказ карты)

№	Контроллер доступа на 4 двери		
A22		OK	Индикатор управления выводом считывателя карт (прием карты)
A23	Считыватель карт Wiegand 1	GND	Заземление
A24		W0	Интерфейс чтения входных данных Wiegand 0
A25		W1	Интерфейс чтения входных данных Wiegand 1
A26		BZ	Вывод управления бипером считывателя карт
A27		ERR	Индикатор управления выводом считывателя карт (отказ карты)
A28		OK	Индикатор управления выводом считывателя карт (прием карты)
B1	Вход датчика постановки области на охрану	Z1	Терминал доступа 1 для постановки области на охрану
B2		GND	Заземление
B3		Z2	Терминал доступа 2 для постановки области на охрану
B4		Z3	Терминал доступа 3 для постановки области на охрану
B5		GND	Заземление
B6		Z4	Терминал доступа 4 для постановки области на охрану
B7	Электронный замок 1	D1+	Релейный вход двери 1 (сухой контакт)
B8		D1-	
B9	Электронный замок 2	D2+	Релейный вход двери 2 (сухой контакт)
B10		D2-	
B11	Электронный замок 3	D3+	Релейный вход двери 3 (сухой контакт)
B12		D3-	

№	Контроллер доступа на 4 двери		
B13	Электронный замок 4	D4+	Релейный вход двери 4 (сухой контакт)
B14		D4-	
B15	Магнитоконтактный датчик	S1	Вход магнитоконтактного датчика двери 1
B16		GND	Заземление
B17		S2	Вход магнитоконтактного датчика двери 2
B18		S3	Вход магнитоконтактного датчика двери 3
B19		GND	Заземление
B20		S4	Вход магнитоконтактного датчика двери 4
B21	Кнопка открытия двери	B1	Вход кнопки открытия двери 1
B22		GND	Заземление
B23		B2	Вход кнопки открытия двери 2
B24		B3	Вход кнопки открытия двери 3
B25		GND	Заземление
B26		B4	Вход кнопки открытия двери 4
C1	Питание	12 В	Катод DC 12 В
C2		GND	Заземление
C3	Батарея	BAT+	Катод батареи DC 12 В
C4		BAT-	Анод батареи DC 12 В
C5	Интерфейс RS-485 считывателя карт	RS485A+	Доступ к считывателю карт RS485A+
C6		RS485A-	Доступ к считывателю карт RS485A-
C7		GND	Заземление

№	Контроллер доступа на 4 двери		
C8		RS485B+	Считыватель карт RS485B+
C9		RS485B-	Считыватель карт RS485B-
C10		GND	Заземление
C11	Интерфейс RS485 контроллера доступа	RS485C+	Связь по восходящей линии связи RS485+
C12		RS485C-	Связь по восходящей линии связи RS485-
C13		GND	Заземление
C14		RS 485D+	Зарезервировано
C15		RS 485D-	
C16		GND	
C17	Тревожный выход	NO / NC1	Тревожный релейный выход 1 (сухой контакт)
C18		COM1	
C19		NO / NC2	Тревожный релейный выход 2 (сухой контакт)
C20		COM2	
C21		NO / NC3	Тревожный релейный выход 3 (сухой контакт)
C22		COM3	
C23		NO / NC4	Тревожный релейный выход 4 (сухой контакт)
C24		COM4	
D1	Вход событий	C8	Тревожный вход событий 8
D2		GND	Заземление
D3		C7	Тревожный вход событий 7
D4		C6	Тревожный вход событий 6
D5		GND	Заземление
D6		C5	Тревожный вход событий 5
D7		C4	Тревожный вход событий 4
D8		GND	Заземление
D9		C3	Тревожный вход событий 3
D10		C2	Тревожный вход событий 2

№	Контроллер доступа на 4 двери		
D11		GND	Заземление
D12		C1	Тревожный вход событий 1

Примечание

- Аппаратный интерфейс тревожного входа нормально разомкнут по умолчанию. Поэтому допускается только нормально открытый сигнал. Он может быть связан с бипером считывателя карт и контроллером доступа, релейным выходом тревоги и релейным выходом двери.
- Привязка тревожного входа при постановке области на охрану выполняется только к тревожному релейному выходу.
- Идентификатор считывателя карт RS-485 должен быть в диапазоне от 1 до 8.

Номер двери	Идентификатор считывателя карт (RS-485)	Описание
Дверь 1	1	Вход
	2	Выход
Дверь 2	3	Вход
	4	Выход
Дверь 3	5	Вход
	6	Выход
Дверь 4	7	Вход
	8	Выход

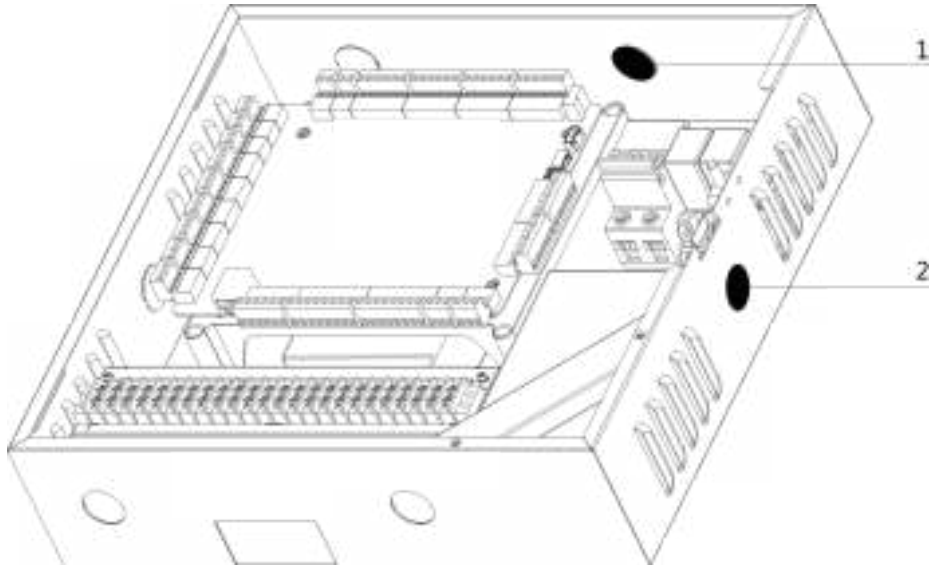
- Для контроллера доступа на 4 двери связь считывателя карт Wiegand и дверью следующая.

Номер двери	Считыватель карт Wiegand	Описание
Дверь 1	1	Вход
	/	Выход
Дверь 2	2	Вход
	/	Выход
Дверь 3	3	Вход
	/	Выход
Дверь 4	4	Вход
	/	Выход

Раздел 5. Подключение

Предупреждение

Кабель высокого напряжения следует пропустить через отверстие 1 и отверстие 2. Во избежание повреждения кабеля и поражения электрическим током на отверстия 1 и 2 должны быть установлены резиновые прокладки.



5.1 Внешние разъемы

5.1.1 Описание разъемов контроллера доступа на 1 дверь

Далее представлена схема разъемов контроллера доступа на 1 дверь.

Рисунок 5-1. Разъемы контроллера доступа на 1 дверь

Английский язык	Русский язык
+12V	+12 В
GND	Заземление
RS-485	RS-485
W	Wiegand
Lock	Замок
Door Magnetic	Магнитоконтактный датчик двери
Exit Button	Кнопка выхода
Fire Alarm Interface	Модуль обнаружения возгораний

5.1.2 Описание разъемов контроллера доступа на 2 двери

Далее представлена схема разъемов контроллера доступа на 2 двери.

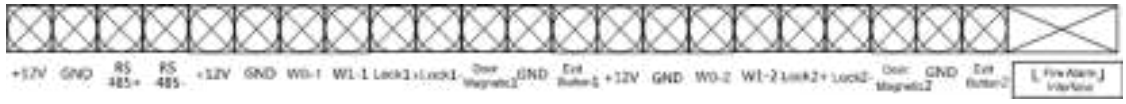


Рисунок 5-2. Разъемы контроллера доступа на 2 двери

Английский язык	**Русский язык**
+12V	+12 В
GND	Заземление
RS-485	RS-485
W	Wiegand
Lock	Замок
Door Magnetic	Магнитоконтактный датчик двери
Exit Button	Кнопка выхода
Fire Alarm Interface	Модуль обнаружения возгораний

5.1.3 Описание разъемов контроллера доступа на 4 двери

Далее представлена схема разъемов контроллера доступа на 4 двери.

Рисунок 5-3. Разъемы контроллера доступа на 4 двери

Английский язык	**Русский язык**
+12V	+12 В
GND	Заземление
RS-485	RS-485
W	Wiegand
Lock	Замок
Door Magnetic	Магнитоконтактный датчик двери
Exit Button	Кнопка выхода
Fire Alarm Interface	Модуль обнаружения возгораний

5.2 Подключение считывателя карт Wiegand

Далее представлена схема подключения считывателя карт Wiegand.

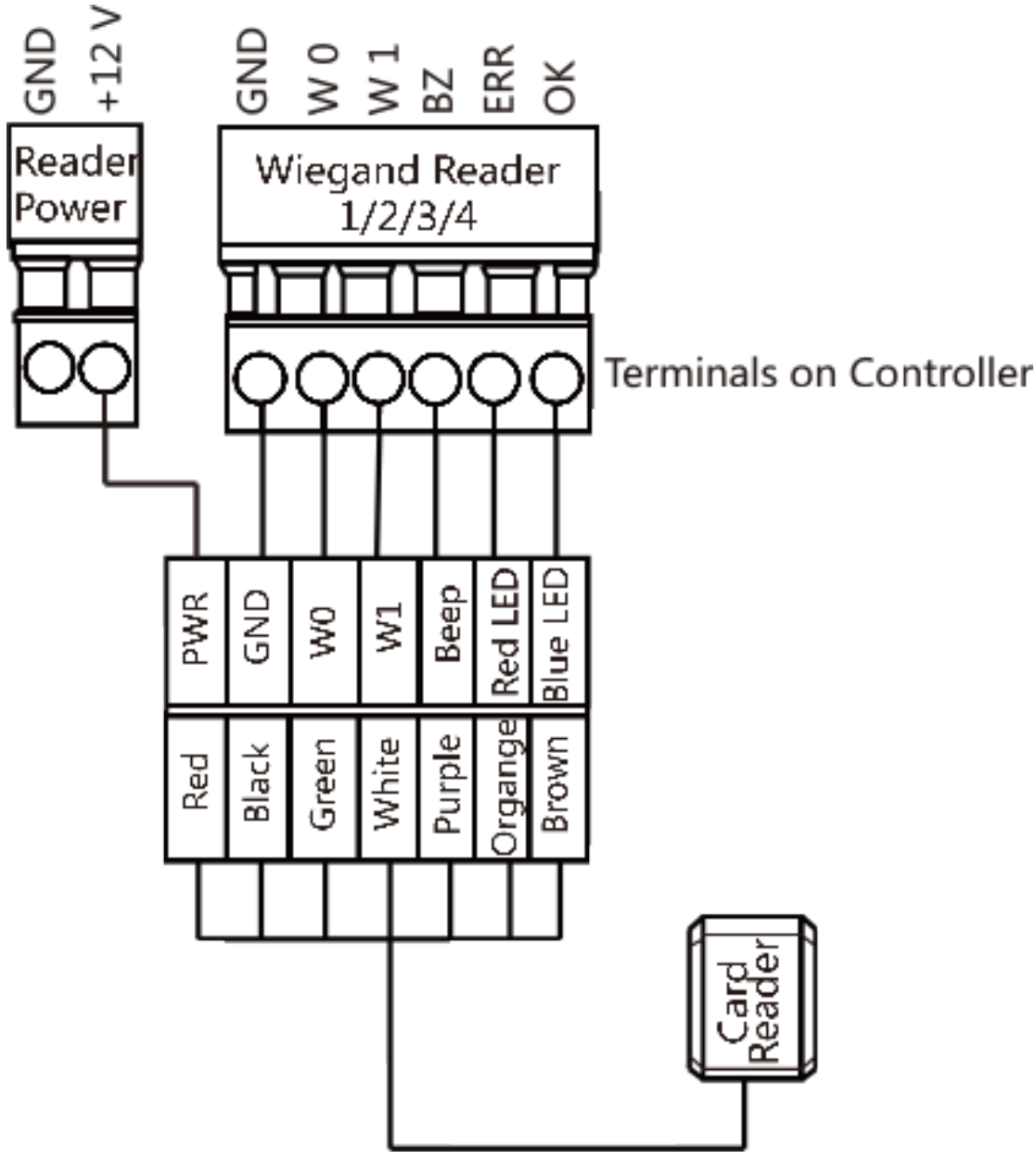


Рисунок 5-4. Схема подключения считывателя карт Wiegand

Английский язык	**Русский язык**
+12V	+12 В
GND	Заземление
RS-485	RS-485
W	Wiegand
BZ	Бипер

Английский язык	**Русский язык**
ERR	Ошибка
OK	ОК
Reader Power	Питание считывателя
Wiegand Reader	Считыватель с Wiegand
Terminals on Controller	Разъемы контроллера
Red	Красный
Black	Черный
Green	Зеленый
White	Белый
Purple	Фиолетовый
Orange	Оранжевый
Brown	Коричневый
Card Reader	Считыватель карт

Примечание

При использовании контроллера доступа для управления светодиодом и бипером считывателя карт Wiegand необходимо подключить разъемы OK / ERR / BZ.

5.3 Подключение считывателя карт RS-485

Далее представлена схема подключения считывателя карт RS-485.

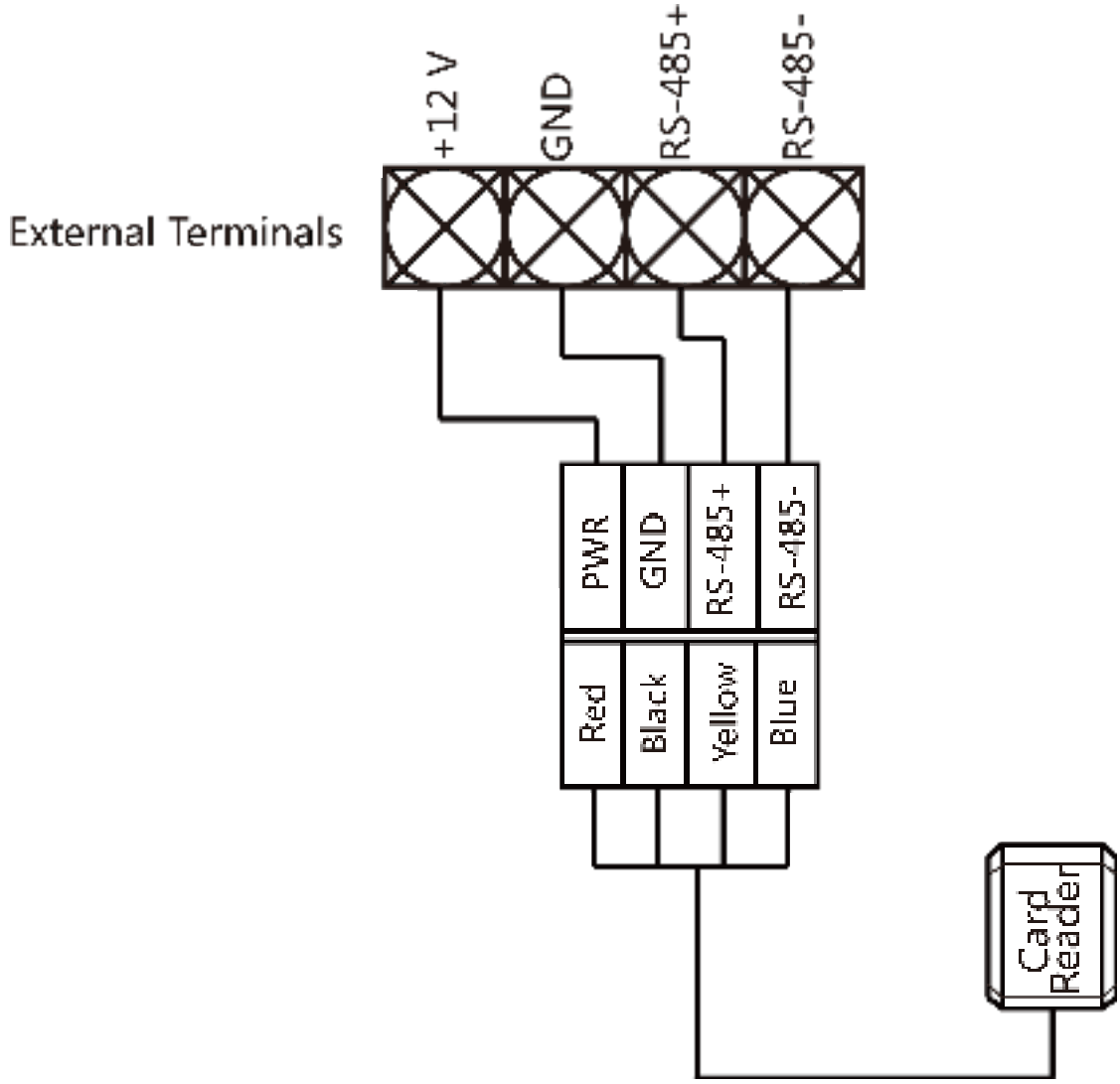


Рисунок 5-5. Схема подключения считывателя карт RS-485

Английский язык	**Русский язык**
+12V	+12 В
GND	Заземление
RS-485	RS-485
External Terminals	Внешние разъемы
PWR	Питание
Red	Красный
Black	Черный
Yellow	Желтый
Blue	Синий
Card Reader	Считыватель карт

Примечание

Если считыватель карт установлен слишком далеко от контроллера доступа, можно использовать внешний источник питания.

5.4 Подключение катодного замка

Далее представлена схема подключения катодного замка.

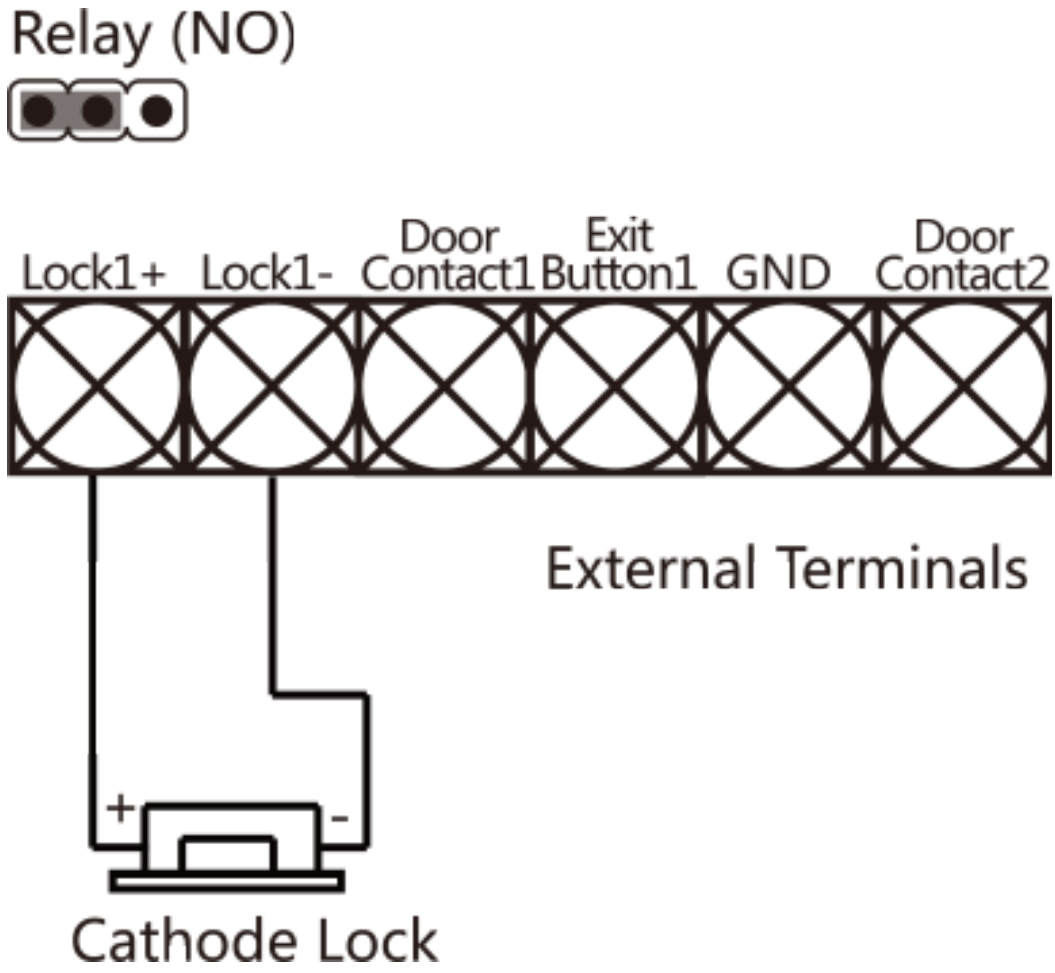


Рисунок 5-6. Схема подключения катодного замка

Английский язык	**Русский язык**
Relay (NO)	Реле (NO)
Lock	Замок
Door Contact	Дверной контакт
Exit Button	Кнопка выхода
GND	Заземление
External Terminals	Внешние разъемы
Cathode Lock	Катодный замок

5.5 Подключение анодного замка

Далее представлена схема подключения анодного замка.

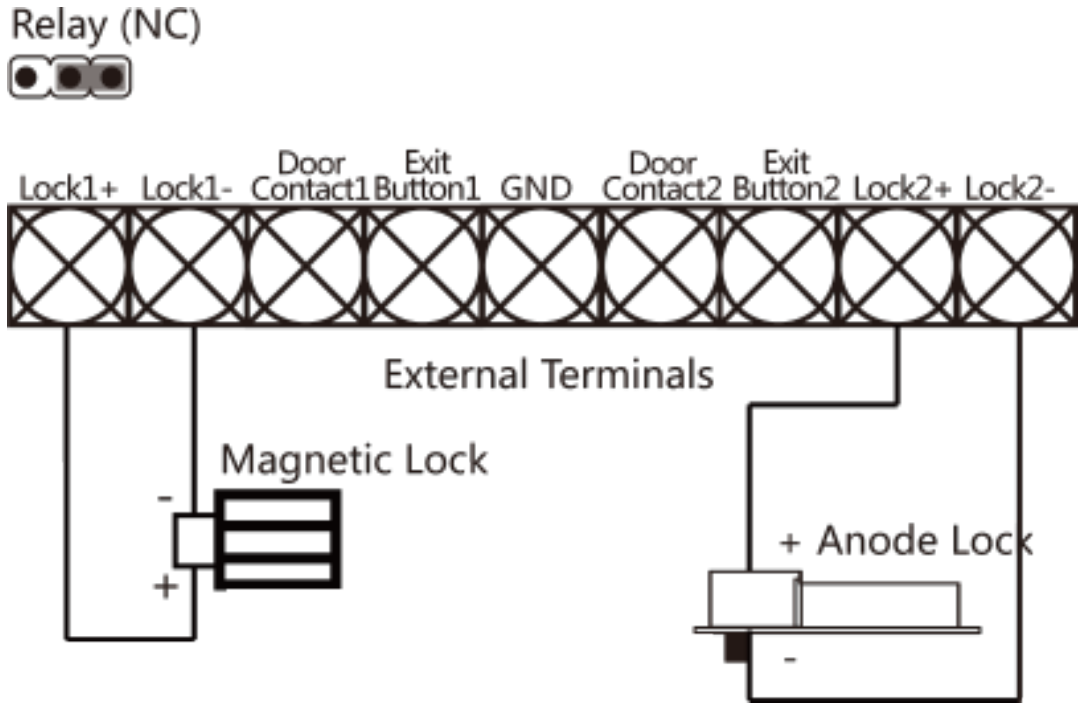


Рисунок 5-7. Схема подключения анодного замка

Английский язык	**Русский язык**
Relay (NC)	Реле (NC)
Lock	Замок
Door Contact	Дверной контакт
Exit Button	Кнопка выхода
GND	Заземление
External Terminals	Внешние разъемы
Magnetic Lock	Электромагнитный замок
Anode Lock	Анодный замок

5.6 Подключение внешнего тревожного устройства

Далее представлена схема подключения внешнего тревожного устройства.

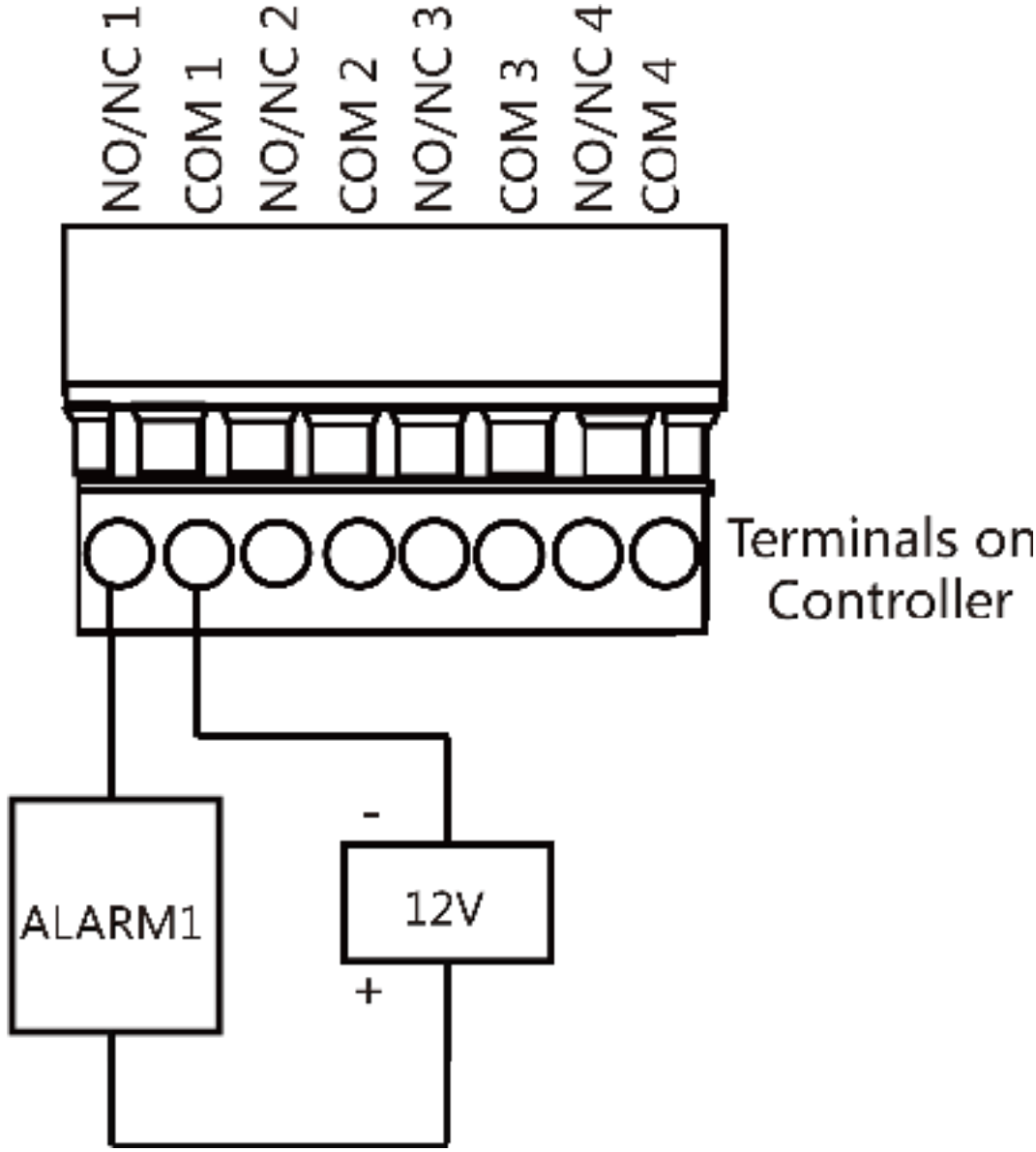


Рисунок 5-8. Подключение внешнего тревожного устройства

Английский язык	**Русский язык**
NO	Нормально открытый
NC	Нормально закрытый
COM	Общий
Terminals on Controller	Разъемы контроллера
Alarm	Тревога
12V	12 В

5.7 Подключение кнопки выхода

Далее представлена схема подключения кнопки выхода.

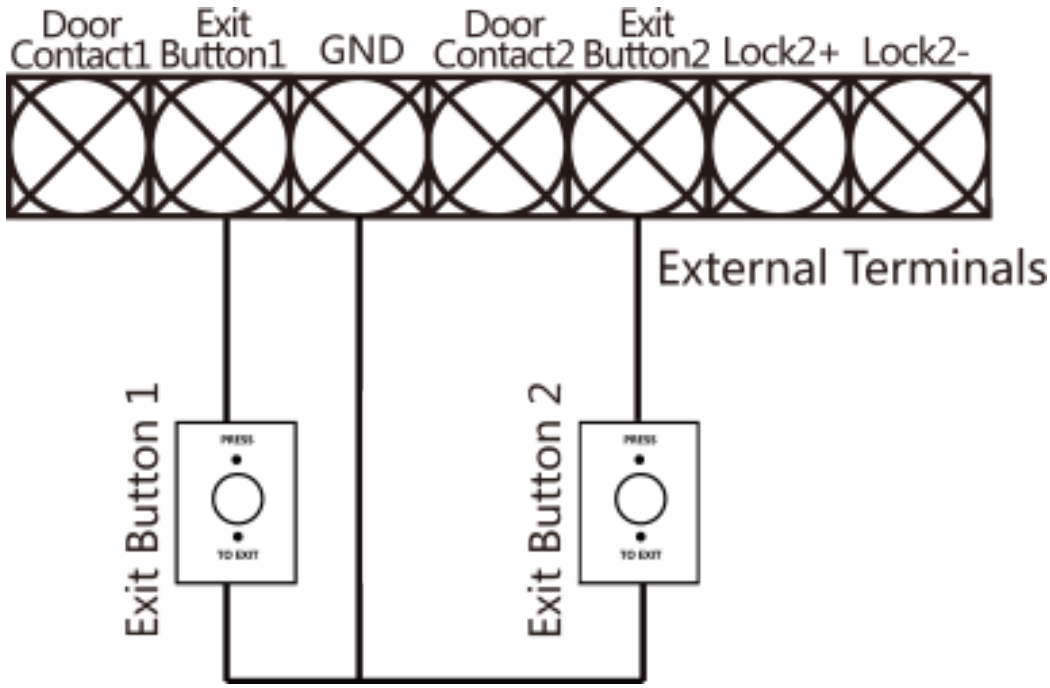


Рисунок 5-9. Подключение кнопки выхода

Английский язык	**Русский язык**
Door Contact	Дверной контакт
Exit Button	Кнопка выхода
GND	Заземление
Lock	Замок
External Terminals	Внешние разъемы

5.8 Подключение дверного контакта

Далее представлена схема подключения дверного контакта.

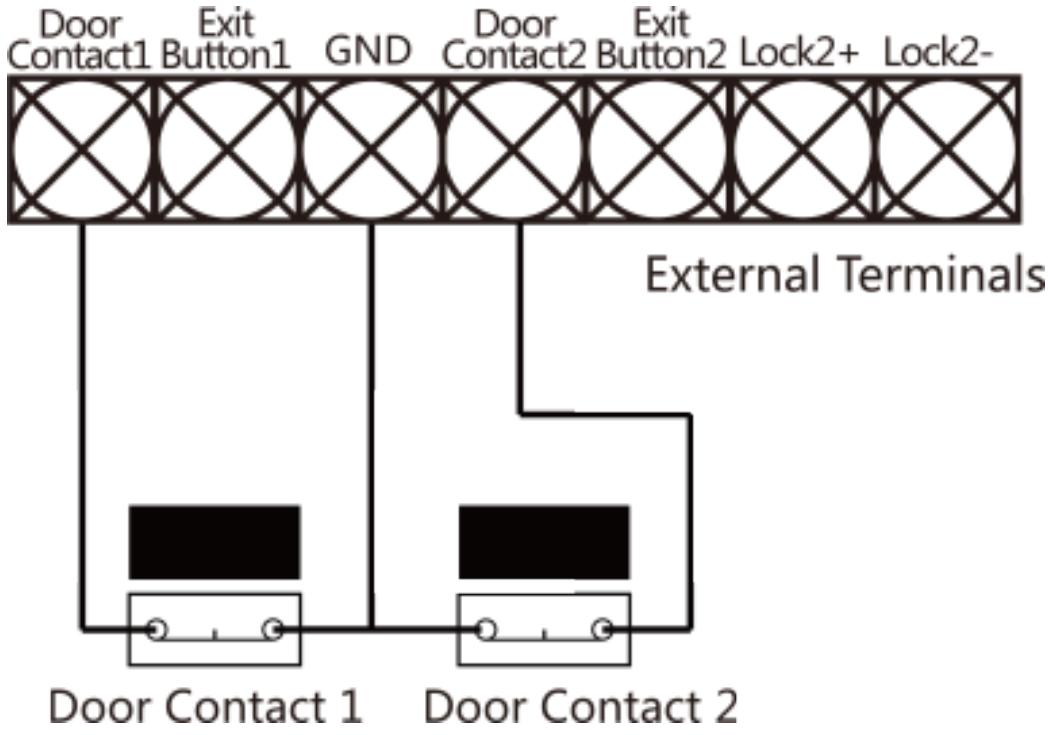


Рисунок 5-10. Подключение дверного контакта

Английский язык	**Русский язык**
Door Contact	Дверной контакт
Exit Button	Кнопка выхода
GND	Заземление
Lock	Замок
External Terminals	Внешние разъемы

5.9 Подключение источника питания

Далее представлена схема подключения источника питания.

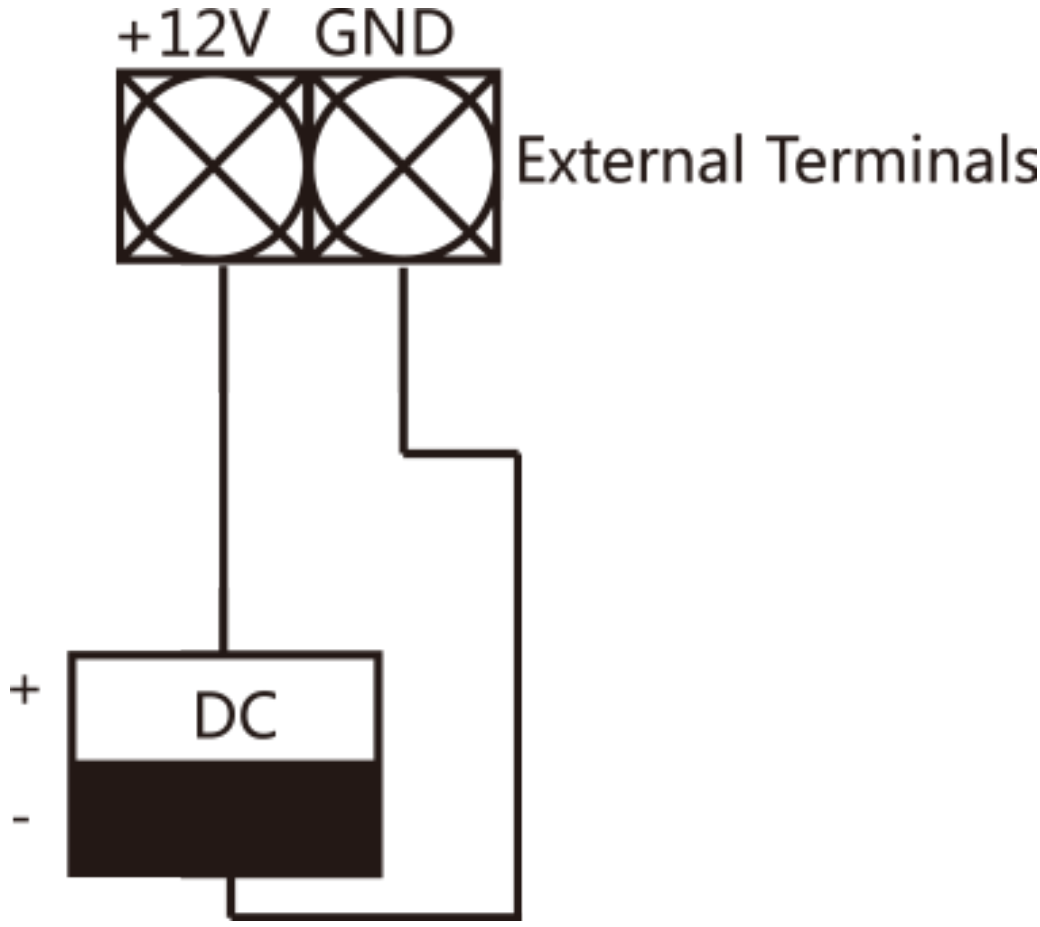


Рисунок 5-11. Подключение источника питания

Английский язык	**Русский язык**
+12V	+12 В
GND	Заземление
DC	Постоянный ток
External Terminals	Внешние разъемы

5.10 Подключение датчика для постановки области на охрану

5.10.1 Подключение датчика для постановки области на охрану: подключение NO (нормально разомкнутый контакт)

Далее представлена схема NO подключения датчика для постановки области на охрану.

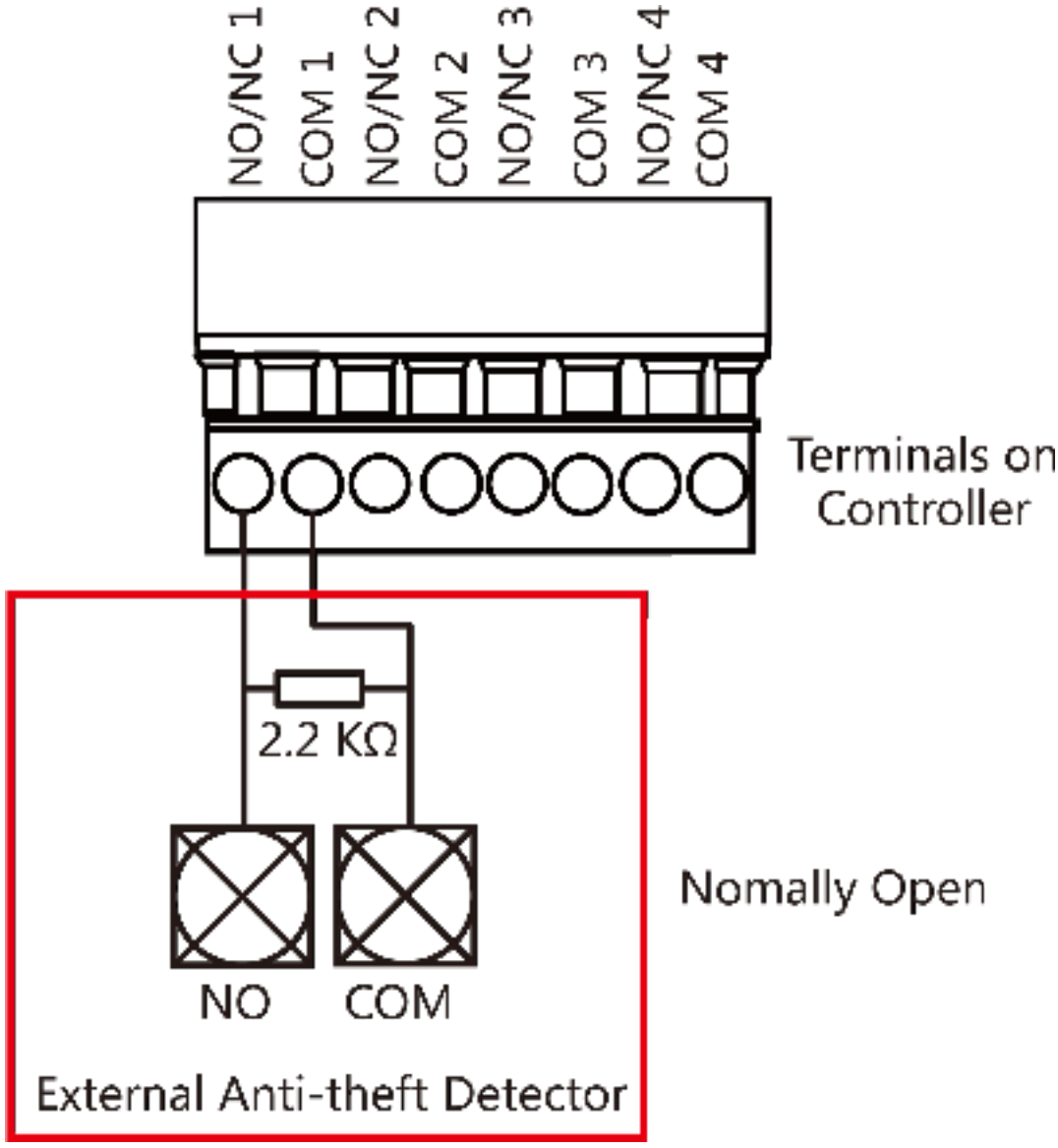


Рисунок 5-12. Подключение NO

Английский язык	**Русский язык**
NO	Нормально открытый
NC	Нормально закрытый
COM	Общий
Terminals on Controller	Разъемы контроллера
External Anti-theft Detector	Внешний датчик предотвращения кражи

5.10.2 Подключение датчика для постановки области на охрану: подключение NC (нормально замкнутый контакт)

Далее представлена схема NC подключения датчика для постановки области на охрану.

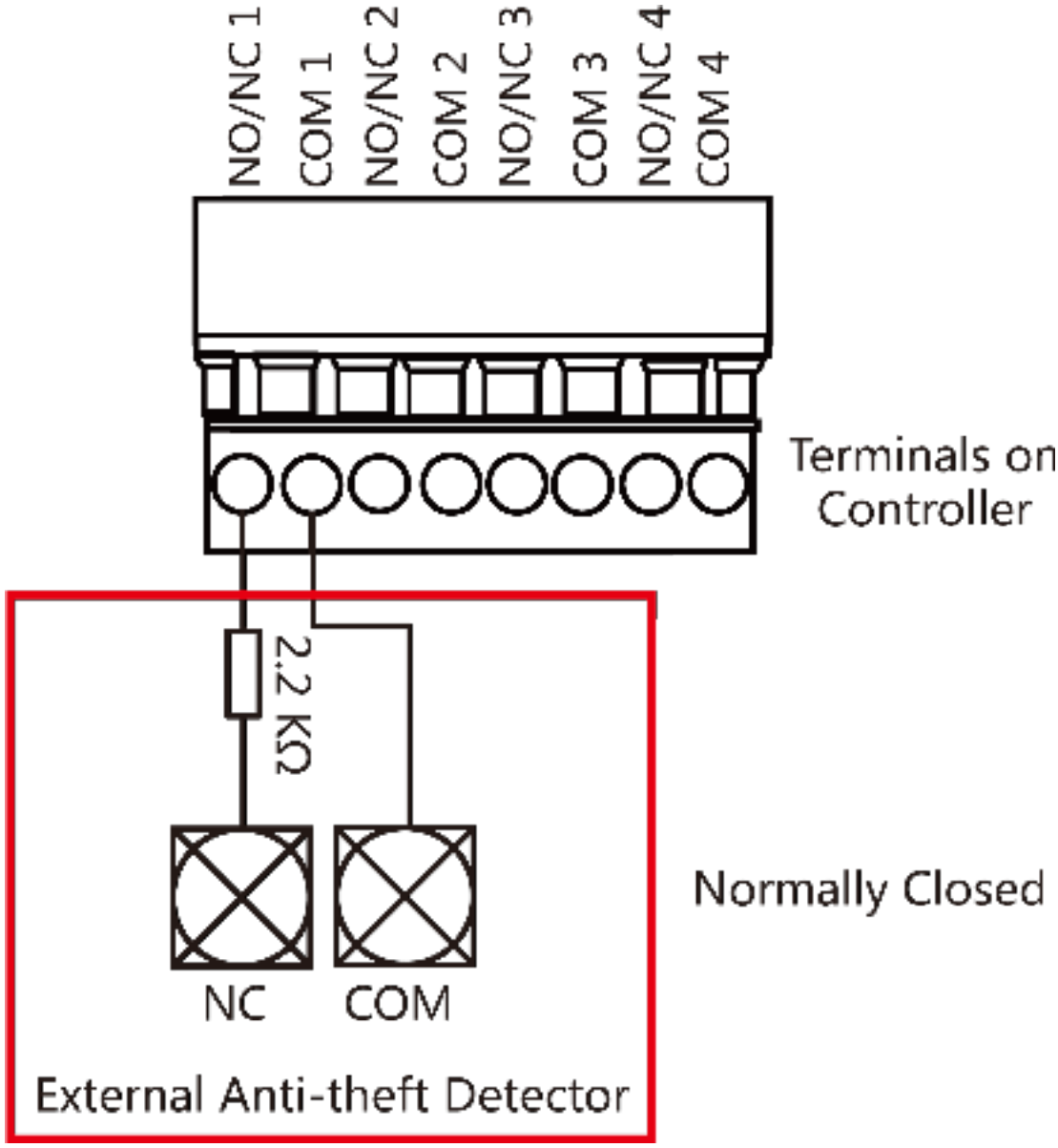


Рисунок 5-13. Подключение NC

Английский язык	**Русский язык**
NO	Нормально открытый
NC	Нормально закрытый
COM	Общий
Terminals on Controller	Разъемы контроллера
External Anti-theft Detector	Внешний датчик предотвращения кражи

5.11 Подключение модуля пожарной тревоги

Далее представлена схема подключения модуля обнаружения возгораний.

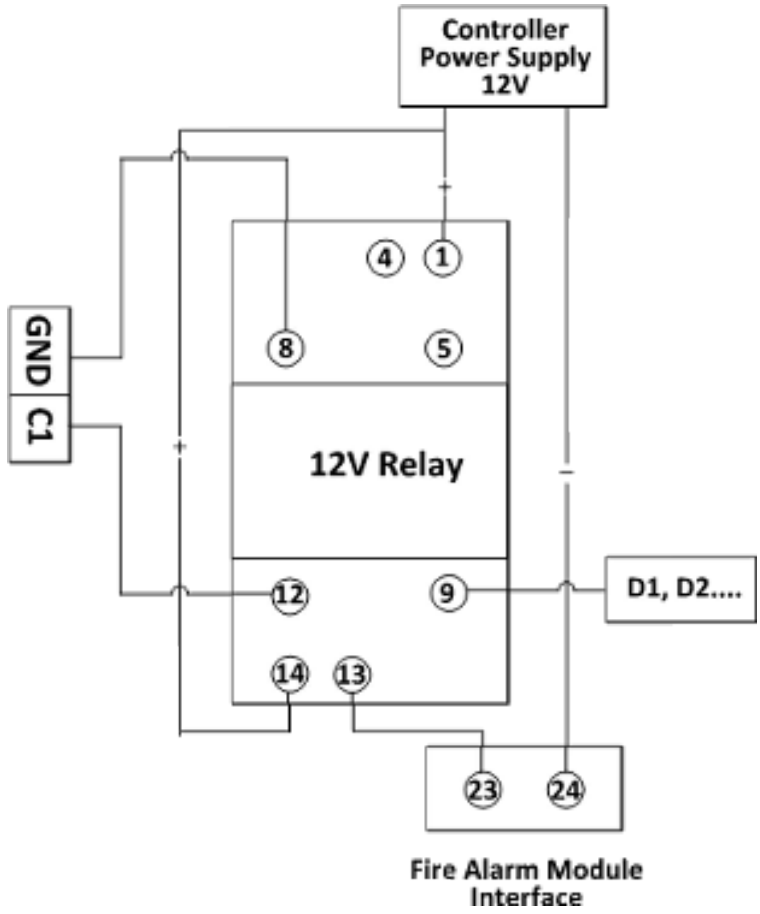


Рисунок 5-14. Подключение модуля обнаружения возгораний

Английский язык	**Русский язык**
Controller Power Supply 12V	Питание контроллера 12 В
12V Relay	Реле 12 В
GND	Заземление
Fire Alarm Module Interface	Модуль обнаружения возгораний

Раздел 6. Настройки

6.1 Инициализация устройства (вариант 1)

Инициализацию устройства можно выполнить с помощью колпачковой перемычки.

Шаги

1. Переведите колпачковую перемычку из положения **Normal** («Нормальное положение»).
2. Отключите питание и перезапустите контроллер доступа. Бипер контроллера издаст длинный звуковой сигнал.
3. Когда звуковой сигнал прекратится, верните колпачковую перемычку обратно в положение **Normal** («Нормальное положение»).
4. Отключите питание и перезапустите контроллер доступа.

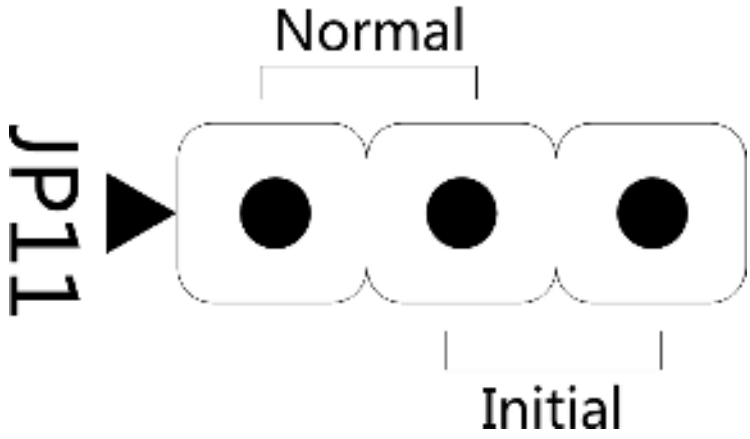


Рисунок 6-1. Колпачковая перемычка контакта инициализации

Английский язык	Русский язык
Normal	Нормальное положение
Initial	Исходное положение

Примечание

Инициализация устройства восстановит все параметры до значений по умолчанию, и все события устройства будут удалены.

6.2 Инициализация устройства (вариант 2)

Инициализацию устройства можно выполнить с помощью колпачковой перемычки.

Шаги

1. Переместите колпачковую перемычку из положения **Normal** («Нормальное положение») в положение **Initial** («Исходное положение»).
2. Отключите питание и перезапустите контроллер доступа. Бипер контроллера издаст длинный звуковой сигнал.

3. Когда звуковой сигнал прекратится, верните колпачковую перемычку обратно в положение **Normal** («Норма»).
4. Отключите питание и перезапустите контроллер доступа.

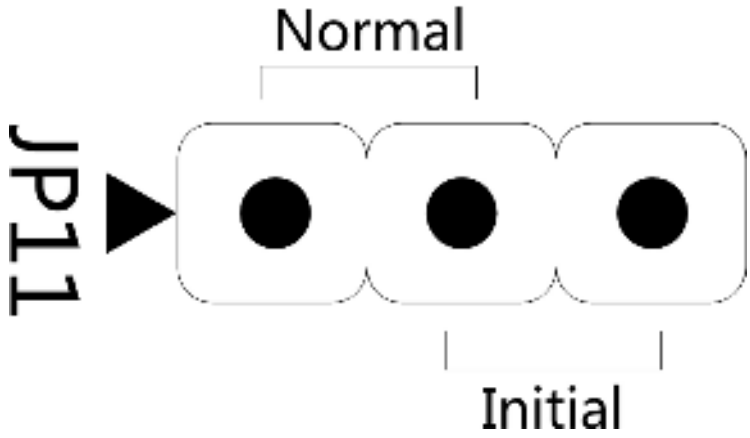


Рисунок 6-2. Колпачковая перемычка контакта инициализации

Английский язык	Русский язык
Normal	Нормальное положение
Initial	Исходное положение

Примечание

Инициализация устройства восстановит все параметры до значений по умолчанию, и все события устройства будут удалены.

6.3 Настройки релейного выхода NO / NC

6.3.1 Настройки релейного выхода замка

Далее представлено состояние подключения релейного выхода замка (NO / NC).

Состояние подключения реле замка (NO)

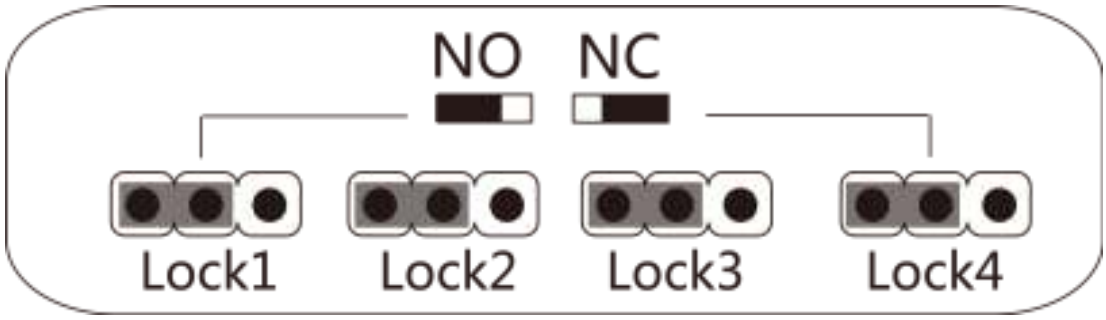


Рисунок 6-3. Состояние NO

Английский язык	Русский язык
Lock	Замок

Состояние подключения реле замка (NC)

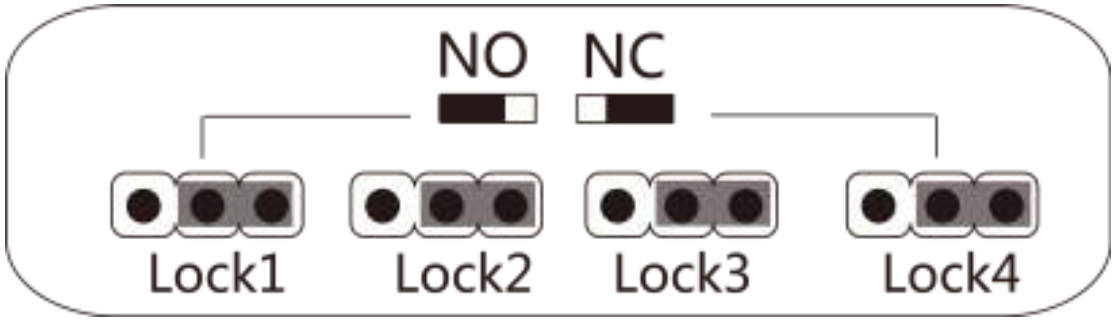


Рисунок 6-4. Состояние NC

Английский язык	Русский язык
Lock	Замок

6.3.2 Настройки тревожного релейного выхода

Далее представлено состояние подключения релейного выхода замка (NO / NC).

Состояние подключение тревожного релейного выхода (NO)

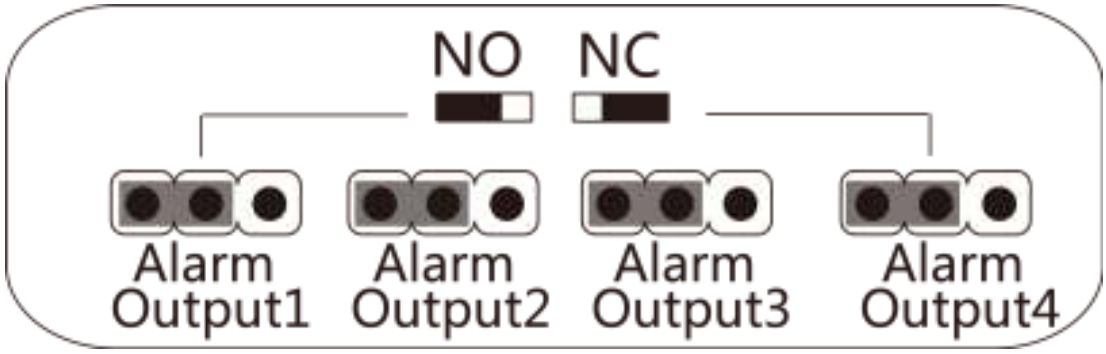


Рисунок 6-5. Состояние NO

Английский язык	Русский язык
Alarm Output	Тревожный выход

Состояние тревожного релейного выхода (NC)

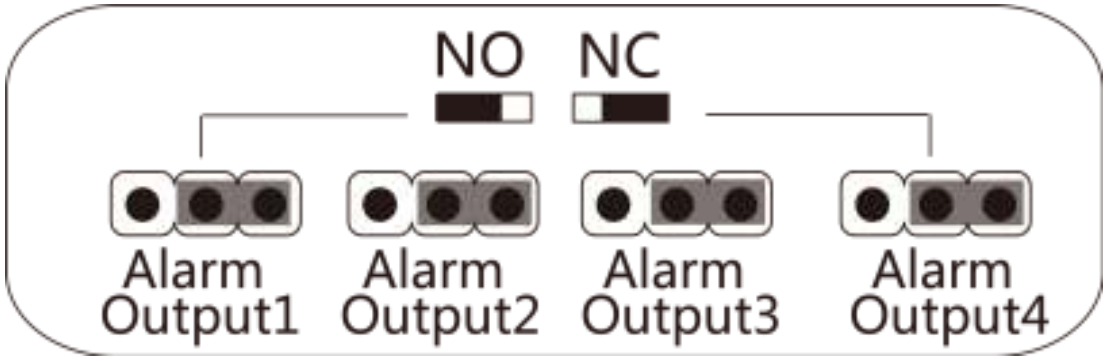


Рисунок 6-6. Состояние NC

Английский язык	**Русский язык**
Alarm Output	Тревожный выход

Раздел 7. Активация

Перед первым входом в систему необходимо активировать устройство. После включения устройства система переключится на страницу активации устройства.

Поддерживается активация через само устройство, активация при помощи ПО SADP и при помощи клиентского ПО. Значения по умолчанию для устройства следующие:

- IP-адрес по умолчанию: 192.0.0.64
- № порта по умолчанию: 8000
- Имя пользователя по умолчанию: admin

7.1 Активация через SADP

Программное обеспечение SADP — это инструмент для обнаружения, активации и изменения IP-адреса устройства через локальную сеть.

Перед началом

- ПО SADP загружено на диск, поставляемый в комплекте, также его можно скачать с официального сайта ***http:// www.hikvision.com/en/***. Установите ПО SADP в соответствии с инструкцией.
- Устройство и ПК, на котором запущено ПО SADP, должны находиться в одной подсети.

Следующие шаги показывают, как активировать устройство и изменить его IP-адрес. Для получения подробной информации о пакетной активации и изменении IP-адресов смотрите ***Руководство пользователя ПО SADP*.**

Шаги

1. Запустите ПО SADP для поиска онлайн устройств.

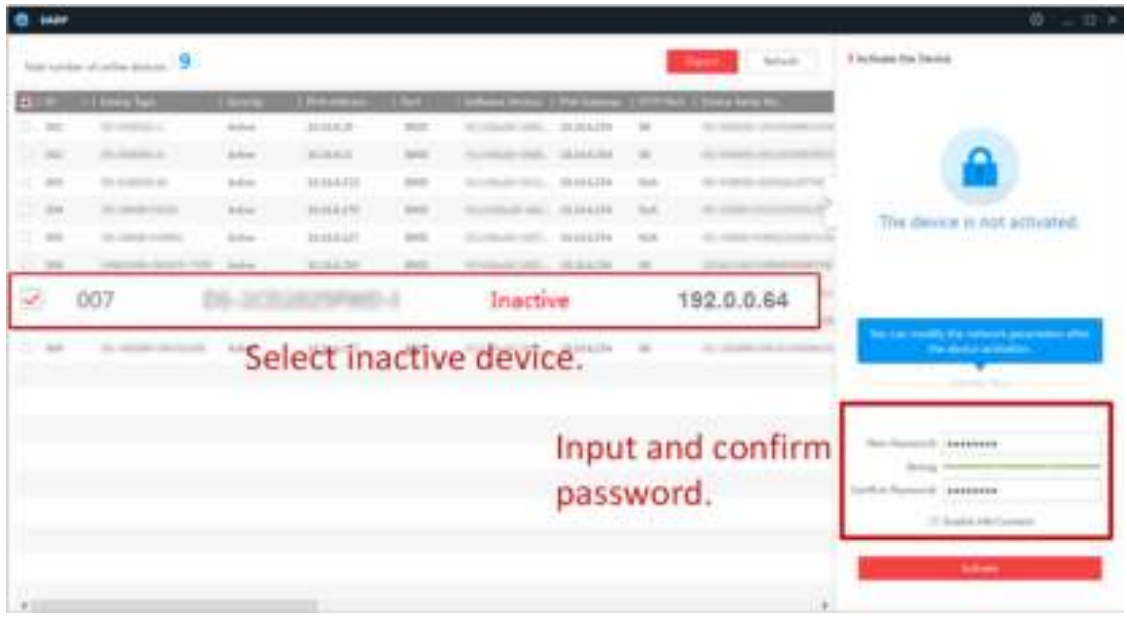
2. Найдите и выберите устройство в списке онлайн устройств.

3. Введите новый пароль (пароль администратора) и подтвердите его.

Предостережение

РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ — настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

4. Нажмите **Activate** («Активировать») для начала активации.



После успешной активации статус устройства изменится на **Active** («Активно»).

5. Измените IP-адрес устройства.
   1) Выберите устройство.
   2) Измените IP-адрес устройства на адрес в той же подсети, к которой подключен компьютер вручную или поставив галочку **Enable DHCP** («Включить DHCP»).
   3) Введите пароль администратора и нажмите **Modify** («Изменить») для изменения IP-адреса.

7.2 Активация устройства через клиентское ПО

Для исправной работы некоторых устройств необходимо создать пароль активации, прежде чем добавлять их в систему.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Перейдите на страницу **Device Management** («Управление устройством»).
2. Нажмите в правой части экрана на странице **Device Management** («Управление устройством») и выберите **Device** («Устройство»).
3. Нажмите **Online Device** («Онлайн устройства»), чтобы отобразить область онлайн устройств. Искомые онлайн устройства отобразятся в списке.
4. Проверьте состояние устройства (отображено в столбце **Security Level** («Уровень безопасности»)) и выберите неактивное устройство.
5. Нажмите **Activate** («Активировать»), чтобы открыть окно активации.
6. Создайте и введите новый пароль в поле **Password** («Пароль») и подтвердите его в поле **Confirm Password** («Подтвердить пароль»).

Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

7. Для активации устройства нажмите **OK**.

Раздел 8. Настройка клиентского ПО

8.1 Работа с клиентским ПО

Контроллер доступа обеспечивает реализацию множества функций, включая управление сотрудниками / посетителями, картами, настройку разрешений и другие расширенные

Примечание

функции.

Для пользователя с разрешениями модуля контроля доступа: вход в модуль **Access Control** («Контроль доступа») и настройка параметров контроля доступа. Информация по настройке прав пользователей для контроллера доступа представлена в разделе *Управление учетной записью Руководства пользователя клиентского программного обеспечения iVMS-4200.*

8.1.1 Добавление устройства

После запуска клиента к клиенту следует добавить устройства для удаленной настройки и управления.

После добавления устройств можно выбрать устройство и нажать **Remote Configuration** («Удаленная настройка»), чтобы при необходимости настроить дополнительные параметры

Примечание

выбранного устройства.

Для некоторых моделей устройств можно открыть окно настройки общих или дополнительных параметров. Чтобы открыть исходное окно удаленной настройки, нажмите **CTRL** и выберите **Remote Configuration** («Удаленная настройка»).

После добавления устройств контроля доступа можно выбрать устройство из списка и нажать **Device Status** («Состояние устройства»), чтобы просмотреть состояние устройства.

Добавление онлайн устройства

Активные онлайн устройства, которые находятся в одной локальной подсети с клиентским ПО, будут отображены в области **Online Device** («Онлайн устройства»). Нажмите кнопку **Refresh Every 60s** («Обновлять каждые 60 с»), чтобы обновлять информацию об активных устройствах.

Добавление одного онлайн устройства

В клиентское ПО можно добавить одно онлайн устройство.

Для добавления онлайн устройств необходимо выполнить следующие действия.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).

2. Нажмите **Device** («Устройство») и выберите **Hikvision Device** («Устройство Hikvision») в качестве устройства для отображения в поле **Online Device** («Онлайн устройство»).

Рисунок 8-1. Онлайн устройство

3. Выберите онлайн устройство в поле **Online Device** («Онлайн устройство»).

Примечание

Прежде чем правильно добавить неактивное устройство необходимо создать для него пароль. Подробная информация представлена в разделе ***Активация***.

4. Нажмите **Add to Client** («Добавить в клиент»), чтобы открыть окно добавления устройства.
5. Введите необходимую информацию.

Адрес

Введите IP-адрес устройства. IP-адреса устройств получаются автоматически в данном режиме добавления.

Порт

Значение по умолчанию: 8000.

Имя пользователя

По умолчанию имя пользователя: admin.

Пароль

Введите пароль устройства.

Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным. Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

6. **Опционально.** После добавления устройства в клиентское ПО нажмите **Synchronize Device Time** («Синхронизировать время устройства»), чтобы синхронизировать время устройства со временем компьютера, на котором работает клиентское ПО.

7. **Опционально.** Нажмите **Export to Group** («Экспортировать в группу»), чтобы создать группу по названию устройства.

По умолчанию можно импортировать все каналы устройства в соответствующую группу.

8. **Опционально.** Добавьте автономные устройства.
   1) Нажмите **Add Offline Device** («Добавление автономных устройств»).
   2) Введите необходимую информацию, в том числе номер канала устройства и номер тревожного входа.
   3) Нажмите **Add** («Добавить»).

   Когда автономное устройство подключается к сети, программное обеспечение подключает его автоматически.
9. Нажмите **Add** («Добавить») для добавления устройств.

Добавление нескольких онлайн устройств

В клиентское ПО можно добавить несколько онлайн устройств.

Для добавления нескольких онлайн устройств необходимо выполнить следующие действия.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device** («Устройство») и выберите **Hikvision Device** («Устройство Hikvision») в качестве устройства для отображения в поле **Online Device** («Онлайн устройство»).
3. Нажмите и удерживайте клавишу **Ctrl**, чтобы выбрать несколько устройств.

Прежде чем правильно добавить неактивное устройство необходимо создать для него пароль. Подробная информация представлена в разделе ***Активация***.

4. Нажмите **Add to Client** («Добавить в клиент»), чтобы открыть окно добавления устройства.
5. Введите необходимую информацию.

   Имя пользователя

   По умолчанию имя пользователя: admin.

   Пароль

   Введите пароль устройства.

   Предостережение

   Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

   Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

6. **Опционально.** После добавления устройств в клиентское ПО нажмите **Synchronize Device Time** («Синхронизировать время устройства»), чтобы синхронизировать время устройств со временем компьютера, на котором работает клиентское ПО.
7. **Опционально.** Нажмите **Export to Group** («Экспортировать в группу»), чтобы создать группу по названию устройства.

   По умолчанию можно импортировать все каналы устройства в соответствующую группу.
8. Нажмите **Add** («Добавить») для добавления устройств.

Добавление всех онлайн устройств

В клиентское ПО можно добавить все онлайн устройства.

Для добавления всех онлайн устройств необходимо выполнить следующие действия.

Шаги

1. Перейдите на страницу **Device Management** («Управление устройством»).
2. Нажмите **Device** («Устройство») и выберите **Hikvision Device** («Устройство Hikvision») в качестве устройства для отображения в поле **Online Device** («Онлайн устройство»).
3. Нажмите **Add All** («Добавить все»), чтобы открыть окно добавления устройства.

   Прежде чем правильно добавить неактивное устройство необходимо создать для него пароль. Подробная информация представлена в разделе ***Активация***.
4. Введите имя пользователя и пароль.

   Имя пользователя

   По умолчанию имя пользователя: admin.

   Пароль

   Введите пароль устройства.

   Предостережение

   Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

   Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.
5. **Опционально.** После добавления устройств в клиентское ПО нажмите **Synchronize Device Time** («Синхронизировать время устройства»), чтобы синхронизировать время устройств со временем компьютера, на котором работает клиентское ПО.

6. **Опционально.** Нажмите **Export to Group** («Экспортировать в группу»), чтобы создать группу по названию устройства.

Примечание
По умолчанию можно импортировать все каналы устройства в соответствующую группу.

7. Нажмите **Add** («Добавить») для добавления устройств.

Добавление устройства по IP-адресу или доменному имени

Добавьте устройство по IP-адресу или доменному имени. Для добавления устройств по IP-адресу или доменному имени необходимо выполнить следующие действия.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device** («Устройство») и выберите **Hikvision Device** («Устройство Hikvision») в качестве необходимого устройства.
3. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
4. Выберите значение **IP/Domain** («IP-адрес / домен») в поле **Adding Mode** («Режим добавления»).
5. Введите необходимую информацию, включая название, IP-адрес, номер порта, имя пользователя и пароль.

   Адрес

   Введите IP-адрес устройства или доменное имя.

   Порт

   Введите № порта устройства. Значение по умолчанию: 8000.

   Имя пользователя

   Введите имя пользователя устройства. По умолчанию имя пользователя: admin.

   Пароль

   Введите пароль устройства.

   Предостережение
   Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным. Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

6. **Опционально.** После добавления устройства в клиентское ПО нажмите **Synchronize Device Time** («Синхронизировать время устройства»), чтобы синхронизировать время устройства со временем компьютера, на котором работает клиентское ПО.
7. **Опционально.** Нажмите **Export to Group** («Экспортировать в группу»), чтобы создать группу по названию устройства.

Примечание

По умолчанию можно импортировать все каналы устройства в соответствующую группу.

8. **Опционально.** Добавьте автономные устройства.
   1) Нажмите **Add Offline Device** («Добавление автономных устройств»).
   2) Введите необходимую информацию, в том числе номер канала устройства и номер тревожного входа.
   3) Нажмите **Add** («Добавить»).

   Когда автономное устройство подключается к сети, программное обеспечение подключает его автоматически.
9. Нажмите **Add** («Добавить») для добавления устройств.

Добавление устройств по сегменту IP-адреса

Для добавления устройств, IP-адреса которых находятся в IP-сегменте, можно указать начальный сегмент IP-адреса и конечный сегмент IP-адреса, имя пользователя, пароль и другие параметры для добавления. Для добавления устройств по сегменту IP-адресов необходимо выполнить следующие действия.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device** («Устройство») и выберите **Hikvision Device** («Устройство Hikvision») в качестве необходимого устройства.
3. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
4. Выберите **IP Segment** («Сегмент IP-адресов») в поле **Adding Mode** («Режим добавления»).
5. Введите необходимую информацию.

   Начальный сегмент IP-адреса

   Введите начальный сегмент IP-адреса.

   Конечный сегмент IP-адреса

   Введите конечный сегмент IP-адреса в том же сегменте сети, что и начальный IP-адрес.

   Порт

   Введите № порта устройства. Значение по умолчанию: 8000.

   Имя пользователя

   По умолчанию имя пользователя: admin.

   Пароль

   Введите пароль устройства.

   Предостережение

   Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется установить пароль надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и спец. символы).

Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

6. **Опционально.** После добавления устройства в клиентское ПО нажмите **Synchronize Device Time** («Синхронизировать время устройства»), чтобы синхронизировать время устройства со временем компьютера, на котором работает клиентское ПО.
7. **Опционально.** Нажмите **Export to Group** («Экспортировать в группу»), чтобы создать группу по названию устройства.

Примечание
По умолчанию можно импортировать все каналы устройства в соответствующую группу.

8. **Опционально.** Добавьте автономное устройство в клиентское ПО.
   1) Нажмите **Add Offline Device** («Добавление автономных устройств»).
   2) Введите необходимую информацию, в том числе номер канала устройства и номер тревожного входа.
   3) Нажмите **Add** («Добавить»).

   Когда автономное устройство подключается к сети, программное обеспечение подключает его автоматически.
9. Нажмите **Add** («Добавить») для добавления устройств.

Добавление устройства по протоколу EHome

Можно добавить устройство контроля доступа, подключенное по протоколу EHome, введя данные учетной записи EHome.

Перед началом
Сначала настройте параметры сетевого центра. Дополнительные информация представлена в разделе ***Настройка параметров сети***. Для добавления устройств через учетную запись Ehome необходимо выполнить следующие действия.

Шаги
1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device** («Устройство») и выберите **Hikvision Device** («Устройство Hikvision») в качестве необходимого устройства.
3. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
4. Выберите параметр **EHome** в поле **Adding Mode** («Режим добавления»).
5. Введите необходимую информацию.

   Учетная запись

   Введите имя учетной записи, зарегистрированное по протоколу EHome.
6. **Опционально.** После добавления устройства в клиентское ПО нажмите **Synchronize Device Time** («Синхронизировать время устройства»), чтобы синхронизировать время устройства со временем компьютера, на котором работает клиентское ПО.
7. **Опционально.** Нажмите **Export to Group** («Экспортировать в группу»), чтобы создать группу по названию устройства.

8. Опционально. Добавьте автономные устройства.
1) Нажмите **Add Offline Device** («Добавление автономных устройств»).
2) Введите необходимую информацию, в том числе номер канала устройства и номер тревожного входа.
3) Нажмите **Add** («Добавить»).

Примечание

Когда автономное устройство подключается к сети, программное обеспечение подключает его автоматически.

9. Нажмите **Add** («Добавить») для добавления устройств.

Импорт устройств в пакетном режиме

Устройства могут быть добавлены в ПО в пакетном режиме, для этого необходимо ввести информацию об устройствах в предварительно заданный файл CSV.

Для импорта устройств в пакетном режиме необходимо выполнить следующие действия.

Шаги

1. Перейдите на страницу **Device Management** («Управление устройством»).
2. Нажмите **Device → Hikvision Device → Add** («Устройство → Устройство Hikvision → Добавить»), чтобы открыть окно добавления устройства.
3. Выберите **Batch Import** («Пакетный импорт») в поле **Adding Mode** («Режим добавления»).
4. Нажмите **Export Template** («Скачать шаблон») и сохраните предварительно выбранный шаблон (файл CSV) на компьютере.
5. Откройте экспортированный файл шаблона и введите необходимую информацию об устройствах, подлежащих добавлению, в соответствующие столбцы.

Режим добавления

Можно ввести значения ***0, 2, 3, 4, 5*** или ***6***, что означает разные режимы добавления. **0**: устройство добавлено по IP-адресу или доменному имени; **2**: устройство добавлено через IP-сервер; **3**: устройство добавлено через HiDDNS; **4**: устройство добавлено по протоколу EHome; **5**: устройство добавлено через серийный интерфейс; **6**: устройство добавлено через Hik-Connect.

Адрес

Измените адрес устройства. Если установить **0** в поле режима добавления, необходимо ввести IP-адрес или доменное имя устройства; если установить **2** в поле режима добавления, необходимо ввести IP-адрес ПК, на котором установлен IP-сервер; если установить **3** в поле режима добавления, необходимо ввести www.hik-online.com.

Порт

Введите № порта устройства. Значение по умолчанию: 8000.

Информация об устройстве

Если установить **0** в поле режима добавления, заполнение данного поля не обязательно; если установить **2** в поле режима добавления, необходимо ввести идентификатор устройства, зарегистрированного на IP-сервере; если установить **3** в поле режима добавления, необходимо ввести доменное имя устройства, зарегистрированное на сервере HiDDNS; если установить **4** в поле режима добавления, необходимо ввести данные учетной записи EHome; если установить **6** в поле режима добавления, необходимо ввести серийный номер устройства.

Имя пользователя

Введите имя пользователя устройства. По умолчанию имя пользователя: admin.

Пароль

Введите пароль устройства.

Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным. Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

Добавление автономных устройств

Введите ***1***, чтобы разрешить добавление автономного устройства, а затем программное обеспечение автоматически подключит его, когда автономное устройство подключится к сети. Если выбрано значение ***0***, значит функция отключена.

Экспорт в группу

Введите **1**, чтобы создать группу по названию устройства. Все каналы устройства будут импортированы в соответствующую группу по умолчанию. Если выбрано значение ***0***, значит функция отключена.

Номер канала

Если в поле **Add Offline Device** («Добавление автономных устройств») установлено значение ***1***, необходимо ввести номер канала устройства. Если в поле **Add Offline Device** («Добавление неактивных устройств») установлено значение ***0***, заполнение данного поля не обязательно.

Номер тревожного входа

Если в поле **Add Offline Device** («Добавление неактивных устройств») установлено значение ***1***, необходимо ввести номер тревожного входа устройства. Если в поле **Add Offline Device** («Добавление неактивных устройств») установлено значение ***0***, заполнение данного поля не обязательно.

Номер серийного интерфейса

Если в поле режима добавления установлено значение ***5***, необходимо ввести номер серийного интерфейса для устройства контроля доступа.

Скорость передачи данных

Если в поле режима добавления установлено значение ***5***, необходимо ввести скорость передачи данных (в бодах) для устройства контроля доступа.

DIP

Если в поле режима добавления установлено значение ***5***, необходимо ввести DIP-адрес для устройства контроля доступа.

Учетная запись Hik-Connect

Если в поле режима добавления установлено значение ***6***, необходимо ввести данные учетной записи Hik-Connect.

Пароль Hik-Connect

Если в поле режима добавления установлено значение ***6***, необходимо ввести пароль учетной записи Hik-Connect.

6. Нажмите и выберите файл шаблона.

7. Нажмите **Add** («Добавить»), чтобы импортировать устройства.

8.1.2 Выбор сценария применения

При первом входе в модуль контроля доступа необходимо выбрать сценарий применения устройства: жилая или нежилая недвижимость.

Для выбора сценария применения устройства при первом входе в модуль контроля доступа необходимо выполнить следующие действия.

Шаги

Примечание

После выбора сценария применения, его невозможно изменить.

1. Нажмите на иконку для перехода в модуль контроля доступа. Появится окно выбора сцены.

Рисунок 8-2. Выбор сценария применения контроллера доступа

2. Выберите сценарий применения устройства: жилая или нежилая недвижимость.

Примечание

В сценарии применения «Жилая недвижимость» при добавлении пользователя нельзя настроить УРВ.

3. Нажмите **OK**.

8.1.3 Настройка других параметров

После добавления устройства контроля доступа можно настроить параметры сети, параметры захвата, параметры RS-485, параметры Wiegand и т. д.

Настройка параметров сети

После добавления устройства контроля доступа можно установить режим загрузки журнала устройства и создать учетную запись EHome через проводную или беспроводную сеть.

Настройка режима загрузки журнала

Настройте режим загрузки журнала через протокол EHome.

Для настройки режима загрузки журнала необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Device Management** («Контроль доступа → Управление устройствами») для входа на страницу управления устройством.

2. Выберите устройство списка и нажмите **Modify** («Изменить»).
3. Нажмите **Network Settings → Uploading Mode** («Параметры сети → Режим загрузки»), чтобы перейти на страницу режима загрузки.
4. Выберите центральную группу из выпадающего списка.
5. Нажмите **Enable** («Включить»), чтобы включить настройку режима загрузки.
6. Выберите режим загрузки из выпадающего списка.
   - Включите **N1** или **G1** для основного и резервного канала.
   - Выберите **Close** («Закрыть»), чтобы деактивировать основной или резервный канал

Примечание

- Не допускается активация N1 или G1 на основном и резервном канале одновременно.
- N1 относится к проводной сети, а G1 относится к GPRS.
- Только устройство с функцией 3G / 4G поддерживает установку канала как G1.
- Подробная информация о настройках проводной сети представлена в разделе ***Создание учетной записи EHome в проводной сети***.
- Подробная информация о настройках беспроводной сети представлена в разделе ***Создание учетной записи EHome в беспроводной сети.***

7. Нажмите **Save** («Сохранить»).

Создание учетной записи EHome в проводной сети

Создайте учетную запись для протокола EHome в проводной сети. После этого можно добавить устройства через протокол EHome.

Для создания учетной записи EHome в режиме проводной связи необходимо выполнить следующие действия.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **Access Control → Device Management** («Контроль доступа → Управление устройствами») для входа на страницу управления устройством.
2. Выберите устройство списка и нажмите **Modify** («Изменить»).
3. Нажмите **Network Settings → Network Center** («Параметры сети → Сетевой центр»), чтобы перейти на страницу сетевого центра.
4. Выберите центральную группу из выпадающего списка.
5. Укажите тип адреса **IP Address** («IP-адрес») или **Domain Name** («Доменное имя»).
6. Введите IP-адрес или доменное имя в соответствии с типом адреса.
7. Введите номер порта для протокола.

   Примечание

   Номер порта беспроводной и проводной сети должен быть таким же, как и номер порта EHome.
8. Выберите **EHome** в поле **Protocol Type** («Тип протокола») и выберите версию EHome.

   Примечание

   При EHome версии **5.0** необходимо создать ключ EHome для учетной записи EHome.
9. Укажите имя учетной записи сетевого центра.
10. Нажмите **Save** («Сохранить»).

Создание учетной записи EHome в беспроводной сети

Создайте учетную запись для протокола EHome в беспроводной сети. После этого можно добавить устройства через протокол EHome.

Для создания учетной записи EHome в режиме беспроводной связи необходимо выполнить следующие действия.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **Access Control → Device Management** («Контроль доступа → Управление устройствами») для входа на страницу управления устройством.
2. Выберите устройство списка и нажмите **Modify** («Изменить»).
3. Нажмите **Network Settings → Wireless Communication Center** («Параметры сети → Центр беспроводной связи»), чтобы перейти на страницу центра беспроводной связи.
4. Выберите центральную группу из выпадающего списка.
5. Введите IP-адрес и номер порта.

Примечание

- Номер порта Ehome по умолчанию: 7660.
- Номер порта беспроводной и проводной сети должен быть таким же, как и номер порта EHome.

6. Выберите **EHome** в поле **Protocol Type** («Тип протокола»).
7. Укажите имя учетной записи сетевого центра.
8. Нажмите **Save** («Сохранить»).

Шифрование M1-карты

Шифрование M1-карты может повысить уровень безопасности при аутентификации. После выпуска карты можно включить функцию шифрования M1-карты в клиентском программном обеспечении.

Перед началом

Для выдачи карты используйте надлежащий настольный считыватель карт. Подробная информация представлена в разделе ***Выпуск стандартной карты.***

Для включения шифрования M1-карты необходимо выполнить следующие действия.

Примечание

Устройство контроля доступа и считыватель карт должны поддерживать данную функцию.

Шаги

1. Нажмите **Access Control → Device Management** («Контроль доступа → Управление устройствами») для входа на страницу управления устройством контроля доступа.
2. Выберите устройство в списке устройств и нажмите **Modify** («Изменить»), чтобы открыть соответствующее окно.
3. Нажмите **M1 Card Encryption** («Шифрование M1-карты»), чтобы перейти на соответствующую страницу.
4. Нажмите **Enable** («Включить»), чтобы включить функцию шифрования M1-карты.
5. Установите идентификатор сектора.

   Диапазон яркости от 1 до 100.
6. Нажмите **Save** («Сохранить») для сохранения настроек.

Примечание

После включения функции шифрования карты M1 необходимо установить идентификатор сектора добавленной карты в качестве идентификатора настроенного сектора.

8.1.4 Управление организацией

Организацией можно управлять, например добавлять, редактировать или удалять организацию. Для управления организацией необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами») для входа на соответствующую страницу.
2. Нажмите кнопку **Add** («Добавить»), появится всплывающее окно добавления организации.
3. Создайте имя для организации.
4. Нажмите **OK**.

Примечание

Можно добавить до 10 уровней организаций.

5. **Опционально.** После добавления организации можно выполнить одно или несколько из следующих действий.

Изменение организации	Выберите добавленную организацию и нажмите **Modify** («Изменить») для изменения ее имени.
Удаление организации	Выберите добавленную организацию и нажмите **Delete** («Удалить»), чтобы удалить ее.

- Если удалить организацию верхнего уровня, организации нижнего уровня тоже будут удалены.
- Организация не может быть удалена, если ранее добавлены сотрудники.

8.1.5 Управление информацией о пользователе

После добавления организации можно добавить пользователя в организацию и управлять добавленными пользователями, например, выпускать карты в пакетном режиме, импортировать и экспортировать информацию пользователя в пакетном режиме и т. д.

Может быть добавлено до 10000 пользователей или карт.

Добавление одного сотрудника

Добавлять сотрудников в клиентское ПО можно по одному. Кроме того, можно ввести следующую информацию о сотруднике: основная информация, подробная информация, разрешение на управление доступом, привязка карты, изображения лица, отпечатка пальца и правило УРВ.

Настройка основной информации пользователя

Можно добавить пользователей в клиентское ПО поочередно и настроить основную информацию о пользователе, в том числе имя, номер телефона и т. д.

Для настройки основной информации при добавлении пользователя необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Выберите организацию из списка и добавьте сотрудника / посетителя.
3. Нажмите **Add** («Добавить»), чтобы открыть окно добавления сотрудника/посетителя.
   Person No. («№ пользователя») будет сгенерирован автоматически и не может быть изменен.
4. Введите основную информацию, включая имя, срок действия учетной записи, пароль.
5. Выберите тип пользователя и его привилегии.

   Стандартный

   Можно установить привилегии для стандартного пользователя, включая **Manage Device Backend** («Управление аппаратной частью устройства») и **Close Delay Enabled** («Включение задержки закрытия двери»).

   Посетитель

   Для посетителя устанавливают максимальное количество открытий двери. При превышении заданного значения посетитель не может снова открыть дверь.

   Черный список

   Добавьте пользователя в черный список. При аутентификации пользователя через устройство будет загружено событие в клиентское ПО.

Управление аппаратной частью устройства

Настройте права администратора для пользователя. После получения разрешений пользователь может войти в систему и настроить параметры устройства.

Включение задержки закрытия двери

Если функция активирована, длительность открытия двери будет увеличена. Увеличить продолжительность открытия двери можно в поле настройки параметров двери.

6. **Опционально.** Задайте изображение лица сотрудника.
   - Нажмите **Upload Picture** («Загрузить изображение») для выбора изображения сотрудника из папки на локальном ПК и загрузки в клиент.
   - Нажмите **Take Photo** («Сделать фото») и сделайте снимок пользователя с помощью камеры ПК.
7. Подтвердите добавление пользователя.
   - Нажмите **OK** для добавления пользователя и закройте окно добавления.
   - Чтобы добавить пользователя и продолжить добавление других пользователей нажмите **Save and Continue** («Сохранить и продолжить»).

Настройка подробной информации

При добавлении пользователя можно настроить подробную информацию, такую как тип ID, номер ID, страна и т. д. Для настройки подробной информации необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Выберите организацию из списка и нажмите **Add** («Добавить»).

Примечание

В первую очередь необходимо добавить основную информацию о сотруднике / посетителе. Подробная информация о настройке основной информации о пользователе представлена в разделе ***Настройка основной информации***.

3. Нажмите **Details** («Подробная информация»).
4. Введите подробную информацию пользователя, включая тип ID, номер ID, страна и т. д.

Привязка устройства

Можно выполнить привязку видеодомофона к пользователю.

Примечание

При выборе значения **Analog Indoor Station** («Аналоговый видеодомофон») будет отображено поле **Door Station** («Вызывная панель»), после чего необходимо будет выбрать вызывную панель для связи с аналоговым видеодомофоном.

5. Подтвердите, чтобы добавить пользователя.
   - Нажмите **OK** для добавления пользователя и закройте окно добавления.
   - Чтобы добавить пользователя и продолжить добавление других пользователей нажмите **Save and Continue** («Сохранить и продолжить»).

Назначение разрешений

При добавлении пользователя можно назначить разрешения (включая разрешения на операции устройства контроля доступа и разрешения на контроль доступа).

Для назначения соответствующих разрешений необходимо выполнить следующие действия.

Шаги

Примечание

Подробная информация о настройке разрешений на контроль доступа представлена в разделе ***Назначение разрешений***.

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Выберите организацию из списка и добавьте сотрудника / посетителя.
3. Нажмите **Add** («Добавить»).
4. Введите основную информацию пользователя.

   Примечание

   Подробная информация о настройке основной информации о пользователе представлена в разделе ***Настройка основной информации.***
5. Нажмите **Permission** («Разрешение»).
6. В списке **Permission(s) to Select** («Разрешения на выбор») выберите необходимые разрешения и нажмите >, чтобы добавить их в список **Selected Permission(s)** («Выбранные разрешения»).
7. Подтвердите, чтобы добавить пользователя.
   - Нажмите **OK** для добавления пользователя и закройте окно добавления.
   - Чтобы добавить пользователя и продолжить добавление других пользователей нажмите **Save and Continue** («Сохранить и продолжить»).

Выпуск стандартной карты

При добавлении пользователя можно выпустить для него стандартную карту с уникальным номером. Для выпуска стандартной карты необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Выберите организацию из списка и нажмите **Add** («Добавить»).

   Примечание

   В первую очередь необходимо добавить основную информацию о сотруднике / посетителе. Подробная информация о настройке основной информации о пользователе представлена в разделе *Настройка основной информации*.
3. Нажмите **Credential → Card** («Учетные данные → Карта»), чтобы перейти на соответствующую страницу.

4. Нажмите **Add** («Добавить») и выберите вкладку **General Card** («Стандартная карта»), чтобы перейти на страницу настройки стандартной карты.

5. Настройте параметры карты.

1) Выберите тип стандартной карты.

Обычная карта

Стандартная карта без дополнительных функций.

Патрульная карта

Считывание карты позволяет персоналу инспектирования проверить рабочее состояние устройства. Разрешения доступа для персонала инспектирования могут быть настроены в зависимости от задач проекта.

Принудительная карта

Дверь может быть открыта при помощи считывания принудительной карты. При этом клиент может создает уведомление о событии принуждения.

Суперкарта

Карта действительна для всех дверей контроллера в течение заданного в расписании времени.

2) **Опционально.** При необходимости в поле **Remark** («Замечание») можно ввести примечание для карточки.

Примечание

В поле примечания допускается использование до 32 символов.

3) Настройте время действия и срок истечения действия карты.

6. Выберите режим считывания карты и введите номер карты.

- Считыватель карт контроллера доступа

1. Поместите карту в считыватель карт контроллера доступа.
2. Нажмите **Read** («Читать»), чтобы получить номер карты.

- Настольный считыватель карт

1. Подключите настольный считыватель карт к ПК, на котором запущен клиент.
2. Нажмите **Set Card Enrollment Station** («Настроить настольный считыватель карт»), чтобы настроить необходимые параметры.
3. Выберите тип настольного считывателя карт.

Примечание

Поддерживаемые типы считывателей карт: DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E и DS-K1F180-D8E.

4. Задайте номер серийного интерфейса, скорость передачи данных, значение лимита времени, параметры бипера или тип номера карты.

5. **Опционально.** Если используется M1-карта, и нужно включить функцию шифрования M1-карты, необходимо нажать **Enable** («Включить») в поле **M1 Card Encryption** («Шифрование M1-карты») и нажать **Modify** («Изменить»), чтобы выбрать сектор.

Примечание

Функция шифрования карты M1 поддерживается DS-K1F100-D8, DS-K1F100-D8E и DS-K1F180-D8E.

6. Нажмите **Save** («Сохранить»).
7. Поместите карту на настольный считыватель.
8. Нажмите **Read** («Читать»), чтобы получить номер карты.

- Ввод вручную
  1. Введите номер карты вручную.
  2. Нажмите **Enter** («Ввод»), чтобы ввести номер карты.

7. Нажмите **OK**.

Необходимая карта будет выдана.

8. Подтвердите, чтобы добавить пользователя.
- Нажмите **OK** для добавления пользователя и закройте окно добавления.
- Чтобы добавить пользователя и продолжить добавление других пользователей нажмите **Save and Continue** («Сохранить и продолжить»).

Сбор отпечатков пальцев в локальном режиме

При добавлении пользователя можно выполнить сбор отпечатков пальцев сотрудника / посетителя с помощью настольного считывателя отпечатков пальцев, подключенного непосредственно к ПК, на котором запущен клиент.

Для сбора отпечатков пальцев с помощью настольного считывателя отпечатков пальцев необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).

2. Выберите организацию из списка и нажмите **Add** («Добавить»).

Примечание

В первую очередь необходимо добавить основную информацию о сотруднике / посетителе. Подробная информация о настройке основной информации о пользователе представлена в разделе ***Настройка основной информации***.

3. Нажмите **Credential → Fingerprint** («Учетные данные → Отпечатки пальцев»), чтобы перейти на соответствующую страницу.

4. В поле **Collection Mode** («Режим сбора») выберите **Local Collection** («Локальный сбор»).

5. Подключите считыватель отпечатков пальцев к ПК и настройте необходимые параметры.
1) Нажмите **Set Fingerprint Machine** («Настроить считыватель отпечатков пальцев»), чтобы открыть соответствующее окно.
2) Выберите тип устройства.

Примечание

Поддерживаемые типы считывателя отпечатков пальцев: DS-K1F800-F, DS-K1F300-F, DS-K1F810-F и DS-K1F820-F.

3) **Опционально.** Для считывателя отпечатков пальцев DS-K1F800-F можно настроить номер серийного интерфейса, скорость передачи данных и параметры сверхурочной работы.

Примечание

- Номер серийного интерфейса должен соответствовать номеру последовательного порта ПК.
- Скорость передачи в бодах должна устанавливаться в соответствии с внешним устройством считывания отпечатков пальцев. Значение по умолчанию: 19200.
- Поле **Timeout after** («Тайм-аут после») относится ко времени сбора отпечатка пальца. Если пользователь не ввел отпечаток пальца, или при вводе отпечатка пальца произошел сбой, устройство укажет, что сбор отпечатка пальца прекращен.

4) Нажмите **Save** («Сохранить»).

6. Зарегистрируйте отпечаток пальца.

1) Нажмите **Start** («Начать»).
2) Чтобы начать сбор, выберите отпечаток пальца на изображении руки.
3) Поднимите и приложите палец к сканеру отпечатков пальцев дважды, чтобы клиент смог получить отпечаток пальца.
1) Выберите тип отпечатка пальца.

Примечание

При сборе одинаковых отпечатков пальцев одного человека, появляется предупреждение с указанием на повторяющийся ID. При сборе одинаковых отпечатков пальцев разных людей, появляется предупреждение с указанием повторяющегося ID и именем пользователя.

7. Подтвердите добавление пользователя.

- Нажмите **OK** для добавления пользователя и закройте окно добавления.
- Чтобы добавить пользователя и продолжить добавление других пользователей нажмите **Save and Continue** («Сохранить и продолжить»).

Сбор отпечатков пальцев в удаленном режиме

При добавлении сотрудника / посетителя можно добавить информацию об отпечатках пальцев в удаленном режиме с помощью модуля считывания отпечатков пальцев устройства контроля доступа.

Для сбора отпечатков пальцев через модуль считывания отпечатков пальцев устройства контроля доступа необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).

2. Выберите организацию из списка и нажмите **Add** («Добавить»).

Примечание

В первую очередь необходимо добавить основную информацию о сотруднике / посетителе. Подробная информация о настройке основной информации о пользователе представлена в разделе ***Настройка основной информации***.

3. Нажмите **Credential** → **Fingerprint** («Учетные данные → Отпечатки пальцев»), чтобы перейти на соответствующую страницу.
4. В поле **Collection Mode** («Режим сбора») выберите **Remote Collection** («Удаленный сбор»).
5. Нажмите **Start** («Начать») и выберите устройство контроля доступа для сбора отпечатков пальцев.

Примечание

Устройство должно поддерживать данную функцию.

6. Зарегистрируйте отпечаток пальца.
   1) Чтобы начать сбор, выберите отпечаток пальца на изображении руки.
   2) Поднимите и приложите палец к сканеру отпечатков пальцев, чтобы клиент смог получить отпечаток пальца.
   3) Выберите тип отпечатка пальца.
   4) Нажмите **Stop** («Остановить»).
7. Подтвердите добавление пользователя.
   - Нажмите **OK** для добавления пользователя и закройте окно добавления.
   - Чтобы добавить пользователя и продолжить добавление других пользователей нажмите **Save and Continue** («Сохранить и продолжить»).

Настройка правила УРВ

Если в сценарии применения устройства не выбрано «Жилая недвижимость», то при добавлении пользователя можно настроить правило УРВ.

Для настройки правила УРВ при добавлении пользователя необходимо выполнить следующие действия.

Шаги

Примечание

Подробная информация о настройках УРВ представлена в разделе ***Учет рабочего времени (УРВ)***.

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Выберите организацию из списка и нажмите **Add** («Добавить»).
3. Введите основную информацию пользователя.

Примечание

Подробная информация о настройке основной информации о пользователе представлена в разделе ***Настройка основной информации.***

4. Нажмите **Attendance Rule** («Правила УРВ»).

Примечание

Эта вкладка отображается, если при первом запуске программного обеспечения выбран режим **Non-Residence** («Нежилая недвижимость»). Подробная информация представлена в разделе ***Выбор сценария применения***.

5. Если для пользователя необходимо настроить УРВ, нажмите **Time and Attendance** («Учет рабочего времени (УРВ))», чтобы включить эту функцию.

   Записи считывания карты будут записаны и проанализированы в рамках УРВ.
6. Настройте правило УРВ для пользователя.

Примечание

Для получения подробной информации об УРВ нажмите **More** («Подробнее»), чтобы перейти к модулю УРВ.

7. Подтвердите, чтобы добавить пользователя.
   - Нажмите **OK** для добавления пользователя и закройте окно добавления.
   - Чтобы добавить пользователя и продолжить добавление других пользователей нажмите **Save and Continue** («Сохранить и продолжить»).

Импорт и экспорт информации о сотруднике / посетителе

Можно импортировать информацию и изображения нескольких пользователей в клиентское ПО в пакетном режиме. Также можно экспортировать информацию и изображения пользователей и сохранить их на компьютере.

Импорт информации о сотруднике / посетителе

Можно импортировать информацию о нескольких пользователях (включая идентификационную информацию, данные отпечатков пальцев и номер карты, привязанной к отпечатку пальца) в клиентское ПО в пакетном режиме посредством импорта файла Excel с локального ПК.

Для импорта данных в пакетном режиме необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Нажмите **Import Person** («Импортировать пользователя») и выберите **Person Information** («Информация о сотруднике / посетителе») в качестве данных для импорта.
3. Во всплывающем окне нажмите **Download Template for Importing Person** («Скачать шаблон для импорта сотрудника / посетителя»), чтобы скачать шаблон.
4. Введите информацию о пользователе в загруженный шаблон.

От f1 до f10

Данные отпечатков пальцев.

От f1card до f10card

Номер карты, привязанной к отпечатку пальца. Если привязка карты не выполнена, поле можно не заполнять.

Примечание

Если у пользователя несколько карт, отделите каждый номер карты точкой с запятой.

5. Войдите в **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»), нажмите **Import Person** («Импортировать пользователя») и выберите файл Excel с информацией о сотруднике / посетителе.
6. Нажмите **OK** для старта импорта.

Примечание

Если номер сотрудника / посетителя уже существует в базе данных клиентского ПО, информация после импорта будет автоматически заменена.

Экспорт информации о сотруднике / посетителе

Экспортируйте данные о добавленном пользователе на локальный ПК в формате Excel. Для экспорта информации пользователей в пакетном режиме необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Нажмите **Export Person** («Импортировать пользователя») и выберите **Person Information** («Информация о сотруднике / посетителе») в качестве данных для экспорта.
3. Выберите путь сохранения экспортированного Excel файла.
4. Выберите элементы информации о сотруднике / посетителе, которые необходимо экспортировать.
5. Нажмите **OK**, чтобы начать экспорт.

От f1 до f10

Данные отпечатков пальцев.

От f1card до f10card

Номер карты, привязанной к отпечатку пальца. Если привязка карты не выполнена, поле можно не заполнять.

Получение информации о пользователе с устройства контроля доступа

Если в добавленном устройстве контроля доступа была настроена информация о пользователе (включая подробную информацию о пользователе, отпечаток пальца, информацию о выданной карте), можно получить информацию с устройства и импортировать ее в клиент для дальнейшей работы.

Для получения информации о пользователе с устройства контроля доступа необходимо выполнить следующие действия.

Шаги

Примечание

- Эта функция поддерживается только устройством, которое было добавлено при помощи TCP / IP.
- Если в информации о пользователе, хранящейся на устройстве, в поле **Name** («Имя») не указаны данные, то это поле будет заполнено номером выданной карты после импорта в клиентское ПО.

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Выберите организацию для импорта сотрудников.
3. Нажмите **Get Person** («Получить информацию пользователя»), чтобы открыть окно выбора устройства. Будут отображены добавленные устройства контроля доступа.
4. Начните получение информации о пользователе.
   - Выберите устройство и нажмите **OK**, чтобы начать получать информацию о пользователе с устройства.
   - Дважды нажмите имя устройства, чтобы начать получать информацию о пользователе с устройства.

   Информация о пользователе, включая подробную информацию о пользователе, информацию об отпечатках пальцев (если настроены) и картах (если настроены), будет импортирована в выбранную организацию.

Выдача карт сотрудникам в пакетном режиме

Можно выдать несколько карт одному пользователю в пакетном режиме.

Для выпуска нескольких карт одному пользователю необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Нажмите **Issue Card in Batch** («Выдача карт в пакетном режиме»).

   Все добавленные пользователи, которым не были выданы карты, будут отображены в списке **Person(s) with No Card Issued** («Пользователи, которым не выданы карты»).

3. Настройте параметры карты.

1) Выберите тип карты.

Примечание

Подробная информация о типах карт представлена в разделе *Выпуск стандартной карты*.

2) В поле **Card Password** («Пароль карты») создайте пароль (от 4 до 8 цифр) для карты.

Примечание

Пароль потребуется, когда владелец карты будет считывать карту и, если для аутентификации по карте требуется пароль. Подробная информация приведена в разделе *Настройка режима и расписания аутентификации при помощи считывателя карт*.

3) Введите количество карт, выданных на каждого пользователя.

Пример

Если выдано 3 карты, можно ввести три номера карты для каждого пользователя.

4) Настройте время действия и срок истечения действия карты.

4. В списке **Person(s) with No Card Issued** («Пользователи, которым не выданы карты») выберите пользователя, которому будут выданы карты.

5. Выберите режим считывания карты и введите номер карты.

Считыватель карт контроллера доступа

Поместите карту на считыватель контроллера доступа и нажмите **Read** («Считать») для получения номера карты.

Настольный считыватель карт

Поместите карту на настольный считыватель и нажмите **Read** («Считать») для получения номера карты.

Примечание

Настольный считыватель карт должен быть подключен к ПК с запущенным клиентом. Нажмите **Set Card Enrollment Station** («Настроить настольный считыватель карт»), чтобы настроить необходимые параметры. Подробная информация представлена в разделе *Выпуск стандартной карты*.

Ввод вручную

Введите номер карты вручную и нажмите **Enter** («Ввод») для внесения номера карты.

После выдачи карты пользователю, информация о нем и о карте будет отображена в списке **Person(s) with Card Issued** («Пользователи, которым выданы карты»).

6. Нажмите **OK**.

Поиск информации о пользователе

После добавления информации о пользователе в клиент можно искать пользователя, задав соответствующие условия поиска.

Возможен стандартный поиск и расширенный поиск.

Стандартный поиск

После добавления информации о пользователе в клиент можно искать пользователя по имени пользователя и по номеру карты.

Для поиска пользователя по имени пользователя и по номеру карты необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Задайте условия поиска.
   - Для поиска по имени пользователя введите ключевое слово имени в поле поиска.
   - Для поиска по номеру карты введите ключевые данные номера карты в поле поиска или используйте настольный считыватель карт. Для этого нажмите **Read** («Считать»), чтобы считать номер карты.

   Примечание

   При считывании с помощью настольного считывателя карт сначала необходимо подключить считыватель карт к ПК, на котором запущен клиент. Нажмите **Read → Set Card Enrollment Station** («Считать → Настройка настольного считывателя карт»), чтобы настроить параметры считывателя. Подробная информация представлена в разделе ***Выпуск стандартной карты***.
3. Нажмите **Search** («Поиск»).
   Результаты поиска будут отображены в списке сотрудников / посетителей.

Расширенный поиск

После добавления информации о пользователе в клиент можно искать пользователя, установив более точные условия поиска, включая номер карты, имя пользователя, номер пользователя.

Для поиска пользователя с более точными условиями поиска необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Нажмите **Advanced Search** («Расширенный поиск») для отображения условий поиска.
3. Задайте условия поиска.

Номер карты

Введите ключевые данные номера карты в поле поиска или используйте настольный считыватель карт. Для этого нажмите **Read** («Считать»), чтобы считать номер карты.

Примечание

При считывании с помощью настольного считывателя карт сначала необходимо подключить считыватель карт к ПК, на котором запущен клиент. Нажмите **Read → Set Card Enrollment Station** («Считать → Настройка настольного считывателя карт»), чтобы настроить параметры считывателя. Подробная информация представлена в разделе ***Выпуск стандартной карты***.

Номер сотрудника / посетителя

Введите ключевые данные номера пользователя.

Имя сотрудника / посетителя

Введите ключевое слово имени пользователя.

Примечание

Имя сотрудника / посетителя должно включать буквы верхнего и нижнего регистра.

4. Нажмите **Search** («Поиск»).
   Результаты поиска будут отображены в списке сотрудников / посетителей.
5. **Опционально.** Нажмите **Reset** («Сбросить») для сброса всех условий поиска.

Сообщить о потере карты

В случае утери карты необходимо сообщить об утере, чтобы соответствующее разрешение на управление доступом было удалено.

Для регистрации утери карты необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. **Опционально.** Найдите сотрудника / посетителя, который потерял карту.

Примечание

Подробная информация о поиске пользователя представлена в разделе ***Поиск информации о пользователе***.

3. Выберите пользователя и нажмите **Modify** («Изменить») для открытия окна редактирования информации пользователя.
4. Нажмите **Credential → Card** («Учетные данные → Карта») для просмотра информации о карте.
5. Выберите утерянную карту и нажмите **Report Card Loss** («Регистрация утери карты»).
   Состояние карты обновится на «утеряна».
6. **Опционально.** Если утерянная карта найдена, можно выбрать карту и нажать **Cancel Card Loss** («Отменить утерю карты»), чтобы отменить регистрацию утери карты.

Состояние карты обновится на обычное состояние.

7. **Опционально.** Если для пользователя назначено разрешение на доступ, появится всплывающее окно с уведомлением о необходимости снова применить разрешение, чтобы оно вступило в силу. Можно нажать **Apply Now** («Применить сейчас») или **Apply Later** («Применить позднее») для применения изменений.

Настройка настольного считывателя карт

Если приложить карту к настольному считывателю карт, он может считать номер карты и показать номер карты в клиентском ПО. Сначала необходимо подключить настольный считыватель карт к ПК, на котором запущен клиент, через интерфейс USB или COM. Затем необходимо настроить параметры настольного считывателя карт.

Для привязки карты к пользователю нажмите **Set Card Enrollment Station** («Настройка настольного считывателя карт»), чтобы открыть соответствующее окно.

Доступны следующие параметры.

Тип

Выберите модель подключенного настольного считывателя карт.

Примечание

В настоящее время поддерживаются следующие модели считывателя карт: DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E и DS-K1F180-D8E.

Тип карты

Это поле доступно только для моделей считывателя карт DS-K1F100-D8E или DS-K1F180-D8E.

Выберите тип карты: EM-карта или IC-карта в соответствии с фактическим типом карты.

Если карта содержит как микросхемы EM и IC, можно выбрать **All** («Все»), чтобы считывать микросхемы EM и IC.

Номер серийного интерфейса и скорость передачи данных

Данные настройки применимы к модели DS-K1F100-M.

Выберите COM-интерфейс, к которому подключается настольный считыватель карт, и установите скорость передачи данных.

Тайм-аут после

Настройте значение в миллисекундах, после которого считывание карты будет недействительно.

Бипер

После успешного считывания номера карты включите или выключите бипер.

Тип номера карты

Настройка типа номера карты

Шифрование M1-карты

Это поле доступно только для моделей считывателя карт DS-K1F100-D8, DS-K1F100-D8E или DS-K1F180-D8E.

Если используется M1-карта, и нужно включить функцию шифрования M1-карты, необходимо нажать **Enable** («Включить») в поле **M1 Card Encryption** («Шифрование M1-карты») и нажать **Modify** («Изменить»), чтобы выбрать сектор шифрования карты.

8.1.6 Настройка графиков и шаблонов

Настройте шаблон, в том числе недельный график работы и график выходных дней. После настройки шаблонов, их можно использовать для настройки разрешений контроля доступа. Подробная информация о настройке разрешений на контроль доступа представлена в разделе ***Назначение разрешений***.

Примечание

Добавление графика рабочей недели

Можно добавить график рабочей недели и настроить разрешения контроля доступа.

Для добавления графика рабочей недели необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Schedule and Template → Week Schedule** («Контроль доступа → Графики и шаблоны → График рабочей недели»), чтобы перейти на соответствующую страницу.

   Примечание

   По умолчанию существует два графика рабочей недели: **Whole Week Schedule** («Расписание на всю неделю») и **Blank Schedule** («Незаполненное расписание»), графики нельзя редактировать или удалять.

   Расписание на всю неделю

   Считывание карты действительно каждый день недели.

   Незаполненное расписание

   Считывание карты недействительно каждый день недели.

2. Добавьте график рабочей недели.
   1) Нажмите **Add Week Schedule** («Добавить график рабочей недели»), чтобы открыть соответствующее окно.
   2) В поле **Week Schedule Name** («Имя графика рабочей недели») введите необходимое имя.
   3) Нажмите **OK**, чтобы добавить график рабочей недели.
3. Нажмите добавленный график рабочей недели, расположенный в списке слева, чтобы посмотреть его свойства.
4. Выберите день недели и укажите период времени на временной шкале.

   Примечание

   Для каждого дня в расписании недели можно установить до 8 периодов времени.

5. **Опционально.** Для изменения настроенной продолжительности необходимо выполнить одну из следующих операций.

- Когда вид курсора изменится на  , можно изменить длительность выбранного отрезка времени, переместив курсор в необходимое положение.
- Наведите курсор на отрезок времени и измените время начала / окончания периода в появившемся диалоговом окне.
- Когда вид курсора изменится на  , переместите курсор в конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.

6. **Опционально.** После настройки графика можно выполнить следующие действия.

   Удалить график дня

   Выберите день и нажмите **Delete Duration** («Удалить период времени»), чтобы удалить расписание выбранного дня.

   Очистить график рабочей недели

   Нажмите **Clear** («Очистить»), чтобы удалить расписание на всю неделю.

   Применить ко всей неделе

   Нажмите **Copy to Week** («Применить к неделе»), чтобы копировать расписание этого дня на всю неделю.
7. Нажмите **Save** («Сохранить»), чтобы сохранить настройки и завершить добавление графика рабочей недели.

Добавление расписания выходных дней

Можно установить расписание выходных дней и настроить параметры расписания, в том числе дату начала, дату окончания и продолжительность указанного периода.

Для добавления расписания выходных дней необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Schedule and Template → Week Schedule** («Контроль доступа → Графики и шаблоны → График рабочей недели»), чтобы перейти на соответствующую страницу.
2. Добавьте группу выходных дней.
   1) Нажмите **Add Holiday Group** («Добавить группу выходных дней»), чтобы открыть окно добавления группы выходных дней.
   2) Создайте имя для группы выходных дней.
   3) Нажмите **OK**.
3. Добавьте период и настройте продолжительность выходных дней.

   Примечание

   Для одной группы выходных дней можно добавить до 16 периодов.

   1) Нажмите **Add Holiday** («Добавить выходной»).
   2) Двигайте курсор, чтобы указать временной интервал. Для данного периода времени будет активировано настроенное разрешение.

Примечание

Для одного периода выходных может быть установлено до 8 временных интервалов.

3) **Опционально.** Когда вид курсора изменится, можно переместить только что отредактированный период времени. Также можно отредактировать отображаемую временную точку, чтобы установить точный период времени.
4) **Опционально.** Когда вид курсора изменится на , можно увеличить или уменьшить выбранный период времени.

4. Нажмите **Save** («Сохранить»).

Добавление шаблона

После настройки графика рабочей недели и группы выходных дней можно добавить и настроить шаблон, который содержит график рабочей недели и график группы выходных дней.

Для добавления и настройки шаблона необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Schedule and Template → Template** («Контроль доступа → Графики и шаблоны → Шаблон»), чтобы перейти на соответствующую страницу.

Примечание

По умолчанию предусмотрено два вида шаблонов: **Whole Week Template** («Шаблон на всю неделю») и **Blank Template** («Незаполненный шаблон»), шаблоны нельзя редактировать или удалять.

Шаблон на всю неделю

Считывание карты действительно каждый день недели, группа выходных дней отсутствует.

Незаполненный шаблон

Считывание карты недействительно каждый день недели, группа выходных дней отсутствует.

2. Добавление шаблона.
1) Нажмите **Add Template** («Добавить шаблон»), чтобы открыть соответствующее окно.
2) В поле **Template Name** («Имя шаблона») введите необходимое имя.
3) Нажмите **OK**, чтобы добавить шаблон.

3. Нажмите добавленный шаблон, расположенный в списке слева, чтобы посмотреть его свойства.

4. Добавьте график рабочей недели и примените его к шаблону.
1) Нажмите вкладку **Week Schedule** («График рабочей недели»), расположенную справа.
2) В поле **Week Schedule** («График рабочей недели») выберите настроенный график рабочей недели.

3) **Опционально.** Нажмите **Add Week Schedule** («Добавить график рабочей недели») для добавления нового графика рабочей недели.

Примечание

Подробная информация о добавлении графика рабочей недели представлена в разделе ***Добавление графика рабочей недели***.

5. Добавьте группу выходных дней и примените ее к шаблону.

Примечание

В один шаблон можно добавить до четырех групп выходных дней.

1) Нажмите **Holiday Group** («Группа выходных дней»).
2) Выберите группу выходных дней в списке.
3) **Опционально.** Нажмите **Add Holiday Group** («Добавить группу выходных дней»), чтобы добавить новый график группы выходного дня.

Примечание

Подробная информация о добавлении группы выходных дней представлена в разделе ***Добавление расписания выходных дней***.

4) Нажмите **Add** («Добавить»), чтобы добавить выбранные графики групп выходных дней в список, расположенный справа.
5) **Опционально.** Нажмите выбранную группу выходных дней в списке и нажмите **Delete** («Удалить»), чтобы удалить выбранную группу.

6. Нажмите **Save** («Сохранить») для сохранения настроек и завершите добавление шаблона.

8.1.7 Управление разрешениями

После добавления пользователя и настройки его учетных данных можно создать права доступа и определить уровень доступа пользователя к дверям.

Назначение разрешений

Для пользователей можно назначить разрешения, чтобы они могли проходить через точки контроля доступа (двери) в соответствии с назначенным разрешением.

Для назначения разрешений контроля доступа необходимо выполнить следующие действия.

Шаги

- Можно добавить до 4 разрешений на одну контрольную точку доступа на одном устройстве.
- Всего можно добавить до 128 разрешений.
- После изменения настроек разрешений необходимо снова применить эти разрешения, чтобы изменения вступили в силу. Изменения разрешений включают в себя изменения графика и шаблона, настроек разрешений, настроек разрешений пользователей и соответствующей информации (включая номер карты, отпечаток пальцев, привязку номера карты и отпечатков пальцев, пароль карты, срок действия карты и др.).

1. Нажмите **Access Control** → **Permission** («Контроль доступа → Разрешения») для перехода на соответствующую страницу.
2. Нажмите **Add** («Добавить»), чтобы открыть окно добавления разрешений.
3. В текстовом поле **Permission Name** («Имя разрешения») введите имя разрешения.
4. Выберите шаблон графика для разрешения.

   Примечание

   Перед настройкой разрешений необходимо настроить шаблон. Можно нажать **Add Template** («Добавить шаблон») для добавления шаблона. Подробная информация представлена в разделе ***Настройка графиков и шаблонов***.
5. В списке пользователей выберите пользователя, которому необходимо назначить разрешение, и нажмите **>**, чтобы добавить пользователя в список **Selected Person** («Выбранный пользователь»).
6. В списке **Access Control Point/Device** («Точка управления доступом / устройство») выберите дверь или вызывную панель, доступ к которым будет назначен выбранному пользователю, и нажмите **>**, чтобы добавить их в выбранный список.
7. Нажмите **OK**.

   Выбранные пользователи получат разрешения на вход / выход через выбранные двери / вызывные панели при помощи настроенных карт или отпечатков пальцев.
8. После добавления разрешений доступа необходимо применить их к устройству контроля доступа, чтобы изменения были применены.
   1) Выберите разрешения, которые вы хотите применить к устройству контроля доступа.

      Для выбора нескольких разрешений удерживайте клавиши **Ctrl** или **Shift**.
   2) Нажмите **Apply All** («Применить все») для начала применения выбранных разрешений к устройству контроля доступа или вызывной панели.

      Примечание

      Вы можете также нажать **Apply Changes** («Применить изменения») для применения измененной части выбранных разрешений к устройству.

Поиск назначенного разрешения

После добавления разрешений на доступ можно искать существующие разрешения, задав условия поиска.

Для поиска назначенного разрешения необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control** → **Permission** («Контроль доступа → Разрешения») для перехода на соответствующую страницу.
2. Нажмите **Advanced Search** («Расширенный поиск»), чтобы открыть соответствующее окно.
3. Задайте условия поиска.

Номер сотрудника / посетителя

Введите ключевые данные номера пользователя.

Имя сотрудника / посетителя

Введите ключевое слово имени пользователя.

Примечание

Имя сотрудника / посетителя должно включать буквы верхнего и нижнего регистра

Номер карты

Введите ключевые данные номера карты.

Имя разрешения

При вводе имени разрешения необходимо проверять буквы верхнего и нижнего регистров.

4. Нажмите **Search** («Поиск»).

   Найденные результаты будут отображены в ниже.

5. Нажмите **Reset** («Сбросить») для сброса всех условий поиска.

8.1.8 Настройка расширенных функций

После настройки информации пользователя, шаблона и разрешения доступа можно настроить расширенные функции устройства контроля доступа, такие как параметры контроля доступа, пароль аутентификации, открытие двери первой картой, запрет повторного прохода и т. д.

По умолчанию в расширенных функциях отображаются три функции: параметры контроля доступа, аутентификация при помощи считывателя карт и разные режимы аутентификации. Можно нажать **Add** («Добавить») на панели вкладок, чтобы выбрать функции, которые необходимо отобразить.

Примечание

Устройство должно поддерживать возможность использования расширенных функций.

Настройка параметров контроля доступа

После добавления устройства контроля доступа можно настроить параметры точек контроля доступа (двери или этажи), тревожных выходов, тревожных входов и считывателя карт.

Настройка параметров устройства контроля доступа

После добавления устройства контроля доступа можно настроить его параметры.

Для настройки параметров устройства контроля доступа необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Advanced Function → Access Control Parameters** («Контроль доступа → Расширенные функции → Параметры контроля доступа»), чтобы перейти на соответствующую страницу.
2. Выберите контроллер доступа, чтобы отобразить его параметры на справа.
3. Поставьте галочку **Enable** («Включить») для включения соответствующей функции.

Примечание

Отображаемые параметры могут различаться в зависимости от устройства контроля доступа.

Резервирование связи считывателя карт RS-485

При подключении карты RS-485 к устройству контроля доступа с резервированием можно включить функцию **RS-485 Communication Redundancy** («Резервирование связи RS-485»).

Введение номера карты нажатием кнопки

При активации данной функции можно ввести номер карты нажатием кнопки.

4. Нажмите **Save** («Сохранить»).
5. **Опционально.** Нажмите **Copy to** («Копировать в...») и выберите устройство контроля доступа, чтобы копировать параметры на выбранное устройство.

Настройка параметров двери

После добавления устройства контроля доступа можно настроить параметры безопасности точки доступа (двери).

Для настройки параметров точки доступа (этажа) необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Advanced Function → Access Control Parameters** («Контроль доступа → Расширенные функции → Параметры контроля доступа»), чтобы перейти на соответствующую страницу.
2. Выберите контроллер доступа и нажмите , чтобы показать двери или этажи выбранного устройства.
3. Выберите дверь или этаж, чтобы отобразить параметры в правой части.
4. Измените параметры двери или этажа.

Магнитоконтактный датчик двери

Выберите состояние дверного контакта: **Remain Closed** («Оставить дверь закрытой») или **Remain Open** («Оставить дверь открытой»).

Тип кнопки выхода

Выберите состояние кнопки выхода: **Remain Closed** («Оставить дверь закрытой») или **Remain Open** («Оставить дверь открытой»).

Время до закрытия двери

После считывания обычной карты и срабатывания реле запускается таймер для блокировки двери.

Увеличение длительности открытого состояния

Магнитоконтактный датчик двери может быть включен с соответствующей задержкой после того, как пользователь считает карту.

Тревога тайм-аута открытой двери

Тревога сработает, если дверь не будет закрыта в течение заданного периода времени.

Код принуждения

Дверь может быть открыта при помощи кода принуждения. При этом клиент может создает уведомление о событии принуждения.

Суперпароль

Пользователь может открыть дверь с помощью суперпароля.

Код отклонения

Создайте код отклонения, который можно использовать для отключения бипера считывателя карт (путем ввода кода отклонения на клавиатуре).

Примечание

- Код отклонения, суперпароль и код принуждения должны отличаться.
- Код отклонения, суперпароль и код принуждения должны отличаться от пароля аутентификации.
- Код принуждения, суперпароль и код отклонения должны содержать от 4 до 8 цифр.

5. Нажмите **Status Duration Settings** («Настройки состояния двери»), чтобы настроить состояние двери. Подробная информация представлена в разделе *Настройка продолжительности открытия двери*.
6. Нажмите **Save** («Сохранить»).
7. **Опционально.** Нажмите **Copy to** («Копировать в...») и выберите дверь / этаж, чтобы копировать параметры на выбранные двери / этажи.

Примечание

Настройки состояния двери и этажа будут также применены к выбранной двери.

Настройка продолжительности открытия / закрытия двери

Можно настроить расписание на неделю для контрольной точки (двери) устройства контроля доступа, чтобы дверь оставалась открытой / закрытой в течение заданного промежутка времени.

Для настройки продолжительности открытия / закрытия двери необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Advanced Function → Access Control Parameters** («Контроль доступа → Расширенные функции → Параметры контроля доступа»), чтобы перейти на соответствующую страницу.
2. Выберите дверь, чтобы отобразить параметры в правой части экрана.

3. Нажмите **Status Duration Settings** («Настройки состояния двери»), чтобы открыть окно состояния двери.
4. Выберите кисть состояния двери как **Remain Open** («Оставить дверь открытой») или **Remain Closed** («Оставить дверь закрытой»).
   - **Оставить дверь открытой:** дверь будет оставаться открытой в течение заданного периода времени. Цвет кисти .
   - **Оставить дверь закрытой:** дверь будет оставаться закрытой в течение заданного периода времени. Цвет кисти .
5. Перемещайте ползунок шкалы времени, чтобы нарисовать цветную полосу в расписании и настроить продолжительность.
6. **Опционально.** Выберите период времени и нажмите **Copy to Whole Week** («Применить ко всей неделе»), чтобы скопировать настройки расписания и времени на другие дни недели.
7. Нажмите **Save** («Сохранить») для сохранения состояния двери.
8. Нажмите **Save** («Сохранить»), чтобы сохранить параметры двери.

Настройка параметров считывателя карты

После добавления устройства контроля доступа можно настроить параметры его считывателя карт.

Для настройки параметров считывателя карты устройства контроля доступа необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Advanced Function → Access Control Parameters** («Контроль доступа → Расширенные функции → Параметры контроля доступа»), чтобы перейти на соответствующую страницу.
2. Выберите контроллер доступа и нажмите , чтобы показать выбранный считыватель карт.
3. Выберите считыватель карт, чтобы отобразить параметры в правой части экрана.
4. Измените параметры считывателя карт.

Примечание

Отображаемые параметры могут различаться в зависимости от устройства контроля доступа. Ниже приведены некоторые параметры. Подробная информация представлена в руководстве пользователя устройства.

Имя

Выберите наименование считывателя карт по своему выбору.

Включить считыватель карт

Выберите **Yes** («Да»), чтобы включить считыватель карт.

Полярность светодиода в норме / Полярность светодиода при ошибке / Полярность бипера

Настройте **OK LED Polarity** («Полярность светодиода в норме») / **Error LED Polarity** («Полярность светодиода при ошибке») / **Buzzer Polarity** («Полярность бипера») основной платы в соответствии с параметрами считывателя карт. Как правило, устройство получает настройки по умолчанию.

Минимальный интервал считывания карты

Если интервал считывания одной и той же карты меньше установленного значения, считывание карты будет недействительным. Можно задать данное значение в диапазоне от 0 до 255.

Максимальный интервал времени при вводе пароля

Если при вводе пароля в устройство для считывания карт интервал между нажатием двух цифр больше установленного значения, цифры, которые пользователь нажал до этого, будут автоматически удалены.

Активировать предел неудачных попыток считывания карты

Можно включить функцию сообщения о тревоге при достижении максимального количества неудачных попыток считывания карты.

Максимальное количество сбоев при считывании карты

Установите максимальное количество неудачных попыток считывания карты.

Включение тревоги тампера

Включите детектор саботажа на считывателе карт.

Определить, когда считыватель карт находится в автономном режиме

Если устройство контроля доступа не может подключиться к считывателю карт в течение установленного времени, считыватель карт отключится автоматически.

Длительность работы бипера

Настройте длительность работы бипера для считывателя карт. Доступный диапазон времени: от 0 до 5 999 с. 0 представляет непрерывную работу бипера.

Тип считывателя карт / Описание считывателя карт

Просмотр типа и описания считывателя карт. Доступны только для чтения.

Уровень распознавания отпечатков пальцев

В выпадающем списке выберите уровень распознавания отпечатков пальцев.

Режим аутентификации при помощи считывателя карт

Можно настроить отображение режима аутентификации при помощи считывателя карт по умолчанию.

5. Нажмите **Save** («Сохранить»).
6. **Опционально.** Нажмите **Copy to** («Копировать в...») и выберите считыватель карт, чтобы копировать параметры на другие считыватели карт.

Настройка параметров тревожного входа

После добавления устройства контроля доступа можно настроить параметры его сети. Для настройки параметров тревожного входа устройства контроля доступа необходимо выполнить следующие действия.

Шаги

Примечание

Если тревожный вход поставлен на охрану, редактирование параметров будет недоступно. Перед настройкой параметров необходимо снять тревожный вход с охраны.

1. Нажмите **Access Control → Advanced Function → Access Control Parameters** («Контроль доступа → Расширенные функции → Параметры контроля доступа»), чтобы перейти на соответствующую страницу.
2. Выберите устройство и нажмите , чтобы показать тревожные входы выбранного устройства контроля доступа.
3. Настройте параметры тревожного входа.

   Имя

   Измените наименование тревожного входа по своему усмотрению.

   Тип датчика

   Тип датчика тревожного входа.

   Типы зон

   Настройте тип зоны для тревожного входа.

   Чувствительность

   Тревожный вход срабатывает, когда длительность сигнала достигает установленного времени. Например, если чувствительность настроена на значение 10 мс, тревожный вход срабатывает, когда длительность сигнала достигает 10 мс.

   Запуск тревожного выхода

   Выберите тревожные выходы для запуска.
4. Нажмите **Save** («Сохранить»).
5. **Опционально.** Переведите переключатель в правом верхнем углу, чтобы поставить или снять тревожный вход с охраны.

Настройка параметров тревожного выхода

Настройте параметры тревожного выхода после добавления устройства контроля доступа.

Для настройки параметров тревожного входа устройства контроля доступа необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Advanced Function → Access Control Parameters** («Контроль доступа → Расширенные функции → Параметры контроля доступа»), чтобы перейти на соответствующую страницу.
2. Выберите устройство и нажмите , чтобы показать тревожные выходы выбранного устройства контроля доступа.
3. Настройте параметры тревожного выхода.

   Задержка на выходе

   Время задержки срабатывания тревожного выхода.
4. Нажмите **Save** («Сохранить»).
5. **Опционально.** Установите переключатель в верхнем правом углу в положение ON («Вкл.»), чтобы активировать тревожный выход.

Настройка индивидуального режима аутентификации

Можно настроить индивидуальный режим аутентификации.

Перед началом

Добавьте сотрудника / посетителя и примените изменения ко всем устройствам. Подробная информация представлена в разделах *Управление информацией о пользователе* и *Управление разрешениями.*

Шаги

1. Нажмите **Access Control → Advanced Function → Card Reader Authentication** («Контроль доступа → Расширенные функции → Аутентификация с помощью считывателя карт»), чтобы перейти на соответствующую страницу.
2. Нажмите имя устройства, чтобы перейти на страницу расширенной настройки индивидуальной аутентификации.
3. Нажмите **Add** («Добавить») и выберите пользователей и режим аутентификации.
4. Нажмите **OK** для сохранения настроек.

   Примечание

   Индивидуальная аутентификация имеет более высокий приоритет, чем другие режимы аутентификации.

   Индивидуальная аутентификация будет автоматически применена к устройству.
5. **Опционально.** На странице индивидуальной аутентификации выберите сотрудника / посетителя и нажмите **Modify** («Изменить»), чтобы изменить режим индивидуальной аутентификации пользователя.
6. **Опционально.** Если не удалось применить режим индивидуальной аутентификации, нажмите **Failed Application** («Неудавшееся применение»), чтобы посмотреть подробности. Выберите применяемые настройки из списка и нажмите **Apply Again** («Применить снова»), чтобы снова применить режим аутентификации пользователя к устройству.

Настройка аутентификации при помощи считывателя карт

Установите правила прохождения через контрольные пункты для считывателя карт устройства контроля доступа.

Для настройки режима и графика аутентификации при помощи считывателя карт необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Advanced Function → Card Reader Authentication** («Контроль доступа → Расширенные функции → Аутентификация с помощью считывателя карт»), чтобы перейти на соответствующую страницу.
2. На панели слева выберите считыватель карт, который необходимо настроить.
3. Установите режим аутентификации для считывателя карт.
   1) Нажмите на кнопку **Configuration** («Настройки»).

   Примечание

   - Пароль представляет собой пароль карты, установленный при выдаче карты. Дополнительная информация представлена в разделе *Добавление одного сотрудника*.
   - Пароль аутентификации — это пароль, установленный для открытия двери. Подробная информация представлена в разделе *Настройка пароля аутентификации*.
   - Поддерживаемый режим аутентификации при помощи считывателя карт зависит от устройства. Отдельные параметры зависят от фактической модели устройства.

   2) Выберите режимы и добавьте их в список выбранных режимов.
   3) **Опционально.**
   4) Нажмите или для настройки порядка отображения.
   5) Нажмите **OK**.

   После завершения процедуры выбора режимов, они будут отображаться на экране в виде значков.
4. Нажмите на значок, чтобы выбрать режим аутентификации устройства для считывания карт. Перемещайте ползунок шкалы времени, чтобы нарисовать цветную полосу в графике. Это значит, что в данный отрезок времени будет использоваться аутентификация при помощи считывателя карт.
5. Повторите этот шаг для установки других отрезков времени.
6. **Опционально.** Выберите настроенный день и нажмите кнопку **Copy to Week** («Применить ко всем дням недели»), чтобы применить эти настройки ко всем дням недели.
7. **Опционально.** Нажмите **Copy to** («Копировать в»), для копирования настроек в другие считыватели карт.
8. Нажмите **Save** («Сохранить»).

Настройка нескольких режимов аутентификации

Настройте управление картами по группам и установите аутентификацию для нескольких карт в одной точке контроля доступа (двери).

Перед началом

Настройте разрешения карты и примените разрешения к устройству контроля доступа. Подробная информация представлена в разделе ***Назначение разрешений***.

Выполните следующие действия, чтобы настроить аутентификацию сразу нескольких карт для одной точки контроля доступа (двери).

Шаги

1. Нажмите **Access Control → Advanced Function → Multiple Authentication** («Контроль доступа → Расширенные функции → Несколько режимов аутентификации»), чтобы перейти на соответствующую страницу.
2. Выберите устройство контроля доступа из списка.
3. Добавьте группу карт для устройства контроля доступа.
   1) На панели **Set Card Group** («Настройка группы карт») нажмите **Add** («Добавить»).
   2) Создайте имя для группы своему усмотрению.
   3) Укажите время начала и время окончания периода действия группы карт.
   4) Выберите карты, которые нужно добавить в группу карт.
   5) Нажмите **OK**.
4. Выберите точку контроля доступа (дверь) выбранного устройства на панели **Set Authentication Group** («Настройка группы аутентификации»).
5. Введите временной интервал для считывания карты.
6. Добавьте группу аутентификации для выбранной точки контроля доступа.
   1) На панели **Set Authentication Group** («Настройка группы аутентификации») нажмите **Add** («Добавить»).
   2) Из выпадающего списка выберите настроенный шаблон для группы аутентификации.

      Примечание

      Информация о настройке шаблона представлена в разделе ***Настройка графиков и шаблонов***.

   3) Выберите тип аутентификации группы из выпадающего списка **Local Authentication** («Локальная аутентификация»), **Local Authentication and Remotely Open Door** («Локальная аутентификация и удаленное открытие двери») или **Local Authentication and Super Password** («Локальная аутентификация и пароль суперпользователя»).

      Локальная аутентификация

      Аутентификация с помощью устройства контроля доступа.

      Локальная аутентификация и удаленное открытие двери

      Аутентификация через устройство контроля доступа и клиентское ПО. После считывания карты появится окно. Дверь может быть разблокирована через клиентское ПО.

Рисунок 8-3. Удаленное открытие двери

Примечание

Выберите **Offline Authentication** («Автономная аутентификация»), чтобы активировать функцию аутентификации по суперпаролю, если устройство контроля доступа было отключено от клиентского ПО.

Локальная аутентификация и суперпароль

Аутентификация с помощью устройства контроля доступа и суперпароля.

4) Выберите добавленную группу карт из списка, расположенного в нижней части экрана слева, и нажмите +, чтобы добавить выбранную группу карт в список справа.
5) **Опционально.** Нажмите ↑ или ↓, чтобы настроить порядок считывания карт.
6) Нажмите на добавленную группу аутентификации в списке справа, чтобы установить количество считываний карт.

Примечание

- Количество попыток считывания карты должно быть больше 0 и не превышать количество добавленных карт в соответствующей группе.
- Максимальное количество считываний карты: 16.

7) Нажмите **OK**.

Примечание

- Для каждой точки контроля доступа (двери) можно добавить до 4 групп аутентификации.
- В группу аутентификации с типом **Local Authentication** («Локальная аутентификация») можно добавить до восьми групп карт.
- В группу аутентификации с типом **Local Authentication and Super Password** («Локальная аутентификация и пароль суперпользователя») или **Local Authentication and Remotely Open Door** («Локальная аутентификация и удаленное открытие двери») можно добавить до 7 групп карт.

7. Нажмите **Save** («Сохранить»).

Настройка открытия двери первой картой

Для одной точки контроля доступа можно назначить несколько первых карт. После первого считывания карты несколько других пользователей получат доступ к дверям и разрешения на другие действия.

Перед началом

Настройте разрешения карты и примените разрешения к устройству контроля доступа. Подробная информация представлена в разделе ***Назначение разрешений***.

Для настройки открытия двери первой картой необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Advanced Function → Open Door with First Card** («Контроль доступа → Расширенные функции → Открытие двери первой картой») для перехода на соответствующую страницу.
2. Выберите устройство контроля доступа из списка.
3. Из выпадающего списка выберите режим для каждого устройства: **Remain Open with First Card** («Оставить дверь открытой при считывании первой карты»), **Disable Remain Open with First Card** («Не оставлять дверь открытой при считывании первой карты») или **First Card Authorization** («Авторизация первой карты»).

   Оставить дверь открытой при считывании первой карты

   После считывания первой карты дверь остается открытой в течение заданного промежутка времени и до истечения оставшегося времени открытия. При выборе этого режима необходимо установить длительность открытого состояния двери.

   Примечание

   Допустимый диапазон длительности открытого состояния двери: от 0 до 1440 минут. По умолчанию длительность открытого состояния составляет 10 минут.

   Не оставлять дверь открытой при считывании первой карты

   Выключить функцию «Оставить дверь открытой при считывании первой карты».

   Авторизация первой карты

   Все режимы аутентификации (за исключением авторизации суперкарты, суперпароля, отпечатков пальцев суперпользователя, принудительной карты и отпечатков пальцев при принуждении) доступны только после авторизации первой карты.

   Примечание

   Авторизация первой карты действует только в текущий день. Срок действия авторизации истекает после 24:00 текущего дня.

   Примечание

   Чтобы отключить режим первой карты, необходимо считать первую карту еще раз.

4. В списке **First Card List** («Список первых карт») нажмите **Add** («Добавить»).

5. Выберите карту в списке и нажмите **OK**, чтобы добавить выбранную карту в качестве первой карты. Добавленная карта будет отображаться на панели **First Card List** («Список первых карт»).
6. **Опционально.** Выберите карту из списка и нажмите **Delete** («Удалить»), чтобы удалить карту из списка первых карт.
7. Нажмите **Save** («Сохранить»).

Настройка запрета двойного прохода

Установите контрольный пункт проверки доступа, через который возможен проход одного человека после считывания карты.

Перед началом

Включите функцию запрета двойного прохода по маршруту.

Для настройки функции запрета двойного прохода выполните следующие действия.

Шаги

Примечание

Для устройства контроля доступа можно одновременно настроить функцию запрета двойного прохода или блокировки нескольких дверей. Подробная информация о блокировке нескольких дверей представлена в разделе ***Настройка блокировки нескольких дверей***.

1. Нажмите **Access Control → Advanced Function → Anti-Passback** («Контроль доступа → Расширенные функции → Запрет двойного прохода»), чтобы перейти на соответствующую страницу.
2. Выберите устройство контроля доступа в списке.
3. Выберите считыватель карт в качестве точки начала маршрута в поле **First Card Reader** («Первый считыватель карт»).
4. Нажмите на текстовое поле выбранного считывателя карт в колонке **Card Reader Afterward** («Следующий считыватель карт»), чтобы открыть выбранный считыватель карт.
5. Выберите считыватель карт, который следует за первым считывателем карт.

   Примечание

   Для одного считывателя карт можно добавить до 4 последующих считывателей карт.
6. В диалоговом окне нажмите **OK**, чтобы сохранить выбранные настройки.
7. Нажмите **Save** («Сохранить») в правом верхнем углу на странице запрета двойного прохода для сохранения настроек и их применения.

Примечание

Супер-учетные данные, такие как суперкарта, суперпароль, супер-отпечаток пальца и т. д., могут не следовать правилам запрета двойного прохода.

Пример

Установите маршрут считывания карты.

Выберите Reader In_01 в качестве начала маршрута, а Reader In_02, Reader Out_04 в качестве связанных считывателей карт. После этого пользователь сможет пройти через точку контроля доступа, считав карту в следующей последовательности: Reader In_01, Reader In_02 и Reader Out_04.

Настройка запрета двойного прохода на различных контроллерах

Можно установить запрет двойного прохода для считывателей карт в различных устройствах контроля доступа. Считайте карту в соответствии с настроенным маршрутом считывания. Только один пользователь может пройти точку контроля доступа после считывания карты.

Примечание

Устройство должно поддерживать данную функцию.

Настройка запрета двойного прохода по маршруту на основе данных карты

Маршрут с запретом двойного прохода зависит от маршрута считывания карты. Сначала необходимо настроить первый считыватель карт, затем — последующие. Таким образом сформируется маршрут с запретом двойного прохода в соответствии с записями входа и выхода на карте.

Для настройки маршрута с запретом двойного прохода в соответствии с записями входа и выхода на карте необходимо выполнить следующие действия.

Шаги

Примечание

В настоящее время устройство поддерживает карту M1, и этот сектор не может быть зашифрован. Подробная информация о шифровании сектора представлена в разделе ***Проверка шифрования M1-карты***.

1. Нажмите **Access Control → Advanced Function → Cross-Controller Anti-passing Back** («Контроль доступа → Расширенные функции → Запрет двойного прохода на различных контроллерах»), чтобы перейти на соответствующую страницу.
2. Нажмите **Enable Cross-Controller Anti-passing Back** («Включить запрет двойного прохода на различных контроллерах»), чтобы включить функцию.
3. Выберите **Based on Card** («На основе карты») в качестве режима запрета двойного прохода.
4. В качестве правила выберите **Route Anti-pass Back** («Запрет двойного прохода по маршруту»).
5. Установите идентификатор сектора.
6. Нажмите **Select Access Controller** («Выбрать контроллер доступа»), чтобы выбрать устройство для защиты от двойного прохода.

   Примечание

   Можно добавить до 64 устройств с функцией защиты двойного прохода.

7. Сначала необходимо настроить первый считыватель карт, затем — последующие.
1) В области считывателя карт нажмите значок слева, чтобы установить считыватель карт в качестве первого устройства.

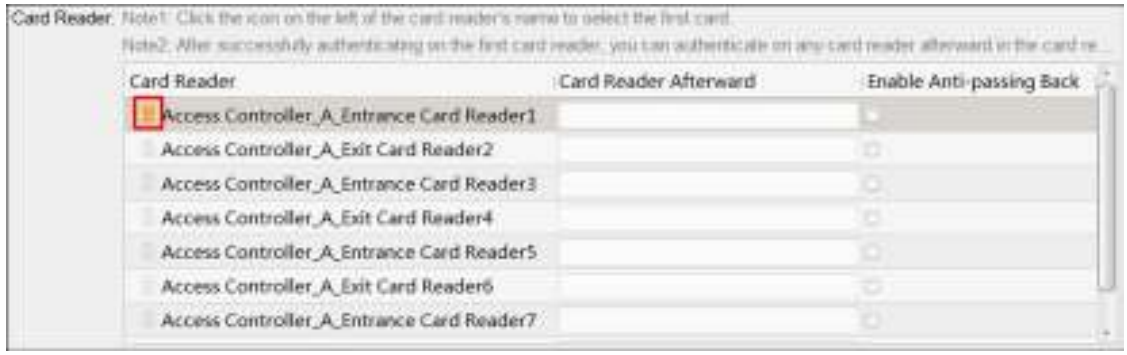


Рисунок 8-4. Выбор первого считывателя карт

Иконка превратится в .
2) Выберите последующие считыватели карт во всплывающем окне.

Примечание

- Для одного считывателя карт можно добавить до 16 дополнительных считывателей карт.
- Отображаемые дополнительные считыватели карт должны быть расположены в порядке выполнения аутентификации.

3) Нажмите **Enable Anti-Pass Back** («Включить функцию запрета двойного прохода»), чтобы включить функцию запрета двойного прохода.

8. Нажмите **Save** («Сохранить»).

Настройка запрета двойного прохода по маршруту на основе данных сети

Маршрут с запретом двойного прохода зависит от маршрута считывания карты. Сначала необходимо настроить первый считыватель карт, затем — последующие. Таким образом сформируется маршрут с запретом двойного прохода в соответствии с записями входа и выхода на считывателе карт.

Для настройки маршрута с запрет двойного прохода в соответствии с записями входа и выхода на считывателе карт необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Advanced Function → Cross-Controller Anti-passing Back** («Контроль доступа → Расширенные функции → Запрет двойного прохода на различных контроллерах»), чтобы перейти на соответствующую страницу.
2. Нажмите **Enable Cross-Controller Anti-passing Back** («Включить запрет двойного прохода на различных контроллерах»), чтобы включить функцию.
3. Выберите **Based on Network** («На основе сети») в качестве режима запрета двойного прохода.
4. В качестве правила выберите **Route Anti-pass Back** («Запрет двойного прохода по маршруту»).

5. В выпадающем списке выберите сервер для настройки запрета двойного прохода.

Примечание

- Можно нажать **Delete Card Swiping Record** («Удалить запись считывания карты») и выбрать карту во всплывающем окне, чтобы удалить информацию о считывании карты на всех устройствах.
- На выбранном сервере может быть сохранено до 5000 записей.

6. Нажмите **Select Access Controller** («Выбрать контроллер доступа»), чтобы выбрать устройство для защиты от двойного прохода.

Примечание

Можно добавить до 64 устройств с функцией защиты двойного прохода.

7. Сначала необходимо настроить первый считыватель карт, затем — последующие.

1) В области считывателя карт нажмите значок слева, чтобы установить считыватель карт в качестве первого устройства.

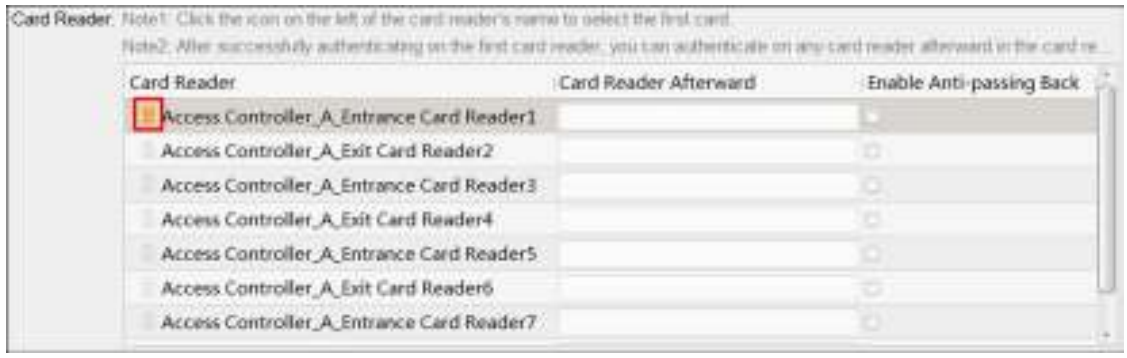


Рисунок 8-5. Выбор первого считывателя карт

Иконка превратится в .

2) Выберите последующие считыватели карт во всплывающем окне.

Примечание

- Для одного считывателя карт можно добавить до 16 дополнительных считывателей карт.
- Отображаемые дополнительные считыватели карт должны быть расположены в порядке выполнения аутентификации.

3) Нажмите **Enable Anti-Pass Back** («Включить функцию запрета двойного прохода»), чтобы включить функцию запрета двойного прохода.

8. Нажмите **Save** («Сохранить»).

Настройка запрета двойного прохода на основе данных считывания карты в точках входа / выхода

Можно настроить считыватель карт только для входа и выхода, без настройки первого считывателя карт и дополнительных считывателей карт. Таким образом сформируется маршрут с запретом двойного прохода в соответствии с записями входа и выхода на карте.

Для настройки запрета двойного прохода в соответствии с записями входа и выхода на карте необходимо выполнить следующие действия.

Шаги

Примечание

В настоящее время устройство поддерживает карту M1, и этот сектор не может быть зашифрован. Подробная информация о шифровании сектора представлена в разделе ***Проверка шифрования M1-карты***.

1. Нажмите **Access Control → Advanced Function → Cross-Controller Anti-passing Back** («Контроль доступа → Расширенные функции → Запрет двойного прохода на различных контроллерах»), чтобы перейти на соответствующую страницу.
2. Нажмите **Enable Cross-Controller Anti-passing Back** («Включить запрет двойного прохода на различных контроллерах»), чтобы включить функцию.
3. Выберите **Based on Card** («На основе карты») в качестве режима запрета двойного прохода.
4. В качестве правила выберите **Entrance/Exit Anti-passing Back** («Запрет двойного прохода на входе / выходе»).
5. Установите идентификатор сектора.
6. Нажмите **Select Access Controller** («Выбрать контроллер доступа»), чтобы выбрать устройство для защиты от двойного прохода.

   Примечание

   Можно добавить до 64 устройств с функцией защиты двойного прохода.
7. В поле считывателей карт нажмите **Enable Anti-pass Back** («Включить запрет двойного прохода»), чтобы выбрать считыватель карт в точке входа и выхода.

   Примечание

   Необходимо настроить как минимум один считыватель карт в точке входа и выхода.
8. Нажмите **Save** («Сохранить»).

Настройка запрета двойного прохода на основе данных сети в точках входа / выхода

Можно настроить считыватель карт только для входа и выхода, без настройки первого считывателя карт и дополнительных считывателей карт. Таким образом сформируется маршрут с запретом двойного прохода в соответствии с записями входа и выхода на считывателе карт.

Для настройки запрета двойного прохода в соответствии с записями входа и выхода на считывателе карт необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Advanced Function → Cross-Controller Anti-passing Back** («Контроль доступа → Расширенные функции → Запрет двойного прохода на различных контроллерах»), чтобы перейти на соответствующую страницу.
2. Нажмите **Enable Cross-Controller Anti-passing Back** («Включить запрет двойного прохода на различных контроллерах»), чтобы включить функцию.
3. Выберите **Based on Network** («На основе сети») в качестве режима запрета двойного прохода.
4. В качестве правила выберите **Entrance/Exit Anti-passing Back** («Запрет двойного прохода на входе / выходе»).
5. В выпадающем списке выберите сервер для настройки запрета двойного прохода.

   Примечание

   - Можно нажать **Delete Card Swiping Record** («Удалить запись считывания карты») и выбрать карту во всплывающем окне, чтобы удалить информацию о считывании карты на всех устройствах.
   - На выбранном сервере может быть сохранено до 5000 записей.
6. Нажмите **Select Access Controller** («Выбрать контроллер доступа»), чтобы выбрать устройство для защиты от двойного прохода.

   Примечание

   Можно добавить до 64 устройств с функцией защиты двойного прохода.
7. В поле считывателей карт нажмите **Enable Anti-pass Back** («Включить запрет двойного прохода»), чтобы выбрать считыватель карт в точке входа и выхода.

   Примечание

   Необходимо настроить как минимум один считыватель карт в точке входа и выхода.
8. Нажмите **Save** («Сохранить»).

Настройка блокировки нескольких дверей

Вы можете установить блокировку нескольких дверей для нескольких дверей одного контроллера доступа. Чтобы открыть одну из дверей, другие двери должны оставаться закрытыми. Это означает, что в блокировке комбинированной группы дверей одновременно может открываться до одной двери.

Для настройки блокировки нескольких дверей необходимо выполнить следующие действия.

Шаги

Примечание

- Функция блокировки нескольких дверей поддерживается только устройством контроля доступа, которое имеет более одной точки контроля доступа (дверей).
- Для устройства контроля доступа можно одновременно настроить функцию запрета двойного прохода или блокировки нескольких дверей. Информация о настройке функции запрета двойного прохода представлена в разделе ***Настройка запрета двойного прохода***.

1. Нажмите **Access Control → Advanced Function → Multi-door Interlocking** («Контроль доступа → Расширенные функции → Блокировка нескольких дверей»), чтобы перейти на соответствующую страницу.
2. Выберите устройство контроля доступа из списка.
3. Нажмите **Add** («Добавить») на панели **Multi-door Interlocking List** («Список блокировки нескольких дверей»), чтобы открыть **Add Access Control Point** («Добавить точку контроля доступа») и открыть соответствующее окно.
4. Выберите точки контроля доступа из списка.

   Примечание

   В одну комбинацию блокировки нескольких дверей можно добавить до четырех дверей.
5. Нажмите **OK**, чтобы добавить выбранные точки контроля доступа для блокировки. Настроенная комбинация блокировки нескольких дверей будет отображаться на панели **Multi-door Interlocking List** («Список блокировки нескольких дверей»).
6. **Опционально.** Выберите из списка добавленную комбинацию блокировки нескольких дверей и нажмите **Delete** («Удалить»), чтобы удалить комбинацию.
7. Нажмите **Save** («Сохранить»).

Настройка пароля аутентификации

Можно ввести пароль аутентификации на клавиатуре считывателя карт, чтобы открыть дверь после введения пароля аутентификации.

Для настройки пароля аутентификации необходимо выполнить следующие действия.

Примечание

- Устройство контроля доступа должно поддерживать функцию пароля аутентификации.
- К одному устройству контроля доступа можно добавить до 500 карт с паролем аутентификации. Пароль должен быть уникальным и не повторяться.

Шаги

1. Нажмите **Access Control → Advanced Function → Authentication Password** («Контроль доступа → Расширенные функции → Пароль аутентификации»), чтобы перейти на соответствующую страницу.
2. Выберите устройство контроля доступа из списка. Все примененные карты и изображения лиц будут отображаться на панели списка карт.

   Примечание

   Подробная информация о настройке и применении разрешений представлена в разделе ***Назначение разрешений***.

3. Выберите поле каждой карты в столбце **Password** («Пароль»), чтобы ввести пароль аутентификации.

Примечание

Пароль аутентификации должен содержать от 4 до 8 цифр.

4. Нажмите **Save** («Сохранить») в правом верхнем углу страницы пароля аутентификации, чтобы сохранить настройки.
   Функция пароля аутентификации будет включена автоматически. Можно установить режим аутентификации считывателя карт устройства контроля доступа: **Card** («Карта») или **Authentication Password** («Пароль аутентификации»). Подробная информация приведена в разделе ***Настройка режима и расписания аутентификации при помощи считывателя карт***.

Настройка правила Wiegand

Основываясь на знании правил загрузки для стороннего Wiegand, можно установить несколько настраиваемых правил Wiegand для связи между устройством и сторонними считывателями карт.

Перед началом

Подключите сторонние считыватели карт к устройству.

Для настройки Wiegand считывателей карт сторонних производителей необходимо выполнить следующие действия.

Шаги

Примечание

- По умолчанию устройство отключает настраиваемую функцию Wiegand. Если устройство включает настраиваемую функцию Wiegand, все интерфейсы Wiegand в устройстве будут использовать настроенный протокол Wiegand.
- Можно установить до 5 Wiegand.
- Подробная информация о настраиваемом Wiegand представлена в разделе ***Описание настраиваемых правил Wiegand***.

1. Нажмите **Access Control → Advanced Function → Custom Wiegand** («Контроль доступа → Расширенные функции → Настраиваемый Wiegand»), чтобы перейти на соответствующую страницу.
2. Выберите настраиваемый Wiegand слева.
3. Нажмите **Enable** («Включить»), чтобы включить пользовательскую настройку Wiegand.
4. Создайте имя для Wiegand.

Примечание

Имя настраиваемого Wiegand может содержать до 32 символов.

5. Нажмите **Select Device** («Выбрать устройство»), чтобы выбрать устройство контроля доступа для настройки пользовательского интерфейса Wiegand.
6. Установите режим четности в соответствии со свойством стороннего считывателя карт.

Примечание

- Общая длина допускается до 80 бит.
- Старт-бит и длина нечетности и старт-бит и длина четности находятся в диапазоне от 1 до 80 бит.
- Старт-бит ID карты, кода производителя, кода сайта и производителя оборудования должны находиться в диапазоне от 1 до 80 бит.

7. Установите правило преобразования выходного сигнала.

1) Нажмите **Set Rule** («Установить правило»), чтобы открыть окно установки правила преобразования выходного сигнала.

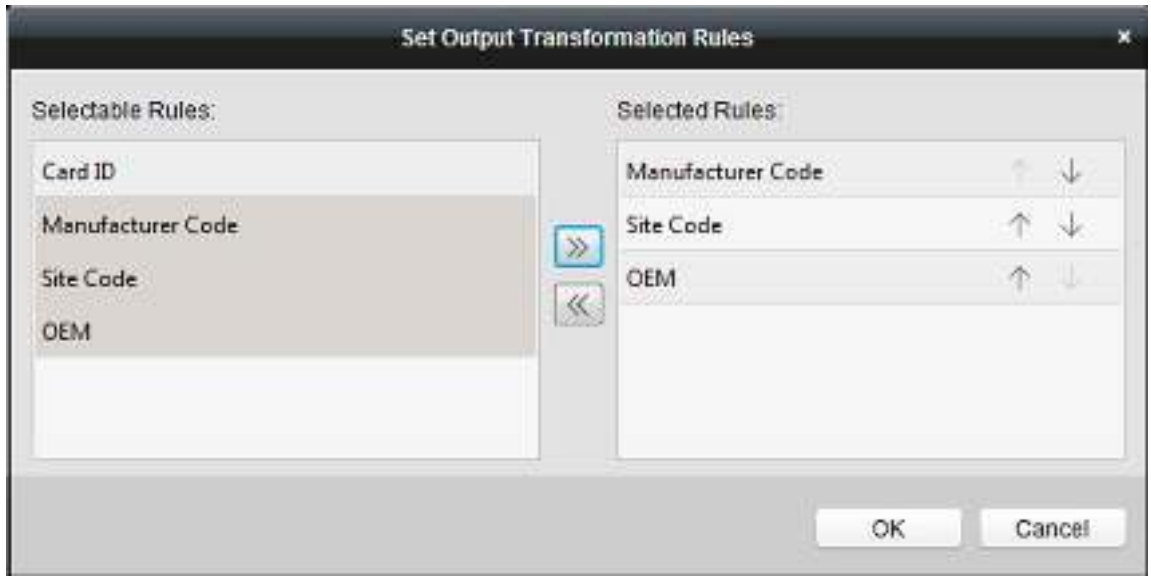


Рисунок 8-6. Настройка правила преобразования выходного сигнала

2) Выберите правила в левом списке.
3) Нажмите , чтобы переместить выбранные правила в список справа.
4) **Опционально.** Нажмите или , чтобы изменить порядок правил.
5) Нажмите **OK**.
6) На вкладке настраиваемого Wiegand установите старт-бит правила, длину и десятичную цифру.

8. Нажмите **Save** («Сохранить»).

8.1.9 Поиск события контроля доступа

Можно искать события истории контроля доступа, включая удаленное событие и локальное событие, через клиент.

Поиск событий контроля доступа, хранящихся в локальном клиенте

Можно искать записи и события доступа к истории из базы данных текущего клиента и экспортировать записи на локальный компьютер.

Шаги

Примечание

Можно искать события контроля доступа за последние три месяца.

1. Нажмите **Access Control → Search → Access Control Event** («Контроль доступа → Поиск → Событие контроля доступа»), чтобы перейти на соответствующую страницу.
2. Выберите **Local Event** («Локальное событие») в качестве источника события.
3. Задайте условия поиска, такие как устройства, тип события, время возникновения события и т. д.
4. Нажмите **Search** («Поиск»), чтобы начать поиск событий контроля доступа. Отобразятся соответствующие события контроля доступа.
5. **Опционально.** После поиска события можно выполнить следующие действия.

Просмотр сведений о сотруднике / посетителе	При возникновении события контроля доступа, которое инициируется сотрудником / посетителем, нажмите событие, чтобы просмотреть сведения о сотруднике / посетителе, включая ID, имя, организацию, номер телефона, контактный адрес и фотографию.
Просмотр видео	При возникновении событий с записью видео нажмите **Playback** («Воспроизведение»), чтобы просмотреть видеофайл, записанный при срабатывании тревоги. **Примечание** Подробная информация о настройке камеры представлена в разделе ***Настройка действий на клиентском ПО при событии доступа***.
Экспорт информации о событии	Нажмите **Export** («Экспорт»), чтобы экспортировать результаты поиска на компьютер в формате CSV.

Поиск событий контроля удаленного доступа

Можно выполнить поиск записей событий контроля доступа, хранящихся на устройстве контроля доступа.

Для поиска событий контроля доступа, хранящихся на устройстве контроля доступа, необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Search → Access Control Event** («Контроль доступа → Поиск → Событие контроля доступа»), чтобы перейти на соответствующую страницу.
2. Выберите **Remote Event** («Удаленное событие») в качестве источника события.
3. Задайте необходимые условия поиска.
4. Нажмите **Search** («Поиск»).

   Отобразятся соответствующие события контроля доступа.
5. **Опционально.** Нажмите **Export** («Экспорт»), чтобы экспортировать результаты поиска на компьютер в формате CSV.

8.1.10 Настройка привязки тревоги контроля доступа

Для добавленного устройства контроля доступа можно настроить привязку действий, например, привязку к клиенту, привязку к устройству или привязку к нескольким устройствам.

Настройка действий на клиентском ПО при событии доступа

Можно назначить действия клиента в соответствии с событием, настроив правило. Например, при обнаружении тревожного события срабатывает звуковое предупреждение, уведомляющее сотрудников службы безопасности.

Шаги

Примечание

Привязанные действия означают связанные операции клиентского ПО, в том числе звуковые предупреждения, отправка Email и т.д.

1. Нажмите **Event Management → Access Control Event** («Управление событием → Событие доступа»).

   Добавленные устройства контроля доступа отобразятся в списке.
2. Выберите ресурс из списка устройств.

   На экране отобразятся типы событий, которые поддерживают выбранный ресурс.
3. Выберите событие (события) и нажмите **Edit Priority** («Изменить приоритет»), чтобы установить приоритет события (событий), который можно использовать для фильтрации событий в центре событий.
4. Установите действия, привязанные к событию.
   1) Выберите событие и нажмите **Edit Linkage** («Изменить привязку»), чтобы настроить действия клиентского ПО при возникновении события.

   Звуковое предупреждение

   Клиентское программное обеспечение выдает звуковое предупреждение при срабатывании тревоги. Выберите сигнал для звукового предупреждения.

   Примечание

   Подробная информация о настройке звукового сигнала тревоги представлена в разделе *Настройка звукового сигнала* Руководства пользователя клиентского программного обеспечения.

   Привязка Email

   Отправьте электронное уведомление о тревоге одному или нескольким получателям.
   2) Нажмите **OK**.
5. Обнаруженное событие будет отправлено в клиентское ПО, которое запустит привязанные действия.
6. **Опционально.** Нажмите кнопку **Copy to** («Копировать на»), чтобы скопировать настройки события на другое устройство контроля доступа, тревожный вход, дверь или считыватель карт.

Настройка привязки устройств при тревожном событии устройства контроля доступа

Можно настроить привязку действий устройства контроля доступа при срабатывании тревожного события. При тревожном событии устройство может активировать тревожный выход, бипер хоста и другие действия.

Для настройки привязки действий устройства контроля доступа при срабатывании тревожного события необходимо выполнить следующие действия.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **Event Management → Event Card Linkage** («Управление событиями → Привязка события карты»).
2. Выберите устройство контроля доступа из списка слева.
3. Нажмите кнопку **Add** («Добавить») для добавления новой привязки.
4. Вы можете выбрать в качестве **Event source** («Источник события») значение **Event Linkage** («Привязка события»).
5. Выберите тип и описание тревоги, чтобы настроить привязку.
6. На панели **Linkage Target** («Привязка цели») установите переключатель во включенное положение, чтобы включить соответствующее действие.

   Бипер хоста

   Устройство контроля доступа выдаст звуковое предупреждение.

   Захват

   Запуск захвата изображений в режиме реального времени.

   Запись

   Запуск записи тревожного события.

   Примечание

   Функция записи должна поддерживаться на устройстве.

   Бипер считывателя карт

   Считыватель карт выдаст звуковое предупреждение.

   Тревожный выход

   Тревожный выход будет активирован для уведомления.

   Зоны

   Постановка области на охрану или снятие области с охраны.

   Примечание

   Устройство должно поддерживать функцию зонирования.

Точка контроля доступа

Возможно только одно из следующих состояний двери: открыта / закрыта, оставить

Примечание

открытой / оставить закрытой.

- Возможно только одно из следующих состояний двери: открыта / закрыта, оставить открытой / оставить закрытой.
- Целевая дверь и дверь, используемая в качестве источника, не могут являться одной дверью.

Воспроизведение голосового предупреждения

Вызывает срабатывание голосового предупреждения. Настроенное голосовое предупреждение будет воспроизведено в соответствии с заданным режимом воспроизведения.

7. Нажмите **Save** («Сохранить»).
8. **Опционально.** После привязки нескольких устройств можно выполнить одно или несколько из следующих действий:

Изменение настроек привязки	Выберите настроенные параметры привязки из списка устройств. Измените параметры события, в том числе источник события и цель привязки.
Удаление настроек привязки	Выберите настроенные параметры привязки из списка устройств и нажмите **Delete** («Удалить»), чтобы удалить их.

Настройка привязки действий устройства при считывании карт

Настройте привязку действий устройства контроля доступа при возникновении события доступа. Считывание определенной карты может инициировать срабатывание тревожного выхода, бипера хоста и другие действия устройства.

Для настройки действий устройства контроля доступа при считывании карты необходимо выполнить следующие действия.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **Event Management → Event Card Linkage** («Управление событиями → Привязка события карты»).
2. Выберите устройство контроля доступа из списка слева.
3. Нажмите кнопку **Add** («Добавить») для добавления новой привязки.
4. Выберите **Card Linkage** («Привязка карты») в качестве источника события.
5. Введите номер карты и выберите карту из выпадающего списка.
6. Выберите считыватель карт, чтобы запустить привязанные события.

7. На панели **Linkage Target** («Привязка цели») установите переключатель во включенное положение, чтобы включить соответствующее действие.

Бипер хоста

Устройство контроля доступа выдаст звуковое предупреждение.

Захват

Запуск захвата изображений в режиме реального времени.

Запись

Запуск записи тревожного события.

Примечание

Функция записи должна поддерживаться на устройстве.

Бипер считывателя карт

Считыватель карт выдаст звуковое предупреждение.

Тревожный выход

Тревожный выход будет активирован для уведомления.

Зоны

Постановка области на охрану или снятие области с охраны.

Примечание

Устройство должно поддерживать функцию зонирования.

Точка контроля доступа

Возможно только одно из следующих состояний двери: открыта / закрыта, оставить

Примечание

открытой / оставить закрытой.

Возможно только одно из следующих состояний двери: открыта / закрыта, оставить открытой / оставить закрытой.

Audio Play («Воспроизведение голосового предупреждения»)

Вызывает срабатывание голосового предупреждения. Настроенное голосовое предупреждение будет воспроизведено в соответствии с заданным режимом воспроизведения.

8. Нажмите **Save** («Сохранить»).

При считывании карты (настроенной в соответствии с шагом 5) с помощью считывателя карт (настроенного в соответствии с шагом 6) запускаются привязанные действия (настроенные в соответствии с шагом 7).

9. **Опционально.** После привязки нескольких устройств можно выполнить одно или несколько из следующих действий:

Удаление настроек привязки	Выберите настроенные параметры привязки из списка устройств и нажмите **Delete** («Удалить»), чтобы удалить их.
	Выберите настроенные параметры привязки из списка устройств.
Изменение настроек привязки	Измените параметры события, в том числе источник события и цель привязки.

Настройка привязки ID сотрудника

Ввод ID сотрудника на указанном считывателе карт может инициировать действия других устройств, такие как срабатывание тревожного выхода, открытие двери и т. д.

Перед началом
Добавьте пользователя. Подробная информация представлена в разделе *Управление информацией о пользователе*.

Шаги
1. Нажмите **Event Management → Event Card Linkage** («Управление событиями → Привязка события карты»), чтобы перейти на соответствующую страницу.
2. Выберите устройство контроля доступа из списка слева.
3. Нажмите кнопку **Add** («Добавить») для добавления новой привязки.
4. Выберите **Employee ID Linkage** («Привязка ID сотрудника») в качестве источника события.
5. Выберите ID сотрудника из выпадающего списка.
6. На панели **Linkage Target** («Привязка цели») установите переключатель во включенное положение, чтобы включить соответствующее действие.

   Бипер хоста

   Устройство контроля доступа выдаст звуковое предупреждение.

   Захват

   Запуск захвата изображений в режиме реального времени.

   Тревожный выход

   Тревожный выход будет активирован для уведомления.

   Точка контроля доступа

   Возможно только одно из следующих состояний двери: открыта / закрыта, оставить

   Примечание
   открытой / оставить закрытой.

   Возможно только одно из следующих состояний двери: открыта / закрыта, оставить открытой / оставить закрытой.
7. Нажмите **Save** («Сохранить»).
   Ввод ID сотрудника в выбранный считыватель карт может инициировать определенные действия (настроенные на шаге 7).

8. После привязки нескольких устройств можно выполнить одно или несколько из следующих действий:

Удаление настроек привязки	Выберите настроенные параметры привязки из списка устройств и нажмите **Delete** («Удалить»), чтобы удалить их.
Изменение настроек привязки	Выберите настроенные параметры привязки из списка устройств. Измените параметры события, в том числе источник события и цель привязки.

Настроить привязку различных устройств

Можно назначить запуск действия другого устройства контроля доступа при тревожном событии, установив соответствующее правило.

Примечание

Устройство должно поддерживать данную функцию.

Настройка привязки различных устройств при тревожном событии устройства контроля доступа

Тревожное событие устройства контроля доступа может инициировать настроенные действия другого устройства контроля доступа, например, срабатывание тревожного выхода, открытие двери и т. д. Существует четыре типа событий: событие устройства, событие тревожного входа, событие двери и событие считывателя карт.

Для настройки действий других устройств контроля доступа при тревожном событии необходимо выполнить следующие действия.

Шаги

Примечание

Устройства должны поддерживать данную функцию.

1. Нажмите **Event Management → Cross-Device Linkage** («Управление событиями → Привязка различных устройств»), чтобы войти в интерфейс настройки привязки устройств.

2. Нажмите **Add** («Добавить») для добавления новой привязки.

3. Выберите тип привязки **Event Linkage** («Привязка события»).

4. Настройте источник события.

1) Выберите устройство контроля доступа в качестве устройства-источника события.

2) Выберите тип события контроля доступа.

Событие устройства

Выберите тип события из выпадающего списка.

Тревожный вход

Выберите тип события (событие области или событие тревожного входа) и выберите имя области или имя тревожного входа из списка.

Событие двери

Выберите тип события и выберите точку контроля доступом из списка.

Событие считывателя карт

Выберите тип события и выберите считыватель карт из списка.

5. Установите целевое устройство контроля доступом в качестве цели привязки.

1) Выберите устройство контроля доступа из списка в качестве цели привязки.
2) Установите переключатель во включенное положение, чтобы включить привязку.

Тревожный выход

Тревожный выход устройства будет активирован и будет направлено уведомление.

Точка контроля доступа

Возможно только одно из следующих состояний двери: открыта / закрыта, оставить открытой / оставить закрытой.

6. Нажмите **Save** («Сохранить»).

Настройка привязки различных устройств при считывании карт

Считывание определенной карты на указанном считывателе карт может инициировать действия других устройств, такие как срабатывание тревожного выхода, открытие двери и т. д.

Для настройки привязки устройств контроля доступа при считывании карты необходимо выполнить следующие действия.

Шаги

1. Нажмите **Event Management → Cross-Device Linkage** («Управление событиями → Привязка различных устройств»), чтобы войти в интерфейс настройки привязки устройств.

2. Нажмите **Add** («Добавить») для добавления новой привязки.

3. Выберите тип привязки **Card Linkage** («Привязка карты»).

4. Настройте источник события.

1) Выберите карту из списка.
2) Выберите устройство контроля доступа в качестве устройства-источника события.
3) Выберите считыватель карт, действия которого будут инициализированы.

5. Установите целевое устройство контроля доступом в качестве цели привязки.

1) Выберите устройство контроля доступа из списка в качестве цели привязки.
2) Установите переключатель во включенное положение, чтобы включить привязку.

Тревожный выход

Тревожный выход устройства будет активирован и будет направлено уведомление.

Точка контроля доступа

Возможно только одно из следующих состояний двери: открыта / закрыта, оставить открытой / оставить закрытой.

6. Нажмите **Save** («Сохранить»).

Настройка привязки различных устройств при детекции ID сотрудника

Ввод ID сотрудника на указанном считывателе карт может инициировать действия других устройств, такие как срабатывание тревожного выхода, открытие двери и т. д.

Для настройки действий других устройств контроля доступа при обнаружении ID сотрудника необходимо выполнить следующие действия.

Шаги

1. Нажмите **Event Management → Cross-Device Linkage** («Управление событиями → Привязка различных устройств»), чтобы войти в интерфейс настройки привязки устройств.

2. Нажмите **Add** («Добавить») для добавления новой привязки.

3. Выберите тип привязки **Employee ID Linkage** («Привязка ID сотрудника»).

4. Введите ID сотрудника.

1) Выберите устройство контроля доступа в качестве устройства-источника события.
2) Выберите считыватель карт, действия которого будут инициализированы.

5. Установите целевое устройство контроля доступом в качестве цели привязки.

1) Выберите устройство контроля доступа из списка в качестве цели привязки.
2) Установите переключатель во включенное положение, чтобы включить привязку.

Тревожный выход

Тревожный выход устройства будет активирован и будет направлено уведомление.

Точка контроля доступа

Возможно только одно из следующих состояний двери: открыта / закрыта, оставить открытой / оставить закрытой.

Примечание

Возможно только одно из следующих состояний двери: открыта / закрыта, оставить открытой / оставить закрытой.

6. Нажмите **Save** («Сохранить»).

8.1.11 Управление состоянием точки контроля доступа

Состояние точки контроля доступа добавленного устройства будет отображаться в режиме реального времени. Можно проверить состояние выбранной точки контроля доступа и соответствующие события. Можно управлять состоянием и устанавливать продолжительность состояния точки контроля доступа.

Группировка точек контроля доступа

Перед тем, как контролировать состояние дверей и устанавливать продолжительность состояния, необходимо организовать точки контроля доступа в группы для удобного управления.

Для группировки точек контроля доступа необходимо выполнить следующие действия.

Шаги

Примечание

- Можно импортировать тревожные входы устройства контроля доступа в группы.
- Для терминала контроля доступа с функцией видеозаписи можно импортировать камеру в группы.
- Подробная информация представлена в разделе *Управление группами*.

1. Нажмите **Device Management → Group** («Управление устройством→ Группа») для перехода на страницу управления группами.
2. Добавьте новую группу.
   1) Нажмите для открытия окна **Add Group** («Добавить группу»).
   2) Создайте имя группы.
   3) **Опционально.** Нажмите **Create Group by Device Name** («Создать группу по имени устройства») для создания новой группы с именем, совпадающим с именем выбранного устройства.
   4) Нажмите **OK**.
3. Нажмите **Import** («Импорт») для импорта точек контроля доступа в группу.
   1) Нажмите **Import** («Импорт»).
   2) Нажмите вкладку **Access Control Point** («Точка контроля доступа»).
   3) Выберите точки контроля доступа из списка.
   4) Выберите группу из списка групп.
   5) Нажмите **Import** («Импорт») для импорта выбранных точек контроля доступа в группу.

Управление состоянием двери

Можно управлять состоянием отдельной точки контроля доступа (дверь): открыть дверь, закрыть дверь, оставить дверь открытой и оставить дверь закрытой.

Для управления состоянием двери необходимо выполнить следующие действия.

Шаги

1. Нажмите **Status Monitor → Door Status** («Мониторинг состояния → Состояние двери»), чтобы перейти на соответствующую страницу.
2. Выберите группу контроля доступа на панели слева.

   Примечание

   Подробная информация об управлении группой контроля доступа представлена в разделе *Группировка точек контроля доступа*.

   Точки контроля доступа выбранной группы контроля доступа будут отображаться справа.
3. Нажмите на панель информации о состоянии, чтобы выбрать дверь.

4. Нажмите кнопки, представленные на панели информации о состоянии, чтобы управлять дверью.

   Открыть дверь

   Открытие двери один раз.

   Закрыть дверь

   Закрытие двери один раз.

   Оставить дверь открытой

   Дверь остается открытой.

   Оставить дверь закрытой

   Дверь остается закрытой.

Примечание

- Убедитесь, что дверь подключена к дверному контакту, иначе состояние двери не может быть отображено в журнале работы.
- Убедитесь, что точка контроля доступа не может быть поставлена на охрану другим клиентским программным обеспечением, иначе невозможно просмотреть изменения состояния двери. Только одно клиентское программное обеспечение может поставить устройство на охрану и позволяет просматривать изменения состояния двери, получать сообщения о тревоге из точки контроля доступа.

Проверка информации о событиях доступа в режиме реального времени

Записи доступа всех устройств контроля доступа будут отображаться в режиме реального времени, включая записи считывания карт, записи распознавания лиц, записи сравнения отпечатков пальцев и т. д.

Шаги

1. Нажмите **Status Monitor** («Мониторинг состояния»), чтобы просматривать записи доступа в режиме реального времени.

   Журналы записей доступа будут отображаться в режиме реального времени. Здесь можно просмотреть подробную информацию о записях, включая номер карты, имя сотрудника, организацию, время события и т. д.

2. **Опционально.** Нажмите **Show Latest Access Record** («Показать последнюю запись доступа»), и последняя запись доступа будет отображена в верхней части списка записей.
3. **Опционально.** Нажмите на событие, чтобы просмотреть сведения о пользователе, в том числе изображения пользователя (захваченное изображение и изображение профиля), номер карты пользователя, имя пользователя, имя организации, телефон, контактный адрес и т. д.

   Отображение результата аутентификации

   Отображение результатов доступа, например, «номер карты не зарегистрирован», «успешно» и т. д.

Проверка тревоги контроля доступа в режиме реального времени

Журналы событий контроля доступа будут отображаться в режиме реального времени, включая исключения устройства, события двери, события считывателя карт и события тревожного входа.

Для проверки тревоги контроля доступа в режиме реального времени необходимо выполнить следующие действия.

Шаги

1. Нажмите **Status Monitor → Access Control Alarm** («Мониторинг состояния → Тревога контроля доступа»), чтобы перейти на соответствующую страницу. Все тревоги контроля доступа будут отображаться в списке в режиме реального времени. Можно просмотреть тип тревоги, время тревоги, местоположение и т. д.
2. Нажмите , чтобы просмотреть тревогу на электронной карте.

   Примечание

   Подробная информация о настройке точки контроля доступа на электронной карте представлена в разделе ***Отображение точки контроля доступа на электронной карте***.
3. **Опционально.** При тревожном событии нажмите соответствующие кнопки для просмотра сцены в режиме реального времени или просмотра захваченного изображения.

   Примечание

   Подробная информация о настройке камеры представлена в разделе ***Настройка действий на клиентском ПО при событии доступа***.
4. **Опционально.** Выберите тревогу, которую клиент может получить при возникновении тревожного события.
   1) Нажмите **Subscribe** («Подписаться»).
   2) Выберите тревоги, включая тревогу исключения устройства, тревогу двери, тревогу считывателя карт и тревожный вход.
   3) Нажмите **OK** для сохранения настроек.

8.1.12 Контроль двери во время просмотра в режиме реального времени

Во время просмотра в режиме реального времени можно управлять подключенной к камере точкой контроля доступа (дверью), например открывать дверь, закрывать дверь и т. д.

Для управления подключенной к камере двери в режиме реального времени необходимо выполнить следующие действия.

Шаги

1. Перейдите в модуль **Live View** («Просмотр в режиме реального времени») и начните просмотр в

   Примечание

   режиме реального времени с тепловизионной камеры.

   Подробная информация о просмотре в режиме реального времени представлена в соответствующем разделе.

2. Выполните привязку камеры к точке контроля доступа.
   1) Нажмите правой кнопкой мыши окно просмотра в режиме реального времени и выберите **Link to Access Control Point** («Выполнить привязку к точке контроля доступа»), чтобы открыть окно **Set Linked Access Control Point** («Настроить соответствующую точку контроля доступа»).
   2) Нажмите **Enable** («Включить»), чтобы включить привязку.
   3) Из списка выберите точку контроля доступа.
   4) Нажмите **OK**.

   Примечание

   Одна камера может быть связана только с одной точкой контроля доступа; к одной и той же точке контроля доступа можно подключить разные камеры.
3. Снова запустите просмотр в режиме реального времени с камеры, чтобы настройки вступили в силу.

   Во время просмотра в режиме реального времени на панели инструментов появятся четыре кнопки управления дверью.
4. Нажмите  , чтобы управлять дверью: открыть, закрыть, оставить открытой или оставить закрытой.

8.1.13 Отображение точки контроля доступа на электронной карте

Можно добавить точку контроля доступа на электронную карту. Когда срабатывает тревога точки контроля доступа, можно просмотреть уведомление о тревоге на электронной карте, узнать подробную информацию о тревоге и управлять дверью.

Для отображения точки контроля доступа в качестве Hot Spot на электронной карте необходимо выполнить следующие действия.

Шаги

Примечание

- Для терминала контроля доступа с функцией видеозаписи также можно добавить камеру на электронную карту для просмотра изображения с камеры в режиме реального времени.
- Подробная информация о работе электронной карты представлена в соответствующем разделе.

1. Перейдите в модуль электронной карты.
2. Нажмите **Edit** («Изменить») на панели инструментов электронной карты, чтобы войти в режим редактирования карты.
3. Нажмите  на панели инструментов, чтобы открыть окно добавления Hot Spot.
4. Выберите точку контроля доступа, которую нужно добавить в качестве Hot Spot.
5. **Опционально.** Измените наименование Hot Spot, выберите цвет наименования и значок, дважды нажав соответствующее поле.
6. Нажмите **OK**.

Значки двери добавляются на карту в качестве Hot Spot, а значки добавленных точек контроля доступа изменятся с на в списке групп камер. Можно перетащить значки точек контроля доступа, чтобы переместить Hot Spot в нужные места.

7. После добавления точки контроля доступа на карту в качестве Hot Spot можно управлять точкой контроля доступа и просматривать информацию о тревоге.

1) Нажмите **Exit Editing Mode** («Выход из режима редактирования») на панели инструментов электронной карты, чтобы войти в режим предварительного просмотра карты.
2) Чтобы управлять точкой контроля доступа, можно нажать правой кнопкой мыши значок точки контроля доступа на карте и выбрать **Open Door** («Открыть дверь»), **Close Door** («Закрыть дверь»), **Remain Open** («Оставить дверь открытой») и **Remain Closed** («Оставить дверь закрытой») для управления дверью.

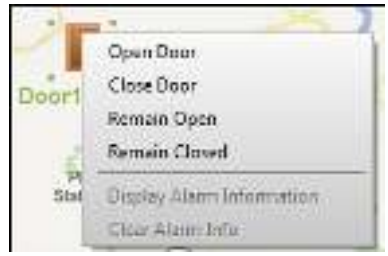


Рисунок 8-7. Управление точкой контроля доступа на карте

3) **Опционально.** При срабатывании тревоги рядом с Hot Spot появится мигающий значок (мигание продолжится в течение 10 секунд). Нажмите значок тревоги, чтобы проверить информацию тревоги, включая тип и время срабатывания тревоги.

Примечание

Чтобы отображать информацию о тревоге на карте, необходимо настроить функцию отображения на электронной карте и выполнить привязку действия к тревоге. Подробная информация представлена в разделе ***Настройка действий на клиентском ПО при событии доступа***.

8.2 Удаленная конфигурация (веб-интерфейс)

Настройте параметры устройства удаленно.

8.2.1 Настройка времени

Выберите часовой пояс устройства, затем синхронизируйте время и параметры DST.

Часовой пояс и синхронизация времени

На странице управления устройствами выберите устройство и нажмите **Remote Configuration → System → Time** («Удаленная настройка → Система → Время»), чтобы перейти на соответствующую страницу.
Выберите часовой пояс, настройте NTP-параметры или синхронизируйте время вручную.

Часовой пояс

Выберите часовой пояс из выпадающего списка.

NTP

Устройство автоматически синхронизирует время с NTP. После добавления NTP необходимо задать адрес сервера NTP, NTP-порт и интервал синхронизации.

Синхронизация времени вручную

Включив функцию **Manual Time Synchronization** («Синхронизация времени в ручном режиме»).

При выборе функции **Synchronize with Computer Time («Синхронизировать с временем на ПК»)**, **Set Time** («Установленное время») примет текущее время на ПК. Деактивируйте функцию **Synchronize with Computer Time** («Синхронизировать с временем на ПК») и нажмите , чтобы установить время на устройстве в ручном режиме.

Нажмите **Save** («Сохранить») для сохранения настроек.

DST («Летнее время»)

На странице управления устройствами нажмите **Remote Configuration → System → Time → DST** («Удаленная конфигурация → Система → Время → DST»), чтобы перейти на соответствующую вкладку.
Включите функцию DST, чтобы установить смещение DST, время начала и время окончания DST. Нажмите **Save** («Сохранить»).

8.2.2 Настройка параметров сети

Настройте параметры сети устройства, в том числе тип NIC, DHCP и HTTP.

На странице управления устройствами нажмите **Remote Configuration → Network → Network Parameters** («Удаленная настройка → Сеть → Параметры сети»), чтобы перейти на соответствующую вкладку.

Тип NIC

Выберите тип NIC из выпадающего списка. Выберите один их предложенных типов: адаптивный, 10M или 100M.

DHCP

При отключении этой функции необходимо вручную настроить IPv4-адрес устройства, IPv4-маску подсети, IPv4-шлюз по умолчанию, MTU и порт.

При включении этой функции система автоматически назначит IPv4-адрес устройства, IPv4-маску подсети, IPv4-шлюз по умолчанию устройства.

HTTP

Настройте порт HTTP, адрес сервера DNS1 и адрес сервера DNS2.

8.2.3 Настройка способа уведомления

Настройте центральную группу для загрузки журнала по протоколу EHome.

На странице управления устройствами нажмите **Remote Configuration → Network → Report Strategy** («Удаленная настройка → Сеть → Способ уведомления»), чтобы перейти на соответствующую вкладку.

Настройте центральную группу для передачи журналов по протоколу EHome. Нажмите **Save** («Сохранить») для сохранения настроек.

Центральная группа

Выберите центральную группу из выпадающего списка.

Основной канал / резервный канал

Устройство будет связываться с центром через основной канал. Когда в основном канале возникает исключение, устройство и центр будут связываться друг с другом через резервный канал.

Примечание

- N1 относится к проводной сети, а G1 относится к GPRS.
- Только устройство с функцией 3G / 4G поддерживает установку канала как G1.

8.2.4 Настройка параметров сетевого центра

Для передачи данных по протоколу EHome настройте центр безопасности, IP-адрес центра, номер порта, протокол EHome, имя пользователя учетной записи EHome и т. д.

На странице управления устройствами нажмите **Remote Configuration → Network → Network Center Parameters** («Удаленная настройка → Сеть → Параметры сетевого центра»), чтобы перейти на соответствующую вкладку.

Выберите центр из выпадающего списка.

После включения функции можно назначить тип адреса центра, IP-адрес / имя домена, номер, порт, создать имя пользователя EHome и т. д.

Примечание

При использовании EHome версии 5.0 необходимо создать ключ EHome для учетной записи EHome.

Нажмите **Save** («Сохранить»).

После создания записи EHome можно добавить устройство по протоколу EHome.

8.2.5 Изменение пароля устройства

Можно изменить пароль устройства.

Перед началом

Устройство должно быть активировано. Подробная информация представлена в разделе *Активация*.

Шаги

1. На странице управления устройствами нажмите **Remote Configuration → System → User** («Удаленная настройка → Система → Пользователь»), чтобы перейти на соответствующую вкладку.
2. Выберите пользователя и нажмите **Edit** («Редактировать»), чтобы перейти на страницу редактирования.
3. Введите старый пароль, затем придумайте и подтвердите новый пароль.

Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

4. Нажмите **OK**.

Результат

Пароль устройства изменен. Для повторного подключения устройства необходимо ввести новый пароль на странице управления устройством.

8.2.6 Настройка режима безопасности

Настройте режим безопасности для входа в клиентское ПО.

На странице управления устройствами нажмите **Remote Configuration → System → Security** (Удаленная настройка → Система → Безопасность»), чтобы перейти на соответствующую страницу.

Из всплывающего списка выберите режим безопасности и нажмите **Save** («Сохранить»).

Режим безопасности

Высокий уровень безопасности при проверке информации пользователя при входе в клиентское программное обеспечение.

Режим совместимости

Режим проверки совместимости информации пользователя со старой версией клиентского программного обеспечения.

8.2.7 Оптимизация имени события

После включения данной функции система загрузит оптимизированное имя события в клиентское программное обеспечение.

На странице управления устройством нажмите **Remote Configuration → Settings → Event → Optimize Event Name** («Удаленная настройка → Настройка → Событие → Оптимизировать имя события»).

Нажмите **Optimize Event Name** («Оптимизировать имя события») и нажмите **Save** («Сохранить»).

Система может загрузить оптимизированное имя события в клиентское программное обеспечение.

8.2.8 Настройка режима события

В зависимости от длины идентификатора сотрудника можно установить другой режим события. Различные режимы событий поддерживают разные возможности событий.

На странице управления устройством нажмите **Remote Configuration → Settings → Event → Event Mode** («Удаленная настройка → Настройка → Событие → Режим события»).

Из всплывающего списка выберите режим события и нажмите **Save** («Сохранить»).

Режим A

Хранение 250 000 событий устройства. Поддерживает идентификатор сотрудника, состоящий из 32 символов (комбинация цифр и строчных букв) или 16 символов (комбинация прописных букв, строчных букв, цифр и специальных символов).

Режим B

Хранение 300 000 событий устройства. Поддерживает идентификатор сотрудника, состоящий из 24 символов (комбинация цифр и строчных букв) или 12 символов (комбинация прописных букв, строчных букв, цифр и специальных символов).

8.2.9 Обслуживание системы

Можно перезагрузить устройство, восстановить его настройки по умолчанию и обновить устройство.

Перезагрузка устройства

На странице управления устройствами нажмите **Remote Configuration → System → System Maintenance** («Удаленная конфигурация → Система → Обслуживание системы»), чтобы перейти на соответствующую вкладку.

Нажмите **Reboot** («Перезагрузка»), чтобы перезагрузить устройство.

Восстановление настроек по умолчанию

На странице управления устройствами нажмите **Remote Configuration → System → System Maintenance** («Удаленная конфигурация → Система → Обслуживание системы»), чтобы перейти на соответствующую вкладку.

Восстановление настроек по умолчанию

Параметры будут сброшены до заводских настроек, за исключением IP-адреса.

Восстановить все

Параметры будут сброшены до заводских настроек. После сброса настроек необходимо активировать устройство.

Обновление

На странице управления устройствами нажмите **Remote Configuration → System → System Maintenance** («Удаленная конфигурация → Система → Обслуживание системы»), чтобы перейти на соответствующую вкладку.
Выберите тип устройства в раскрывающемся списке, затем нажмите **Browse** («Обзор»), выберите файл обновления на локальном компьютере и нажмите **Upgrade** («Обновить»).

Примечание

- При выборе считывателя карт в качестве типа устройства следует выбрать номер считывателя карт из раскрывающегося списка.
- Обновление длится около 2 минут. Не выключайте устройство во время обновления. После обновления устройство перезагрузится автоматически.

8.3 Учет рабочего времени (УРВ)

Модуль «Учет рабочего времени (УРВ)» обеспечивает отслеживание и мониторинг начала и завершения работы сотрудников, отслеживание рабочего времени и опозданий, ранних уходов, времени перерывов и прогулов сотрудников.

Примечание

В данном разделе представлены настройки, которые необходимо установить для получения отчетов УРВ. Записи доступа, полученные после установки настроек, будут учтены в статистике.

8.3.1 Управление графиком смены

Рабочая смена — это практика трудоустройства, при которой работы ведутся в непрерывном цикле 24 часа в сутки каждый день недели. В данном режиме рабочий день подразделяется на смены, установленные периоды времени, в течение которых сотрудники посменно выполняют свои обязанности.

Установите график работы отдела, график работы сотрудников и временный график.

Добавить период времени

Можно добавить период времени для расписания смены. Для добавления периода времени необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль УРВ и перейдите на вкладку **Shift Schedule Management** («Управление расписанием смены»).
2. Нажмите **Shift Settings → Time Period Settings** («Настройки смены → Настройки периода времени»), чтобы перейти на соответствующую страницу.
3. Нажмите **Add** («Добавить»), чтобы добавить период времени.
4. Настройте параметры периода времени.

Минимальное количество посещений

Установите минимальное количество посещений.

Примечание

Если в качестве контрольных точек регистрации начала и окончания рабочего дня настроены разные считыватели карт, можно нажать **Absence time is not included in effective work hours** («Время отсутствия не включается в эффективное рабочее время»), чтобы исключить время отсутствия из рабочих часов.

Требуется регистрация входа / выхода

Настройте необходимый период действия для регистрации входа / выхода.

Опоздание / ранний уход с работы

Установите период времени для опозданий и ранних уходов.

Исключить перерыв из рабочего времени

Нажмите, чтобы исключить перерыв из рабочего времени.

Примечание

Можно установить до 3 перерывов.

Установить период с оплатой по времени

Настройте ставку и минимальную единицу времени.

5. Нажмите **Save** («Сохранить»).
   Добавленный период времени будет отображаться в списке на панели слева.

Добавление смены

Можно добавить смену для расписания смены.

Перед началом

Сначала добавьте необходимый период времени. Подробная информация представлена в разделе ***Добавить период времени***. Для добавления смены необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Shift Schedule Management → Shift Settings → Shift** («Управление расписанием смены → Настройки смены → Смена»), чтобы перейти на соответствующую страницу.
3. Нажмите **Add** («Добавить»), чтобы добавить смену.
4. Введите имя смены.
5. Выберите период смены из выпадающего списка.
6. Выберите добавленный период времени и нажмите на временную шкалу, чтобы применить выбранный период времени.
7. Нажмите **Save** («Сохранить»).
   Добавленная смена будет отображаться в списке на панели слева.

Настройка графика работы отдела

Установите график работы смены для отдела, чтобы назначить соответствующий график для каждого сотрудника в отделе.

Перед началом
В модуле УРВ отдел отображается в списке вместе с соответствующей организацией. Сначала необходимо добавить отделы и сотрудников в модуле **Access Control** («Контроль доступа»). Подробная информация представлена в разделах ***Управление организацией*** и ***Управление информацией о пользователе***.

Для настройки графика работы отдела необходимо выполнить следующие действия.

Шаги
1. Нажмите **Time & Attendance** → **Shift Schedule Management** («УРВ → Управление расписанием смены»), чтобы перейти на соответствующую страницу.
2. Выберите отдел и нажмите **Department Schedule** («Расписание отдела»), чтобы открыть окно расписания отдела.
3. Нажмите **Time and Attendance** («УРВ»).

   График посещаемости распространяет на всех сотрудников отдела, кроме тех, кто исключен из графика.
4. Выберите смену из выпадающего списка.
5. Настройте дату начала и дату окончания периода.
6. Настройте другие параметры для расписания, в том числе **Check-in Not Required** («Регистрация прихода не требуется»), **Check-out Not Required** («Регистрация ухода с работы не требуется»), **Effective for Holiday** («Применяется в праздничные дни»), **Effective for Overtime** («Расписание сверхурочной работы») или **Effective for Multiple Shift Schedules** («Действует для нескольких смен»).

   Примечание

   Нажмите **Effective for Multiple Shift Schedules** («Действует для нескольких смен»), чтобы выбрать необходимые периоды времени из добавленных периодов времени для сотрудников отдела.

   График работы для нескольких смен

   Данный график содержит более одного периода времени. Сотрудник может зарегистрировать приход / уход во время действия любого периода времени, при этом статус УРВ будет эффективным.
   Существует график работы для нескольких смен с тремя периодами времени: с 00:00 до 07:00, с 08:00 до 15:00 и с 16:00 до 23:00. Статус УРВ сотрудника с данным графиком работы будет эффективным в любом из трех периодов времени. Если сотрудник приходит на работу в 07:50, будет применен ближайший период времени с 08:00 до 15:00 для регистрации его прихода.
7. **Опционально.** Нажмите **Set as Default for All Persons in Department** («По умолчанию для всех сотрудников отдела»).
   Для всех сотрудников отдела будет использоваться этот график смен по умолчанию.

8. **Опционально.** Если в выбранном отделе есть дополнительные отделы, можно нажать **Set as Shift Schedule for All Sub Departments** («Установить график смен для всех дополнительных отделов»), чтобы применить расписание отдела к его дополнительным отделам.
9. Нажмите **Save** («Сохранить»).

Настройка графика работы сотрудника

Назначьте график сменной работы для одного сотрудника. Также можно просматривать и экспортировать детали графика работы сотрудника.

Перед началом

В модуле контроля доступа добавьте отдел и сотрудника. Подробная информация представлена в разделах ***Управление организацией и Управление информацией о пользователе***.

Для настройки графика работы сотрудника необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Shift Schedule Management** («Управление расписанием смены»), чтобы перейти на соответствующую страницу.
3. Выберите отдел и сотрудника.
4. Нажмите **Person Schedule** («Расписание сотрудника»), чтобы открыть окно расписания.
5. Нажмите **Time and Attendance** («УРВ»).

   К выбранному сотруднику будет применен настроенный график УРВ.
6. Выберите смену из выпадающего списка.
7. Настройте дату начала и дату окончания периода.
8. Настройте другие параметры для расписания, в том числе **Check-in Not Required** («Регистрация прихода не требуется»), **Check-out Not Required** («Регистрация ухода с работы не требуется»), **Effective for Holiday** («Применяется в праздничные дни»), **Effective for Overtime** («Расписание сверхурочной работы») или **Effective for Multiple Shift Schedules** («Действует для нескольких смен»).

   Примечание

   Нажмите **Effective for Multiple Shift Schedules** («Действует для нескольких смен»), чтобы выбрать необходимые периоды времени из добавленных периодов времени для сотрудников отдела.

   График работы для нескольких смен

   Данный график содержит более одного периода времени. Сотрудник может зарегистрировать приход / уход во время действия любого периода времени, при этом статус УРВ будет эффективным.
   Существует график работы для нескольких смен с тремя периодами времени: с 00:00 до 07:00, с 08:00 до 15:00 и с 16:00 до 23:00. Статус УРВ сотрудника с данным графиком работы будет эффективным в любом из трех периодов времени. Если сотрудник приходит на работу в 07:50, будет применен ближайший период времени с 08:00 до 15:00 для регистрации его прихода.
9. Нажмите **Save** («Сохранить»).

Настройка временного графика работы

Добавьте временный график для сотрудника, и ему будет назначен временный график смены. Также можно просматривать и экспортировать детали временного графика работы.

Перед началом

Добавьте отдел и сотрудника в модуль контроля доступа и установите правило УРВ для сотрудника. Подробная информация представлена в разделах ***Управление организацией*** и ***Управление информацией о пользователе***.

Для настройки временного графика работы необходимо выполнить следующие действия.

Шаги

Примечание

Временный график имеет более высокий приоритет, чем график работы отдела и сотрудника.

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Shift Schedule Management** («Управление расписанием смены»), чтобы перейти на соответствующую страницу.
3. Выберите отдел и сотрудника.
4. Нажмите **Temporary Schedule** («Временное расписание»), чтобы открыть окно расписания.
5. Нажмите , чтобы установить дату смены.
6. Выберите период времени.
7. Нажмите шкалу времени, чтобы применить период времени для выбранной даты.
8. **Опционально.** Нажмите **Advanced Settings** («Расширенные настройки») и выберите расширенные правила УРВ для временного расписания.
9. Нажмите **Add** («Добавить»).

Проверить и изменить график смен

Можно проверить и изменить график смен. Для проверки и изменения необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Shift Schedule Management** («Управление расписанием смены»), чтобы перейти на соответствующую страницу.
3. Выберите отдел и сотрудников.
4. Нажмите **View** («Просмотр»), чтобы открыть окно **Shift Schedule Details** («Подробная информация о расписании смены»). Будет отображена подробная информация о расписании смены.
5. Измените информацию обычной смены.
   1) Нажмите **Normal Schedule** («Обычная смена»).
   2) Выберите смену из списка.
   3) Нажмите **Attendance Rule Settings** («Настройки правила УРВ), чтобы открыть соответствующую страницу.
   4) Выберите необходимые правила УРВ и нажмите **OK**.

5) Нажмите , чтобы установить дату смены.
6) Нажмите **Save** («Сохранить»).

6. **Опционально.** Нажмите **Temporary Schedule** («Временное расписание смены») и выполните одну из следующих операций.

Добавить Добавить временное расписание для выбранного сотрудника.

Изменить период времени.

Удалить временное расписание.

8.3.2 Коррекция записи регистрации прихода / ухода вручную

Если статус УРВ неверен, можно вручную исправить запись о регистрации прихода / ухода. Также можно редактировать, удалить, выполнять поиск или экспортировать записи о регистрации.

Перед началом

- Необходимо добавить организации и сотрудников в модуль **Access Control** («Контроль доступа»). Подробная информация представлена в разделах ***Управление организацией*** и ***Управление информацией о пользователе***.
- Статус УРВ некорректен.

Для изменения записей регистрации прихода / ухода необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Attendance Handling → Check-in/out Correction** («Обработка записей УРВ → Изменения записей регистрации прихода / ухода»), чтобы перейти на соответствующую страницу.
3. Нажмите **Add** («Добавить»), чтобы перейти в окно изменения записей регистрации прихода на работу / ухода с работы.
4. Установите параметры коррекции записи о регистрации прихода / ухода.
   - Поставьте **Check-in** («Регистрация прихода») и установите фактическое время начала работы.
   - Поставьте **Check-out** («Регистрация ухода») и установите фактическое время окончания работы.
5. Нажмите **Employee Name** («Имя сотрудника») и выберите сотрудника.
6. **Опционально.** При необходимости создайте примечание.
7. Нажмите **Add** («Добавить»).
8. **Опционально.** После добавления корректировки записи регистрации прихода / ухода выполните следующие действия.

Поиск

Задать условия поиска измененных записей регистрации прихода на работу / ухода с работы.

Изменение

Изменить выбранные записи регистрации прихода на работу / ухода с работы.

Удаление

Удалить выбранные измененные записи регистрации прихода на работу / ухода с работы.

Отчет

Создать отчет и просмотреть измененные записи регистрации прихода на работу / ухода с работы.

Экспорт

Экспорт измененных записей регистрации прихода на работу / ухода с работы.

Примечание
Экспортируемые файлы сохраняются в формате CSV.

8.3.3 Добавление отпусков и командировок

Добавьте отпуск или командировку для сотрудника.

Перед началом
Необходимо добавить организации и сотрудников в модуль **Access Control** («Контроль доступа»). Подробная информация представлена в разделах ***Управление организацией*** и ***Управление информацией о пользователе***.

Для добавления отпуска или командировки необходимо выполнить следующие действия.

Шаги
1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Attendance Handling → Leave and Business Trip** («Обработка записей УРВ → Отпуска и командировки»), чтобы перейти на соответствующую страницу.
3. Нажмите **Add** («Добавить»), чтобы открыть окно добавления заявки на отпуск и командировку.
4. Выберите тип отпуска или командировки из выпадающего списка.

   Примечание
   Настройте тип отпуска в расширенных настройках. Подробная информация представлена в разделе ***Настройка типа отпуска***.
5. Установите период отпуска или командировки.
6. Нажмите **Employee Name** («Имя сотрудника») и выберите сотрудника для применения во всплывающем окне добавления сотрудника.
7. **Опционально.** При необходимости создайте примечание.
8. Нажмите **Add** («Добавить»).

   Добавленный отпуск и командировка отображаются на странице **Leave and Business Trip** («Отпуск и командировка»).
9. **Опционально.** После добавления отпуска или командировки выполните следующие действия.

   Изменение

   Выберите отпуск и командировку и нажмите **Modify** («Изменить»), чтобы отредактировать заявку.

Удаление

Выберите отпуск и командировку и нажмите **Delete** («Удалить»), чтобы удалить заявку.

Отчет

Нажмите **Report** («Отчет»), чтобы создать отчет об отпуске или командировке.

Экспорт

Нажмите **Export** («Экспорт»), чтобы экспортировать сведения об отпуске или командировке на локальный компьютер.

Примечание
Экспортируемые файлы сохраняются в формате CSV.

8.3.4 Расчет данных о посещаемости

Перед поиском и просмотром обзора данных УРВ, подробных данных УРВ сотрудников, данных об отклонениях УРВ сотрудников, информации о сверхурочной работе сотрудников и журнала считывания карт необходимо рассчитать данные УРВ.

Автоматический расчет данных УРВ

Можно установить расписание, чтобы клиент мог автоматически рассчитывать данные УРВ в заданное время каждый день.

Для настройки времени автоматического расчета данных УРВ необходимо выполнить следующие действия.

Шаги

Примечание
Будут рассчитаны данные УРВ предыдущего дня.

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Attendance Handling → Attendance Calculation** («Обработка записей УРВ → Расчет данных УРВ»), чтобы перейти на соответствующую страницу.
3. На панели **Auto-Calculate Attendance** («Автоматический расчет посещаемости») установите время, в которое клиент должен рассчитывать данные каждый день.
4. Нажмите **Save** («Сохранить»).

Расчет данных УРВ вручную

Рассчитайте данные о посещаемости вручную, предварительно установив диапазон данных.

Для расчета данных УРВ вручную необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Attendance Handling → Attendance Calculation** («Обработка записей УРВ → Расчет данных УРВ»), чтобы перейти на соответствующую страницу.

3. На панели **Manually Calculate Attendance** («Расчет данных УРВ вручную») установите время начала и время окончания, чтобы определить диапазон данных УРВ.
4. Нажмите **Calculate** («Расчет»).

Примечание
Клиентское ПО может рассчитать данные о посещаемости только за три месяца.

8.3.5 Расширенные настройки

Можно настроить дополнительные параметры УРВ, включая базовые параметры УРВ, параметры правил УРВ, параметры контрольных точек УРВ, параметры выходных дней и параметры типа отпуска.

Настройка основных параметров

Можно настроить основные параметры УРВ, включая день начала каждой недели, дату начала каждого месяца и нерабочий день.

Для настройки основных параметров УРВ необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Advanced Settings → Basic Settings** («Расширенные настройки → Основные настройки»), чтобы перейти на страницу основных настроек.
3. Установите день начала каждой недели и дату начала каждого месяца, выбрав параметры из списка.
4. Настройте параметры для нерабочих дней.

   Установить как нерабочий день

   Выберите даты нерабочих дней.

   Установить цвет нерабочих дней в отчете

   Выберите цвет в окне **Select Color** («Выбрать цвет»). Нерабочие дни в отчете будут отмечены настроенным цветом.

   Установить отметку о нерабочем дне в отчете

   Введите отметку, и поле нерабочего дня в отчете будет отображаться с отметкой.
5. Установите тип аутентификации, и клиент будет рассчитывать записанные данные УРВ на основе выбранного типа аутентификации.
6. Нажмите **Save** («Сохранить»).

Настройка правила УРВ

Перед настройкой смены можно настроить правило УРВ для всех смен. Можно настроить правило для явки / отсутствия, регистрации прихода на работу / ухода с работы и сверхурочной работы.

Для настройки правила УРВ необходимо выполнить следующие действия.

Шаги

Примечание

Параметры, настроенные здесь, будут установлены по умолчанию для нового добавленного периода времени. Это не повлияет на ранее установленные периоды времени.

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Advanced Settings → Attendance Rule Settings** («Расширенные настройки → Настройки правила УРВ»), чтобы перейти на соответствующую страницу.
3. Настройте параметры правил, включая параметры явки / отсутствия, параметры регистрации прихода на работу / ухода с работы и сверхурочной работы.
4. **Опционально.** Нажмите **Non-scheduled Work Day** («Незапланированный рабочий день») и установите правило сверхурочной работы для нерабочих дней.
5. Нажмите **Save** («Сохранить»).

Настройка контрольного пункта УРВ

Можно настроить считыватели карт точки управления доступа в качестве контрольного пункта УРВ, чтобы считывание карт обеспечивало регистрацию сотрудника для УРВ.

Перед началом

Добавьте устройство контроля доступа перед настройкой пункта УРВ. Для подробной информации просмотрите раздел ***Добавление устройства***.

Для настройки считывателя карт точки управления доступа в качестве контрольного пункта УРВ необходимо выполнить следующие действия.

Шаги

Примечание

По умолчанию все считыватели карт устройства контроля доступа назначены в качестве контрольного пункта проверки посещаемости.

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Advanced Settings → Attendance Check Point Settings** («Расширенные настройки → Настройки контрольного пункта УРВ»), чтобы перейти на соответствующую страницу.
3. **Опционально.** Отключите функцию **Set All Card Readers as Check Points** («Назначение всех считывателей карт в качестве контрольных пунктов УРВ»).

   В качестве контрольных пунктов УРВ будут назначены только считыватели карт, перечисленные в списке.
4. Нажмите , чтобы открыть окно добавления пункта УРВ.
5. Настройте соответствующие параметры.

   Имя пункта УРВ

   Настройте имя пункта УРВ.

   Считыватель карт

   Выберите считыватель карт из списка в качестве контрольного пункта УРВ.

Функция пункта УРВ

Выберите функцию контрольной точки из раскрывающегося списка. Можно установить контрольную точку как контрольную точку регистрации начала / окончания работы, контрольную точку регистрации начала работы или контрольную точку регистрации окончания работы.

Расположение двери

Введите имя расположения двери.

Описание контрольной точки

При необходимости введите описания контрольных точек.

6. Нажмите **Add** («Добавить»).

Добавленные контрольные пункты УРВ отобразятся в списке.

7. **Опционально.** После добавления контрольной точки УРВ выполните одну из следующих операций.

Отредактируйте информацию о контрольной точке УРВ.

Удалите контрольные пункты УРВ.

Настройка выходных дней

Добавьте выходной день, в течение которого регистрация прихода / ухода осуществляться не будет.

Добавить выходной день с фиксированной датой

Можно настроить выходной день, который будет действовать только один раз. Для настройки выходного дня с фиксированной датой необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Advanced Settings → Holiday Settings** («Расширенные настройки → Настройка параметров выходного дня»), чтобы перейти на соответствующую страницу.
3. Нажмите , чтобы открыть окно добавления выходного дня.
4. Нажмите вкладку **Fixed Date** («Фиксированная дата»).

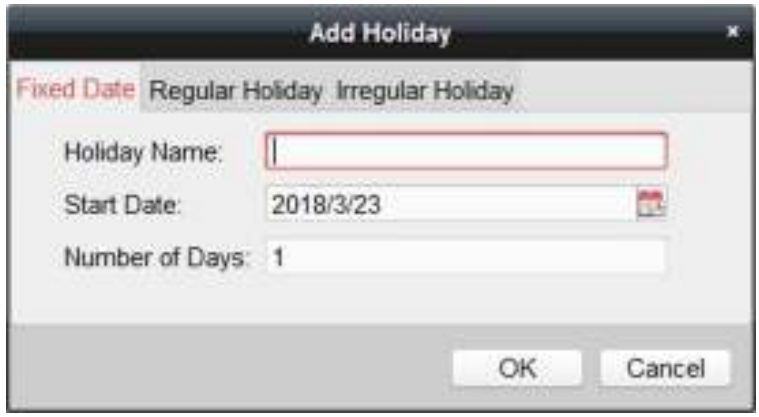


Рисунок 8-8. Добавление выходного дня с фиксированной датой

5. Введите имя выходного дня.
6. Настройте дату начала: первый день выходного дня.
7. Установите количество выходных дней.
8. **Опционально.** Выполните следующие действия, чтобы добавить выходной день.

   Измените информацию о выходных днях.

   Удалите выходной день из списка выходных дней.

Добавление постоянного выходного дня

Настройте выходной день, который будет действовать на регулярной основе в течение установленного срока, в том числе Новый год, Рождество и т. д.

Для добавления постоянного выходного дня необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Advanced Settings → Holiday Settings** («Расширенные настройки → Настройка параметров выходного дня»), чтобы перейти на соответствующую страницу.
3. Нажмите , чтобы открыть окно добавления выходного дня.
4. Нажмите вкладку **Regular Holiday** («Обычный выходной день»).

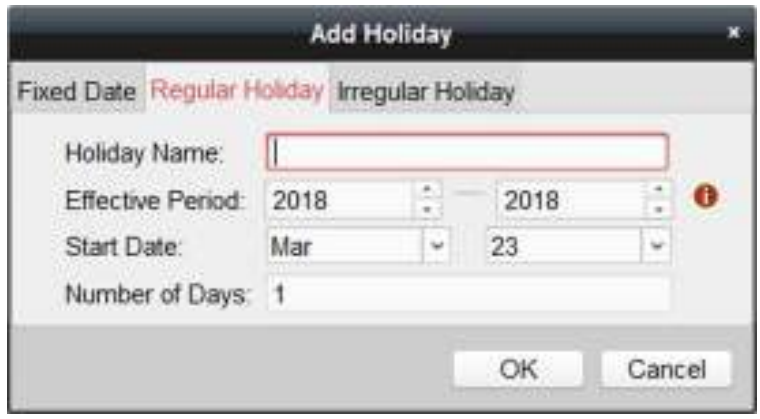


Рисунок 8-9. Добавление обычного выходного дня

5. Настройте параметры выходного дня.

   Дата начала

   Первый выходной день.

   Срок действия

   Длительность (в годах), в течение которых будут действовать выходные дни. Например, если период действия выходных дней установлен с 2018 по 2019 год, дата начала установлена на 31 декабря, количество дней равно 3, то выходные дни будут длиться с 31.12.2018 г. по 02.01.2019 г. и с 31.12.2019 г. по 02.01.2020 г.
6. Нажмите **OK**.

7. Опционально. Выполните следующие действия, чтобы добавить выходной день.

Измените информацию о выходных днях.

Удалите выходной день из списка выходных дней.

Добавление выходного дня с плавающей датой

Настройте выходной день, который будет действовать в разные дни ежегодно в течение установленного срока.

Для добавления выходного дня с плавающей датой необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Advanced Settings → Holiday Settings** («Расширенные настройки → Настройка параметров выходного дня»), чтобы перейти на соответствующую страницу.
3. Нажмите , чтобы открыть окно добавления выходного дня.
4. Нажмите вкладку **Irregular Holiday** («Выходной день с плавающей датой»).

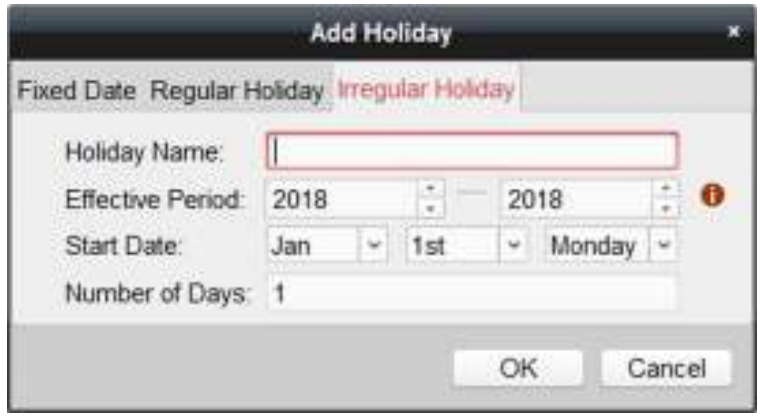


Рисунок 8-10. Добавление выходного дня с плавающей датой

5. Настройте параметры выходного дня.

Дата начала

Первый выходной день.

Срок действия

Длительность (в годах), в течение которых будут действовать выходные дни. Например, если период действия выходных дней установлен с 2018 по 2019 год, дата начала установлена на 31 декабря, количество дней равно 3, то выходные дни будут длиться с 31.12.2018 г. по 02.01.2019 г. и с 31.12.2019 г. по 02.01.2020 г.

Примечание

Такой сценарий возможен, когда выходные дни применены на два года в рамках срока действия.

6. Нажмите **OK**.

7. **Опционально.** Выполните следующие действия, чтобы добавить выходной день.
   - Измените информацию о выходных днях.
   - Удалите выходной день из списка выходных дней.

Настройка типа отпуска

Можно настроить тип отпуска согласно текущим требованиям. По умолчанию существует три основных типа отпуска: отпуск, отгул и командировка.

Выполните следующие шаги, чтобы добавить, изменить или удалить тип отпуска.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Attendance Settings → Leave Type Settings** («Расширенные → Настройки типа отпуска»), чтобы перейти на соответствующую страницу.
3. Нажмите , чтобы добавить основной тип отпуска на левой панели.
4. **Опционально.** Для добавления основных типов отпуска необходимо выполнить следующие действия.
   - Изменить основной тип отпуска.
   - Удалить основной тип отпуска.
5. Нажмите , чтобы добавить второстепенный тип отпуска на левой панели.
6. **Опционально.** Для добавления основных типов отпуска необходимо выполнить следующие действия.
   - Изменить второстепенный тип отпуска.
   - Удалить второстепенный тип отпуска.

8.3.6 Просмотр отчета УРВ

После расчета УРВ можно проверить сводку УРВ, подробную информацию УРВ, отклонения от нормы, сверхурочную работу, журналы считывания карт и отчеты, основанные на рассчитанных данных УРВ.

Получение обзора данных УРВ сотрудников

Можно искать необходимое время явки сотрудника, фактическое время явки, время опоздания, время досрочного ухода, время отсутствия, время сверхурочной работы, время досрочного ухода и т. д. за период времени, что позволяет получить обзор данных УРВ сотрудников.

Перед началом

- Добавьте организацию и сотрудников в модуле контроля доступа и считайте карты сотрудников. Подробная информация представлена в разделах ***Управление организацией*** и ***Управление информацией о пользователе***.
- Рассчитайте данные УРВ.

Примечание

- Клиентское ПО автоматически рассчитает данные УРВ за предыдущий день в 1:00 утра следующего дня.
- Клиентское ПО должно быть включенным в 1:00 утра, чтобы автоматически рассчитать данные УРВ за предыдущий день. Если расчет не был выполнен автоматически, можно выполнить расчет данных УРВ вручную. Подробная информация представлена в разделе ***Расчет данных о посещаемости вручную***.

Для поиска всех данных УРВ сотрудников за определенный период времени необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Attendance Statistics → Attendance Summary** («Статистика записей УРВ → Сводка УРВ»), чтобы перейти на соответствующую страницу.
3. Выберите отдел из выпадающего списка.
4. **Опционально.** Введите имя сотрудника для поиска.
5. Выберите дату начала и окончания искомого посещения.
6. **Опционально.** Нажмите **Reset** («Сбросить»), чтобы сбросить все условия поиска, затем повторно отредактируйте условия поиска.
7. Нажмите **Search** («Поиск»).

   После этого на странице появятся результаты поиска. Можно просмотреть требуемое время явки сотрудника, фактическое время явки, время опоздания, время досрочного ухода с работы, время отсутствия, время сверхурочной работы, время отпуска и т. д.
8. **Опционально.** После поиска выполните следующие действия.

Отчет	Формирование отчета УРВ.
Экспорт	Экспортируйте результаты на локальный компьютер.

Поиск подробных данных УРВ сотрудников

Можно искать данные о каждой записи УРВ сотрудника с подробной информацией, включая дату явки, смену, действующий временной период, начало работы, окончание работы, время регистрации прихода, время регистрации выхода, опоздание, ранний уход с работы, период посещения, период отсутствия, период отпуска и период сверхурочной работы.

Перед началом

- Добавьте организацию и сотрудников в модуле контроля доступа и считайте карты сотрудников. Подробная информация представлена в разделах ***Управление организацией*** и ***Управление информацией о пользователе***.
- Рассчитайте данные УРВ.

Примечание

- Клиентское ПО автоматически рассчитает данные УРВ за предыдущий день в 1:00 утра следующего дня.
- Клиентское ПО должно быть включенным в 1:00 утра, чтобы автоматически рассчитать данные УРВ за предыдущий день. Если расчет не был выполнен автоматически, можно выполнить расчет данных УРВ вручную. Подробная информация представлена в разделе ***Расчет данных о посещаемости вручную***.

Для поиска подробных данных УРВ сотрудника необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Attendance Statistics → Attendance Details** («Статистика записей УРВ → Подробная информация УРВ»), чтобы перейти на соответствующую страницу.
3. Выберите отдел из выпадающего списка.
4. **Опционально.** Введите имя сотрудника для поиска.
5. Выберите дату начала и окончания искомого посещения.
6. **Опционально.** Проверьте запись УРВ, которую необходимо найти.
7. **Опционально.** Нажмите **Reset** («Сбросить»), чтобы сбросить все условия поиска, затем повторно отредактируйте условия поиска.
8. Нажмите **Search** («Поиск»).

   Подробная информация УРВ отображается ниже. Можно просматривать записи УРВ, включая дату явки, смену, действующий временной период, начало работы, окончание работы, время регистрации прихода, время регистрации выхода, опоздание, ранний уход с работы, период посещения, период отсутствия, период отпуска и период сверхурочной работы.
9. **Опционально.** После поиска выполните следующие действия.

Отчет	Формирование отчета УРВ.
Экспорт	Экспортируйте результаты на локальный компьютер.

Поиск данных УРВ с отклонением от нормы

Можно искать и получать статистику данных УРВ с отклонением от нормы, включая ID сотрудника, имя и отдел, тип отклонения, время начала / окончания и дату отклонения.

Перед началом

- Добавьте организацию и сотрудников в модуле контроля доступа и считайте карты сотрудников. Подробная информация представлена в разделах ***Управление организацией*** и ***Управление информацией о пользователе***.
- Рассчитайте данные УРВ.

Примечание

- Клиентское ПО автоматически рассчитает данные УРВ за предыдущий день в 1:00 утра следующего дня.
- Клиентское ПО должно быть включенным в 1:00 утра, чтобы автоматически рассчитать данные УРВ за предыдущий день. Если расчет не был выполнен автоматически, можно выполнить расчет данных УРВ вручную. Подробная информация представлена в разделе ***Расчет данных о посещаемости вручную***.

Для поиска подробных данных УРВ с отклонением от нормы необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Attendance Statistics → Abnormal Attendance** («Статистика записей УРВ → УРВ с отклонением от нормы»), чтобы перейти на соответствующую страницу.
3. Выберите отдел из выпадающего списка.
4. **Опционально.** Введите имя сотрудника для поиска.
5. Выберите дату начала и окончания искомого посещения.
6. **Опционально.** Нажмите **Reset** («Сбросить»), чтобы сбросить все условия поиска, затем повторно отредактируйте условия поиска.
7. Нажмите **Search** («Поиск»).

   Результат отображается ниже. Можно просмотреть ID сотрудника, имя, отдел, тип отклонения, время начала, время окончания и дату отклонения.
8. **Опционально.** После поиска выполните следующие действия.

Отчет	Формирование отчета УРВ.
Экспорт	Экспортируйте результаты на локальный компьютер.

Поиск данных о сверхурочной работе сотрудников

Можно получить статистику сверхурочной работы выбранного сотрудника за указанный период времени. Можно проверить подробную информацию о сверхурочной работе, включая ID сотрудника, имя и отдел, дату прихода, продолжительность сверхурочной работы и тип сверхурочной работы.

Перед началом

- Добавьте организацию и сотрудников в модуле контроля доступа и считайте карты сотрудников. Подробная информация представлена в разделах ***Управление организацией*** и ***Управление информацией о пользователе***.
- Рассчитайте данные УРВ.

Примечание

- Клиентское ПО автоматически рассчитает данные УРВ за предыдущий день в 1:00 утра следующего дня.
- Клиентское ПО должно быть включенным в 1:00 утра, чтобы автоматически рассчитать данные УРВ за предыдущий день. Если расчет не был выполнен автоматически, можно выполнить расчет данных УРВ вручную. Подробная информация представлена в разделе ***Расчет данных о посещаемости вручную***.

Для поиска сверхурочной работы сотрудников необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Attendance Statistics → Overtime Search** («Статистика записей УРВ → Поиск сверхурочной работы»), чтобы перейти на соответствующую страницу.
3. Выберите отдел из выпадающего списка.
4. **Опционально.** Введите имя сотрудника для поиска.
5. Выберите дату начала и окончания искомого посещения.
6. **Опционально.** Нажмите **Reset** («Сбросить»), чтобы сбросить все условия поиска, затем повторно отредактируйте условия поиска.
7. Нажмите **Search** («Поиск»).

   Подробная информация о сверхурочной работы отображается ниже. Можно просмотреть ID сотрудника, имя, отдел, дату сверхурочной работы, продолжительность сверхурочной работы и тип сверхурочной работы.
8. **Опционально.** После поиска выполните следующие действия.

Отчет	Формирование отчета УРВ.
Экспорт	Экспортируйте результаты на локальный компьютер.

Проверка журналов считывания карт сотрудников

Можно просматривать журналы считывания карт сотрудников, чтобы узнать подробную информацию о считывании карт сотрудников.

Перед началом

- Добавьте организацию и сотрудников в модуле контроля доступа и считайте карты сотрудников. Подробная информация представлена в разделах ***Управление организацией*** и ***Управление информацией о пользователе***.
- Рассчитайте данные УРВ.

Примечание

- Клиентское ПО автоматически рассчитает данные УРВ за предыдущий день в 1:00 утра следующего дня.
- Клиентское ПО должно быть включенным в 1:00 утра, чтобы автоматически рассчитать данные УРВ за предыдущий день. Если расчет не был выполнен автоматически, можно выполнить расчет данных УРВ вручную. Подробная информация представлена в разделе ***Расчет данных о посещаемости вручную***.

Для поиска и просмотра журнала считывания карт необходимо выполнить следующие действия.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Attendance Statistics → Card Swiping Log** («Статистика записей УРВ → Журнал считывания карт»), чтобы перейти на соответствующую страницу.
3. Настройте условия поиска, включая отдел, имя сотрудника или дату прихода на работу.
4. **Опционально.** Нажмите **Reset** («Сбросить») для сброса всех условий поиска.
5. Нажмите **Search** («Поиск»).

   Результаты поиска перечислены на этой странице.

   Можно просмотреть подробные сведения о результате, включая ID, имя, отдел, время, режим аутентификации и номер карты.
6. **Опционально.** После поиска и просмотра журнала считывания карт выполните одну из следующих операций.

   Отчет Формирование отчета УРВ.

   Экспорт Экспортируйте результаты на локальный компьютер.

Создание отчета УРВ

После расчета данных УРВ можно создавать отчеты, в которых отображается состояние УРВ сотрудников за определенный период времени.

Создание мгновенного отчета

Поддерживается функция создания серии отчетов УРВ вручную для просмотра посещаемости сотрудников.

Перед началом
Рассчитайте данные УРВ.

Примечание
Рассчитайте данные УРВ вручную или установите расписание таким образом, чтобы клиентское ПО производило расчет данных автоматически каждый день. Для подробной информации обратитесь к разделу ***Расчет данных УРВ***.

Для мгновенного создания отчета УРВ необходимо выполнить следующие действия.

Шаги
1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Attendance Statistics → Report** («Статистика УРВ → Отчет»), чтобы перейти на страницу отчета.
3. На панели **Instant Report** («Мгновенный отчет») выберите тип отчета из выпадающего списка.
4. Выберите сотрудника или отдел.
5. Укажите период, во время которого данные УРВ будут отображены в отчете.
6. Нажмите **Generate** («Генерировать»).

Настроить расписание создания отчета

Клиентское ПО поддерживает 5 типов отчетов. Можно предварительно определить содержимое отчета и автоматически отправлять отчет на указанный адрес электронной почты.

Для настройки расписания создания отчета необходимо выполнить следующие действия.

Шаги

Примечание
Установите параметры электронной почты, прежде чем включить функцию автоматической отправки электронной почты. Подробная информация представлена в разделе *Настройка параметров электронной почты*.

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени).
2. Нажмите **Attendance Statistics → Report** («Статистика УРВ → Отчет»), чтобы перейти на страницу отчета.

3. На панели **Scheduled Report** («Запланированный отчет») нажмите **Add** («Добавить»), чтобы предварительно определить параметры отчета.
4. Настройте параметры отчета.

   Сотрудник / посетитель

   Выберите добавленного сотрудника и нажмите для добавления сотрудника.
5. **Опционально.** Настройте график автоматического отправления отчета на электронный адрес.
   1) Выберите **Auto-Sending Email** («Отправление на электронную почту в автоматическом режиме») и включите эту функцию.
   2) Установите период, в течение которого клиентское ПО будет отправлять отчеты.
   3) Выберите дату (даты) отправления отчета.
   4) Установите время отправления отчета.

      Пример

      Установите период с 10.03.2018 по 10.04.2018, выберите пятницу в качестве даты отправки и установите время отправки в 20:00:00, клиентское ПО будет отправлять отчеты в 20:00 по пятницам с 10.03.2018 по 10.04.2018.

      Примечание

      Перед настройкой времени выполните расчет статистики УРВ. Рассчитайте данные УРВ вручную или установите расписание таким образом, чтобы клиентское ПО производило расчет данных автоматически каждый день. Для подробной информации обратитесь к разделу ***Расчет данных УРВ***.
   5) Введите электронный адрес получателя.

      Примечание

      Нажмите , чтобы добавить новый адрес электронной почты. Можно добавить до 5 адресов электронной почты.
6. Нажмите **Save** («Сохранить»).
7. **Опционально.** После добавления настроенного отчета выполните следующие действия.

   Изменение отчета

   Выберите отчет и нажмите **Modify** («Изменить»), чтобы изменить его параметры.

   Удаление отчета

   Выберите отчет и нажмите **Remove** («Удалить»), чтобы удалить отчет.

   Создание отчета

   Нажмите **Generate** («Создать»), чтобы мгновенно сгенерировать отчет и просматривать его содержание.

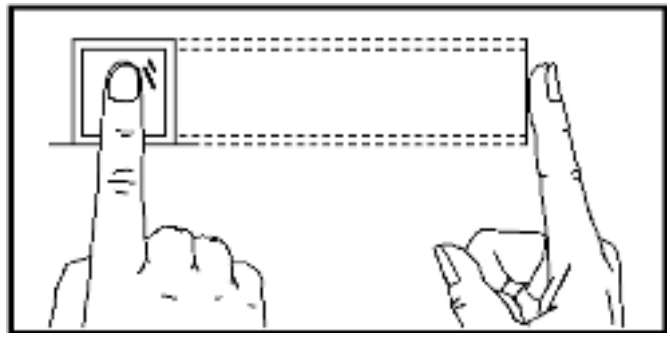
Приложение A. Рекомендации по сканированию отпечатков пальцев

Рекомендуемый палец

Рекомендуется использовать большой, указательный или средний палец.

Правильное сканирование

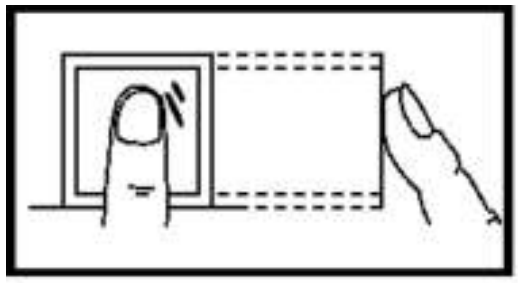
На рисунке ниже показан правильный способ сканирования пальца:



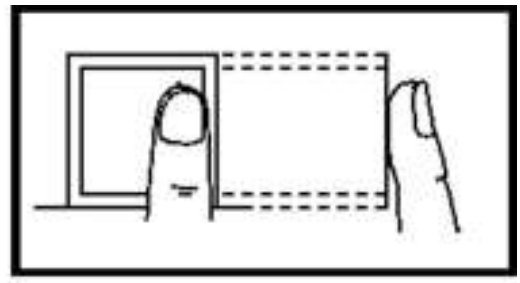
Вы должны прижать палец к сканеру горизонтально. Центр сканируемого пальца должен совпадать с центром сканера.

Неправильное сканирование

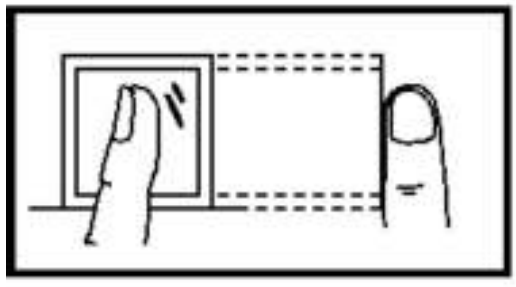
Приведенные ниже рисунки показывают неверные способы сканирования отпечатков пальцев:



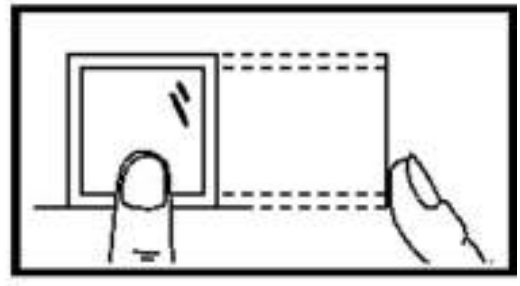
Vertical



Edge I



Side



Edge II

Английский язык	Русский язык
Vertical	Вертикальное положение
Edge	Край
Side	Боковое положение

Окружающая среда

Не подвергайте сканер воздействию прямых солнечных лучей, высоких температур, влажных условий и дождя. Когда палец сухой, сканер может не распознать отпечаток пальца. Можно подуть на палец и снова приложить его к сканеру.

Другое

Если у вас неглубокий отпечаток пальца или его сложно сканировать, рекомендуется использовать другие методы аутентификации.
Если на сканируемом пальце есть травмы, сканер может его не распознать. Можно использовать другой палец и повторить попытку снова.

Приложение B. Описание DIP-переключателей

Расположение переключателей от № 1 до № 8 означает расположение от младшего бита к старшему.

Когда переключатель находится в положении **ON** («ВКЛ.»), это означает, что переключатель включен, в противном случае переключатель выключен. Если вы установите DIP-переключатели, как показано на рисунке ниже, двоичное значение будет равно 00001100, а десятичное значение равно 12.

Приложение C. Пользовательская настройка Wiegand

В качестве примера используйте Wiegand 44 со следующими значениями настроенных параметров **Custom Wiegand** («Настраиваемый Wiegand»):

Имя настраиваемого Wiegand	Wiegand 44				
Общая длина	44				
Правило преобразования (десятичный знак)	По правилу формата [4]=[1][4][0][0]				
Режим четности	Четность XOR				
Старт-бит контроля нечетности		Длина			
Старт бит контроля четности		Длина			
Старт-бит четности XOR	0	Длина каждой группы	4	Общая длина	40
Старт-бит ID-карты	0	Длина	32	Десятичный знак	10
Старт-бит кода объекта		Длина		Десятичный знак	
Старт-бит OEM		Длина		Десятичный знак	
Старт-бит кода производителя	32	Длина	8	Десятичный знак	3

Данные Wiegand

Данные Wiegand = действительные данные + данные четности

Общая длина

Длина данных Wiegand.

Правило комбинации

Четыре байта. Будут отображены комбинированные типы допустимых данных. В примере отображается комбинация идентификатора карты и кода производителя. Допустимые данные могут быть одним правилом или комбинацией нескольких правил.

Режим четности

Действительный паритет для данных Wiegand. Выберите четные или нечетные данные.

Старт-бит и длина контроля нечетности

Если выбрать **Odd Parity** («Старт-бит»), данные элементы будут доступны. Если старт-бит контроля нечетности равен 1, а длина равна 12, тогда система начнет расчет проверки нечетности с бита 1. Будет вычислено 12 битов. Результат будет в бите 0. (Бит 0 – первый бит).

Контроль на четность и длина

Если выбрать **Even Parity** («Контроль на четность»), данные элементы будут доступны. Если старт-бит контроля четности равен 12, а длина равна 12, тогда система начнет расчет проверки четности с бита 12. Будет вычислено 12 битов. Результат будет в стоп-бите.

Четность XOR, длина каждой группы, длина четности

Если выбрать **XOR Parity** («Четность XOR»), данные элементы будут доступны. Основываясь на таблице выше, старт-бит равен 0, длина каждой группы равна 4, а длина четности равна 40. Это означает, что система выполнит расчет каждого 4 бита, начиная с бита 0, что в итоге даст 40 битов (10 групп). Результат будет в последних 4 битах. (Итоговая длина аналогична длине каждой группы).

Старт-бит ID-карты, длина и десятичный знак

Данные параметры доступны при использовании правила преобразования. Основываясь на таблице выше, старт-бит ID-карты равен 0, длина равна 32 и десятичный знак равен 10. Это означает, что, начиная с бита 0, 32 бита представляют собой ID-карту. (Здесь длина рассчитана по биту). А длина десятичного знака равна 10 битов.

Старт-бит кода объекта, длина и десятичный знак

Данные параметры доступны при использовании правила преобразования. Подробная информация представлена в описании ID-карты.

Старт-бит OEM, длина и десятичный знак

Данные параметры доступны при использовании правила преобразования. Подробная информация представлена в описании ID-карты.

Старт-бит кода производителя, длина и десятичный знак

Данные параметры доступны при использовании правила преобразования. Основываясь на таблице выше, старт-бит кода производителя равен 32, длина равна 8 и десятичный знак равен 3. Это означает, что, начиная с бита 32, 8 битов представляют собой код производителя. (Здесь длина рассчитана по биту). А длина десятичного знака равна 3.


See Far, Go Further