



ACCO SOFT

Программа для настройки

СКУД ACCO NET

Руководство по эксплуатации

ACCO NET 1.8

Версия программы 1.19.11

acco soft_ru 02/22

SATEL sp. z o.o.
ул. Budowlanych 66
80-298 Gdańsk
POLAND
тел. +48 58 320 94 00
www.satel.eu

Компания SATEL ставит своей целью постоянное совершенствование качества своих изделий, что может приводить к изменениям в технических характеристиках и программном обеспечении. Информацию о введенных изменениях Вы можете найти на веб-сайте:
<https://support.satel.pl>

В руководстве используются следующие обозначения:



- примечание;



- важная информация предупредительного характера.

Изменения, введенные в версии программы 1.19.11

**Сетевой
контроллер
АССО-NT**

Поддержка нового модуля: АССО-КР2

**Модули контроля
доступа**

Новая опция: Игнорировать настройки шлюза

Зоны доступа

Новая опция: Шлюз.

СОДЕРЖАНИЕ

1.	Введение	4
2.	Установка	4
2.1	Системные требования.....	4
2.2	Установка программы ACCO Soft.....	4
3.	Первый запуск программы ACCO Soft	4
3.1	Регистрация в программе	4
4.	Описание программы ACCO Soft	5
4.1	Главное меню программы	5
4.1.1	Список неисправностей / тревог	6
4.1.2	Лицензии	7
4.1.2.1	Окно «Лицензии интеграции».....	7
4.1.2.2	Получение лицензии.....	10
4.1.2.3	Загрузка лицензии.....	11
4.2	Структура системы	12
4.2.1	Список объектов и сетевых контроллеров	12
4.2.1.1	Перезапуск сетевого контроллера.....	13
4.2.2	Объекты	14
4.2.2.1	Добавление объекта	14
4.2.2.2	Настройка объектов.....	14
4.2.2.3	Удаление объекта.....	15
4.2.3	Сетевые контроллеры.....	16
4.2.3.1	Добавление сетевого контроллера ACCO-NT, подключенного к сети Ethernet 16	
4.2.3.2	Добавление сетевого контроллера ACCO-NT перед его подключением к сети Ethernet.....	16
4.2.3.3	Настройка сетевого контроллера	16
4.2.3.4	Удаленное обновление прошивки сетевого контроллера	18
4.2.3.5	Удаление сетевого контроллера	18
4.2.4	Модули контроля доступа	18
4.2.4.1	Идентификация модулей контроля доступа в системе.....	19
4.2.4.2	Добавление модуля перед его подключением к системе.....	19
4.2.4.3	Окно «Результаты»	20
4.2.4.4	Таблица со списком модулей контроля доступа	21
4.2.4.5	Настройка модуля контроля доступа.....	22
4.2.4.6	Удаленное обновление прошивки модуля контроля доступа.....	41
4.2.4.7	Удаление модуля контроля доступа.....	42
4.2.5	Зоны доступа	42
4.2.5.1	Создание зоны доступа	42
4.2.5.2	Таблица со списком зон доступа	43
4.2.5.3	Настройка зон доступа	44
4.2.5.4	Удаление зоны доступа	47
4.2.6	Интеграция.....	47
4.2.6.1	Настройка системы охранной сигнализации.....	47
4.2.6.2	Добавление системы охранной сигнализации.....	49
4.2.6.3	Таблица со списком систем охранной сигнализации	49
4.2.6.4	Настройка интеграции	50
4.2.6.5	Назначение зоны доступа	51
4.2.6.6	Удаление системы охранной сигнализации.....	51
4.2.7	Модули расширения.....	52
4.2.7.1	Добавление модуля расширения	52
4.2.7.2	Настройки модуля расширения	52
4.2.7.3	Удаление модуля расширения	52

4.2.8	Входы	53
4.2.8.1	Нумерация входов в системе.....	53
4.2.8.2	Настройка входов	53
4.2.9	Выходы.....	55
4.2.9.1	Нумерация выходов в системе	56
4.2.9.2	Настройка выходов.....	56
4.2.10	Маршруты	59
4.2.10.1	Создание маршрута.....	59
4.2.10.2	Настройка маршрута.....	59
4.2.10.3	Удаление маршрута.....	60
4.2.11	Состояние	60
4.2.11.1	Неисправности сетевого контроллера	61
4.2.11.2	Состояние питания сетевого контроллера.....	62
4.2.11.3	Закладка «Входы».....	62
4.2.11.4	Закладка «Выходы»	62
4.2.12	Импорт	62
4.2.12.1	Импорт данных из файла в формате CSV	62
4.2.12.2	Импорт данных из файла с расширением kkd	63
5.	Приложение 1 «Описание интеграции систем»	65
6.	Приложение 2 «Интегрированные зоны»	66
6.1	Примеры	67
6.1.1	Пример 1	67
6.2	Сигнализация блокировки точки прохода / зоны доступа устройствами СКУД	68
6.2.1	Оптическая сигнализация.....	69
6.2.1.1	Приоритеты состояний системы ACCO NET	69
6.2.1.2	Клавиатуры	69
6.2.1.3	Клавиатура со считывателем бесконтактных карт.....	69
6.2.1.4	Считыватели бесконтактных карт.....	69
6.2.1.5	Считыватель ключей DALLAS iButton	70
6.2.2	Звуковая сигнализация	70

1. Введение

Программа ACCO Soft предназначена для настройки СКУД ACCO NET. Связь между программой и системой осуществляется удаленно с помощью сети Ethernet.

Данные сохраняются во всех сетевых контроллерах системы, модулях контроля доступа и в модулях расширения.

2. Установка

2.1 Системные требования

Программа ACCO Soft требует для работы среды Java версии 8. Скачайте эту версию программы и установите на компьютер.

2.2 Установка программы ACCO Soft

1. Запустите интернет-браузер.
2. Введите адрес: [https://\[адрес компьютера, на котором установлено ПО ACCO Server\]](https://[адрес компьютера, на котором установлено ПО ACCO Server]) и зарегистрируйтесь в приложении ACCO Web как Администратор (по умолчанию: логин «admin» и пароль «admin»). Если связь будет осуществляться не с помощью порта по умолчанию, а другого порта, адрес системы необходимо ввести следующим образом: [https://\[адрес сервера:номер порта\]](https://[адрес сервера:номер порта]).
3. Щелкните по команде «Программы» в меню с левой стороны экрана. Будут отображены ссылки к установочным файлам программ ACCO-NT Conf, ACCO Soft и Map Editor.
4. Щелкните по ссылке ACCO Soft (для системы Windows или Linux) и загрузите установочный файл на диск.
5. Запустите установочный файл и поступайте согласно подсказкам.



После каждого обновления системы ACCO NET загрузите и установите новейшую версию программы ACCO Soft.

3. Первый запуск программы ACCO Soft

3.1 Регистрация в программе

Доступ к программе защищен паролем. При первом запуске программы доступ можно получить с помощью установленных по умолчанию логина «admin» и пароля «admin» (не нужно их вводить, достаточно щелкнуть по кнопке «Соединить»).

В поле «Адрес системы» введите сетевой адрес компьютера, на котором установлен ACCO Server. Адрес может быть введен в виде IP-адреса (4 десятичных числа, разделенных точками) или названия.

Если порт (RMI) для связи между ACCO Server и программой ACCO Soft не является портом по умолчанию 2500, то после адреса IP и двоеточия следует ввести порт для осуществления связи.



Заводской пароль доступа к программе для Администратора следует изменить перед тем, как приступить к эксплуатации системы в приложении ACCO Web.

Доступ ко всем функциям программы предоставлен Администратору системы ACCO NET. Уровень доступа остальных пользователей можно

определить с помощью приложения ACCO Web (см. руководство по эксплуатации ACCO Web).

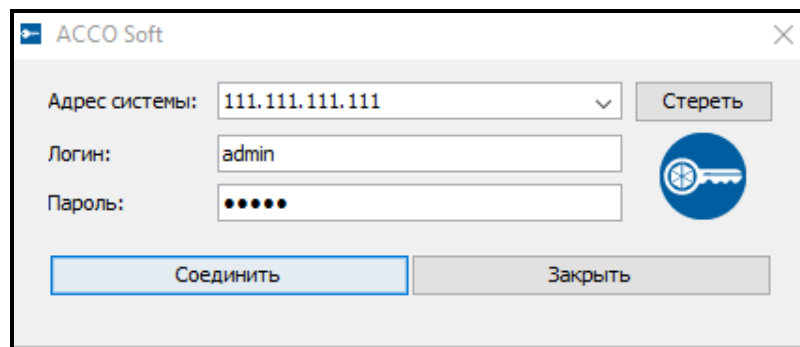



Рис. 1. Окно регистрации после запуска программы ACCO Soft.

4. Описание программы ACCO Soft



Если в главном меню программы будет отображаться кнопка , то это означает, что в данный момент кто-то другой настраивает систему ACCO NET.

4.1 Главное меню программы

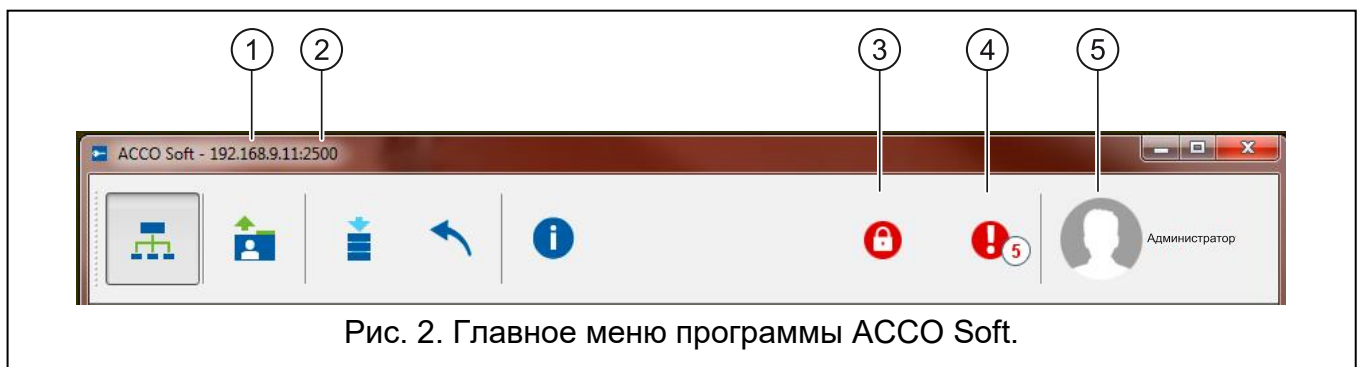




Рис. 2. Главное меню программы ACCO Soft.

Пояснения к рисунку 2:

- ① сетевой адрес компьютера, на котором установлен ACCO Server.
- ② номер порта для связи между ACCO Server и программой ACCO Soft.
- ③ кнопка, информирующая о блокировке базы данных. Если подвести к ней указатель мыши, отобразится информация о том, что другой пользователь начал редактирование и не сохранил введенные изменения. Блокировка перестает действовать после сохранения изменений или по истечении 15 минут (настройки по умолчанию) с момента введения последнего изменения. По истечении этого времени можно разблокировать базу данных, щелкнув по кнопке . Время действия блокировки можно изменить в приложении ACCO Web.

О блокировке будет информировать также сообщение, которое отобразится:

- если Вы зарегистрированы в программе, а другой пользователь начнет редактировать данные,
- если Вы запустите программу, а другой пользователь уже будет редактировать данные.

- ④ кнопка, информирующая о текущих неисправностях / тревогах в системе. Рядом отображается их количество. Список неисправностей / тревог будет отображен после нажатия кнопки (см. раздел «Список неисправностей / тревог»). Если программа ACCO Soft не будет соединена с ACCO Server, отображается кнопка , сообщающая об отсутствии связи.
- ⑤ имя и фотография зарегистрированного пользователя.

Кнопки:



- кнопка позволяет открыть окно настроек системы.



- кнопка позволяет импортировать данные, касающиеся пользователей, из файлов с расширением kkd (из программы ACCO-SOFT-LT) и из файлов в формате CSV.



- кнопка позволяет сохранить введенные изменения.



- кнопка позволяет отменить все введенные изменения с момента последнего сохранения данных.



- кнопка позволяет открыть окно с информацией о версии системы ACCO NET, программы ACCO Soft, а также версиях и сетевых адресах сервера и базы данных. Дополнительно, окно предоставляет доступ к лицензиям ПО ACCO Soft и ACCO Server и интегрирования систем (см. раздел «Лицензии»).

4.1.1 Список неисправностей / тревог

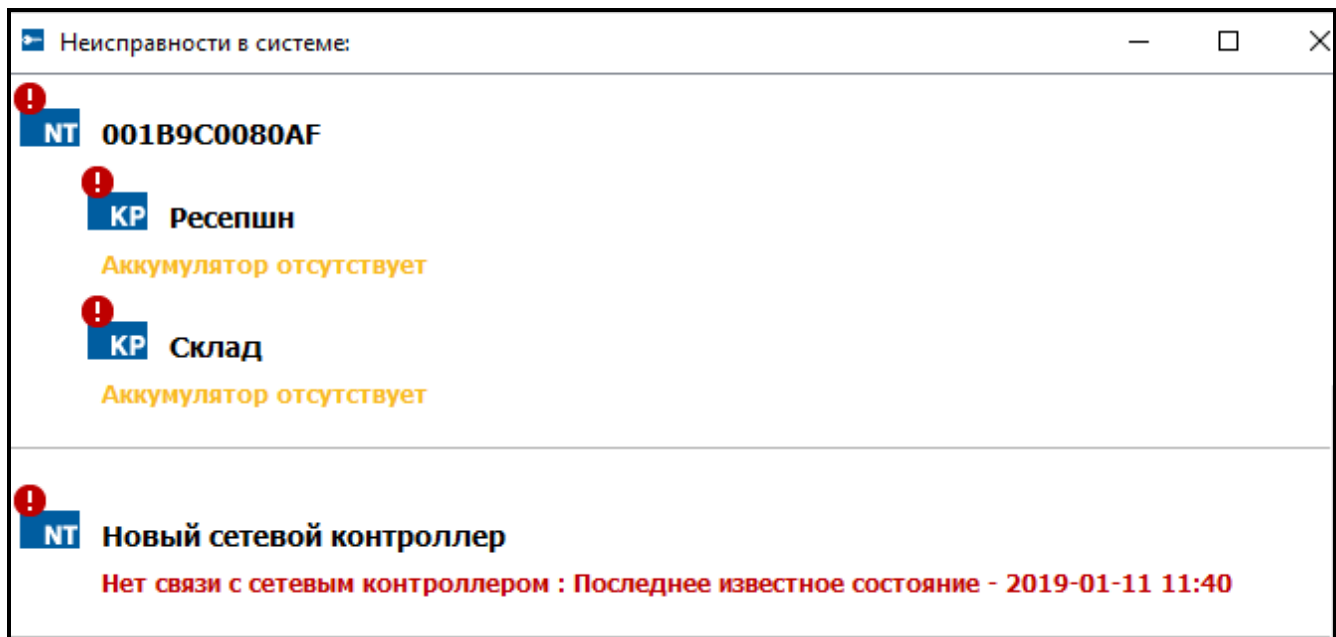


Рис. 3. Пример списка текущих неисправностей в системе.

В окне в древовидной структуре отображаются все устройства, входящие в состав СКУД. Под названием устройства, в котором произошла авария / тревога, будет отображено соответствующее сообщение. Цвет сообщения имеет следующее значение:

красный – тревога;

оранжевый – неисправность;


зеленый – подтвержденная тревога / неисправность;

серый – память тревоги / неисправности.

4.1.2 Лицензии



Рис. 4. Окно с информацией о версии системы ACCO NET, программ и базы данных, а также с кнопками, позволяющими получить доступ к лицензиям.

В окне, которое откроется после нажатия кнопки  в главном меню программы, отображается «Информация о лицензиях» и кнопки:

Показать [рядом с лицензией ACCO Soft] – нажмите, чтобы открыть окно с лицензионным соглашением для ACCO Soft.

Показать [рядом с лицензией ACCO NET] – нажмите, чтобы открыть окно с лицензионным соглашением для ACCO Server.

Управлять [рядом с лицензией интеграции] – нажмите, чтобы открыть окно «Лицензии интеграции».

4.1.2.1 Окно «Лицензии интеграции»

Также см. раздел «Интеграция».

Сетевому контроллеру ACCO-NT можно назначить приемно-контрольные приборы INTEGRA или INTEGRA Plus. Интеграция сетевого контроллера ACCO-NT с одной системой охранной сигнализации бесплатна. Лицензионный ключ необходим, если сетевой контроллер ACCO-NT должен быть интегрирован больше чем с одним приемно-контрольным прибором. Ключ генерируется для конкретного сетевого контроллера ACCO-NT. Он определяет максимальное количество поддерживаемых приемно-контрольных приборов.

Владелец – название компании / имя и фамилия, на которые был сгенерирован лицензионный ключ.

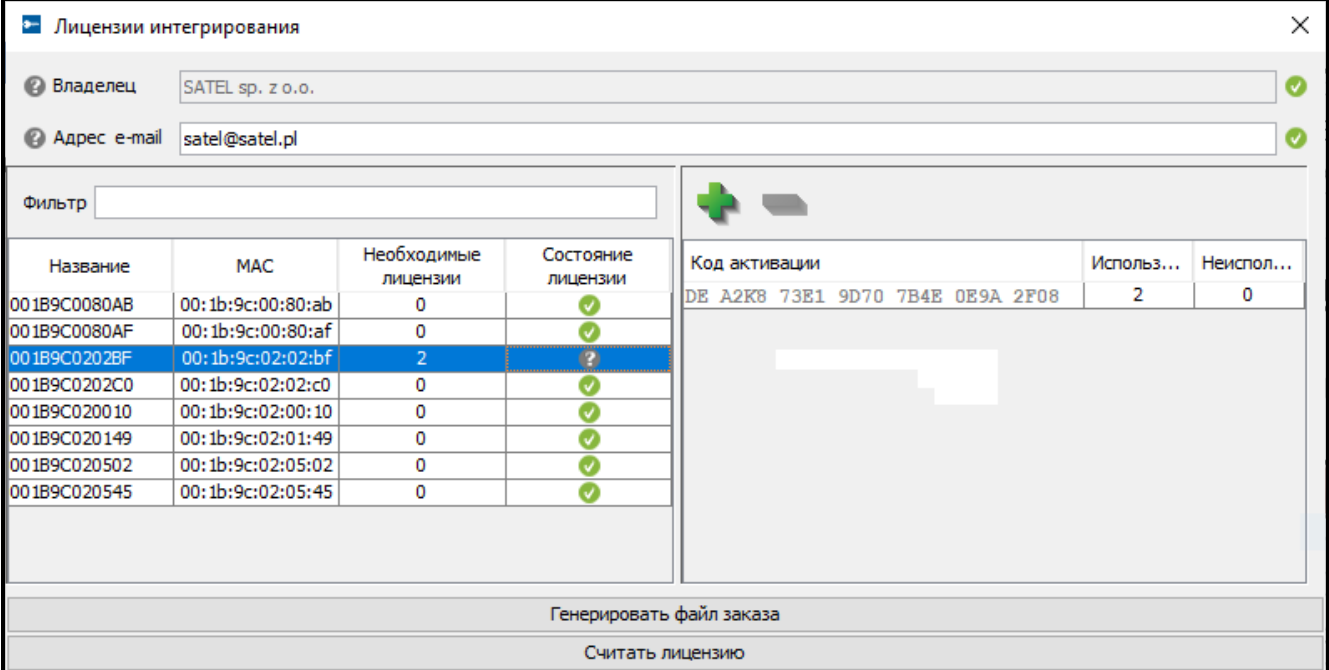
Адрес e-mail – адрес электронной почты, на который будет отправлен лицензионный ключ.

Таблица со списком сетевых контроллеров ACCO-NT в системе ACCO NET

Фильтр – в поле можно ввести часть адреса или MAC-адрес сетевого контроллера.

Данные фильтруются после ввода любого символа.

Название – индивидуальное название сетевого контроллера.



Название	MAC	Необходимые лицензии	Состояние лицензии
001B9C0080AB	00:1b:9c:00:80:ab	0	✓
001B9C0080AF	00:1b:9c:00:80:af	0	✓
001B9C0202BF	00:1b:9c:02:02:bf	2	?
001B9C0202C0	00:1b:9c:02:02:c0	0	✓
001B9C020010	00:1b:9c:02:00:10	0	✓
001B9C020149	00:1b:9c:02:01:49	0	✓
001B9C020502	00:1b:9c:02:05:02	0	✓
001B9C020545	00:1b:9c:02:05:45	0	✓

Код активации	Используй...	Неиспол...
DE A2K8 73E1 9D70 7B4E 0E9A 2F08	2	0

Рис. 5. Окно «Лицензии интегрирования»

MAC – идентификационный номер платы Ethernet (MAC) сетевого контроллера.

Необходимые лицензии – количество лицензий необходимых для интеграции. Оно соответствует уменьшенному на один количеству добавленных систем безопасности (см. раздел «Интеграция»), (одна система охранной сигнализации не требует лицензии).

Состояние лицензии – в поле может отображаться следующая информация:




-  – лицензия зашифрована (иконка отобразится, если введенный текст лицензионного ключа для данного сетевого контроллера ACCO-NT не был дешифрован из-за отсутствия связи между ACCO Server и сетевым контроллером ACCO-NT или после перезапуска программы ACCO Server, если программа еще не соединилась с данным сетевым контроллером ACCO-NT),
-  – недостаточное количество требуемых лицензий,
-  – требуемых лицензий достаточно.

Таблица со списком кодов активации

По щелчку на сетевой контроллер ACCO-NT отобразится таблица со списком кодов активации:



– нажмите, чтобы добавить код активации.



– нажмите, чтобы удалить выделенный код активации.

Код активации – номер кода активации, который можно купить у авторизованного дилера компании SATEL. Код состоит из 26 символов (цифр и букв). Он определяет количество лицензий, которые можно получить для интегрированных систем охранной сигнализации.

Использованные лицензии – количество использованных лицензий для систем охранной сигнализации.

Неиспользованные лицензии – количество неиспользованных лицензий для систем охранной сигнализации.

Кнопки

Генерировать файл заказа (slr) – нажать, чтобы открыть окно «Лицензии – итоги», которое позволяет генерировать файл заказа на ключ лицензии (см. раздел «Окно «Лицензии – итоги»»).

Считать лицензию – нажать, чтобы открыть окно «Считать лицензию», в которое можно скопировать ключ лицензии (см. раздел «Окно «Считать лицензию»»).

Окно «Лицензии – итоги»

В окне отображается сводная информация на основе данных из окна «Лицензии интеграции». Эта информация сохраняется в файле с расширением .slr, на основе которого будет сгенерирован ключ лицензии.

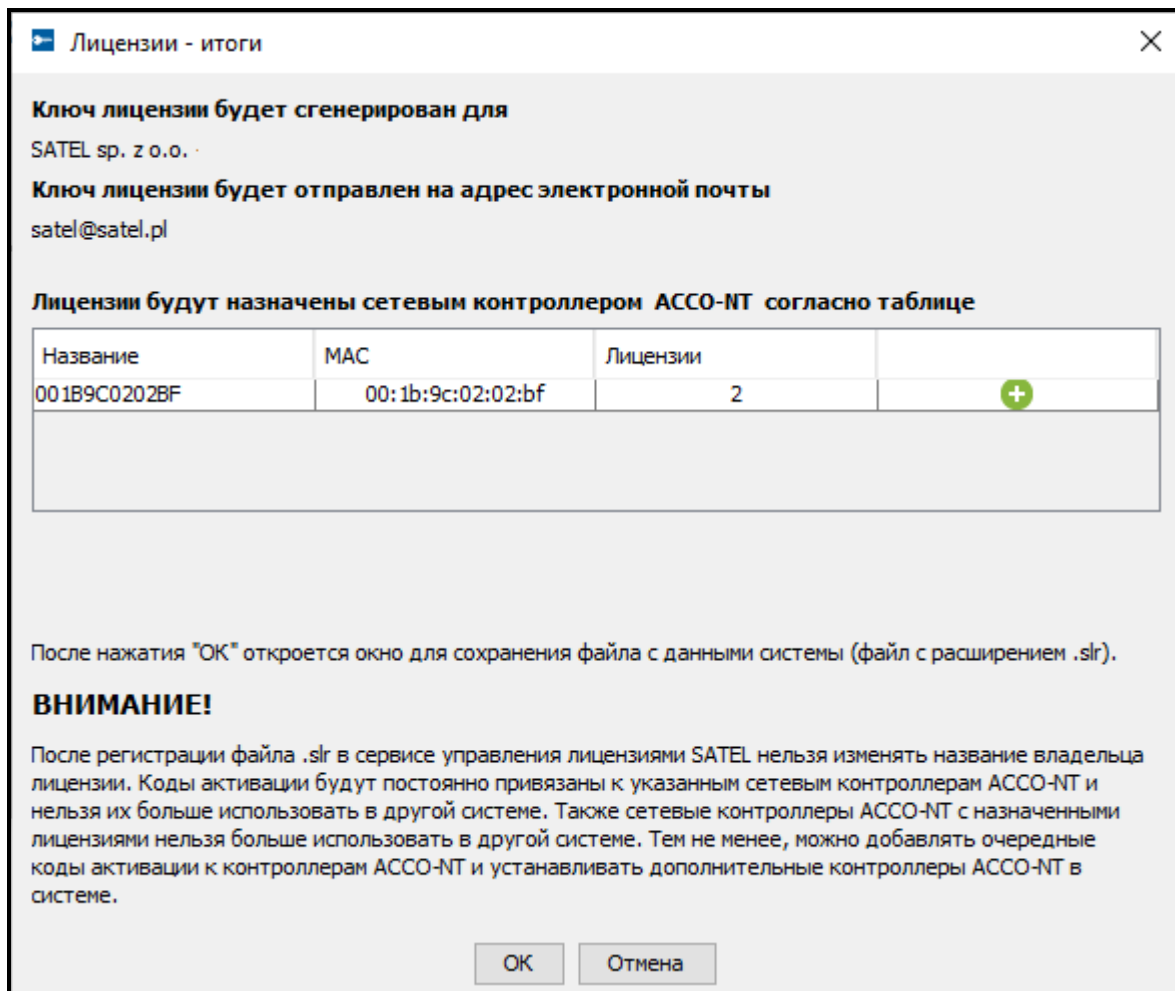


Рис. 6. Окно «Лицензии – итоги».

В таблице со списком сетевых контроллеров ACCO-NT, которым назначены лицензии, в последней графе отображается следующая информация:

- + – новая лицензия,
- ✓ – лицензия не изменена,
- ✓+ – лицензия изменена.

OK – нажмите кнопку, чтобы сгенерировать файл заказа на ключ лицензии. Откроется окно, в котором можно указать, где сохранен файл (с расширением .slr), содержащий отображаемые данные (см. раздел «Получение лицензии»).

Окно «Считать лицензию»

В окне следует ввести ключ лицензии, полученный в электронном письме.

OK – кнопка позволяет загрузить в систему ключ лицензии, содержащий лицензии на системы охранной сигнализации. Кнопка будет активной после вставки скопированного текста ключа лицензии. В случае ошибок в тексте отобразится соответствующее сообщение.

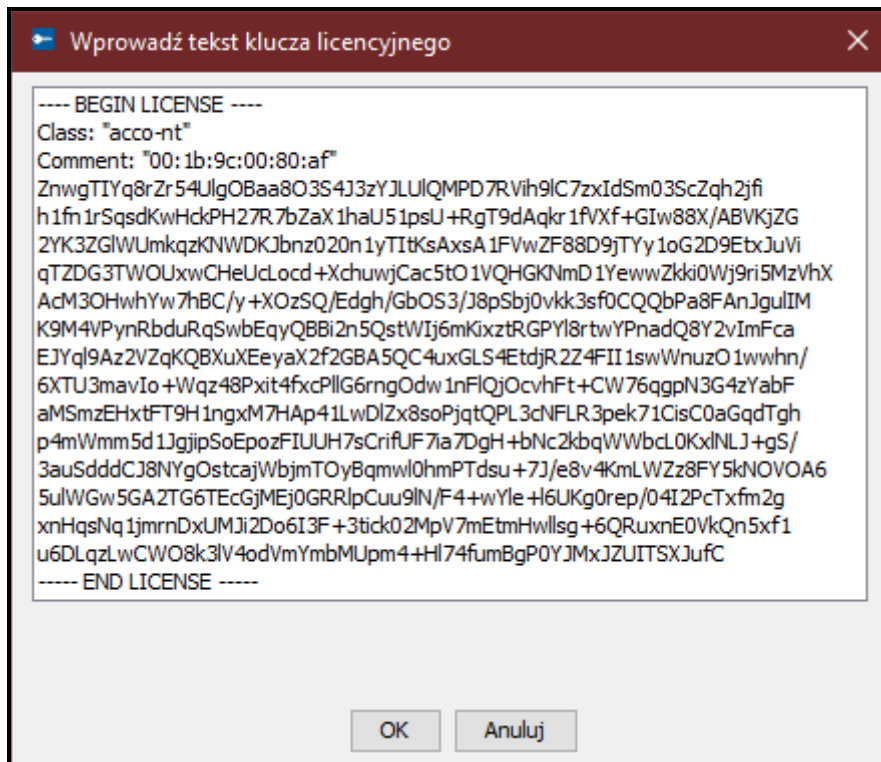


Рис. 7. Окно с примером ключа лицензии.

4.1.2.2 Получение лицензии

1. Согласно процедуре, описанной в разделе «Добавление системы охранной сигнализации», добавьте систему или системы охранной сигнализации.

2. В главном меню программы щелкните по кнопке .

3. В открывшемся окне нажмите кнопку «Управлять».

4. В поле «Владелец» введите название компании или имя и фамилию, на которые должен быть сгенерирован ключ лицензии.

5. В поле «Адрес e-mail» введите адрес, на который должен быть отправлен ключ лицензии.

6. В таблице со списком сетевых контроллеров ACCO-NT выделите сетевой контроллер, который должен обслуживать настроенные системы охранной сигнализации.

7. Когда отобразится таблица со списком кодов активации, нажмите кнопку .

8. В окне «Код активации» введите номер кода, который находится на Вашем активационном талоне. Если данный сетевой контроллер ACCO-NT должен

обслуживать больше систем, чем это предусматривает добавляемый код, то необходимо ввести очередные коды.



Не следует вводить код активации для большего числа систем, чем добавлено в закладке «Интеграция» (см. раздел «Интеграция»).

9. Если очередной сетевой контроллер ACCO-NT должен обслуживать системы безопасности, выделите его и повторите действия из пунктов 7 и 8.
10. Щелкните кнопку «Генерировать файл заказа (slr)».
11. В окне «Лицензии – итоги» проверьте, все ли данные правильны, и прочитайте информацию в нижней части окна.
12. Щелкните по кнопке «ОК».
13. В открывшемся окне укажите, где сохранить файл с Вашими данными и с данными системы (файл с расширением .slr). Можно изменить название сохраняемого файла. Щелкните по кнопке «Сохранить».
14. Зарегистрируйте файл в сервисе управления лицензиями SATEL. С этой целью запустите интернет-браузер и введите адрес: <https://license.satel.pl>.



После регистрации файла с расширением .slr в сервисе управления лицензиями SATEL:


- *нельзя изменить название владельца лицензии,*
- *коды активации будут постоянно привязаны к указанным Вами сетевым контроллерам ACCO-NT, и их нельзя использовать в другой системе,*
- *сетевые контроллеры ACCO-NT, которым будут назначены лицензии, не могут устанавливаться в другой системе.*

15. На открывшейся странице щелкните по «ACCO NET».
16. Вы будете перенаправлены на страницу регистрации ACCO NET.
17. Нажмите «Выбрать файл» и в открывшемся окне укажите путь к сгенерированному файлу.
18. Щелкните по кнопке «Регистрация». Отобразится подтверждение регистрации файла. Дополнительное подтверждение Вы получите также в электронном письме, отправленном на адрес, который Вы указали при вводе своих данных.
19. Ключ лицензии, содержащий заказанные Вами лицензии, Вы получите в следующем письме.

4.1.2.3 Загрузка лицензии

1. Если Вы получите ключ лицензии, убедитесь, что связь между ACCO Server и сетевым контроллером / сетевыми контроллерами ACCO-NT для загрузки ключа лицензии осуществляется правильно.



2. В главном меню программы щелкните по кнопке .
3. В открывшемся окне нажмите кнопку «Управлять».
4. В окне «Лицензии интеграции» щелкните по кнопке «Считать лицензию».
5. Когда откроется окно «Считать лицензию», вставьте скопированный ключ лицензии, который Вы получили.



Текст ключа лицензии должен начинаться с "---- BEGIN LICENSE ----", и заканчиваться фразой "---- END LICENSE ----".

6. Щелкните по кнопке «ОК».

7. Когда ключ лицензии будет загружен, в графе «Состояние лицензии», рядом с сетевым контроллером / сетевыми контроллерами, для которого / для которых он был считан, будет отображена соответствующая информация.

4.2 Структура системы

Описание кнопок



- кнопка позволяет добавить объект.



- кнопка позволяет удалить выделенный объект.



- кнопка позволяет добавить сетевой контроллер.



- кнопка позволяет удалить сетевой контроллер.

4.2.1 Список объектов и сетевых контроллеров

В списке отображаются объекты и назначенные им сетевые контроллеры. Также отображается ветка со списком сетевых контроллеров без назначения. Рядом с каждым сетевым контроллером отображается иконка, которая означает:



– отсутствие связи с ACCO Server дольше 60 минут (белый восклицательный знак на красном фоне),



– отсутствие связи с ACCO Server короче 60 минут (белый восклицательный знак на оранжевом фоне),



– связь с ACCO Server ОК (белый символ на зеленом фоне).

В скобках за названием сетевого контроллера отображается информация о его состоянии:

- Состояние сетевого контроллера неизвестно,
- Отсутствие связи,
- Сетевой контроллер ОК,
- Восстановление установок (полное),
- Восстановление конфигурационных настроек сетевого контроллера,
- Загрузка конфигурации (ACCO Server передает на сетевой контроллер изменения, введенные в конфигурации системы),
- Регистрация сетевых контроллеров,
- Идентификация (во время поиска модулей контроля доступа),
- Рассылка пользователей (рассылка данных, касающихся пользователей, на модули контроля доступа),
- Режим работы контроллера,
- Несовпадение ключей шифрования (касается ключа шифрования данных, которыми обмениваются ACCO Server и сетевой контроллер),
- Введение изменений в памяти сетевого контроллера,
- Введение изменений в памяти модулей контроля доступа,
- Цифры / числа (информация о данных, обрабатываемых в данный момент).

Кнопки, находящиеся под списком объектов и сетевых контроллеров:



– кнопка позволяет упорядочить все объекты из списка по названию от А до Я.



– кнопка позволяет упорядочить все объекты из списка по названию от Я до А.

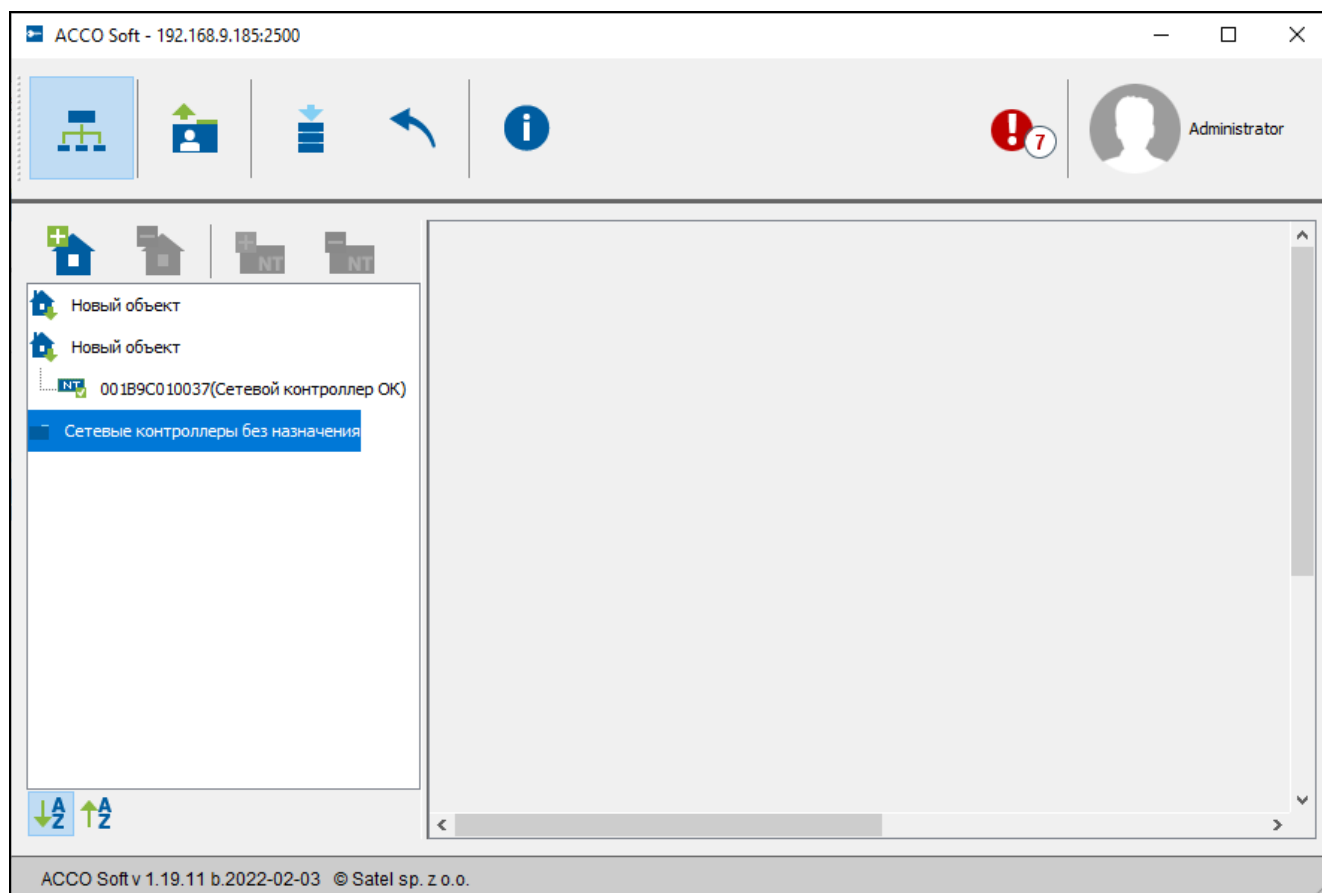


Рис. 8. Список объектов и сетевых контроллеров.


4.2.1.1 Перезапуск сетевого контроллера

1. Чтобы перезапустить сетевой контроллер, необходимо выделить выбранные устройства в списке.
2. Щелкните правой кнопкой мыши.
3. Щелкните по появившемуся запросу «Перезапуск устройства».




Опция «Перезапуск устройства» доступна только, если связь между сетевым контроллером и ACCO Server осуществляется правильно.

В случае каких-либо проблем со связью и с перезапуском сетевого контроллера, отобразится соответствующее сообщение.

4. Иконки отображаются рядом с названием сетевого контроллера и будут информировать в режиме реального времени о процессе перезапуска сетевого контроллера.
5. Повторное отображение иконки  означает, что сетевой контроллер перезапущен.

4.2.2 Объекты

4.2.2.1 Добавление объекта

Щелкните по кнопке . Новый объект появится в списке (см. раздел «11»).

4.2.2.2 Настройка объектов

Щелкните по выбранному объекту в списке объектов, чтобы его запрограммировать. Параметры объекта будут отображены в закладках «Настройка объекта» и «Управление сетевыми контроллерами».

Параметры объекта

Закладка «Настройка объекта»

Имя – индивидуальное название объекта (до 32 символов).

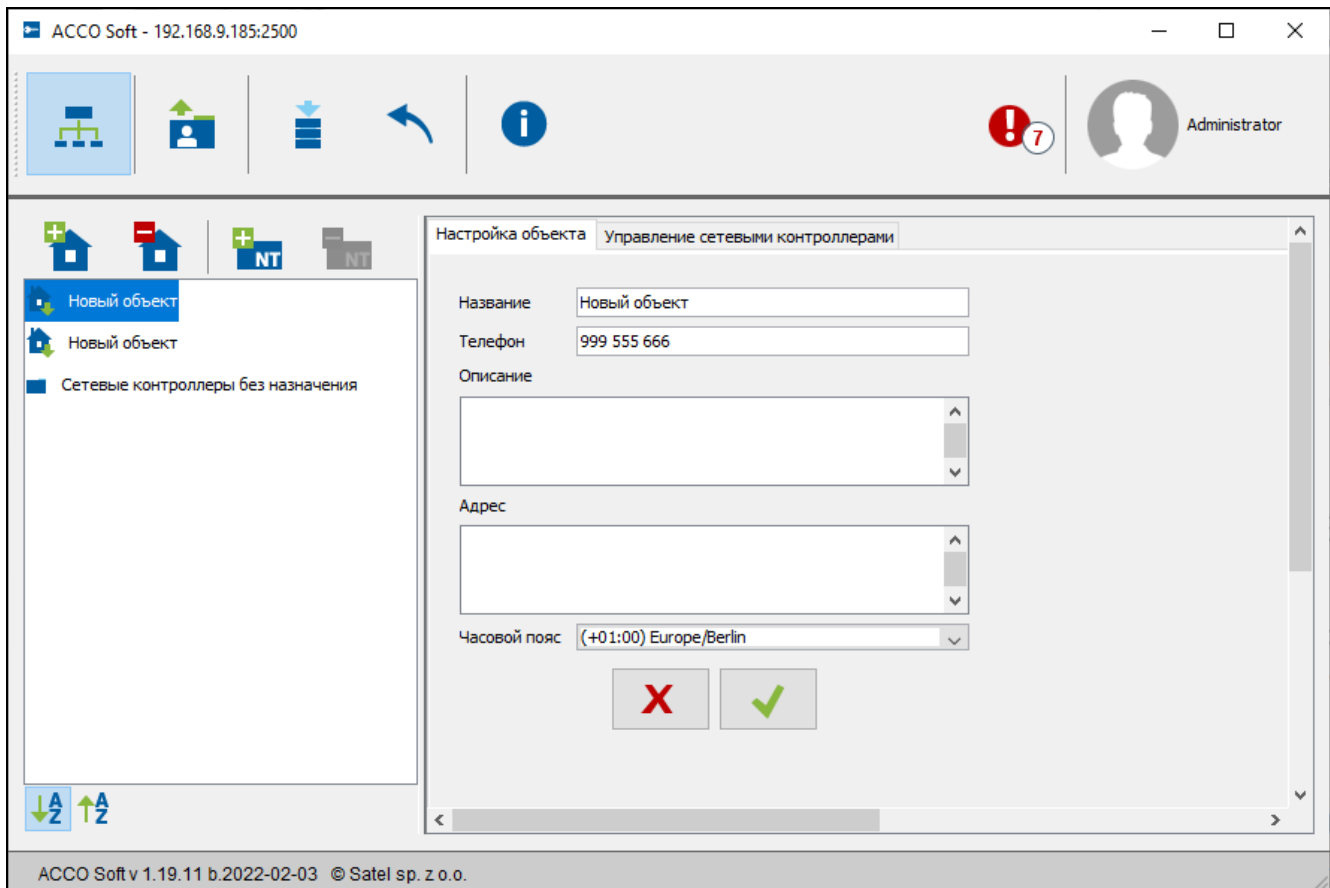
Телефон – номер телефона объекта.

Описание – в поле можно ввести дополнительное описание объекта.

Адрес – адрес объекта.

Часовой пояс – разница между универсальным временем (GMT) и временем в зоне.

Это позволит записывать события в базу данных с правильным временем, а также отображать события в приложении ACCO Web и отображать правильное время на дисплеях клавиатур, подключенных к модулям контроля доступа.



ACCO Soft v 1.19.11 b.2022-02-03 © Satel sp. z o.o.

Рис. 9. Закладка «Настройка объекта».

После ввода каких-либо изменений отобразятся кнопки:



– щелкните, чтобы отменить введенные изменения.



– щелкните, чтобы подтвердить введенные изменения.

Закладка «Управление сетевыми контроллерами»

Сетевые контроллеры на объекте – список сетевых контроллеров, назначенных объекту.

Сетевые контроллеры без назначения – список сетевых контроллеров, которые еще не были назначены объектам.

Кнопки со стрелками предназначены для назначения сетевых контроллеров в соответствующий список – в список сетевых контроллеров на объекте или в список сетевых контроллеров без назначения.

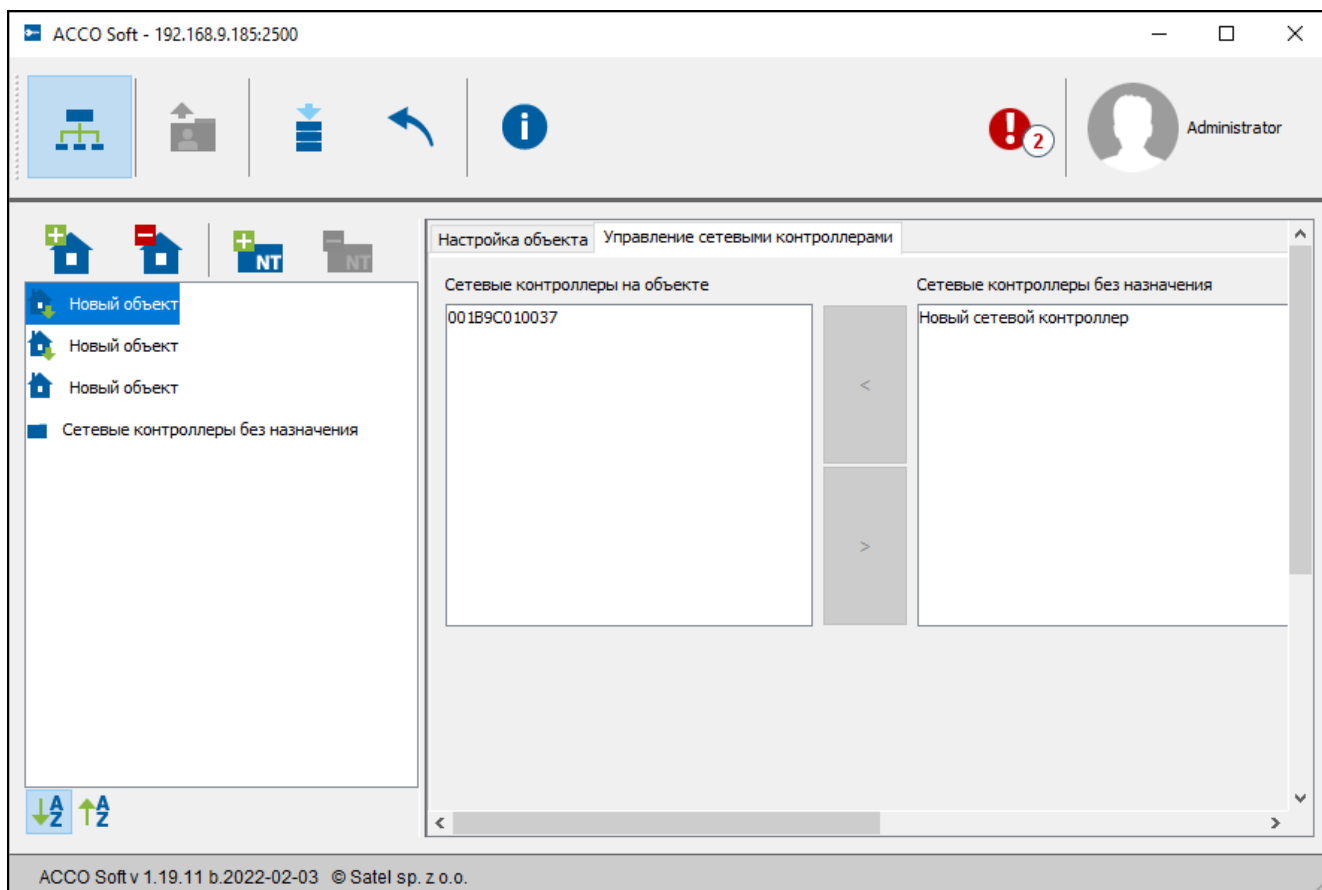



Рис. 10. Закладка «Управление сетевыми контроллерами».

4.2.2.3 Удаление объекта

1. Если Вы хотите удалить объект, необходимо выделить его в списке объектов.
2. Если Вы хотите за один раз удалить несколько объектов, щелкните мышью на одном из объектов и, удерживая нажатой клавишу Ctrl, выберите очередные объекты с помощью левой клавиши мыши.
3. Если Вы хотите удалить все объекты одновременно, щелкните мышью на одном из объектов и нажмите одновременно клавиши Ctrl+A.

4. Щелкните мышью по кнопке .

5. Когда отобразится запрос на подтверждение удаления объекта, щелкните по «Да». Сетевые контроллеры объекта, который был удален, отобразятся в списке сетевых контроллеров без назначения.

6. Сохраните введенные изменения.

4.2.3 Сетевые контроллеры

4.2.3.1 Добавление сетевого контроллера ACCO-NT, подключенного к сети Ethernet

1. Выделите в списке объект для назначения ему добавляемого сетевого контроллера.
2. Перейдите к закладке «Управление сетевыми контроллерами».
3. Выделите сетевой контроллер в списке «Сетевые контроллеры без назначения». В нем отображаются сетевые контроллеры, которые подключились к ACCO Server (как название отображается MAC-адрес сетевого контроллера).
4. Щелкните по стрелке, чтобы перенести сетевой контроллер в список «Сетевые контроллеры на объекте».
5. Когда отобразится вопрос, сохранить ли настройки, щелкните по «Да».
6. Сетевой контроллер отобразится в списке объектов и сетевых контроллеров как назначенный данному объекту.

4.2.3.2 Добавление сетевого контроллера ACCO-NT перед его подключением к сети Ethernet

1. Выделите в списке объект для назначения ему добавляемого сетевого контроллера.
2. С помощью кнопки  добавьте сетевой контроллер. Он отобразится в списке объектов и сетевых контроллеров как назначенный данному объекту.
3. Выделите сетевой контроллер.
4. Щелкните по закладке «Настройка сетевого контроллера». Задайте настройки сетевого контроллера, за исключением MAC-адреса, и сохраните настройки (см. рис. 11).
5. После подключения сетевого контроллера к сети Ethernet и установления связи между сетевым контроллером и ACCO Server, щелкните по символу меню в поле «MAC-адрес». Отобразится список MAC-адресов сетевых контроллеров, не назначенных объектам.
6. Выберите из списка MAC-адрес соответствующего сетевого контроллера.
7. Когда отобразится вопрос, привязать ли устройства друг к другу, щелкните по «Да».

4.2.3.3 Настройка сетевого контроллера

Щелкните по выбранному сетевому контроллеру в списке объектов и сетевых контроллеров, чтобы его настроить. Параметры отобразятся в закладке «Настройка сетевого контроллера».

Настройка сетевого контроллера

Название – индивидуальное название сетевого контроллера (до 45 символов). По умолчанию в качестве названия отображается MAC-адрес сетевого контроллера.

MAC-адрес – уникальный идентификационный номер сетевой платы Ethernet (MAC) сетевого контроллера. Если в поле отображается «Привязать к устройству...», можно щелкнуть по полю и выбрать MAC-адрес из списка.

Описание – в поле можно дополнительно ввести описание сетевого контроллера.

Время отсутствия питания АС [мин] – время, в течение которого сетевой контроллер должен оставаться без сетевого питания, чтобы была сообщена неисправность. Эта задержка предотвращает извещение о кратковременном пропадании питания, не влияющем на нормальную работу системы. Максимальное значение – 60 минут.

IP-адрес – IP-адрес сетевого контроллера.

Тип – модель сетевого контроллера.




Настройка сетевого контроллера	Модули контроля доступа	Зоны доступа	Интегрирование	Модули расширения	Входы	Выходы	Маршруты	Состояние
Название	Здание А							
MAC-адрес	00:1b:9c:01:00:37							
Описание								
Время отсутствия питания АС [мин]	0							
IP-адрес	192.168.9.61							
Тип	ACCO-NT2							
Версия	1.15.937 2022-03-08 udp log  							
Ключ шифрования	<input type="text"/> 							
Отказ в доступе при ошибке интегрирования	<input type="checkbox"/>							
Лицензия	Лицензия для этого прибора не считана							

Рис. 11. Закладка «Настройка сетевого контроллера».

Версия – версия прошивки сетевого контроллера (номер версии и дата сборки). Рядом могут отображаться иконки, сообщающие о версии:



– актуальная (белая галочка на зеленом фоне),



– требует обновления (белый восклицательный знак на оранжевом фоне).



– кнопка позволяет обновить прошивку сетевого контроллера (см. раздел «Удаленное обновление прошивки сетевого контроллера»).

Ключ шифрования – последовательность до 12 буквенно-цифровых символов (цифры, буквы и специальные символы), определяющая ключ шифрования данных, передаваемых между сервером ACCO Server и сетевым контроллером. **Он должен совпадать с ключом, заданным в сетевом контроллере с помощью программы ACCO-NT Conf.** Сервер установит связь только с тем устройством, которое использует соответствующий ключ.



– щелкните по кнопке, чтобы отобразилось введенное значение.

Отказ в доступе при ошибке интегрирования – если включить эту опцию, то в случае отсутствия связи с сетевым контроллером получение доступа к интегрированной зоне контроля доступа невозможно до момента восстановления правильной связи. Если отменить выбор опции, то в случае отсутствия связи с сетевым контроллером, доступ к интегрированным зонам системы контроля доступа можно получить по тем же принципам, которые применяются без интеграции. Опция касается всех приемно-контрольных приборов, назначенных данному сетевому контроллеру ACCO-NT (см. раздел «Интеграция»).



Если опция «Отказ в доступе при ошибке интегрирования» выключена, и была потеряна связь между ACCO NET и системой безопасности, то зона доступа системы ACCO NET в режиме «Охрана», перейдет в режим «Зона доступа заблокирована». Благодаря этому можно получить доступ к отдельным точкам прохода системы ACCO NET. Когда пользователю предоставляется доступ к определенной зоне доступа, в зоне восстанавливается «Дежурный режим». После восстановления связи между системами, состояние зоны доступа снова изменится на «Охрана».

Лицензия – номер лицензии, назначенной сетевому контроллеру, или сообщение, сообщающее о состоянии лицензии.

После ввода какого-либо изменения отобразятся кнопки:



– щелкните, чтобы отменить введенные изменения.



– щелкните, чтобы подтвердить введенные изменения.

4.2.3.4 Удаленное обновление прошивки сетевого контроллера



После обновления прошивки ACCO-NT рекомендуется обновить прошивку всех модулей контроля доступа, подключенных к этому сетевому контроллеру (см. раздел «Удаленное обновление прошивки модуля контроля доступа»).

1. Если в поле «Версия», рядом с текущей версии прошивки прибора, отображается иконка , щелкните по кнопке .
2. В открывшемся окне отобразится информация о текущей версии прошивки устройства, а также информация о новой доступной версии (см. рис. 12).
3. Щелкните по кнопке «Обновление».
4. Окно обновления прошивки сетевого контроллера.
5. По завершении обновления отобразится соответствующее сообщение.
6. Щелкните по кнопке «ОК» и закройте окно «Версия микропрограммы».

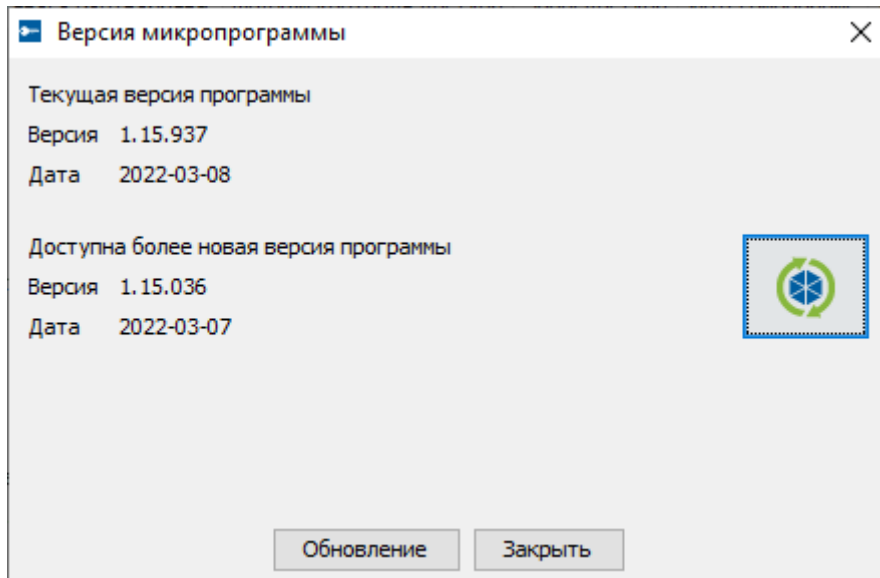


Рис. 12. Окно обновления прошивки сетевого контроллера.

4.2.3.5 Удаление сетевого контроллера

1. В списке объектов и сетевых контроллеров выделите сетевой контроллер для удаления.
2. Щелкните мышью по кнопке .
3. Когда отобразится вопрос, удалить ли сетевой контроллер, щелкните по «Да». Если удаляемый сетевой контроллер был назначен объекту, он будет перенесен в список сетевых контроллеров без назначения. Если удаляемый сетевой контроллер не был назначен объекту (находился в списке сетевых контроллеров без назначения), он будет удален из системы.
4. Сохраните введенные изменения.

4.2.4 Модули контроля доступа

Описание кнопок



- щелкните, чтобы добавить модуль.



- щелкните, чтобы удалить из списка модулей выбранный модуль (см. раздел «Удаление модуля контроля доступа»).



- щелкните, чтобы запустить процедуру идентификации модулей, подключенных к сетевому контроллеру. По завершении отобразится окно «Результаты» с информацией об идентификации модулей контроля доступа (см. раздел «Идентификация модулей контроля доступа в системе»). Кнопка доступна, если сетевой контроллер, к которому подключены модули контроля доступа, в состоянии «Сетевой контроллер ОК» (состояние отображается в скобках рядом с названием сетевого контроллера, в списке объектов и сетевых контроллеров) и введенные изменения сохранены.



- щелкните, чтобы запустить процедуру обновления прошивки выбранного модуля / модулей. Кнопка доступна, если нет изменений для сохранения (см. раздел «Удаленное обновление прошивки модуля контроля доступа»).

Под кнопками отображается количество сетевых контроллеров. После подведения указателя мыши к числу отобразится информация о том, сколько модулей контроля доступа подключено к первой и ко второй шине RS-485 данного ACCO-NT.

4.2.4.1 Идентификация модулей контроля доступа в системе

Каждый модуль контроля доступа должен быть идентифицирован, чтобы сетевой контроллер ACCO-NT был в состоянии установить с ним связь. Это позволит загрузить и сохранить его данные.

1. В списке объектов и сетевых контроллеров выделите сетевой контроллер, к которому подключены модули.

2. Перейдите к закладке «Модули контроля доступа» и нажмите кнопку .

3. В открывшемся окне отобразится информация о прогрессе процесса идентификации (процедуру можно прервать с помощью кнопки «Загрузить результаты»).

4. Откроется окно «Результаты» (см. раздел «Окно «Результаты»»). Рядом с новыми модулями контроля доступа отобразится состояние «Новый».

5. Щелкните по кнопке «Подтвердить».

6. Откроется окно с вопросом, сохранить ли настройки. Щелкните по «Да».



Функцию идентификации следует каждый раз запускать заново, если к какой-либо из шин будет подключено новое устройство, или будет изменен адрес в подключенном устройстве.



Отключение идентифицированного устройства от шины связи вызовет:

- *формирование события, сообщающего о неисправности сетевого контроллера типа «Начало неисправности. Модуль контроля доступа отсутствует. Адрес устройства...»,*
- *изменение цвета шрифта в списке модулей контроля доступа (см. раздел «Таблица со списком модулей контроля доступа»).*

Пользователи могут получить доступ к разделу сразу после регистрации модуля контроля доступа, контролирующего точку прохода в зоне доступа.

4.2.4.2 Добавление модуля перед его подключением к системе

1. В списке объектов и сетевых контроллеров выделите сетевой контроллер для добавления модуля контроллера доступа.

2. Щелкните по кнопке .
3. В открывшемся окне выберите адрес модуля и тип модуля, а затем щелкните по «Добавить».
4. Настройте модуль и сохраните настройки.
5. После подключения модуля контроля доступа к сетевому контроллеру (подключенному к сети Ethernet), щелкните по кнопке .
6. В открывшемся окне отобразится информация о прогрессе процесса идентификации (процедуру можно прервать с помощью кнопки «Загрузить результаты»).
7. Откроется окно «Результаты» (см. раздел «Окно «Результаты»»). Рядом с модулем контроля доступа отобразится состояние «Измененные данные».
8. Щелкните по кнопке «Подтвердить».
9. Откроется окно с вопросом, сохранить ли настройки. Щелкните по «Да».

4.2.4.3 Окно «Результаты»

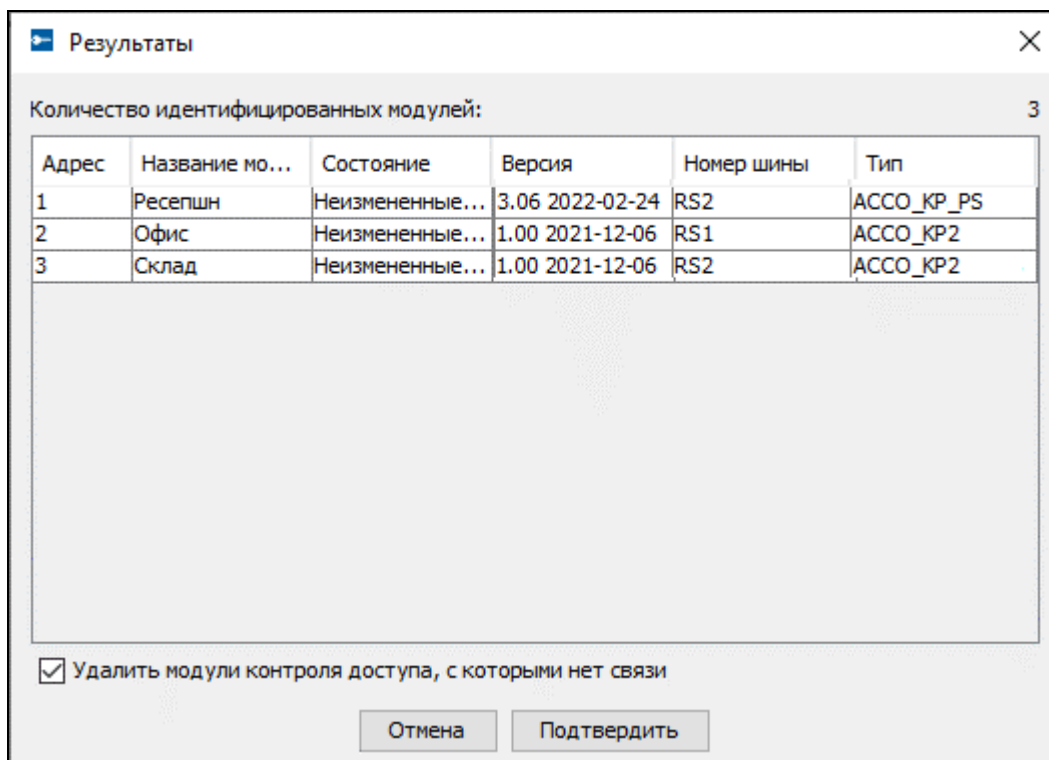


Рис. 13. Окно «Результаты», которое отображается после того, как завершена процедура идентификации модулей контроля доступа.

Число идентифицированных модулей контроля доступа – количество обнаруженных и идентифицированных модулей контроля доступа.

Адрес – адрес, установленный в модуле контроля доступа.

Название модуля – название модуля контроля доступа.

Состояние – в поле может отображаться следующая информация:

Неизмененные данные – модуль, данные которого совпадают с данными в программе.

Новый – модуль, добавленный в систему.

Измененные данные – модуль, данные которого не совпадают с данными в программе.

Нет связи – модуль, который раньше был в системе, и с которым во время процедуры идентификации сетевой контроллер не установил связь.

Версия – версия прошивки модуля контроля доступа (номер версии и дата сборки).

Номер шины – номер шины RS-485, к которой подключен идентифицированный модуль контроля доступа.

Тип – модель модуля контроля доступа.

Удалить модули контроля доступа, с которыми нет связи – если опция включена, то модули контроля доступа, с которыми не удалось установить связь, будут удалены после нажатия кнопки «Подтвердить». Если опция выключена, то после нажатия на кнопку «Подтвердить» модули контроля доступа не будут удалены.

Отмена – кнопка позволяет отменить процедуру идентификации.

Подтвердить – кнопка позволяет подтвердить данные, считанные во время идентификации.

4.2.4.4 Таблица со списком модулей контроля доступа

Адрес – внешний адрес модуля.


Название – индивидуальное название модуля контроля доступа (до 32 символов). Названия модулей контроля доступа могут быть напечатаны следующими цветами:


серым – модуль контроля доступа добавлен, но еще не сохранен;

красным – модуль контроля доступа сохранен; нет связи с модулем контроля доступа;


черным – модуль контроля доступа сохранен; связь ОК.

Состояние – информация о состоянии модуля контроля доступа. Отдельные иконки отображают следующие состояния:

 – тревога / неисправность (белый восклицательный знак на красном фоне),

 – память тревоги / неисправности (белый восклицательный знак на сером фоне),

 – все ОК (белый символ на зеленом фоне),

 – отсутствие связи с сетевым контроллером (белый вопросительный знак на сером фоне).

По щелчку на иконке отобразится закладка «Состояние».

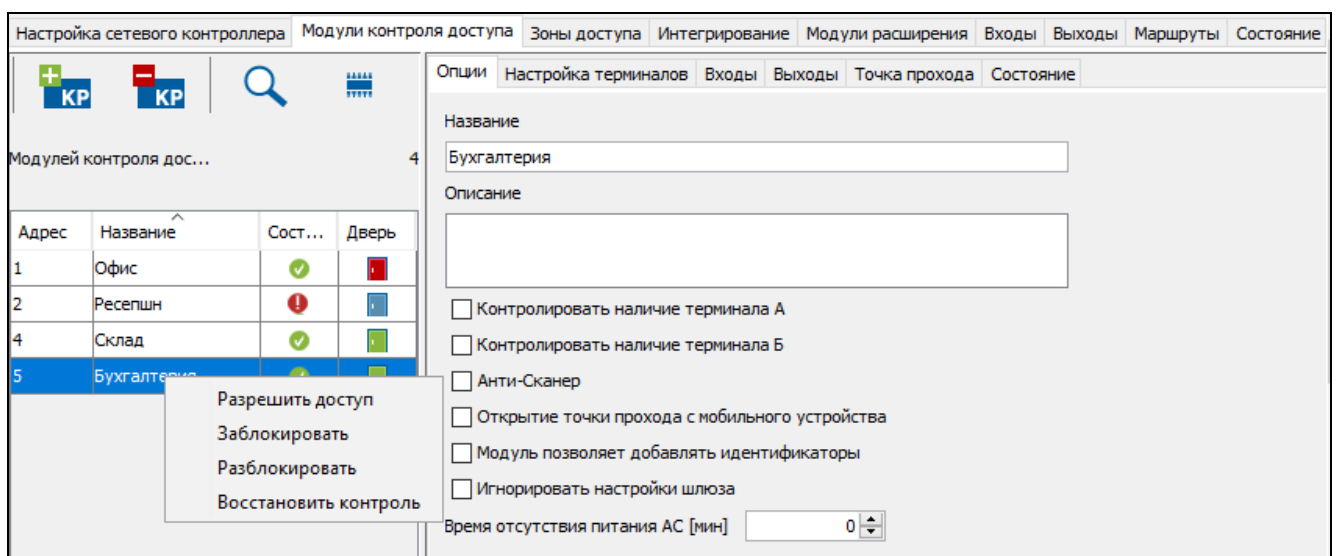


Рис. 14. Список модулей контроля доступа в закладке «Модули контроля доступа».

Дверь – информация о состоянии точки прохода и двери, контролируемой модулем контроля доступа. Отдельные иконки отображают следующие состояния:



– точка прохода заблокирована (закрытая красная дверь),



– точка прохода заблокирована, и дверь открыта (приоткрытая красная дверь),



– тревога – блокировка точки прохода (красный колокольчик и закрытая красная дверь),



– тревога – блокировка точки прохода и дверь открыта (красный колокольчик и приоткрытая красная дверь),



– дежурный режим (точка прохода контролируется) и дверь закрыта (закрытая зеленая дверь),



– дежурный режим (точка прохода контролируется) и дверь открыта (приоткрытая зеленая дверь),



– точка прохода разблокирована (закрытая синяя дверь),



– точка прохода разблокирована, и дверь открыта (приоткрытая синяя дверь),



– пожар – разблокировка точки прохода (красный огонек и закрытая синяя дверь),



– пожар – разблокировка точки прохода и дверь открыта (красный огонь и приоткрытая синяя дверь).

После выделения выбранного модуля контроля доступа в списке и щелчка по нему правой клавишей мыши отобразится выпадающее меню:

Разрешить доступ – после выбора функции точка прохода, контролируемая выбранным модулем контроля доступа, откроется на время, заданное в поле «Время на вход» в закладке «Точка прохода».

Заблокировать – после выбора функции точки прохода будет постоянно перекрыта. Точка прохода будет заблокирована до момента изменения ее состояния пользователем с полномочием «Переключение» (если раньше не появится событие, которое другим образом изменит состояние точки прохода).

Разблокировать – после выбора функции точки прохода будет постоянно перекрыта. Точка прохода будет заблокирована до момента изменения ее состояния пользователем с полномочием «Переключение» (если раньше не появится событие, которое другим образом изменит состояние точки прохода).

Восстановить контроль – после выбора функции будет включен дежурный режим, то есть контроль точки прохода будет восстановлен.

4.2.4.5 Настройка модуля контроля доступа

Щелкните по выбранному модулю в списке модулей контроля доступа, чтобы настроить его. Параметры модуля отобразятся в закладках в окне рядом.

Закладка «Опции»

Название – индивидуальное название модуля контроля доступа (до 32 символов).

Описание – в поле можно дополнительно добавить описание модуля контроля доступа.

Контролировать наличие терминала А / Б – если опция включена, модуль проверяет наличие клавиатур и считывателей карт, работающих в качестве терминала А или Б. В первую очередь проверяется наличие клавиатур, а потом наличие считывателей карт. Если опция выключена, модуль не будет сообщать, что терминал отсутствует (не будет вызвана тревога, не будет сохранено событие, и не будет активирован выход «Отсутствие терминала»).

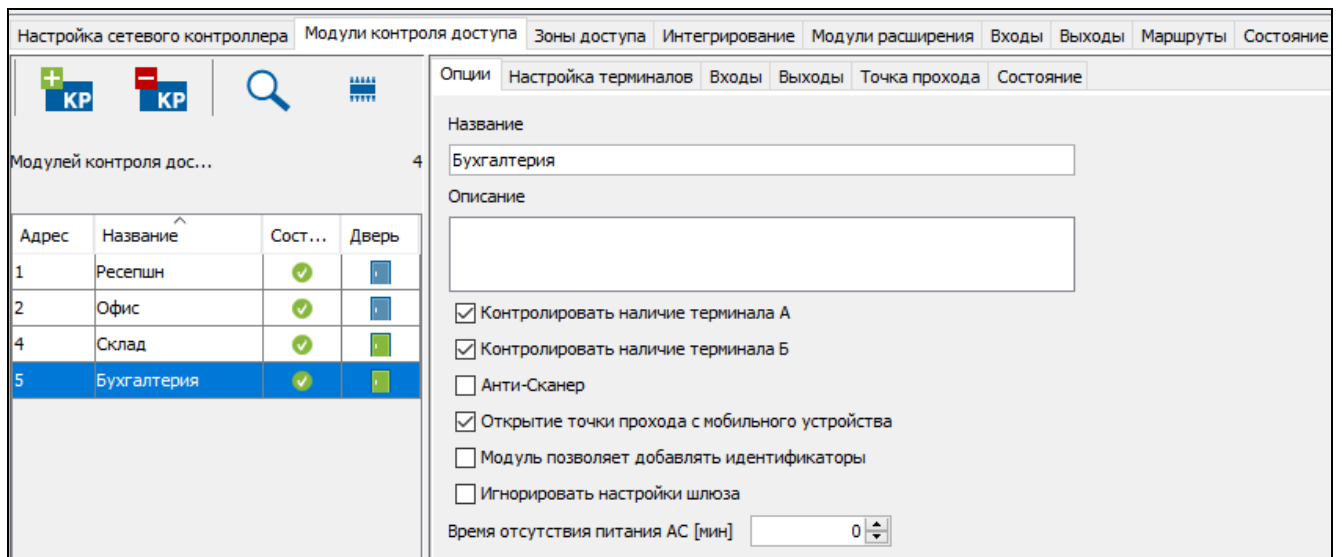


Рис. 15. Закладка «Опции».



Модуль не в состоянии проверять наличие считывателей ключей DALLAS iButton. В случае подключения этого типа считывателя рекомендуется не включать опцию «Контролировать наличие терминала А / Б».

Анти-Сканер – если опция включена, 5 попыток получить доступ с помощью неизвестной карты, ключа или кода за 3 минуты вызовут блокировку терминалов приблизительно на 5 минут.

Открытие точки прохода с мобильного устройства – после включения опции пользователи имеют возможность получить доступ с помощью мобильных устройств.

Модуль позволяет добавлять идентификаторы – если опция включена, модуль контроля доступа будет отображаться во время добавления пользователю карты / проверки карты пользователя в приложении ACCO Web. Если эта опция будет выключена, модуль контроля доступа не будет отображаться (не касается модулей, к которым подключены считыватели, поддерживающие форматы DALLAS, EM Marin и Wiegand 40/42/56 – они отображаются всегда).



Карта, добавленная с помощью считывателя, поддерживающего определенный тип формата Wiegand, будет считываться только терминалами, поддерживающими этот тип формата, и терминалами, считывающими более короткие номера карт (карты с меньшей битностью). Например: если карта будет добавлена с помощью считывателя, поддерживающего формат Wiegand 34, то она будет считываться терминалами, поддерживающими форматы Wiegand 34/32/26. Поэтому рекомендуется добавлять карты на терминалах, считывающих самые длинные номера карт (карты с наибольшей битностью). Добавленная таким образом карта будет поддерживаться всеми считывателями в системе, в том числе теми, которые считывают более короткие номера карт (карты с меньшей битностью).

Игнорировать настройки шлюза – если опция включена, точка прохода в зоне доступа, выполняющей функцию шлюза, работает независимо от настроек шлюза (см. описание опции «Шлюз»).

Время отсутствия питания АС [мин] – функция относится к модулям ACCO-KP-PS, ACCO-KPWG-PS и ACCO-KP2. Она позволяет определить время, в течение которого модуль может быть лишен сетевого питания. По истечении этого времени будет сообщена неисправность. Время программируется в минутах и может составлять

максимально 255 минут. Ввод значения 0 означает, что неисправность питания АС не будет сообщаться.

После ввода какого-либо изменения отобразятся кнопки:



– щелкните, чтобы отменить введенные изменения.



– щелкните, чтобы подтвердить введенные изменения.

Закладка «Настройка терминалов»

Закладка «Терминал А / Б»

Формат передачи А / Б – функция позволяет определить формат передачи для терминалов, поддерживаемых модулем контроля доступа.



В случае формата WIEGAND двукратное прикладывание к считывателю одной и той же карты (идентификатора) распознается как удержание карты. Некоторые считыватели могут не поддерживать эту функцию, поэтому стоит проверить корректность их работы.

Рекомендуется выбрать формат EM Marin для работы считывателей бесконтактных карт CZ-EMM3 и CZ-EMM4 компании SATEL в системе ACCO NET.

Подсветка терминала А / Б – функция, определяющая способ работы подсветки клавиш и дисплея в клавиатурах, подключенных к модулю. Доступны следующие возможности:

- подсветка выключена;
- автоматическая подсветка включается после нажатия любой клавиши или после поднесения карты;
- постоянная подсветка.

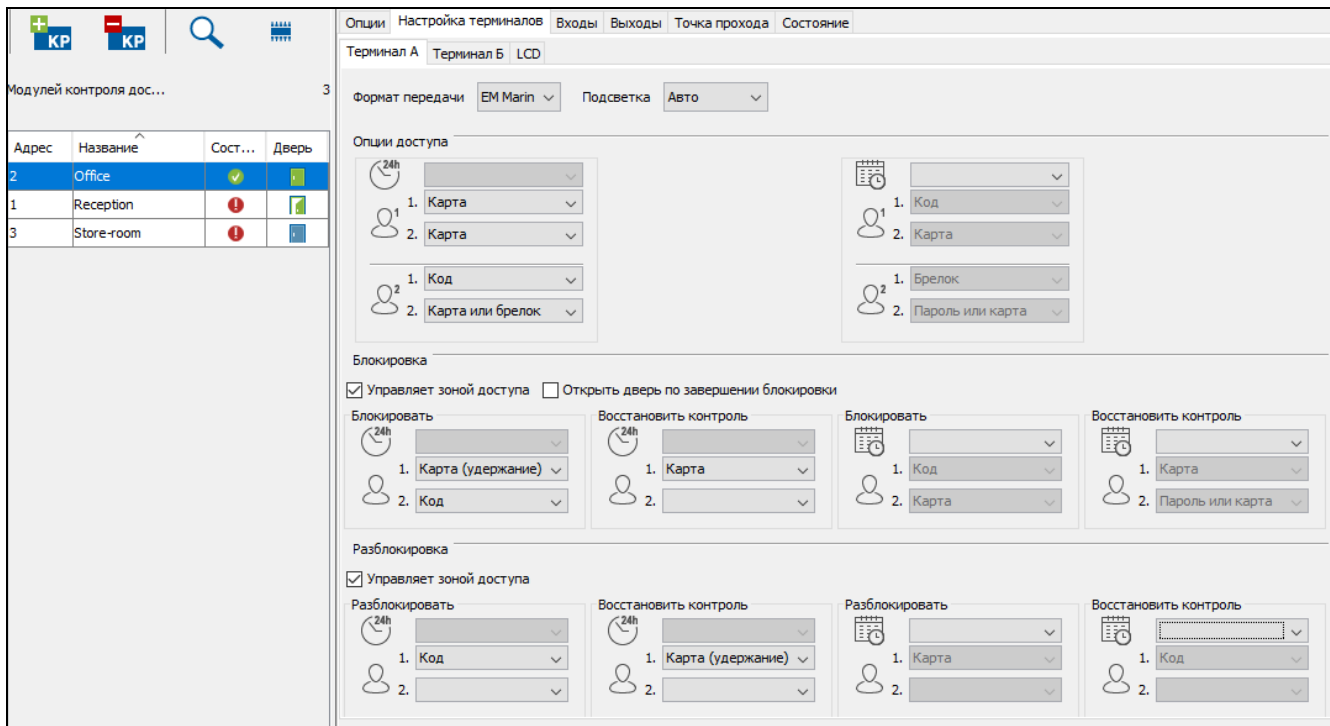


Рис. 16. Закладка «Терминал А».

Опции доступа



Если пользователю должен быть предоставлен доступ к данной зоне доступа, то в приложении ACCO Web у него должна быть активна опция «Уполномоченный на доступ», и ему должен быть назначен соответствующий график доступа (→«Пользователи» →«Список» →[название пользователя] →закладка «Зоны доступа»).

Если доступ должен предоставляться на основании двух идентификаторов:

- после использования 1-го идентификатора устройства, выполняющие функцию терминалов, сообщат о необходимости использовать 2-й идентификатор (ЖКИ-клавиатура отобразит сообщение на дисплее, клавиатуры и считыватели бесконтактных карт подадут дополнительный звуковой сигнал – 3 коротких звука),
- у пользователя есть 30 секунд, чтобы применить 2-й идентификатор.

Конфигурация опций доступа, представленная в настоящем разделе, возможна для сетевого контроллера ACCO-NT с версией прошивки 1.14.xxx или более новой. Для сетевого контроллера с более ранней версией прошивки уже существующий тип идентификатора, определяющий способ доступа, будет назначен первому пользователю для терминала А по следующим правилам:

- карта = 1-й идентификатор: карта, 2-й идентификатор: не определен,
- код = 1-й идентификатор: код, 2-й идентификатор: не определен,
- карта и код = 1-й идентификатор: код или карта, 2-й идентификатор: код или карта,
- карта или код = 1-й идентификатор: код или карта, 2-й идентификатор: не определен.

Конфигурационные настройки для терминала Б будут недоступны.

В случае использования сетевого контроллера ACCO-NT с версией прошивки 1.14.xxx или более новой, после обновления системы ACCO NET до версии 1.7, уже существующие настройки опций доступа будут назначены по вышеописанным правилам первому пользователю как действующие круглосуточно для обоих терминалов данного модуля контроля доступа.

Доступ можно получать или подтверждать с помощью:

- кода,
- карты,
- радиобрелока,
- кода или карты,
- карты или радиобрелока,
- кода или радиобрелока,
- кода, карты или радиобрелока.



– правила доступа, действующие круглосуточно



Если не будут определены правила доступа, действующие круглосуточно, то доступ будет разрешаться пользователям по правилам, действующим в период времени, определенный выбранным графиком доступа.



– правила доступа пользователя:

1. – первый идентификатор,
2. – второй идентификатор (если он не будет выбран, то пользователь получит доступ с помощью первого идентификатора).



– правила подтверждения доступа вторым пользователем (настраивайте, только если получение доступа должно зависеть от второго пользователя):

1. – первый идентификатор,
2. – второй идентификатор (если он не будет выбран, то для подтверждения доступа достаточно будет первого идентификатора).



У пользователя, подтверждающего доступ, в приложении ACCO Web должна быть включена опция «Подтверждение» (→«Пользователи» →«Список» →[название пользователя] →закладка «Зоны доступа»).



– правила доступа, действующие в период времени, определенный графиком доступа



Если не будут определены правила доступа, действующие в период времени, определенный графиком доступа, то доступ будет предоставляться по правилам, действующим круглосуточно.



– щелкните по полю, если в период времени, определенный графиком доступа, доступ должен разрешаться пользователям по правилам, отличающимся от действующих круглосуточно. Отобразится список созданных в приложении ACCO Web графиков доступа. Щелкните по одному из них.



– правила доступа пользователя:

1. – первый идентификатор,
2. – второй идентификатор (если он не будет выбран, то пользователь получит доступ с помощью первого идентификатора).



– правила подтверждения доступа вторым пользователем (настраивайте, только если получение доступа должно зависеть от второго пользователя):

1. – первый идентификатор,
2. – второй идентификатор (если он не будет выбран, то для подтверждения доступа достаточно будет первого идентификатора).



У пользователя, подтверждающего доступ, в приложении ACCO Web должна быть включена опция «Подтверждение» (→«Пользователи» →«Список» →[название пользователя] →закладка «Зоны доступа»).

Опции управления – Блокировка



Опции управления правильно действуют только в том случае, если один из входов модуля контролирует состояние двери (запрограммирован как «Датчик открытия двери»).

Если пользователь должен управлять зоной доступа, у него должен быть доступ к данной зоне и право переключать ее состояние (активны опции «Уполномоченный на доступ» и «Переключение» в приложении ACCO Web (→«Пользователи» →«Список» →[название пользователя] →закладка «Зоны доступа»), и должен быть назначен график доступа.

Если управление зоной доступа должно осуществляться с помощью двух идентификаторов:

- после использования 1-го идентификатора устройства, выполняющие функцию терминалов, сообщают о необходимости использовать 2-й идентификатор (ЖКИ-клавиатура отобразит сообщение на дисплее, клавиатуры и считыватели бесконтактных карт подадут дополнительный звуковой сигнал – 3 коротких звука),*
- у пользователя есть 30 секунд, чтобы применить 2-й идентификатор.*

Следует определить идентификаторы, предназначенные как для блокировки зоны доступа, так и для восстановления контроля в ней.

Если:

- первые идентификаторы, предназначенные для блокировки зоны доступа, такие же, как первые идентификаторы, предназначенные для разблокировки зоны доступа и/или*
- первые идентификаторы, предназначенные для восстановления контроля в заблокированной зоне доступа, такие же, как первые идентификаторы для восстановления контроля в разблокированной зоне доступа,*

то от состояния двери зависит, как изменится состояние зоны доступа. Если дверь закрыта, то после использования идентификатора зона доступа будет заблокирована, или будет восстановлен контроль в заблокированной зоне доступа. Если дверь открыта, то после использования идентификатора зона доступа будет заблокирована, или будет восстановлен контроль в разблокированной зоне доступа.

Конфигурация опций блокировки, представленная в настоящем разделе, возможна для сетевого контроллера ACCO-NT с версией прошивки 1.14.xxx или выше. Для сетевых контроллеров с более ранней версией прошивки блокировка точек прохода и зон доступа, а также восстановление их контроля будет возможно по правилам, действовавшим в системе версии 1.5.

В случае использования сетевого контроллера ACCO-NT с версией прошивки 1.14.xxx или более новой, после обновления системы ACCO NET до версии 1.7, уже существующие настройки опций управления зонами доступа будут использоваться также в новой системе. Если опция «Блокировать зону доступа после удержания карты» ранее была включена, то после обновления системы для всех терминалов входа в этой зоне доступа будет включена опция «Управляет зоной доступа».

Зону доступа можно блокировать или восстанавливать в ней контроль с помощью:

- кода,
- карты,
- карты (удержание),
- кода или карты,
- карты (поднесение или удержание),
- кода или карты (удержание),
- кода или карты (поднесение или удержание).

Управляет зоной доступа – после включения опции можно блокировать зону доступа и восстанавливать в ней контроль с помощью терминала входа в этой зоне доступа. В случае интеграции блокировка зоны СКУД с использованием терминала входа будет вызывать постановку на охрану интегрированного раздела (группы) системы охранной сигнализации.

Открыть дверь по завершении блокировки – если опция включена, и пользователь восстановит контроль точки прохода или зоны доступа (с включенной опцией «Управляет зоной доступа»), то он получит доступ к точке прохода.



– правила блокировки зоны доступа, действующие круглосуточно



Если не будут определены правила блокировки зоны доступа, действующие круглосуточно, то зоны доступа можно будет блокировать по правилам, действующим в период времени, определенный выбранным графиком доступа.



– правила блокировки зоны доступа пользователем:

1. – первый идентификатор,
2. – второй идентификатор (если он не будет выбран, то пользователь заблокирует зону доступа с помощью первого идентификатора).



– правила восстановления контроля в заблокированной зоне доступа, действующие круглосуточно



Если не будут определены правила восстановления контроля в заблокированной зоне доступа, действующие круглосуточно, то контроль в зоне доступа можно будет восстановить по правилам, действующим в период времени, определенный выбранным графиком доступа.



– правила восстановления пользователем контроля в заблокированной зоне доступа:

1. – первый идентификатор,
2. – второй идентификатор (если он не будет выбран, то пользователь заблокирует зону доступа с помощью первого идентификатора).



– правила блокировки зоны доступа в период времени, определенный графиком доступа



Если не будут определены правила блокировки зон доступа, действующие в период времени, определенный графиком доступа, то блокировка зон доступа будет возможна по правилам, действующим круглосуточно.



– щелкните по полю, если в период времени, определенный графиком доступа, зона доступа должна блокироваться по правилам, отличающимся от действующих круглосуточно. Отобразится список созданных в приложении ACCO Web графиков доступа. Щелкните по одному из них.



– правила блокировки зоны доступа пользователем:

1. – первый идентификатор,
2. – второй идентификатор (если он не будет выбран, то пользователь заблокирует зону доступа с помощью первого идентификатора).



– правила восстановления контроля в заблокированной зоне доступа в период времени, определенный графиком доступа



Если не будут определены правила восстановления контроля в заблокированной зоне доступа, действующие круглосуточно, то контроль в зоне доступа можно будет восстановить по правилам, действующим в период времени, определенный выбранным графиком доступа.



– щелкните по полю, если в период времени, определенный графиком доступа, восстановление контроля в заблокированной зоне доступа должно происходить по правилам, отличающимся от действующих круглосуточно. Отобразится список созданных в приложении ACCO Web графиков доступа. Щелкните по одному из них.



– правила восстановления пользователем контроля в заблокированной зоне доступа:

1. – первый идентификатор,
2. – второй идентификатор (если он не будет выбран, то пользователь заблокирует зону доступа с помощью первого идентификатора).

Опции управления – Блокировка



Опции управления правильно действуют только в том случае, если один из входов модуля контролирует состояние двери (запрограммирован как «Датчик открытия двери»).

Если пользователь должен управлять зоной доступа, у него должен быть доступ к данной зоне и право переключать ее состояние (активны опции «Уполномоченный на доступ» и «Переключение» в приложении ACCO Web (→«Пользователи» →«Список» →[название пользователя] →закладка «Зоны доступа»), и должен быть назначен график доступа.

Если управление зоной доступа должно осуществляться с помощью двух идентификаторов:

- после использования 1-го идентификатора устройства, выполняющие функцию терминалов, сообщают о необходимости использовать 2-й идентификатор (ЖКИ-клавиатура отобразит сообщение на дисплее, клавиатуры и считыватели бесконтактных карт подадут дополнительный звуковой сигнал – 3 коротких звука),
- у пользователя есть 30 секунд, чтобы применить 2-й идентификатор.

Следует определить идентификаторы, предназначенные как для блокировки зоны доступа, так и для восстановления контроля в ней.

Если:

- первые идентификаторы, предназначенные для блокировки зоны доступа, такие же, как первые идентификаторы, предназначенные для разблокировки зоны доступа и/или
- первые идентификаторы, предназначенные для восстановления контроля в разблокированной зоне доступа, такие же, как первые идентификаторы для восстановления контроля в заблокированной зоне доступа,

то от состояния двери зависит, как изменится состояние зоны доступа. Если дверь открыта, то после использования идентификатора зона доступа будет заблокирована, или будет восстановлен контроль в разблокированной зоне доступа. Если дверь закрыта, то после использования идентификатора зона доступа будет заблокирована, или будет восстановлен контроль в заблокированной зоне доступа.

Конфигурация опций блокировки, представленная в настоящем разделе, возможна для сетевого контроллера ACCO-NT с версией прошивки 1.14.xxx или выше. Для сетевых контроллеров с более ранней версией прошивки

блокировка точек прохода и зон доступа, а также восстановление их контроля будет возможно по правилам, действовавшим в системе версии 1.5.

В случае использования сетевого контроллера ACCO-NT с версией прошивки 1.14.xxx или более новой, после обновления системы ACCO NET до версии 1.7, уже существующие настройки опций управления зонами доступа будут использоваться также в новой системе. Если опция «Блокировать зону доступа после удержания карты» ранее была включена, то после обновления системы для всех терминалов входа в этой зоне доступа будет включена опция «Управляет зоной доступа».

Зону доступа можно разблокировать или восстановить в ней контроль с помощью:

- кода,
- карты,
- карты (удержание),
- кода или карты,
- карты (поднесение или удержание),
- кода или карты (удержание),
- кода или карты (поднесение или удержание).

Управляет зоной доступа – после включения опции можно разблокировать зону доступа и восстановить в ней контроль с помощью терминала входа в эту зону доступа.



– правила блокировки зоны доступа, действующие круглосуточно



Если не будут определены правила разблокировки зоны доступа, действующие круглосуточно, то контроль в зоне доступа можно будет восстанавливать по правилам, действующим в период времени, определенный выбранным графиком доступа.



– правила блокировки зоны доступа пользователем:

1. – первый идентификатор,
2. – второй идентификатор (если он не будет выбран, то пользователь заблокирует зону доступа с помощью первого идентификатора).



– правила восстановления контроля в заблокированной зоне доступа, действующие круглосуточно



Если не будут определены правила восстановления контроля в заблокированной зоне доступа, действующие круглосуточно, то контроль в зоне доступа можно будет восстановить по правилам, действующим в период времени, определенный выбранным графиком доступа.



– правила восстановления пользователем контроля в разблокированной зоне доступа:

1. – первый идентификатор,
2. – второй идентификатор (если он не будет выбран, пользователь восстановит контроль в зоне доступа с помощью первого идентификатора).



– правила блокировки зоны доступа в период времени, определенный графиком доступа



Если не будут определены правила восстановления контроля в заблокированной зоне доступа, действующие в период времени, определенный выбранным графиком доступа, контроль в зоне доступа можно будет восстановить по правилам, действующим круглосуточно.



– щелкните по полю, если в период времени, определенный графиком доступа, зона доступа должна блокироваться по правилам, отличающимся от действующих круглосуточно. Отобразится список созданных в приложении ACCO Web графиков доступа. Щелкните по одному из них.



– правила блокировки зоны доступа пользователем:

1. – первый идентификатор,
2. – второй идентификатор (если он не будет выбран, то пользователь заблокирует зону доступа с помощью первого идентификатора).



– правила восстановления контроля в разблокированной зоне доступа в период времени, определенный графиком доступа



Если не будут определены правила восстановления контроля в разблокированной зоне доступа, действующие в период времени, определенный выбранным графиком доступа, контроль в зоне доступа можно будет восстановить по правилам, действующим круглосуточно.



– щелкните по полю, если в период времени, определенный графиком доступа, восстановление контроля в разблокированной зоне доступа должно происходить по правилам, отличающимся от действующих круглосуточно. Отобразится список созданных в приложении ACCO Web графиков доступа. Щелкните по одному из них.



– правила восстановления пользователем контроля в разблокированной зоне доступа:

1. – первый идентификатор,
2. – второй идентификатор (если он не будет выбран, пользователь восстановит контроль в зоне доступа с помощью первого идентификатора).

Примеры

Пример определения опций доступа

Выбранный график доступа дает пользователям право доступа с 8:00 до 16:00. В этот период времени пользователь получит доступ с помощью двух идентификаторов: 1-го – кода и 2-го – карты. Второй пользователь подтвердит доступ также с помощью двух идентификаторов: 1. – радиобрелка и 2. – кода или карты. В остальное время (до 8:00 и с 16:00, когда не действует выбранный график) пользователь получит доступ с помощью двух идентификаторов: 1. – карты и 2. – карты, а второй пользователь подтвердит доступ также с помощью двух идентификаторов: 1. – кода и 2. – карты или радиобрелка.

В период времени с 8:00 до 16:00 пользователь получит доступ, если:

- он введет код и подтвердит его кнопкой # или «ОК», после чего поднесет к считывателю карту,
- пользователь, имеющий право подтверждения, использует радиобрелок, после чего введет код и подтвердит его кнопкой # или «ОК», либо поднесет к считывателю карту.

А в период времени с 16:00 до 8:00 пользователь получит доступ, если:

- поднесет карты к считывателю по очереди,
- пользователь, имеющий право подтверждения, введет код и подтвердит его кнопкой # или «ОК», после чего поднесет к считывателю карту или использует радиобрелок.

Пример определения опций блокировки зоны доступа и восстановления контроля в заблокированной зоне доступа

Выбранный график доступа позволяет пользователям управлять зоной доступа в период времени с 6:00 до 18:00. В это время пользователь заблокирует зону доступа с помощью двух идентификаторов: 1. – кода и 2. – карты, и восстановит контроль в заблокированной зоне доступа с помощью: 1. – карты и 2. – кода или карты. В остальное время (до 6:00 и с 18:00, когда не действует выбранный график) он заблокирует зону доступа с помощью двух идентификаторов: 1. – карты (удержание) и 2. – кода, и восстановит контроль в заблокированной зоне доступа с помощью: 1. – карты.

В период времени с 6:00 до 18:00 пользователь заблокирует зону доступа, если введет код и подтвердит его кнопкой # или «ОК», после чего поднесет к считывателю карту. Он восстановит контроль в заблокированной зоне доступа, если поднесет к считывателю карту, после чего введет код и подтвердит его кнопкой # или «ОК», либо поднесет к считывателю карту.

А в интервал времени с 18:00 до 6:00 пользователь заблокирует зону доступа, если в течение около 3 секунд удержит у считывателя карту, после чего введет код и подтвердит его кнопкой # или «ОК». Он восстановит контроль в заблокированной зоне доступа, если поднесет к считывателю карту.

Пример определения опций разблокировки зоны доступа и восстановления контроля в разблокированной зоне доступа

Выбранный график доступа позволяет пользователям управлять зоной доступа в период времени с 10:00 до 14:00. В этот период времени пользователь разблокирует зону доступа с помощью одного идентификатора: 1. – карты, и восстановит контроль в разблокированной зоне с помощью: 1. – кода. В остальное время (до 10:00 и с 14:00, когда не действует выбранный график) он разблокирует зону доступа с помощью одного идентификатора: 1. – кода, и восстановит контроль в разблокированной зоне с помощью: 1. – карты (удержание).

В период времени с 10:00 до 14:00 пользователь разблокирует зону доступа, если поднесет к считывателю карту. Контроль в разблокированной зоне он восстановит, если введет код и подтвердит его кнопкой # или «ОК».

А в период времени с 14:00 до 10:00 пользователь разблокирует зону доступа, если введет код и подтвердит его кнопкой # или «ОК». Он восстановит контроль в разблокированной зоне доступа, если в течение около 3 секунд удержит у считывателя карту.

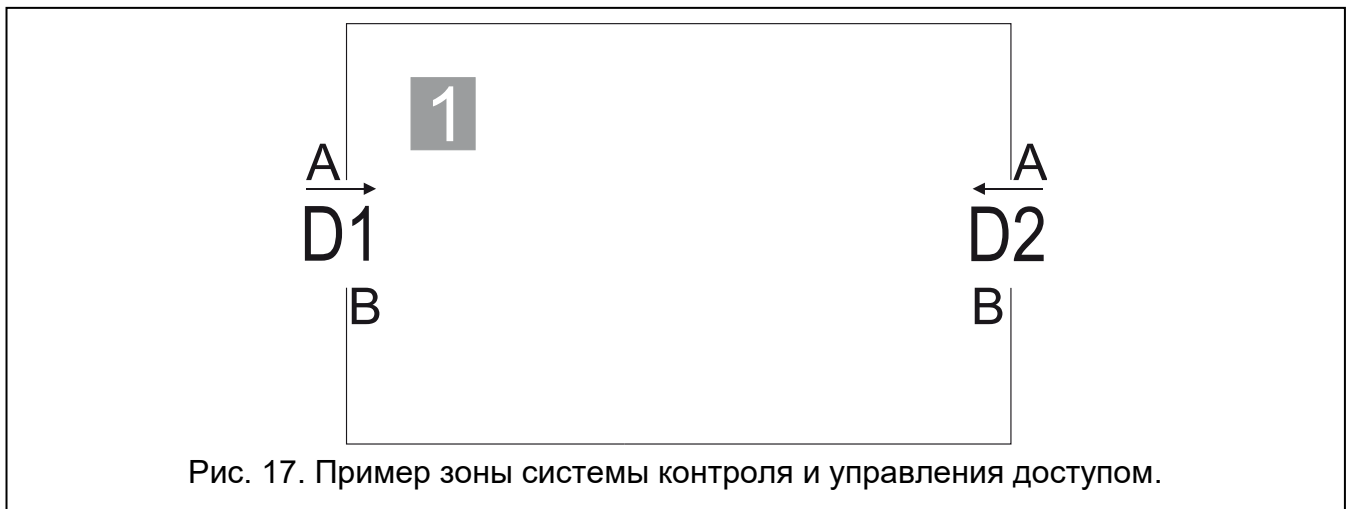
Пример управления зоной доступа с двумя точками прохода

Пояснения к рисунку 17:

1 (номер на сером фоне) – зона системы контроля и управления доступом.

D1 – модуль контроля доступа, назначенный зоне 1. Терминал А – это вход в зону 1, а терминал Б – выход из зоны 1.

D2 – модуль контроля доступа, назначенный зоне 1. Терминал А – это вход в зону 1, а терминал Б – выход из зоны 1.



БЛОКИРОВКА ЗОНЫ ДОСТУПА

Для блокировки зоны 1:

- если в зоне есть терминал входа, для которого включена опция «Управляет зоной доступа», используйте этот терминал.



Если Вы заблокируете таким образом зону контроля доступа, интегрированную с разделом (группой) системы охранной сигнализации, то поставите на охрану раздел системы охранной сигнализации.

- если в зоне нет терминала входа, для которого включена опция «Управляет зоной доступа» – заблокируйте все точки прохода.

РАЗБЛОКИРОВКА ЗОНЫ ДОСТУПА

Для разблокировки зоны 1:

- если в зоне есть терминал входа, для которого включена опция «Управляет зоной доступа», используйте этот терминал.
- если в зоне нет терминала входа, для которого включена опция «Управляет зоной доступа», разблокируйте все точки прохода.



Если зона интегрирована с разделом (группой) системы охранной сигнализации, поставленным на охрану, с помощью терминалов невозможно разблокировать ни зону, ни точки прохода.

ВОССТАНОВЛЕНИЕ КОНТРОЛЯ В ЗОНЕ ДОСТУПА

Для того, чтобы восстановить контроль в заблокированной или разблокированной зоне 1:

- если в зоне есть терминал входа, для которого включена опция «Управляет зоной доступа», используйте этот терминал.
- если в зоне нет терминала входа, для которого включена опция «Управляет зоной доступа», восстановите контроль для всех точек прохода.

Закладка «LCD»

Служебный проход – если опция включена, то после предоставления доступа отобразится сообщение «Служебный проход». Если вход / выход осуществляется по служебным делам, пользователь должен нажать клавишу ▲. Пока клавиша не нажата, сообщение будет отображаться на дисплее клавиатуры. В подробности события в таком случае добавляется соответствующая информация. Она полезна,

если регистрируемые модулем проходы пользователей должны использоваться для учета рабочего времени.



Функция не осуществляется, если состояние двери не контролируется, или если дверь открыта.

Показать название пользователя на клавиатуре – после включения опции на дисплее клавиатуры, с помощью которой получен доступ к точке прохода, отобразится название пользователя, который получил доступ.

Показать название пользователя на обеих клавиатурах – после включения опции на дисплее обеих клавиатур, подключенных к модулю контроля доступа, отобразится название пользователя, который получил доступ. Включение опции включает одновременно также опцию «Показать имя пользователя на клавиатуре».

Формат времени на ЖКИ – функция позволяет выбрать способ отображения времени и даты на дисплее клавиатуры.

После ввода какого-либо изменения отобразятся кнопки:



– щелкните, чтобы отменить введенные изменения.



– щелкните, чтобы подтвердить введенные изменения.

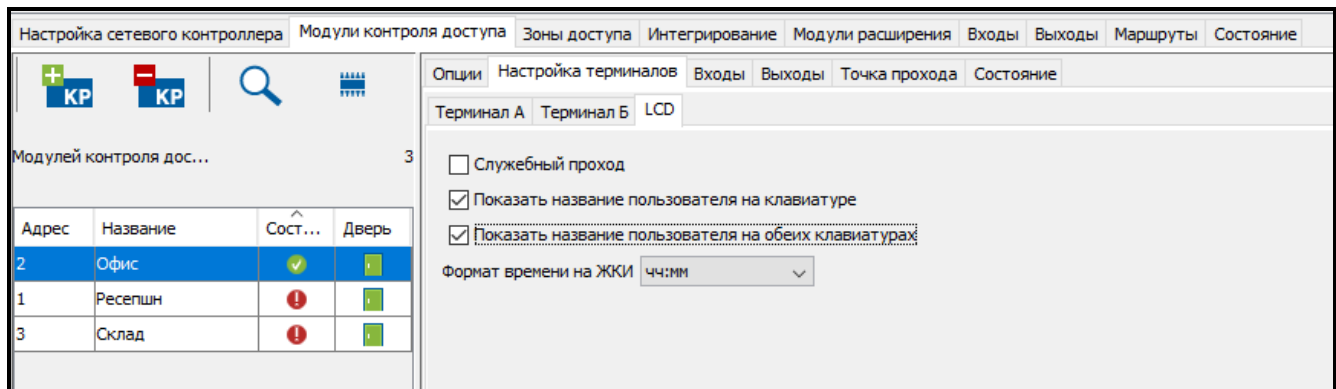


Рис. 18. Закладка «LCD».

Закладка «Входы»

Таблица со списком входов модуля контроля доступа

Номер – номер входа модуля контроля доступа.

Тип реакции (см. раздел «Типы реакции входов модуля контроля доступа»).

Тип – можно выбрать:

NO – вход поддерживает устройство с выходом типа NO (с нормально разомкнутыми контактами),

NC – вход поддерживает устройство с выходом типа NC (с нормально замкнутыми контактами).

Параметр доступен только для программируемых входов.

Чувствительность [мс] – время, в течение которого состояние входа должно быть измененным, чтобы этот факт был зарегистрирован. Это время можно запрограммировать в диапазоне от 10 мс до 2,55 с. Параметр доступен только для программируемых входов.

с полномочиём «Переключение». Время, в течение которого вход будет активен, не влияет на время блокировки точки прохода.

Сигнал звонка – включение выхода типа «Сигнал звонка».

Информация 1÷4 – формирование запрограммированного события. Его содержание можно определить в нижней таблице.

i События, запрограммированные для типа реакции «Информация 1÷4», не являются глобальными. Их следует определить для каждого модуля контроля доступа отдельно.

i В модуле ACCO-KP2 некоторым входам назначены постоянные конкретные типы реакции:

SIG1A – подключение терминала А: данные (0),

SIG2A – подключение терминала А: данные (1),

TMPA – проверка наличия терминала А,

ITMP – подключение тамперной цепи,

SIG1B – подключение терминала Б: данные (0),

SIG2B – подключение терминала Б: данные (1),

TMPB – проверка наличия терминала Б.

Закладка «Выходы»

Таблица со списком выходов модуля контроля доступа

Номер – номер выхода модуля контроля доступа.

Тип выхода (см. раздел «Типы выходов модуля контроля доступа»).

Время активности – если выход должен включаться на время, следует запрограммировать это время. По его истечении выход выключится. Можно задать значения от 1 до 120 секунд или минут. Параметр доступен только для программируемых выходов.

в мин/сек – выберите, должно ли время активности отсчитываться в секундах или минутах. Параметр доступен только для программируемых выходов.

Полярность – опция определяет, как действует выход. В случае обратной полярности в активном состоянии:

- выход отсоединяется от массы,
- клемма NO релейного выхода размыкается, а клемма NC замыкается.

Параметр доступен только для программируемых выходов.

Типы выходов модуля контроля доступа

Тип выхода можно выбрать после щелчка правой клавишей мыши по полю:

Не используется

Состояние двери – выход сообщает о текущем состоянии двери (если модуль контролирует состояние двери с помощью входа «Датчик открытия двери»). Активируется при открытии двери и остается активным до момента ее закрытия. Выход, запрограммированный как «Состояние двери», не может осуществлять другие функции.

Индикатор – после выбора типа рядом с таблицей отобразятся следующие функции, которые выход может реализовать:

Открытие двери – выход активируется на запрограммированное время после открытия двери (если модуль контролирует состояние двери с помощью входа «Датчик открытия двери»).

Сигнал звонка – включается на запрограммированное время после подачи сигнала на вход, запрограммированный как «Сигнал звонка».

Неисправность – после выбора типа рядом с таблицей отобразятся следующие функции, которые выход может реализовать:

Несанкционированный доступ – запускается на запрограммированное время после открытия двери без разрешения доступа, когда точка прохода закрыта (если модуль контролирует состояние двери с помощью входа «Датчик открытия двери»).

Длительное открытие двери – выход активируется на запрограммированное время, если дверь останется открытой по истечении «Максимального времени открытия двери», (если модуль контролирует состояние двери с помощью входа «Датчик открытия двери»).

Терминал отсутствует – выход активируется на запрограммированное время, если во время теста было обнаружено отсутствие терминала (клавиатуры или считывателя). Модуль контролирует наличие терминалов только при включении соответствующих опций («Контролировать наличие терминала А / Б»).

Попытка подбора идентификатора – выход включается на запрограммированное время, если система зарегистрировала 5 попыток получения доступа с помощью незарегистрированной в системе карты, ключа iButton или кода. Выход активируется независимо от включения опции «Анти-Сканер».

Неисправность питания АС – выход активируется в случае пропадания сетевого питания модуля ACCO-KP-PS / ACCO-KPWG-PS / ACCO-KP2 по истечении времени, запрограммированного как «Время отсутствия питания АС». Выход остается активным до момента восстановления сетевого питания. Выход остается активным до момента восстановления сетевого питания.

Разряженный аккумулятор – выход включится, если напряжение аккумулятора, подключенного к модулю ACCO-KP-PS / ACCO-KPWG-PS / ACCO-KP2 падает ниже 11 В на время дольше 12 минут (3 теста аккумулятора). Выход остается активным, пока напряжение аккумулятора не превысит 11 В на более, чем 12 минут (3 теста аккумулятора).

Саботаж – выход включается, если будет нарушен вход ITMP.

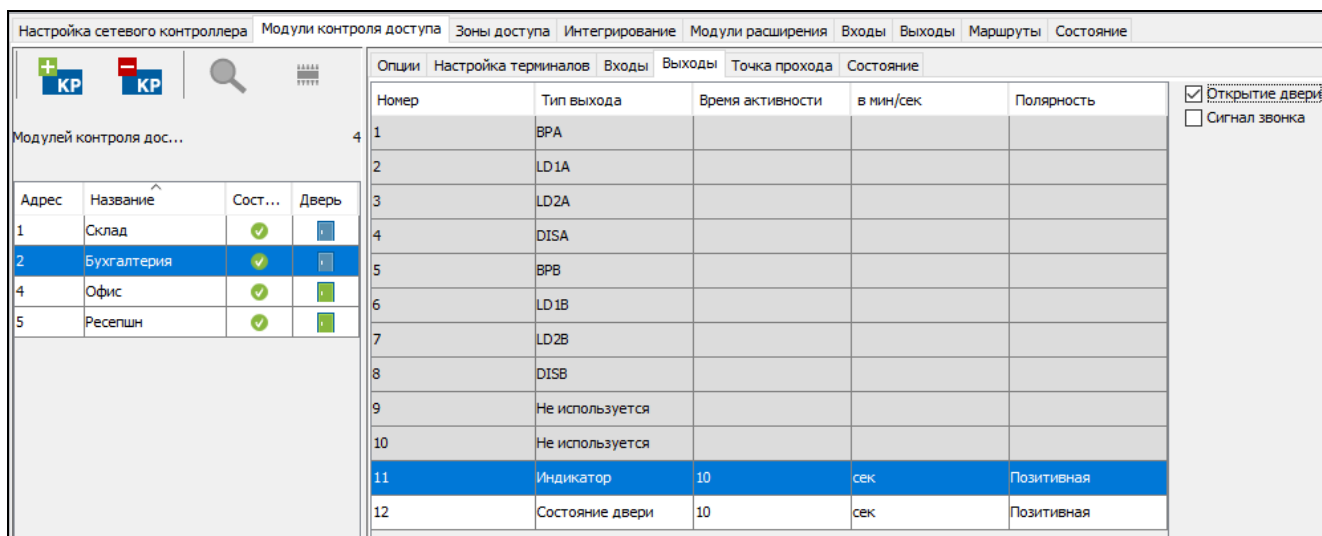


Рис. 20. Закладка «Выходы».

Доступ со считывателя – после выбора типа рядом с таблицей отобразятся следующие функции, которые выход может реализовать:

Доступ со считывателя А / Б – выход включается, если пользователю будет разрешен доступ со считывателя А / Б.



В модуле ACCO-KP2 некоторым выходам назначен постоянный определенный функционал:

BPA – управление звуком терминала А,

LD1A – управление зеленым светодиодом терминала А,

LD2A – управление красным светодиодом терминала А,

DISA – блокировка действия терминала А,

BPB – управление звуком терминала Б,

LD1B – управление зеленым светодиодом терминала Б,

LD2B – управление красным светодиодом терминала Б,

DISB – блокировка действия терминала Б,

Закладка «Точка прохода»

Терминалы – в виде таблицы отображается информация о том, какая зона выхода / входа была назначена терминалу А / Б модуля.

Выключение реле после открытия двери – если опция включена, реле, управляющее работой устройства, активирующего проход, выключится после открытия двери.

Выключение реле после закрытия двери – если опция включена, реле, управляющее работой устройства, активирующего проход, выключится после закрытия двери.

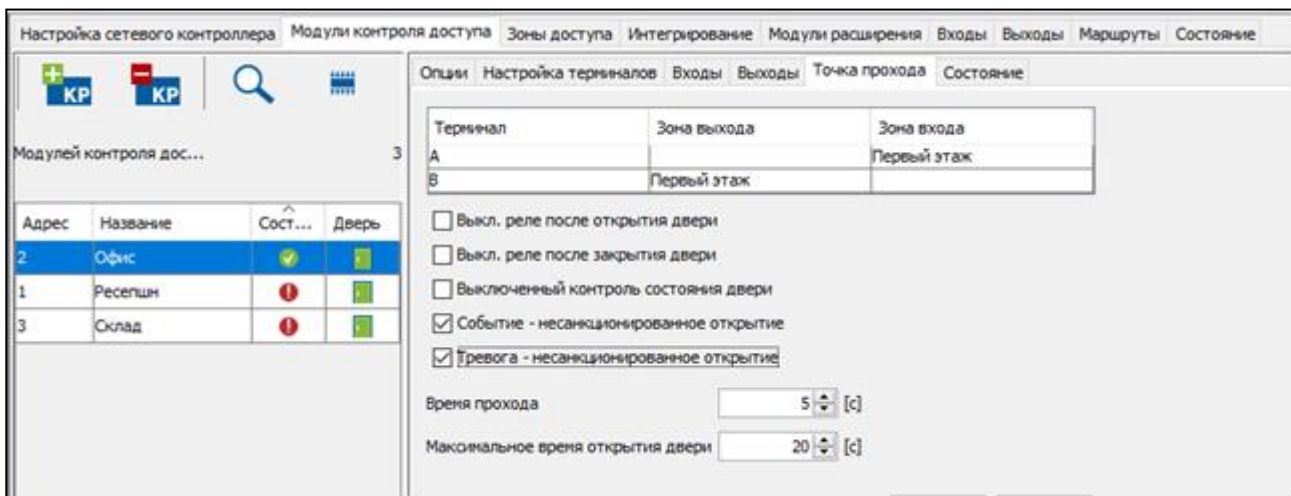


Рис. 21. Закладка «Точка прохода» для выбранного модуля контроля доступа.



Если опции, определяющие момент выключения реле, не будут включены, реле будет выключено по истечении «Времени на вход».

В следующих случаях реле выключается по истечении «Времени на вход», несмотря на включение одной из опций, определяющих момент выключения реле:

- входы не сообщают о состоянии двери (не установлен датчик, контролирующий состояние двери),
- включена опция «Выключен контроль состояния двери»,
- пользователь получил доступ, но не открыл дверь.

Выключенный контроль состояния двери – включение этой опции рекомендуется, если на модуль не поступает информация о состоянии двери (датчик,

контролирующий состояние, поврежден или по какой-то причине не подключен). Это предотвращает формирование несоответствующих событий. Если опция включена:

- предоставление доступа означает открытие двери (формирует событие, сообщаемое о проходе без контроля состояния двери),
- часть событий не формируется (например, события, сообщаемые о несанкционированном открытии двери, о длительном открытии двери и т. д.),
- не работает опция «Служебный проход»,
- проход в зоне доступа, выполняющей функцию шлюза, действует независимо от настроек шлюза (см. описание опции «Шлюз»).



Опцию «Выключенный контроль состояния двери» следует включать в исключительных ситуациях, так как она значительно ограничивает функционал СКУД.

Событие – несанкционированное открытие – если опция включена, то в случае открытия двери без авторизации будет сформировано событие типа «Несанкционированный доступ».

Тревога – несанкционированное открытие – если опция включена, в случае открытия двери без авторизации будет вызвана тревога и событие типа «Несанкционированный доступ».

Время на вход – время, в течение которого реле включается после получения доступа, позволяя открыть дверь. Можно задать время в диапазоне от 1 до 60 секунд.

Максимальное время открытия двери – время, в течение которого дверь может остаться открытой после выключения реле. Если дверь будет открыта дольше предусмотренного времени, будет сформировано соответствующее событие. Кроме того, активируется выход, запрограммированный как «Длительное открытие двери». Можно задать время в диапазоне от 1 до 60 секунд.

После ввода какого-либо изменения отобразятся кнопки:



– щелкните, чтобы отменить введенные изменения.



– щелкните, чтобы подтвердить введенные изменения.

Закладка «Состояние»



Если между сетевым контроллером и модулем контроля доступа не будет связи, отобразится информация об отсутствии связи между устройствами, а также дата и время последней передачи, полученной сетевым контроллером от модуля контроля доступа.

Состояние точки прохода – текущее состояние точки прохода:

- Точка прохода контролируется (дежурный режим),
- Точка прохода заблокирована,
- Точка прохода разблокирована,
- Неизвестное (нет связи с модулем контроля доступа).

Питание – текущее значение напряжения питания модуля контроля доступа.

Версия микропрограммы – версия прошивки модуля контроля доступа (номер версии и дата сборки).

Качество связи – текущее процентное соотношение отправленных данных (с сетевого контроллера на модуль) к полученным данным (с модуля на сетевой контроллер).

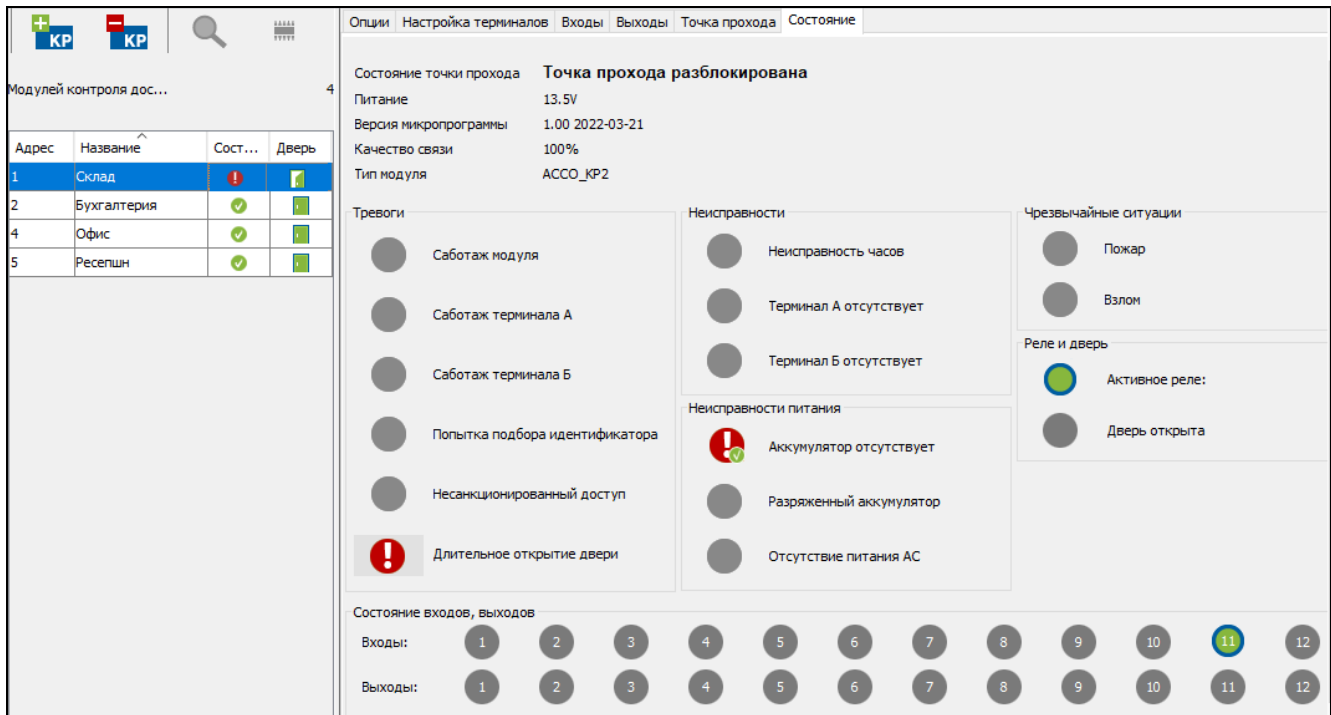


Рис. 22. Закладка «Состояние».

Тип модуля – модель модуля контроля доступа

Тревога – с помощью иконок отображается состояние: «Саботаж модуля», «Саботаж терминала А / Б», «Попытка подбора идентификатора», «Несанкционированный доступ» и «Длительное открытие двери».

Неисправности – с помощью иконок отображается состояние: «Неисправность часов» и «Терминал А / Б отсутствует».

Неисправность питания – с помощью иконок отображается состояние: «Аккумулятор отсутствует», «Аккумулятор разряжен» и «Отсутствие питания АС».

Тревоги – с помощью иконок отображается: «Взлом» в случае блокировки точки прохода в режиме тревоги взлома и «Пожар» в случае разблокировки точки прохода в режиме пожарной тревоги.

Отдельные иконки отображают следующие состояния:



– тревога / неисправности отсутствуют (серый фон).



– тревога / неисправность (белый восклицательный знак на красном фоне),



– подтвержденная тревога / неисправность (белый восклицательный знак на красном фоне и белый символ на зеленом фоне).



– память тревоги / неисправности (белый восклицательный знак на сером фоне),



– память подтвержденной тревоги / неисправности (белый восклицательный знак на сером фоне и белый символ на зеленом фоне).



– нет информации о состоянии (белый вопросительный знак на сером фоне).



Существует возможность подтверждения аварий и тревог. Если Вы хотите подтвердить аварию / тревогу, нажмите кнопку рядом.

Реле и дверь – с помощью иконок отображаются состояния: «Активное реле» и «Дверь открыта»

Состояние входов, выходов – с помощью иконок отображается состояние входов и выходов.

Отдельные иконки означают:



– активное реле / дверь открыта / активный вход / активный выход (зеленый кружок в синем кольце).



– неактивное реле / дверь закрыта / неактивный вход / неактивный выход (серый фон).




– неизвестное состояние (белый вопросительный знак на сером фоне).

4.2.4.6 Удаленное обновление прошивки модуля контроля доступа

1. Чтобы обновить прошивку модуля / модулей контроля доступа, необходимо выделить выбранный модуль или модули в таблице со списком модулей контроля доступа.



2. Щелкните по кнопке .

3. В открывшемся окне будет отображаться информация о текущей версии прошивки всех выделенных устройств, а также о новых доступных версиях для модулей ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS и ACCO-KP2 (см. рис. 23).



Данные модулей контроля доступа могут отображаться следующими цветами:

серый – неизвестная версия прошивки модуля контроля доступа;

черный – устаревшая версия прошивки модуля контроля доступа;

зеленый – обновленная версия прошивки модуля контроля доступа;

красный – несоответствующая языковая версия прошивки модуля контроля доступа.

4. Щелкните по кнопке «Обновление».

5. Откроется окно с названиями модулей контроля доступа, прошивка которых будет обновлена. Щелкните по кнопке «ОК».

6. Начнется процесс обновления прошивки.



Во время удаленного обновления прошивки модуля контроля доступа остальные модули, подключенные к сетевому контроллеру, работают в автономном режиме (описание можно найти в руководстве сетевого контроллера ACCO-NT).

В случае каких-либо проблем отобразится сообщение с соответствующей информацией. Необходимо будет повторно запустить обновление.

7. По завершении обновления отобразится соответствующее сообщение. Щелкните по «ОК», а затем «Заккрыть».

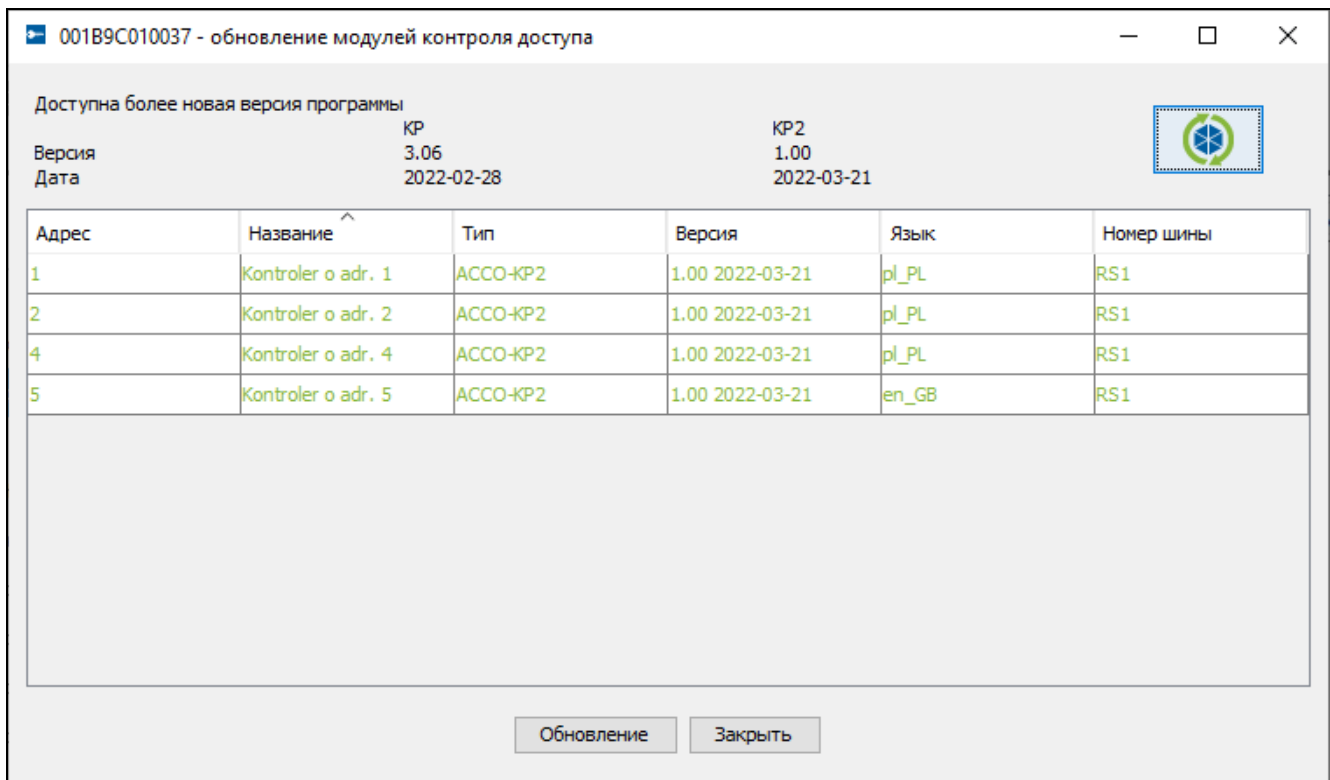



Рис. 23. Окно обновления прошивки модулей контроля доступа.

4.2.4.7 Удаление модуля контроля доступа

1. Если Вы хотите удалить один модуль контроля доступа, выделите выбранный модуль контроля доступа в таблице со списком модулей контроля доступа.
2. Если Вы хотите удалить одновременно несколько модулей контроля доступа, выделите один из модулей контроля доступа и, удержав нажатой клавишу Ctrl, выберите очередные модули с помощью левой клавиши мыши.
3. Если Вы хотите удалить одновременно все модули контроля доступа, выделите один из них и нажмите одновременно клавиши Ctrl+A.
4. Щелкните мышью по кнопке .
5. Когда отобразится вопрос, удалить ли модуль / модули контроля доступа, щелкните по «Да».
6. Сохраните введенные изменения.

4.2.5 Зоны доступа

Зона доступа – это выделенная территория на объекте. Разделение объекта на зоны упрощает администратору управление СКУД.

Описание кнопок



- щелкните, чтобы добавить зону доступа.



- щелкните, чтобы удалить выделенную зону доступа (см. раздел «Удаление зоны доступа»).

Под кнопками отображается количество зон доступа.

4.2.5.1 Создание зоны доступа

1. Выделите сетевой контроллер в списке объектов и сетевых контроллеров.

2. Щелкните по кнопке . Новая зона доступа появится в таблице.

4.2.5.2 Таблица со списком зон доступа

№ – порядковый номер зоны доступа.

Зона доступа – индивидуальное название зоны доступа (до 32 символов). Названия зон доступа могут быть напечатаны следующими цветами:

серый – зона доступа, которой не назначены модули контроля доступа;

черный – зона доступа с назначенными модулями контроля доступа.

Состояние – информация о текущем состоянии зоны доступа:

Загрузка состояния,

Дежурный режим,

Зона доступа разблокирована,

Зона доступа заблокирована,

Охрана,

Задержка на вход (время задержки на вход в интегрированном разделе системы охранной сигнализации),

Задержка на выход (< 10 с) (время задержки на выход в интегрированном разделе системы охранной сигнализации, время задержки – меньше 10 секунд),

Задержка на выход (> 10 с) (время задержки на выход в интегрированном разделе системы охранной сигнализации, время задержки – больше 10 секунд),

Разного типа (разное состояние точек прохода, контролируемых модулями контроля доступа в одной зоне доступа),

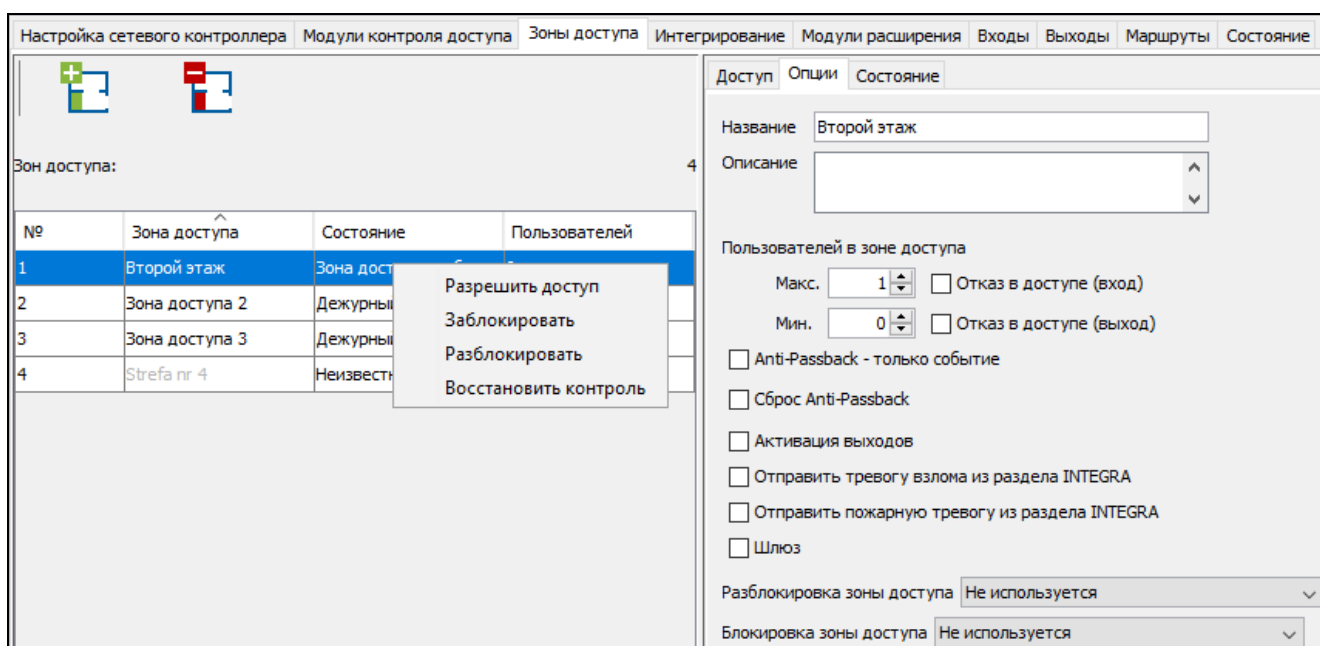
Тревога в зоне доступа,

Пожар в зоне доступа,

Неизвестное (перед сохранением созданной зоны доступа),

Недоступно (несоответствующая версия прошивки сетевого контроллера ACCO-NT).

Пользователей – количество пользователей, находящихся в текущий момент в зоне доступа.



№	Зона доступа	Состояние	Пользователей
1	Второй этаж	Зона доступа	4
2	Зона доступа 2	Дежурный режим	
3	Зона доступа 3	Дежурный режим	
4	Strefa nr 4	Неизвестно	

Настройка сетевого контроллера | Модули контроля доступа | **Зоны доступа** | Интегрирование | Модули расширения | Входы | Выходы | Маршруты | Состояние

Доступ | Опции | Состояние

Название: Второй этаж

Описание:

Пользователей в зоне доступа

Макс. 1 Отказ в доступе (вход)

Мин. 0 Отказ в доступе (выход)

Anti-Passback - только событие

Сброс Anti-Passback

Активация выходов

Отправить тревогу взлома из раздела INTEGRA

Отправить пожарную тревогу из раздела INTEGRA

Шлюз

Разблокировка зоны доступа: Не используется

Блокировка зоны доступа: Не используется

Рис. 24. Список зон доступа в закладке «Зоны доступа».

После выбора зоны доступа / нескольких зон доступа в списке и после щелчка по ней / по ним правой клавишей мыши, отобразится ниспадающее меню:

Разрешить доступ – после выбора этой функции точки прохода, контролируемые модулями контроля доступа в выбранной зоне доступа / в выбранных зонах доступа, будут открыты.

Заблокировать – после выбора этой функции все точки прохода будут постоянно перекрыты.

Разблокировать – после выбора этой функции все точки прохода будут постоянно открыты.



Если данный модуль назначен в несколько зон доступа, то блокировка или разблокировка одной из зон вызовет, соответственно, блокировку или разблокировку модуля в остальных зонах доступа, в которые он назначен.

Восстановить контроль – после выбора функции будет включен дежурный режим, то есть контроль точки прохода будет восстановлен.

4.2.5.3 Настройка зон доступа

Щелкните по выбранной зоне доступа в списке зон доступа, чтобы ее запрограммировать. Параметры зоны доступа отобразятся в закладках «Доступ» и «Опции».

Параметры зон доступа

Закладка «Доступ»

Адрес – адрес модуля контроля доступа.

Модуль контроля доступа – название модуля контроля доступа.

Терминал А / Б – выберите терминал (А или Б) в данном модуле для осуществления функции входа в зону доступа и выхода из зоны доступа.

Настройка сетевого контроллера				Зоны доступа				Интегрирование				Модули расширения				Входы				Выходы				Маршруты				Состояние			
Зон доступа:				Доступ				Опции				Состояние																			
№	Зона доступа	Состояние	Пользователей	Адрес	Модуль контроля доступа	Терминал А	Терминал Б	Вход	Выход	Вход	Выход	Вход	Выход	Вход	Выход	Вход	Выход														
1	Второй этаж	Дежурный режим	0	2/Офис				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>														
2	Зона доступа № 3	Неизвестное	0	1/Ресепшн				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>														
3	Зона доступа № 4	Неизвестное	0	3/Склад				<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>														
4	Зона доступа № 5	Неизвестное	0																												
5	Зона доступа № 6	Неизвестное	0																												
6	Первый этаж	Зона доступа разбл...	0																												

Рис. 25. Закладка «Доступ».

Закладка «Опции»

Название – индивидуальное название зоны доступа (до 32 символов).

Описание – в поле можно дополнительно описать зону доступа.

Пользователей в зоне доступа

Макс. – поле позволяет определить максимальное количество пользователей, которые могут одновременно пребывать в зоне доступа. Можно задать значения от 1 до 8000. Значение можно редактировать, щелкнув по полю мышью (можно ввести значение с помощью клавиатуры или выбрать его с помощью стрелок). Если параметр «минимальное число пользователей в зоне доступа» будет больше параметра «максимальное число пользователей в зоне доступа», то максимальное количество пользователей в зоне будет автоматически увеличено – оно будет на 1 больше минимального количества пользователей в зоне доступа.

Отказ в доступе (вход) – если опция включена, доступ к зоне с максимальным количеством пользователей заблокирован.



Включение опции «Отказ в доступе» для зоны не влияет на способ работы выхода типа «Индикатор макс. числа пользователей», связанного с этой зоной.

Мин. – поле позволяет определить минимальное количество пользователей, которые должны одновременно пребывать в зоне доступа. Можно задать значения от 0 до 7999. Значение можно редактировать, щелкнув по полю мышью (можно ввести значение с помощью клавиатуры или выбрать его с помощью стрелок). Если параметр «максимальное число пользователей в зоне доступа» будет меньше минимального, то значение минимального количества в зоне доступа автоматически уменьшится – оно будет на 1 меньше максимального количества пользователей в зоне доступа.

Отказ в доступе (выход) – если опция включена, нельзя покинуть зону, если в ней находится минимальное количество пользователей.



Включение опции «Отказ в доступе (выход)» для зоны не сказывается на способе работы выхода типа «Индикатор мин. числа пользователей» с привязкой к этой зоне.

Anti-Passback – только событие – если опция включена, функция запрета повторного прохода только регистрирует соответствующее событие.

Сброс Anti-Passback – если опция включена, то будет активно поле «В [чч:мм]», в котором можно определить время для сброса функции «Anti-Passback». Пользователи, чей выход из зоны доступа не был зарегистрирован, будут в состоянии получить доступ к зоне доступа по истечении заданного времени.

Активация выходов – если опция включена, зона доступа может управлять выходами типа «Активация доступом».

Отправить тревогу взлома из раздела INTEGRA – если включить опцию, в случае тревоги взлома в интегрированном разделе (группе) системы охранной сигнализации будет запрещен доступ в зоне доступа системы ACCO NET (доступ постоянно запрещен в случае взлома). Опция относится к интеграции системы ACCO NET и системы охранной сигнализации (см. раздел «Интеграция»).

Отправить пожарную тревогу из раздела INTEGRA – если включить опцию, пожарная тревога в интегрированном разделе системы охранной сигнализации откроет все двери в зоне доступа системы ACCO NET (открытие двери в случае пожара). Опция относится к интеграции системы ACCO NET и системы охранной сигнализации (см. раздел «Интеграция»).

Шлюз – если опция включена, зона доступа выполняет функцию шлюза, т. е. в зоне доступа может быть открыта только 1 дверь. Если одна из дверей открыта, невозможно открыть остальные точки прохода. Это не относится к точкам прохода со включенной опцией «Игнорировать настройки шлюза» или «Выключить контроль состояния двери».



Зона доступа может работать как шлюз, если контролируется состояние двери (ко входу модуля, запрограммированному как «Датчик открытия двери» подключен датчик).

У администратора есть доступ к точкам прохода в зоне доступа, выполняющей функцию шлюза, независимо от настроек шлюза.

Разблокировка зоны доступа – можно выбрать, должна ли зона доступа быть разблокирована в определенное время (поля «Начало [чч:мм]» и «Конец [чч:мм]»)

или по графику доступа (график можно выбрать из списка в поле «Графики», если он был создан в приложении ACCO Web).

Блокировка зоны доступа – можно выбрать, должна ли зона доступа быть заблокирована в определенное время (поля «Начало [чч:мм]» и «Конец [чч:мм]») или по графику доступа (график можно выбрать из списка в поле «Графики», если он был создан в приложении ACCO Web).

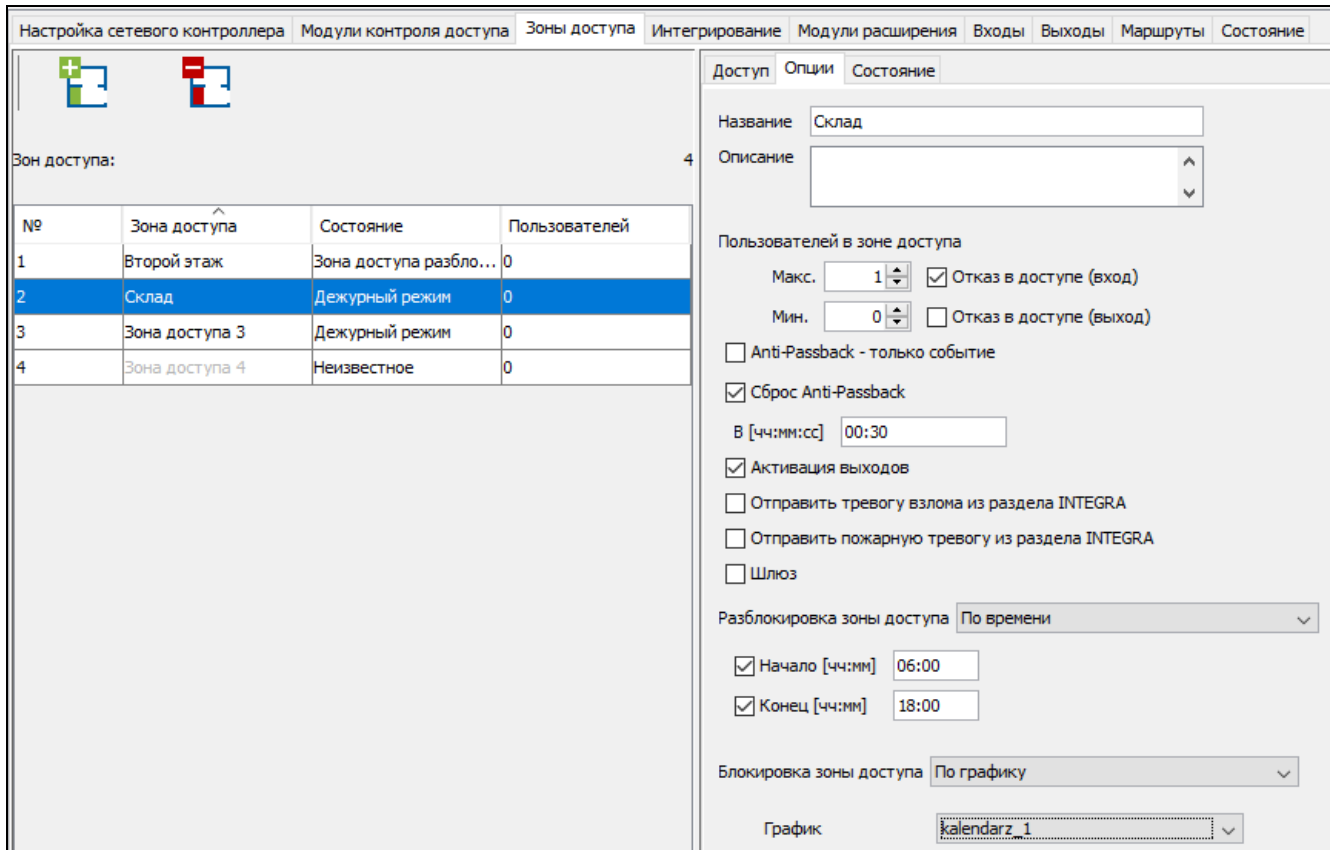


Рис. 26. Закладка «Опции».

После ввода какого-либо изменения отобразятся кнопки:



– щелкните, чтобы отменить введенные изменения.



– щелкните, чтобы подтвердить введенные изменения.

Закладка «Состояние»

В таблице отображается текущее состояние модулей контроля доступа, назначенных в зону доступа.

Адрес – адрес модуля контроля доступа.

Название – индивидуальное название модуля контроля доступа.

Состояние – информация о состоянии модуля контроля доступа. Иконки для отображения состояния устройства описаны в разделе «Таблица со списком модулей контроля доступа».


Дверь – информация о состоянии точки прохода и двери, контролируемой модулем контроля доступа. Иконки для отображения состояния точки прохода и двери описаны в разделе «Таблица со списком модулей контроля доступа».

Настройка сетевого контроллера				Модули контроля доступа				Зоны доступа				Интегрирование				Модули расширения				Входы				Выходы				Маршруты				Состояние			
Зон доступа:																6																			
№	Зона доступа	Состояние	Пользователей																																
1	Второй этаж	Дежурный режим	0																																
2	Зона доступа № 3	Неизвестное	0																																
3	Зона доступа № 4	Неизвестное	0																																
4	Зона доступа № 5	Неизвестное	0																																
5	Зона доступа № 6	Неизвестное	0																																
6	Первый этаж	Зона доступа разблокирована	0																																

Состояние			
Состояние модулей контроля доступа в зоне доступа			
Адрес	Название	Состояние	Дверь
1	Ресепшн	❗	🚪
2	Офис	🟢	🚪

Рис. 27. Закладка «Состояние».

4.2.5.4 Удаление зоны доступа

1. Если Вы хотите удалить одну зону доступа, выделите выбранную зону доступа в таблице со списком зон доступа.
2. Если Вы хотите удалить за один раз несколько зон доступа, выделите одну из зон доступа и, удерживая нажатой клавишу Ctrl, выберите очередные зоны доступа с помощью левой клавиши мыши.
3. Если Вы хотите удалить все зоны доступа одновременно, выделите одну из зон доступа и нажмите одновременно клавиши Ctrl+A.
4. Щелкните мышью по кнопке .
5. Когда отобразится вопрос, удалить ли зону доступа / зоны доступа, щелкните по «Да».
6. Сохраните введенные изменения.



Нельзя удалить зону доступа, в которую назначены модули контроля доступа.

4.2.6 Интеграция

Интеграция системы ACCO NET с системами безопасности на базе приборов INTEGRA или INTEGRA Plus (версия прошивки 1.17 или более поздняя) осуществляется по сети Ethernet. К системе охранной сигнализации должен быть подключен модуль ETHM-1 Plus (версия прошивки 2.03 или более поздняя) или ETHM-1 (версия прошивки 1.07 или более поздняя). Связь осуществляется через канал связи GUARDX.



ACCO NET использует для связи с прибором порт, используемый, например, GUARDX, INTEGRA CONTROL или INTEGRUM. Если система ACCO NET подключена к приемно-контрольному прибору, то другим программам нельзя подключиться к прибору, используя тот же самый Ethernet-модуль.

За соединение и обмен данными между системами отвечает ACCO Server.

Интеграция дает возможность одновременного управления зонами доступа СКУД и разделами (группами) системы охранной сигнализации. Один сетевой контроллер ACCO-NT позволяет создать 255 зон доступа. Один приемно-контрольный прибор позволяет создать максимально 32 раздела системы охранной сигнализации. Одному разделу можно назначить одну зону доступа ACCO NET. Оставшаяся часть системы ACCO NET может работать автономно.

4.2.6.1 Настройка системы охранной сигнализации

Информацию о настройке приемно-контрольного прибора и Ethernet-модуля можно найти в руководствах к этим устройствам.

Настройки приемно-контрольного прибора

В приемно-контрольном приборе необходимо:

- запрограммировать идентификатор для связи между системами: «Идентификатор ACCO» (ПО DLOADX → «Связь» → «Настройка связи»).



Идентификаторы связи в приемно-контрольном приборе и ПО DLOADX и ACCO Soft (закладка «Интеграция» → выбранная система охранной сигнализации → закладка «Конфигурация» → поле «Идентификатор ACCO») должны быть идентичны.

Ниже описаны случаи, в которых могут появиться некоторые ограничения при включении режима охраны в приборе. Если:

- включена опция «Grade 2 / 3»:
 - в системе охранной сигнализации: режим охраны можно включить только в соответствии с требованиями стандарта EN 50131 – соответственно для Grade 2 / 3; в ACCO Web дополнительная информация будет отображаться в событиях,
 - в СКУД: зону доступа можно заблокировать всегда,
- определено время для опции «Блокировка во время обхода охранника» и пользователь типа «Охранник» применил пароль / идентификатор:
 - в системе охранной сигнализации: поставленный на охрану раздел (группа) будет заблокирован на запрограммированное время; в приложении ACCO Web дополнительная информация будет отображаться в событиях,
 - в СКУД: зона доступа в состоянии «Охрана»,
- пользователь типа «Включает временную блокировку групп» применил пароль / идентификатор:
 - в системе охранной сигнализации: поставленный на охрану раздел будет заблокирован на время, индивидуально запрограммированное для данного пользователя; в приложении ACCO Web дополнительная информация будет отображаться в событиях,
 - в СКУД: зона доступа в состоянии «Охрана»,
- определен тип раздела (группы) «С блокировкой на время», включена опция «Время блокировки по умолчанию», определено время в поле «Время блокировки групп по умолчанию»:
 - в системе охранной сигнализации: после постановки на охрану раздел будет заблокирован на время, определенное установщиком,
 - в СКУД: зону доступа можно заблокировать; раздел системы охранной сигнализации блокируется автоматически на время? определенное установщиком, блокировка отображается в ПО DLOADX.
- определен тип раздела (группы) «С блокировкой на время»:
 - в системе охранной сигнализации: после постановки на охрану раздел будет заблокирован на время, определенное пользователем,
 - в СКУД: зону доступа можно заблокировать; раздел системы охранной сигнализации не блокируется на время,



В системе охранной сигнализации во время блокировки режим охраны может выключить только пользователь с полномочием «Доступ к заблокированным на время группам». В СКУД пользователь может восстановить контроль в группе с помощью терминала входа, для которого включена опция «Управляет зоной доступа», если:

- ему назначено полномочие «Переключение»,
- у него есть доступ к данной зоне доступа согласно назначенному ему графику доступа.

- запрограммированы общие опции, касающиеся режима охраны:
 - в системе охранной сигнализации: режим охраны можно включить, если нет условий, которые не позволяют включить режим охраны – в зависимости от состояния зон, выходов, аварий в системе охранной сигнализации,
 - в СКУД: зону доступа можно заблокировать всегда.

Настройка Ethernet-модуля (ETHM-1, ETHM-1 Plus)

В Ethernet-модуле следует:

- включить опцию «GUARDX» и «GSM» для системы ACCO NET для установления связи через сеть TCP/IP;
- запрограммировать номер порта TCP, который будет использоваться для связи с системой ACCO NET, если он должен отличаться от 7091 (поле «Порт»);
- запрограммировать ключ (последовательность до 12 буквенно-цифровых символов– цифры, буквы и специальные символы) для шифрования данных во время связи с системой ACCO NET (поле «Ключ GUARDX/Java»).

Описание кнопок



- щелкните, чтобы добавить систему охранной сигнализации.



- щелкните, чтобы удалить выбранную систему охранной сигнализации (см. раздел «Удаление системы охранной сигнализации»).


Рядом с кнопками отображается цифра в формате x/y, где «x» – это количество систем охранной сигнализации, интегрированных с системами ACCO-NT, «y» – это максимальное количество систем охранной сигнализации для сетевого контроллера ACCO-NT (см. раздел «Лицензии»).

Цвета означают:

- черный – максимальное количество поддерживаемых систем безопасности для данного сетевого контроллера ACCO-NT не превышено,
- красный – максимальное количество поддерживаемых систем безопасности для данного сетевого контроллера ACCO-NT превышено.

4.2.6.2 Добавление системы охранной сигнализации

1. Выберите прибор в списке объектов и приборов.

2. Щелкните по кнопке . В таблице появится новая система охранной сигнализации.

4.2.6.3 Таблица со списком систем охранной сигнализации

В таблице отображается список систем охранной сигнализации, интегрированных с системой ACCO NET.

Номер – порядковый номер системы охранной сигнализации.

Название – название системы охранной сигнализации.

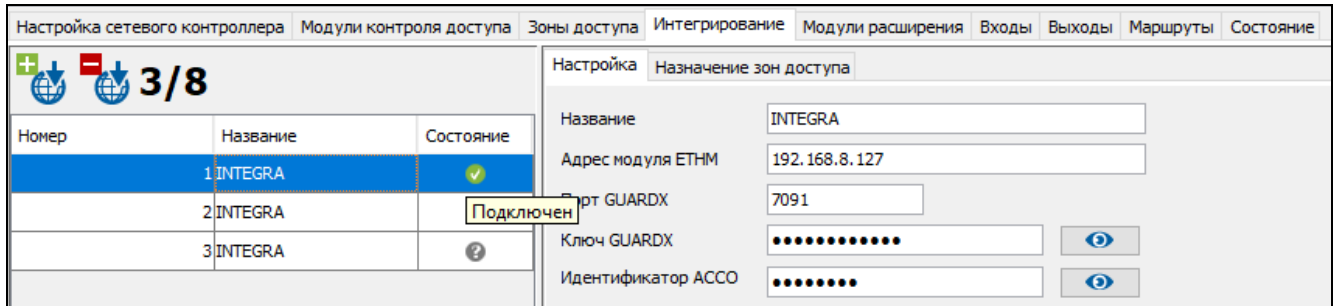


Рис. 28. Таблица со списком систем в закладке «Интегрирование».

Состояние – информация о состоянии связи между системой охранной сигнализации и ACCO NET. Отдельные иконки означают:

- проблемы со связью. Если подвести курсор мыши к иконке, отобразится описание: «Занято», «Нет связи», «Неправильный ключ GUARDX», «Превышен лимит INTEGRA» или «Неправильная настройка соединения» (белый восклицательный знак на красном фоне),
- связь между ACCO Server и Ethernet-модулем работает правильно. Если подвести курсор мыши к иконке, отобразится надпись «Подключен» (белый символ на зеленом фоне),
- данные не были сохранены в базе данных; если подвести курсор мыши к иконке, отобразится надпись «Неизвестное» (белый вопросительный знак на сером фоне).

4.2.6.4 Настройка интеграции

Щелкните по выбранной системе охранной сигнализации, чтобы настроить интеграцию с системой ACCO NET. Данные отображаются в закладках «Настройка» и «Назначение зон доступа».

Закладка «Настройка»

Название – название системы охранной сигнализации в системе ACCO NET.

Адрес модуля ЕТНМ – IP-адрес Ethernet-модуля, подключенного к прибору INTEGRA.

Порт GUARDX – номер TCP-порта для связи ACCO NET с приемно-контрольным прибором.

Ключ GUARDX – последовательность до 12 буквенно-цифровых символов (цифры, буквы и специальные символы), предназначенная для шифрования данных, которыми обменивается система ACCO NET с приемно-контрольным прибором. Щелкните по , чтобы увидеть последовательность символов.

Идентификатор ACCO – идентификатор для интеграции системы ACCO NET с приемно-контрольным прибором. Он состоит из 8 цифр. Щелкните по , чтобы увидеть последовательность символов.

После ввода какого-либо изменения отобразятся кнопки:

- щелкните, чтобы отменить введенные изменения.
- щелкните, чтобы подтвердить введенные изменения.

Рис. 29. Закладка «Настройка».

Закладка «Назначение зон доступа»

Показать все – выделить опцию, если в таблице с зонами доступа должны отображаться все разделы (группы) системы охранной сигнализации. Их количество зависит от типа прибора. Если опция выключена, в таблице отображаются только разделы, созданные в данной системе, считанные из памяти приемно-контрольного прибора, автоматически после установления связи между системами.

№ – порядковый номер.

Раздел – INTEGRA – название раздела в системе охранной сигнализации.

Зона доступа – ACCO – название зоны доступа в СКУД, интегрированной с разделом системы охранной сигнализации.

4.2.6.5 Назначение зоны доступа


1. В графе «Зона доступа – ACCO» щелкните правой клавишей мыши по полю, соответствующему разделу (группе) системы охранной сигнализации.
2. Когда отобразится список доступных зон доступа системы ACCO NET, выберите зону для назначения. Название выбранной зоны отобразится в поле.
3. Аналогично назначаются другие зоны доступа ACCO NET.
4. Сохраните введенные изменения.

№	Раздел - INTEGRA	Зона доступа - ACCO
1	Ofis	Второй этаж
2	Sklad	Первый этаж
3	Razdel 3	
4	Razdel 4	

Рис. 30. Закладка «Назначение зон доступа».

4.2.6.6 Удаление системы охранной сигнализации

1. Выделите выбранную систему в таблице со списком систем.

2. Щелкните по кнопке .

3. Когда отобразится вопрос, удалить ли систему, щелкните по «Да».

4. Сохраните введенные изменения.

4.2.7 Модули расширения

Настройка сетевого контроллера			Модули контроля доступа			Зоны доступа			Интегрирование			Модули расширения			Входы			Выходы			Маршруты			Состояние		
Адрес	Тип	Название	№	Функция входа	Название	Тип	Чувствительность...	Активация по гра...	Актив.	№	Тип выхода	Название	Режим раб...	Время акти...	в мин/сек	Поляризация	Инверсия	Активен	Приложение							
0	INT-PP	подвал	9	Блокировка зоны д...	Wejście 9	NO	320	Blugo	<input checked="" type="checkbox"/>	9	Индикатор ...	Wyjście 9	Индикатор	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>							
1	INT-ORS	склад	10	Разблокировка зон...	Wejście 10	NO	320		<input checked="" type="checkbox"/>	10	Индикатор ...	Wyjście 10	Индикатор	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>							
2	INT-O	коридор	11	Разблокировка зон...	Wejście 11	NO	320	Blugo	<input checked="" type="checkbox"/>	11	Логическая ...	Wyjście 11	Индикатор	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>							
3	INT-RX-S	ворота	12	Блокировка точки ...	Wejście 12	NO	320		<input checked="" type="checkbox"/>	12	Логическое ...	Wyjście 12	Индикатор	2	мин	Позитивная	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>							
4	INT-RX-S	INT-RX-S	13	Разблокировка зон...	Wejście 13	NO	320		<input checked="" type="checkbox"/>	13	Индикатор ...	Wyjście 13	Индикатор	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>							
5	---		14	Блокировка точки ...	Wejście 14	По выходу	320		<input checked="" type="checkbox"/>	14	Индикатор ...	Wyjście 14	Индикатор	2	мин	Позитивная	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>							
6	---		15	Не используется					<input type="checkbox"/>	15	Брелок	Wyjście 15	Перекл.	2	мин	Позитивная	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>							
7	---		16	Не используется					<input type="checkbox"/>	16	Активация ...	Wyjście 16	Вкл. на врем...	20	сек	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>							

Рис. 31. Закладка «Модули расширения».

4.2.7.1 Добавление модуля расширения

Только после добавления модуля расширения согласно следующей процедуре модуль будет поддерживаться системой.

1. Щелкните по адресу, который соответствует адресу, установленному в модуле расширения.
2. Щелкните правой клавишей мыши по столбцу «Тип». Откроется список типов модулей расширения.
3. Выберите соответствующий тип модуля расширения.
4. В столбце «Название» введите название модуля расширения.
5. Сохраните введенные изменения.

4.2.7.2 Настройки модуля расширения

Адрес – адрес модуля расширения.

Тип – тип модуля расширения. Для выбора: INT-O, INT-E, INT-PP, INT-RX-S, INT-ORS и INT-IORS.

Название – индивидуальное название модуля расширения.

После выделения выбранного модуля расширения, в случае модулей расширения входов / выходов / входов и выходов, рядом со списком модулей расширения отобразится одна или две таблицы с информацией о входах / выходах в выбранном модуле расширения (описание входов – см. с. 54; описание выходов – см. с. 56).

4.2.7.3 Удаление модуля расширения

1. В таблице со списком модулей расширения выберите модуль, который должен быть удален.
2. В столбце «Тип», после щелчка правой клавишей мыши, выберите пустое поле.
3. Сохраните введенные изменения.

4.2.8 Входы

Система контроля доступа поддерживает входы:

- **проводные** – на плате сетевого контроллера и в модулях расширения.
- **виртуальные** – входы, которые не существуют физически, но которые могут быть запрограммированы как тип «По выходу».

4.2.8.1 Нумерация входов в системе

Входы получают номера следующим образом:

- проводным входам на плате сетевого контроллера назначаются номера от 1 до 8.
- номера входов в модулях расширения зависят от адреса модуля расширения в системе (для отдельных адресов модулей расширения номера входов забронированы, например, для модуля расширения с адресом 0 входам будут назначены номера от 9 до 16, для модуля расширения с адресом 1 входам будут назначены номера от 17 до 24 и т. д.).

4.2.8.2 Настройка входов

Щелкните по закладке «Входы». Выделите вход, чтобы его запрограммировать.

Назначение входа в зону доступа

1. Запрограммируйте для входа один из типов: «Блокировка зоны доступа», «Разблокировка зоны доступа», «Блокировка тревога» или «Разблокировка пожар».
2. С правой стороны окна в части «Опции реакции» назначьте вход в выбранную зону доступа или во все зоны доступа.

№	Функция входа	Название	Тип	Чувствительность [мс]	Активация по графику	Актив.	Модуль:
1	Саботаж	Вход 1	NO	320	Biuro	<input checked="" type="checkbox"/>	подвал
2	Блокировка зоны доступа	Вход 2	NO	320		<input checked="" type="checkbox"/>	Тип модуля: INT-PP
3	Разблокировка зоны доступа	Вход 3	Отсутствует	320		<input checked="" type="checkbox"/>	Адрес модуля: 0
4	Блокировка Тревога	Вход 4	Отсутствует	320		<input checked="" type="checkbox"/>	Номер входа: 7
5	Разблокировка Пожар	Вход 5	Отсутствует	320		<input checked="" type="checkbox"/>	Тип
6	Разрешение доступа	Вход 6	NC	320		<input checked="" type="checkbox"/>	
7	Блокировка точки прохода	Вход 7	Отсутствует	320		<input checked="" type="checkbox"/>	
8	Блокировка точки прохода	Вход 8	NC	320		<input checked="" type="checkbox"/>	
9	Блокировка зоны доступа	Вход 9	NO	320	Biuro	<input checked="" type="checkbox"/>	
10	Разблокировка точки прохода - пожар	Вход 10	NO	320		<input checked="" type="checkbox"/>	
11	Разблокировка зоны доступа	Вход 11	NO	320	Biuro	<input checked="" type="checkbox"/>	
12	Блокировка точки прохода - тревога	Вход 12	NO	320		<input checked="" type="checkbox"/>	
13	Разблокировка точки прохода	Вход 13	NO	320		<input checked="" type="checkbox"/>	
14	Блокировка точки прохода	Вход 14	По выходу	320		<input checked="" type="checkbox"/>	
15	Не используется					<input type="checkbox"/>	
16	Не используется					<input type="checkbox"/>	Для выбора
17	Не используется					<input type="checkbox"/>	
18	Не используется					<input type="checkbox"/>	
19	Не используется					<input type="checkbox"/>	
20	Не используется					<input type="checkbox"/>	
21	Не используется					<input type="checkbox"/>	
22	Не используется					<input type="checkbox"/>	

Рис. 32. Закладка «Входы».

Назначение входа модулю контроля доступа

1. Запрограммируйте для входа тип входа: «Открытие точки прохода», «Блокировка точки прохода», «Разблокировка точки прохода», «Блокировка точки прохода – тревога» или «Разблокировка точки прохода – пожар».
2. В открывшемся окне выберите модуль контроля доступа, которому должен быть назначен вход, и щелкните по «ОК».

Параметры входов

Таблица со списком входов

№ – порядковый номер входа в системе.

Тип реакции (см. раздел «Тип входа»).

Название – индивидуальное название входа (до 32 символов).

Тип шлейфа – можно запрограммировать:

Отсутствует – нет подключенного устройства,

NO – поддержка устройства с выходом типа NO (с нормально разомкнутыми контактами),

NC – поддержка устройства с выходом типа NC (с нормально замкнутыми контактами).

По выходу – состояние зависит от состояния выбранного выхода (вход не поддерживает подключенные устройства).

Чувствительность [мс] – время, в течение которого состояние входа должно быть измененным, чтобы этот факт был зарегистрирован. Это время можно запрограммировать в пределах от 20 мс до 5,1 с.

Активация по графику – если опция включена, вход будет поддерживаться только в течение времени, определенного графиком доступа. График доступа можно выбрать после щелчка правой клавишей мыши по полю. График доступа можно создать в приложении ACCO Web.

Актив. – если опция включена, вход поддерживается. Опция доступна, если для входа был выбран тип входа.

Информация о входе

После выделения входа в списке, рядом с таблицей, отобразятся:

- название, тип и адрес модуля, а также номер входа в модуле,
- параметры:
 - номер выхода (тип шлейфа «По выходу»),
 - модуль контроля доступа (тип входа «Разрешение доступа», «Блокировка / Разблокировка точки прохода», «Блокировка точки прохода – тревога» или «Разблокировка точки прохода – пожар»),
 - выбранная зона доступа или все (тип входа: «Блокировка / Разблокировка зоны доступа», «Блокировка тревога» или «Разблокировка пожар»).

Тип входа

Тип можно выбрать после щелчка правой клавишей мыши по полю.

Не используется

Без функции – вход используется для комплексных логических операций на выходах. Активный вход не вызовет непосредственно никакую реакцию.

Блокировка зоны доступа – активный вход заблокирует все точки прохода, контролируемые модулями контроля доступа, назначенными выбранной зоне доступа. Точки прохода будут заблокированы, пока вход будет активен (если раньше не появится событие, которое другим образом изменит состояние точки прохода).

Разблокировка зоны доступа – активный вход разблокирует все точки прохода, контролируемые модулями контроля доступа, назначенными выбранной зоне доступа. Точки прохода останутся разблокированными, пока выход будет активен (если раньше не появится событие, которое другим образом изменит состояние точки прохода).

Блокировка – тревога – постоянный запрет на доступ ко всем точкам прохода в зоне доступа из-за тревоги. Точки прохода останутся перекрытыми до момента изменения их состояния с помощью кода или длительного удержания карты пользователем с полномочием «Переключение».

Разблокировка – пожар – постоянное разрешение доступа ко всем точкам прохода в зоне доступа из-за пожара. Двери остаются открытыми, пока не будет восстановлено нормальное состояние всех входов модуля контроля доступа или сетевого контроллера ACCO-NT. Точки прохода может переключать пользователь с полномочием «Переключение».

Разрешение доступа – активный вход вызовет разрешение доступа к двери, контролируемой выбранным модулем контроля доступа на время, запрограммированное в поле «Время прохода» (в закладке «Точка прохода» после выделения соответствующего модуля контроля доступа в списке). Модуль контроля доступа следует выбрать в окне, которое отобразится после выбора данного типа входа.

Блокировка точки прохода – активный вход заблокирует точку прохода, контролируемую выбранным модулем контроля доступа. Модуль контроля доступа следует выбрать в окне, которое откроется после выбора типа входа. Точка прохода будет заблокирована до момента изменения ее состояния пользователем с полномочием «Переключение» или с помощью соответствующих функций в программе ACCO Soft или в приложении ACCO Web.

Разблокировка точки прохода – активный вход разблокирует точку прохода, контролируемую выбранным модулем контроля доступа. Модуль контроля доступа следует указать в окне, которое будет отображено после выбора этого типа реакции для входа. Точка прохода останется разблокированной до момента изменения ее состояния пользователем с полномочием «Переключение» или с помощью соответствующих функций в программе ACCO Soft или в приложении ACCO Web.

Блокировка точки прохода – тревога – постоянное перекрытие точки прохода, контролируемой выбранным модулем контроля доступа, из-за тревоги. Модуль контроля доступа следует указать в окне, которое отобразится после выбора этого типа реакции для входа. Точка прохода останется закрытой до момента изменения ее состояния пользователем с полномочием «Переключение».

Разблокировка точки прохода – пожар – постоянное открытие точки прохода, контролируемой выбранным модулем контроля доступа, в случае пожара. Модуль контроля доступа следует выбрать в окне, которое откроется после выбора типа входа. Дверь останется открытой, пока не будет восстановлено нормальное состояние входа модуля контроля доступа. Точку прохода может переключать пользователь с полномочием «Переключение».

Саботаж – активирование входа вызовет:

- неисправность сетевого контроллера ACCO-NT, о которой будет сообщать соответствующая иконка в закладке «Состояние»;
- тревогу саботажа на выходе «Тревога саботажа из прибора».

4.2.9 Выходы

Система контроля доступа поддерживает выходы:

- **проводные** – на плате сетевого контроллера и в модулях расширения.
- **виртуальные** – выходы, которые не существуют физически, но могут использоваться, например, для осуществления логических функций.

4.2.9.1 Нумерация выходов в системе

Выходы получают номера следующим образом:

- проводным выходам на плате сетевого контроллера назначаются номера от 1 до 8.
- номера выходов в модулях расширения зависят от адреса модуля расширения в системе (для отдельных адресов номера выходов забронированы, например, для модуля расширения с адресом 0 выходам будут назначены номера от 9 до 16, для модуля расширения с адресом 1 выходам будут назначены номера от 17 до 24 и т. д.).

4.2.9.2 Настройка выходов

Щелкните по закладке «Выходы». Выделите выход, чтобы его запрограммировать.

Параметры выходов

Таблица со списком выходов

№ – номер выхода в системе.

Тип выхода (см. раздел «Типы выходов»).

Название – индивидуальное название выхода (до 32 символов).

Режим работы – выберите режим работы выхода:

Вкл. на время (событие продлевает) – выход будет включаться на время, определенное в поле «Время активности». Когда выход активен, его повторная активация перезапустит отсчет времени активности.

Вкл. на время (событие выключает) – выход будет включаться на время, определенное в поле «Время активности». Когда выход активен, его повторная активация выключит выход.

Вкл. на время (игнорирование событий) – выход будет включаться на время, определенное в поле «Время активности». Когда выход активен, его повторная активация не имеет влияния на состояние выхода.

Переключение – активация выхода переключит его состояние на противоположное (если он был включен, то будет выключен, а если был выключен, то будет включен).

Индикатор – выход будет активен, пока не исчезнет управляющий сигнал.

Время активности – время, в течение которого выход активен. Можно задать значения от 0 до 127 секунд или минут. Если будет задано значение 0, выход будет активен, когда будет подаваться управляющий сигнал.



Если для выхода типа: «Логическое произведение выходов», «Логическая сумма выходов», «Логическое произведение входов» или «Логическая сумма входов» будет задано время активности, то выход будет активен, пока будет подаваться управляющий сигнал и потом в течение заданного времени.

в мин/сек – выберите единицу времени для времени активности.

Поляризация – опция определяет способ работы выхода. В случае обратной поляризации в активном состоянии:

- выход типа ОС будет отсоединен от массы,
- клемма NO релейного выхода будет разомкнута, а клемма NC замкнута.

Инверсия – если опция включена, то физическое состояние выхода будет противоположным состоянию, отображаемому в системе (включенный выход отображается как неактивный, а выключенный – как активный).

Актив. – если опция включена, выход поддерживается. Опция доступна, если для выхода был выбран тип.

Приложение – если опция включена, выход можно активировать на карте в приложении ACCO Web.

Настройка сетевого контроллера										Модули контроля доступа	Зоны доступа	Интегрирование	Модули расширения	Входы	Выходы	Маршруты	Состояние
№	Тип выхода	Название	Режим работы	Время активно...	в мин/сек	Поляризация	Инверсия	Активен	Приложение	Модуль:	Здание А						
1	Индикатор блокировки точек пр...	Выход 1	Вкл. на время (и...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Тип модуля:	ACCO-NT						
2	Индикатор разблокировки точе...	Выход 2	Индикатор	2	мин	Позитивная	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Адрес модуля:	-						
3	Логическое произведение выхо...	Выход 3	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Номер выхода:	2						
4	Логическая сумма выходов	Выход 4	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Офис <input checked="" type="checkbox"/> Ресепшн <input checked="" type="checkbox"/> Склад							
5	Активация доступом	Выход 5	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
6	По графику	Выход 6	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
7	Тревога - Несанкционированный...	Выход 7	Перекл.	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
8	Тревога саботажа из прибора	Выход 8	Перекл.	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
9	Индикатор блокировки зон дост...	Выход 9	Индикатор	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
10	Индикатор разблокировки зон д...	Выход 10	Индикатор	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
11	Логическая сумма входов	Выход 11	Индикатор	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
12	Логическое произведение входов	Выход 12	Индикатор	2	мин	Позитивная	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
13	Индикатор разблокировки зон д...	Выход 13	Индикатор	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>								
14	Индикатор блокировки зон дост...	Выход 14	Индикатор	2	мин	Позитивная	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
15	Брелок	Выход 15	Перекл.	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>								
16	Активация доступом	Выход 16	Вкл. на время (с... 20	сек	сек	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
17	Индикатор блокировки точек пр...	Выход 17	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
18	Индикатор разблокировки точе...	Выход 18	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
19	Индикатор контроля зон доступа	Выход 19	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
20	Индикатор контроля точек прох...	Выход 20	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
21	Индикатор максимального числа...	Выход 21	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
22	Индикатор минимального числа ...	Выход 22	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
23	Режим охраны	Output 23	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
24	Тревога саботажа из модулей р...	Wyjście 24	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
25	Тревога саботажа из модулей к...	Wyjście 25	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								
26	Доступ разрешен	Wyjście 26	Вкл. на время (с...	2	мин	Позитивная	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>								

Рис. 33. Закладка «Выходы».

Информация о выходе

После выбора выхода в списке, рядом с таблицей, отобразятся:

- название, тип и адрес модуля, а также номер выхода в модуле,
- параметры, определяемые для данного типа выхода:
 - номера выходов (тип выхода «Логическое произведение выходов» или «Логическая сумма выходов»),
 - номера входов (тип выхода «Логическое произведение входов» или «Логическая сумма входов»),
 - зона доступа – одна или все (тип выхода «Активация доступом»),
 - зона доступа – выбранные (тип выхода: «Режим охраны», «Индикатор блокировки / разблокировки зон доступа», «Индикатор блокировки зон доступа в режиме тревоги», «Индикатор разблокировки зон доступа в режиме пожар», «Индикатор контроля зон доступа», «Индикатор макс. числа пользователей» или «Индикатор мин. числа пользователей»),
 - точка прохода – выбранные (тип выхода: «Индикатор блокировки / разблокировки точек прохода», «Индикатор блокировки точек прохода в режиме тревоги», «Индикатор разблокировки точек прохода в режиме пожар» или «Индикатор контроля точек прохода», «Тревога – Несанкционированный доступ», «Тревога саботажа из модулей контроля доступа», «Доступ разрешен» или «Отказ в доступе»),
 - график доступа (тип выхода «По графику»).
 - модуль расширения (тип выхода «Тревога саботажа из модулей контроля доступа»).

Типы выходов

Тип выхода можно выбрать после щелчка правой клавишей мыши по полю.

Не используется

Логическое произведение выходов – выход активируется, когда все управляющие выходы активны.

Логическая сумма выходов – выход активируется, когда любой из управляющих выходов активен.

Логическое произведение входов – выход активируется, когда все управляющие входы активны.

Логическая сумма входов – выход активируется, когда любой из управляющих входов активен.

Брелок – выход активируется после нажатия кнопки брелка.

Активация доступом – выход активируется после получения доступа к выбранной зоне доступа с включенной опцией «Активация выходов».

Индикатор блокировки зон доступа – выход активируется, когда любая из выбранных зон доступа будет заблокирована.

Индикатор разблокировки зон доступа – выход активируется, когда любая из выбранных зон доступа будет разблокирована.

Индикатор блокировки зон доступа в режиме тревоги – выход активируется, когда любая из точек прохода в любой из выбранных зон доступа постоянно перекрыта из-за тревоги.

Индикатор разблокировки зон доступа в режиме пожар – выход активируется, когда любая из точек прохода в любой из выбранных зон доступа постоянно открыта из-за пожара.

Индикатор блокировки точек прохода – выход активируется, когда любая из выбранных точек доступа будет заблокирована.

Индикатор разблокировки точек прохода – выход активируется, когда любая из выбранных точек доступа будет разблокирована.

Индикатор блокировки точек прохода в режиме тревоги – выход активируется, когда любая из выбранных точек прохода будет постоянно перекрыта из-за тревоги.

Индикатор разблокировки точек прохода в режиме пожар – выход активируется, когда к любой из выбранных точек прохода будет постоянно разрешен доступ из-за пожара.

Индикатор контроля зон доступа – выход активируется, когда состояние любой из выбранных зон доступа контролируется.

Индикатор контроля точек прохода – выход активируется, когда состояние любой из выбранных точек прохода контролируется.

По графику – выход активируется в соответствии с окнами времени выбранного графика доступа.

Индикатор макс. числа пользователей – выход активируется, если в любой из выбранных зон доступа пребывает максимальное число пользователей.

Индикатор мин. числа пользователей – выход активируется, если в любой из выбранных зон доступа пребывает минимальное количество пользователей.

Режим охраны – выход активируется, если в любом из выбранных интегрированных разделов (групп) системы охранной сигнализации включен режим охраны.

Тревога – Несанкционированный доступ – выход активируется, если любая из выбранных точек прохода вызовет тревогу «Несанкционированный доступ».

Тревога саботажа из прибора – выход активируется при активации входа, запрограммированного как «Саботаж». Будет вызвана тревога саботажа сетевого контроллера ACCO-NT.

Тревога саботажа из модулей расширения – выход активируется, если любой из выбранных модулей расширения вызовет тревогу саботажа.

Тревога саботажа из модулей контроля доступа – выход активируется, если любой из выбранных модулей контроля доступа вызовет тревогу саботажа.

Доступ разрешен – выход активируется, если будет предоставлен доступ к любой из выбранных точек прохода.

Отказ в доступе – выход активируется, если не будет предоставлен доступ к любой из выбранных точек прохода.

4.2.10 Маршруты

Маршрут – это путь, по которому пользователь должен следовать, передвигаясь по объекту. Такое решение может использоваться, например, в случае компаний, занимающихся уборкой помещений.

Описание кнопок




- кнопка позволяет добавить маршрут.



- кнопка позволяет удалить выбранный маршрут (см. раздел «Удаление маршрута»).

4.2.10.1 Создание маршрута

1. Выделите сетевой контроллер в списке объектов и сетевых контроллеров.
2. Щелкните по кнопке . Новый маршрут появится в списке.
3. Щелкните правой клавишей мыши по столбцу «Зона доступа» и выберите одну из зон доступа.
4. Можно определить минимальное время пребывания пользователя в данной зоне доступа.
5. Если Вы хотите назначить маршруту очередные зоны доступа, повторите действия, описанные в пунктах 3 и 4.
6. Сохраните введенные изменения.

4.2.10.2 Настройка маршрута

Щелкните по закладке «Маршруты». Выделите маршрут, чтобы его запрограммировать.

Название – индивидуальное название маршрута (до 45 символов).

После ввода нового названия или изменения названия отобразятся кнопки:



– щелкните, чтобы отменить введенные изменения.



– щелкните, чтобы подтвердить введенные изменения.

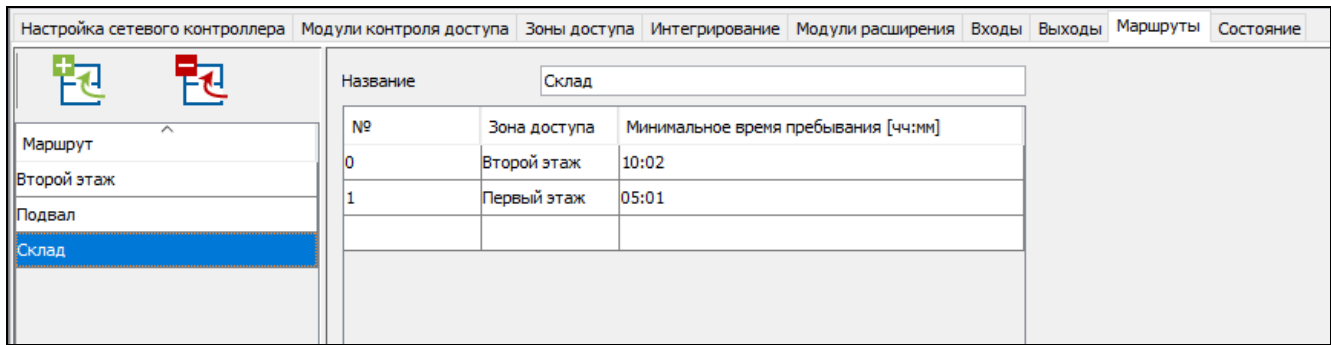


Рис. 34. Закладка «Маршруты».

Таблица для определения маршрута

№ – число, определяющее последовательность зон доступа на маршруте.

Зона доступа – название зоны доступа, входящей в маршрут.

Минимальное время пребывания [мм:сс] – минимальное время пребывания пользователя в данной зоне доступа, по истечении которого он будет в состоянии перейти в очередную зону доступа. Максимальное значение – 59 минут и 59 секунд.

Если в столбце «Зона доступа» отображается название зоны доступа, то после щелчка правой клавишей мыши по строке таблицы отобразится меню:


Вверх – перенос выделенной зоны доступа на одно поле вверх.

Удалить – удаление выделенной зоны доступа из списка.

Вниз – перенос выделенной зоны доступа на одно поле вниз.

4.2.10.3 Удаление маршрута

1. Если Вы хотите удалить один маршрут, выделите выбранный маршрут в списке маршрутов.
2. Если Вы хотите удалить за один раз несколько маршрутов, выделите один из них и, удерживая нажатой клавишу Ctrl, выберите очередные маршруты с помощью левой клавиши мыши.
3. Если Вы хотите удалить все маршруты одновременно, выделите один из них и нажмите одновременно клавиши Ctrl+A.

4. Щелкните мышью по кнопке .

5. Когда отобразится вопрос на подтверждение удаления маршрута, щелкните по «Да».

6. Сохраните введенные изменения.

4.2.11 Состояние

В закладке «Состояние» отображается информация о текущем состоянии: сетевого контроллера, питания, а также выходов сетевого контроллера и модулей расширения.



Если между ACCO Server и сетевым контроллером не будет связи, отобразится информация об отсутствии связи, а также дата и время последнего получения данных сервером от сетевого контроллера.

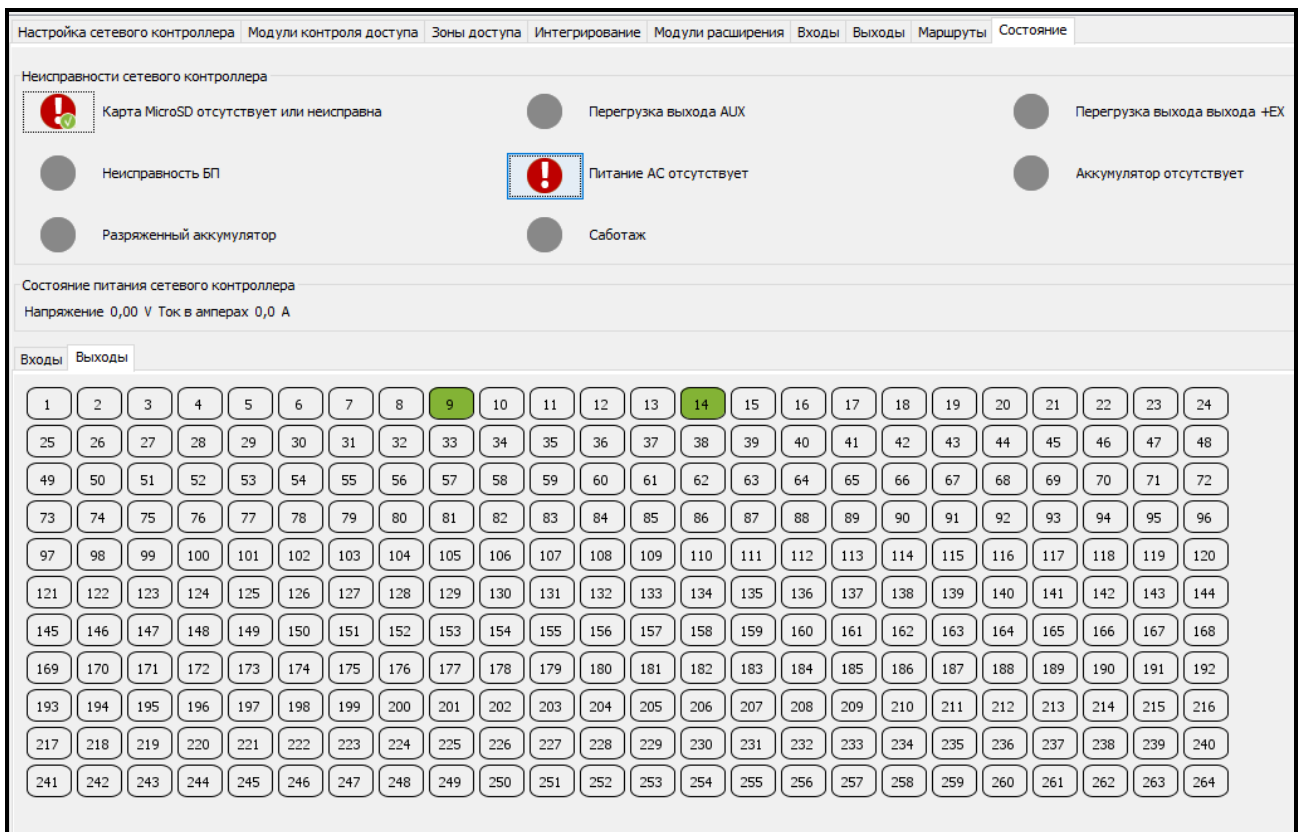








Рис. 35. Закладка «Состояние» для системы.

4.2.11.1 Неисправности сетевого контроллера

В этой области отображаются иконки, сообщающие о:

- неисправности или отсутствию карты MicroSD,
- перегрузке выхода питания AUX,
- перегрузке выхода питания устройств, подключенных к шине модулей расширения +EX,
- неисправности блока питания,
- отсутствию питания АС (переменного тока),
- отсутствию аккумулятора (его наличия или разряда),
- разряженном аккумуляторе,
- саботаже сетевого контроллера.

Отдельные иконки отображают следующие состояния:

-  – все ОК (серый фон),
-  – неисправность (белый восклицательный знак на красном фоне),
-  – подтвержденная неисправность (белый восклицательный знак на красном фоне и белый символ на зеленом фоне),
-  – память неисправности (белый восклицательный знак на сером фоне),
-  – память подтвержденной неисправности (белый восклицательный знак на сером фоне и белый символ на зеленом фоне),
-  – неизвестное состояние (белый вопросительный знак на сером фоне).



Для подтверждения аварии используется находящаяся рядом с ней кнопка.

4.2.11.2 Состояние питания сетевого контроллера

В этой области отображается информация о состоянии питания сетевого контроллера.

4.2.11.3 Закладка «Входы»

В закладке отображается информация о состоянии входов. Цвет означает:
серый – вход неактивен,
зеленый – вход активен.

4.2.11.4 Закладка «Выходы»

В закладке отображается информация о состоянии выходов. Цвет означает:
серый – выход неактивен,
зеленый – выход активен.

4.2.12 Импорт


Кнопка «Импорт» позволяет импортировать данные, касающиеся пользователей и графиков, из программы ACCO-SOFT-LT (файлы с расширением kkd) и из файлов в формате CSV.

4.2.12.1 Импорт данных из файла в формате CSV



Импорт пакета данных, относящихся к нескольким десяткам пользователей, может продолжаться даже от 10 до 20 минут.



1. В главном окне щелкните по кнопке .
2. В открывшемся меню выберите запрос «Импорт из csv».
3. Выберите файл с данными, которые Вы хотите импортировать.
4. В открывшемся окне определите способ шифрования данных.
5. Подберите названия столбцов для импортированных данных. **Для столбца с именами пользователей необходимо выбрать «Название».**
6. Щелкните по кнопке «Проверка», чтобы проверить данные выбранного файла.
7. Если данные правильны, щелкните по кнопке «Импортировать», чтобы запустить процедуру импорта данных. По ее завершении отобразится соответствующее сообщение.
8. Если данные неправильны, выберите другой файл и повторите действия из пунктов 4 - 7.

Набор знаков – выберите набор символов, соответствующий языку импортированного файла.

Разделитель полей – введите символ, который в импортированном файле предназначен для разделения текста по столбцам.

Разделитель строк – введите символ, который в импортированном файле предназначен для разделения текстовых данных.

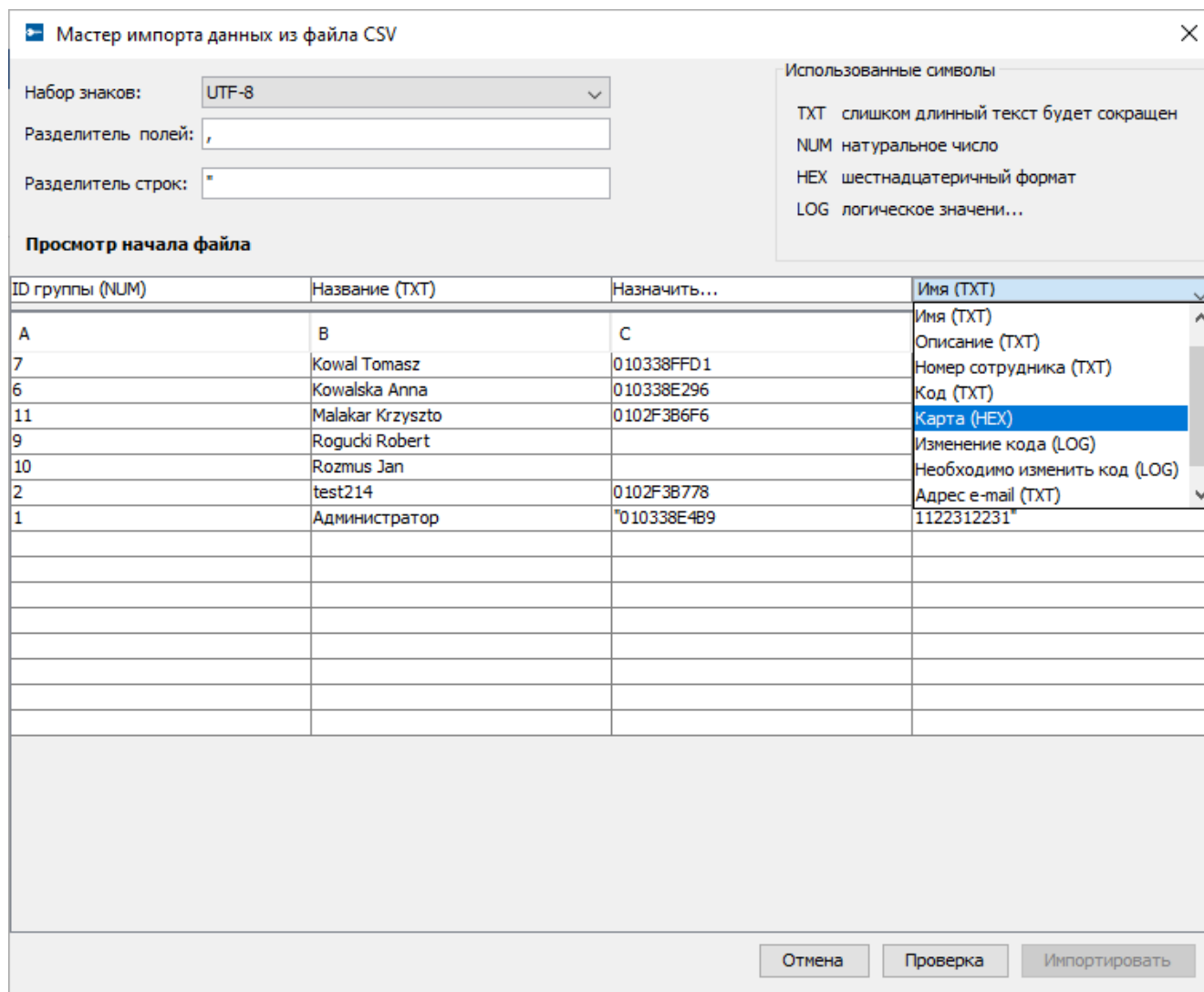


Рис. 36. Окно импорта данных из файла в формате CSV.

Назначить... – щелкните правой клавишей мыши по названию колонки. Отобразится ниспадающее меню со списком ярлыков данных, которые импортированы из файла. Подберите соответствующий ярлык в соответствии с содержанием столбца.


Отмена – щелкните, чтобы отменить введенные изменения.

Проверка – щелкните, чтобы проверить данные в импортированном файле. По завершении проверки отобразится сообщение с информацией о ее результате. Кнопка будет активна после назначения ярлыка «Название» столбцу с импортированными названиями пользователей.

Импортировать – щелкните, чтобы запустить процедуру импорта данных. Кнопка будет активна по завершении проверки данных в импортируемом файле.

4.2.12.2 Импорт данных из файла с расширением kkd



1. В главном окне щелкните по кнопке .
2. В открывшемся меню выберите запрос «Импорт из ACCO-SOFT-LT».
3. Выберите файл с данными, которые Вы хотите импортировать.
4. Если в программе ACCO-SOFT-LT Вы определили свой ключ шифрования, выберите опцию «Нестандартный ключ шифрования» и введите ключ в соответствующее поле. В противном случае не ставьте галочку рядом с полем «Нестандартный ключ шифрования»

5. Определите способ шифрования данных.
6. Определите, какие данные должны импортироваться.
7. Щелкните по кнопке «Продолжить».
8. Откроется окно с информацией об импорте данных (см. рис. 38). Щелкните по кнопке «Импорт», чтобы запустить процедуру импорта данных. По ее завершении отобразится соответствующее сообщение.

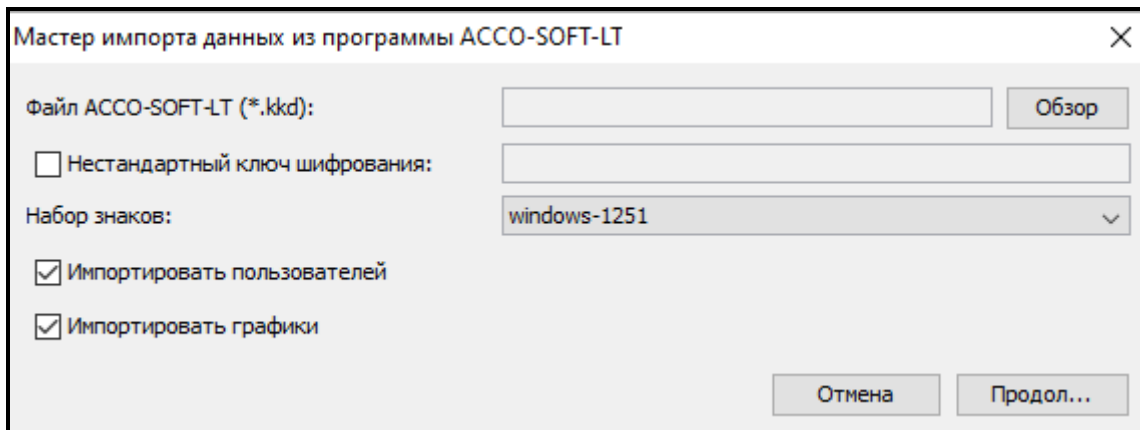


Рис. 37. Окно импорта данных из программы ACCO-SOFT-LT.

Файл ACCO-SOFT-LT (*.kkd) – название файла с данными.

Обзор – щелкните, чтобы указать путь доступа к выбранному файлу с данными.

Нестандартный ключ шифрования – выберите опцию и введите индивидуальный ключ (пароль) шифрования данных конфигурационного файла, который был использован в программе ACCO-SOFT-LT.

Набор знаков – выберите набор символов, соответствующий языку импортируемого файла.

Импортировать пользователей – выберите опцию, если Вы хотите импортировать данные, касающиеся пользователей.

Импортировать расписания – выберите опцию, если Вы хотите импортировать данные, касающиеся графиков. Импортированные данные отобразятся в приложении ACCO Web как графики доступа – недельные и дневные.

Отмена – щелкните, чтобы отменить введенные изменения.

Продолжить – щелкните, чтобы подтвердить введенные данные. Откроется окно с информацией о данных, импортированных из программы ACCO-SOFT-LT (см. рис. 38).

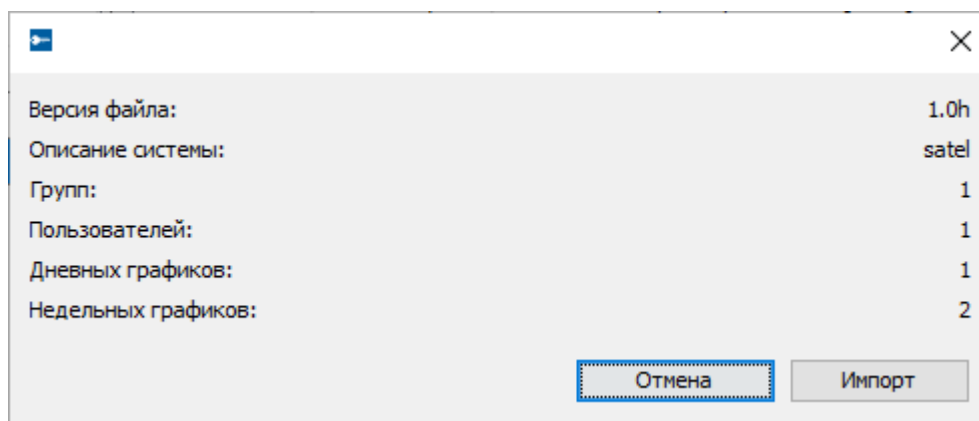


Рис. 38. Окно с информацией о данных, импортированных из программы ACCO SOFT LT.

5. Приложение 1 «Описание интеграции систем»

- Блокировка зоны доступа в СКУД включает режим охраны в разделе (группе) системы охранной сигнализации.
- Восстановление контроля в зоне доступа СКУД выключает режим охраны в разделе системы охранной сигнализации.
- Постановка на охрану раздела системы охранной сигнализации блокирует зону доступа СКУД.
- Выключение режима охраны в разделе системы охранной сигнализации восстанавливает контроль в зоне доступа СКУД.



Если были изменены настройки модулей контроля доступа при включенном режиме охраны, то после сохранения новых настроек режим охраны будет выключен автоматически.

Можно включить режим охраны в разделе (группе) системы охранной сигнализации:

- заблокировав зону доступа СКУД с помощью программы ACCO Soft или приложения ACCO Web,
- заблокировав точку прохода с помощью терминала входа в эту зону; для этого терминала должна быть включена опция «Управляет зоной доступа»,
- заблокировав точки прохода, контролируемые модулями контроля доступа данной зоны доступа (только при соответствующей конфигурации терминалов, подключенных к модулям контроля доступа).



Зона контроля доступа может быть заблокирована только с помощью терминала входа, для которого была включена опция «Управляет зоной доступа». С помощью терминала выхода можно блокировать только дверь (блокировка всех дверей в зоне доступа блокирует зону доступа).

Если зона доступа заблокирована, и ей назначено несколько модулей контроля доступа, то попытка пользователя с полномочием «Переключение» получить доступ к двери, приведет к изменению состояния зоны доступа на «Разного типа» и к предоставлению доступа.

При разблокировке зоны доступа с помощью программы ACCO Soft или приложения ACCO Web зона доступа будет снята с охраны.

При разблокировке с помощью программы ACCO Soft или приложения ACCO Web точки прохода в зоне доступа, находящейся под охраной, эта зона доступа по-прежнему будет находиться под охраной.

В случае интеграции изменение состояния раздела (группы) системы охранной сигнализации влияет на состояние зоны доступа СКУД. Например: объект разделен на две зоны доступа. Каждой из них назначено по две точки прохода, из чего одна общая. Обе зоны доступа СКУД интегрированы с разделами системы охранной сигнализации (как на рис. 39). В случае, если:

- раздел системы охранной сигнализации ставится на охрану, все точки прохода, назначенные интегрированной зоне доступа СКУД, блокируются,
- раздел системы охранной сигнализации снимается с охраны:
 - проверяется текущее состояние соседнего раздела. Если соседний раздел поставлен на охрану, то общая точка прохода обеих зон останется заблокированной.

- проверяется текущее состояние общей точки прохода обеих зон. Если она разблокирована, то останется разблокированной.

В остальных случаях контроль точки прохода будет восстановлен.

Раздел (группу) системы охранной сигнализации можно снять с охраны, восстановив дежурный режим в зоне контроля доступа.


Тревоги из системы охранной сигнализации могут передаваться в СКУД (см. опции «Отправить тревогу взлома из раздела INTEGRA» и «Отправить пожарную тревогу из раздела INTEGRA»). Тревога, вызванная в системе охранной сигнализации, может быть удалена только в системе охранной сигнализации.

Тревоги из СКУД не передаются в систему охранной сигнализации.

Подробную информацию можно найти в приложении «Интегрированные зоны».

6. Приложение 2 «Интегрированные зоны»

Чтобы поставить систему на охрану, можно заблокировать зону СКУД:

- с помощью считывателя, работающего в качестве терминала входа, подключенного к одному из модулей контроля доступа в зоне доступа; для этого терминала должна быть включена опция «Управляет зоной доступа»,
- с помощью ПО ACCO Soft – в закладке «Зоны доступа» необходимо выбрать зону доступа в списке зон, нажать правую клавишу мыши и из открывшегося меню выбрать функцию «Заблокировать»,
- с помощью приложения ACCO Web – в меню с левой стороны выберите «Управление», затем «Структура», перейдите к закладке «Зоны доступа», выберите выбранную зону доступа в списке и щелкните по кнопке ,
- с помощью приложения ACCO Web – в меню с левой стороны выберите «Карты», откройте соответствующую карту, подведите курсор к выбранной зоне доступа, щелкните левой клавишей мыши и выберите функцию «Заблокировать»,
- по запрограммированному времени или назначенному графику доступа – в программе ACCO Soft в закладке «Зоны доступа» выберите зону доступа из списка, перейдите к закладке «Опции» и с помощью функции «Блокировка зоны доступа» определите время или назначьте график доступа,
- активацией входа сетевого контроллера ACCO-NT – в ПО ACCO Soft в закладке «Входы» запрограммируйте выбранный вход как «Блокировка зоны доступа»,




Пользователь может заблокировать зону доступа, только если:

- использует терминал входа, для которого включена опция «Управляет зоной доступа»,
- ему назначено полномочие «Переключение»,
- согласно назначенному ему графику доступа ему предоставлен доступ к данной зоне доступа.

Определенное время и запрограммированный график доступа не имеют приоритета. Это означает, что возникновение других событий в модуле может изменить состояние зоны доступа до истечения запрограммированного времени блокировки.

Если для данного терминала будет выбран одинаковый тип идентификатора для получения доступа и для блокировки, то после использования идентификатора доступ будет разрешен. Состояние точки прохода / зоны доступа не изменится.

Чтобы снять систему с охраны, можно восстановить контроль в зоне доступа СКУД:

- с помощью считывателя, работающего в качестве терминала входа, подключенного к одному из модулей контроля доступа в зоне доступа; для этого терминала должна быть включена опция «Управляет зоной доступа»,
- с помощью ПО ACCO Soft – в закладке «Зоны доступа» подведите курсор к выбранной зоне в списке, щелкните правой клавишей мыши и в открывшемся меню выберите функцию «Восстановить контроль»,
- с помощью приложения ACCO Web – в меню с левой стороны выберите «Управление», затем «Структура», перейдите к закладке «Зоны доступа», выберите выбранную зону доступа в списке и щелкните по кнопке ,
- с помощью приложения ACCO Web – в меню с левой стороны щелкните по команде «Карты», откройте соответствующую карту, подведите курсор к зоне доступа на карте, щелкните левой клавишей мыши и выберите функцию «Восстановить контроль»,
- после восстановления нормального состояния нарушенного входа сетевого прибора ACCO-NT (запрограммированного как «Блокировка зоны доступа»),



Пользователь может восстановить дежурный режим в зоне доступа, только если:

- он использует терминал входа, для которого включена опция «Управляет зоной доступа»,
- ему назначено полномочие «Переключение»,
- согласно назначенному ему графику доступа ему предоставлен доступ к данной зоне доступа.

Если для данного терминала будет выбран одинаковый тип идентификатора для получения доступа и для блокировки, то после использования идентификатора доступ будет разрешен. Состояние точки прохода / зоны доступа не изменится.

6.1 Примеры

6.1.1 Пример 1

Пояснения к рисунку 39:

1 и **2** (номера на черном фоне) – зоны доступа СКУД, интегрированные с разделами (группами) системы охранной сигнализации.

D1 – модуль контроля доступа, назначенный зоне доступа 1. Терминал А – это вход в зону доступа 1, терминал Б – это выход из зоны доступа 1.

D2 – модуль контроля доступа, назначенный зонам доступа 1 и 2. Терминал А – это вход в зону доступа 2 и выход из зоны доступа 1. Терминал Б – это выход из зоны доступа 2 и вход в зону доступа 1.

D3 – модуль контроля доступа, назначенный зоне доступа 2. Терминал А – это вход в зону доступа 2, а терминал Б – это выход из зоны доступа 2.



Рис. 39. Пример зон доступа СКУД, интегрированных с разделами (группами) системы охранной сигнализации.

Постановка на охрану



С целью постановки на охрану раздела (группы) системы охранной сигнализации следует заблокировать зону доступа СКУД. Это можно сделать только с помощью терминала входа в эту зону доступа. Для этого терминала должна быть включена опция «Управляет зоной доступа».

Управление зоной доступа 1

Если Вы хотите поставить на охрану зону доступа 1, используйте терминал А точки прохода D1 или терминал Б точки прохода D2.

Управление зоной доступа 2

Если Вы хотите поставить на охрану зону доступа 2, используйте терминал А точки прохода D2 или терминал А точки прохода D3.

Снятие с охраны



С целью снятия с охраны раздела системы охранной сигнализации следует восстановить контроль в зоне доступа СКУД. Это можно сделать только с помощью терминала входа в эту зону доступа. Для этого терминала должна быть включена опция «Управляет зоной доступа».

Управление зоной доступа 1

Если Вы хотите снять с охраны зону доступа 1, используйте терминал А точки прохода D1 или терминал Б точки прохода D2.

Управление зоной доступа 2

Если Вы хотите снять с охраны зону доступа 2, используйте терминал А точки прохода D2 или терминал А точки прохода D3.

6.2 Сигнализация блокировки точки прохода / зоны доступа устройствами СКУД

Описание дополнительной сигнализации, связанной с интеграцией систем.

6.2.1 Оптическая сигнализация

6.2.1.1 Приоритеты состояний системы ACCO NET


Если в системе ACCO NET одновременно возникли события различного типа, светодиоды в устройствах СКУД сообщают о них согласно следующему приоритету (устройство сообщает о событии с самым высоким приоритетом):


1. Нет связи между сетевым контроллером ACCO-NT и модулем контроля доступа ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS или ACCO-KP2.
2. Блокировка точки прохода из-за тревоги взлома.
3. Блокировка точки прохода.
4. Разблокировка точки прохода из-за пожарной тревоги.
5. Разблокировка точки прохода.
6. Ошибка интеграции (см. описание таблицы со списком систем охранной сигнализации в закладке «Интеграция», графа «Состояние»).

6.2.1.2 Клавиатуры


После блокировки точки прохода / зоны доступа на дисплее клавиатуры может отобразиться название пользователя, который запустил эту функцию.



Светодиодная индикация состояния точки прохода / зоны доступа:

 (красный цвет) – светодиод горит, сигнализируя тревогу, если в системе охранной сигнализации была вызвана тревога взлома или пожарная тревога. Сигнализация тревоги продолжается в течение 10 секунд (также звуковая сигнализация). По истечении этого времени светодиод начинает мигать, сигнализируя память тревоги. После устранения причины тревоги сигнализацию памяти тревоги в клавиатуре можно сбросить, подтвердив память тревоги в ПО ACCO Soft или в приложении ACCO Web.

 (желтый цвет):




- светодиод горит – точка прохода / зона доступа заблокирована, интегрированный раздел (группа) поставлен на охрану,
- светодиод медленно мигает – точка прохода заблокирована из-за тревоги взлома в системе охранной сигнализации.

 (зеленый цвет) – светодиод медленно мигает, когда точка прохода разблокирована из-за пожарной тревоги в системе охранной сигнализации.

 (желтый цвет) и  (зеленый цвет):

- светодиоды медленно мигают по очереди – ошибка интеграции,
- светодиоды быстро мигают по очереди – отсутствие связи между сетевым контроллером ACCO-NT и модулем контроля доступа ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS или ACCO-KP2.

6.2.1.3 Клавиатура со считывателем бесконтактных карт

Светодиодная индикация клавиатуры (светодиоды ,  и ) аналогична индикации остальных клавиатур.

6.2.1.4 Считыватели бесконтактных карт

Двухцветный светодиод в считывателях CZ-EMM и CZ-EMM2 сигнализирует состояние точки прохода / зоны доступа следующим образом:

- медленные вспышки зеленого цвета – точка прохода разблокирована из-за пожарной тревоги в системе охранной сигнализации,

- медленные вспышки красного цвета – точка прохода / зона доступа заблокирована, интегрированный раздел (группа) поставлен на охрану, или точка прохода заблокирована из-за тревоги взлома в системе охранной сигнализации,
- медленные вспышки зеленого и красного цвета – ошибка интеграции,
- быстрые вспышки зеленого и красного цвета – нет связи между сетевым контроллером ACCO-NT и модулем контроля доступа ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS или ACCO-KP2.

Светодиодная индикация состояния точки прохода / зоны доступа в считывателях CZ-EMM3 и CZ-EMM4:

- медленные вспышки зеленого цвета – точка прохода разблокирована из-за пожарной тревоги в системе охранной сигнализации,
- медленные вспышки красного цвета – точка прохода / зона доступа заблокирована, интегрированный раздел поставлен на охрану, или точка прохода заблокирована из-за тревоги взлома в системе охранной сигнализации,
- медленные вспышки зеленого и красного цвета – ошибка интеграции,
- быстрые вспышки зеленого и красного цвета – нет связи между сетевым контроллером ACCO-NT и модулем контроля доступа ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS или ACCO-KP2.

6.2.1.5 Считыватель ключей DALLAS iButton

Светодиодная индикация состояния точки прохода / зоны доступа в считывателях с помощью двухцветного светодиода:

- медленные вспышки зеленого цвета – точка прохода разблокирована из-за пожарной тревоги в системе охранной сигнализации,
- медленные вспышки красного цвета – точка прохода / зона доступа заблокирована, интегрированный раздел (группа) поставлен на охрану, или точка прохода заблокирована из-за тревоги взлома в системе охранной сигнализации,
- медленные вспышки зеленого и красного цвета – ошибка интеграции,
- быстрые вспышки зеленого и красного цвета – нет связи между сетевым контроллером ACCO-NT и модулем контроля доступа ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS или ACCO-KP2.

6.2.2 Звуковая сигнализация

Устройства, совместимые с модулями ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS или ACCO-KP2 (клавиатура, клавиатура со считывателем бесконтактных карт и считыватель бесконтактных карт) генерируют:

Продолжительный звуковой сигнал каждые 3 секунды, завершённый серией коротких звуковых сигналов продолжительностью в 10 секунд и 1 продолжительным звуковым сигналом – отсчет задержки на выход (если время короче 10 секунд, то будет сгенерирована только завершающая серия коротких звуковых сигналов).

Постоянный звуковой сигнал– тревога.

2 коротких звуковых сигнала каждую секунду – отсчет времени на вход или восстановление точки прохода / зоны доступа, то есть снятие с охраны раздела.

1 короткий звуковой сигнал и 2 коротких звуковых сигнала – предоставление доступа, затем блокировка точки прохода / зоны доступа, то есть постановка раздела (группы) на охрану.