

Программно-аппаратный комплекс

«Модуль для модернизации МИБ 101»

Версия документа 1.0

Руководство администратора

Версия приложения 0.2.5

СОДЕРЖАНИЕ

1. Введение	4
2. Общие сведения	5
3. Требования к уровню подготовки администратора	6
4. Подготовка к работе	7
4.1. Конфигурирования локальных DNS	7
4.2. Проверка конфигурации локальных DNS	8
4.3. Выпуск сертификатов	8
4.4. Установка IP-адреса Контроллера	8
4.5. Установка стандартных паролей учетных записей Контроллера	9
5. Начало работы	11
5.1. Настройка IP-адреса	14
5.2. Загрузка сертификата и ключа шифрования	16
5.3. Установка пароля Суперпользователя	19
5.4. Смена пароля Администратора Системы	21
5.5. Синхронизация системного времени с сервером NTP	22
5.6. Ручная установка даты и времени	24
5.7. Установка часового пояса	26
6. Обновление программного обеспечения	28
6.1. Обновление прошивки Контроллера	28
6.2. Обновление системного ПО Модуля	33
6.3. Обновление прикладного ПО Модуля	36
7. Обеспечение ИБ. Идентификация и аутентификация	38
7.1. Настройка парольной политики	38
7.2. Самостоятельная смена пароля пользователем	41
7.3. Встроенные учетные записи	42
7.3.1. Учетная запись Администратора Системы	42
7.3.2. Учетная запись Суперпользователя	44
7.3.3. Учетная запись POS протокола	45
8. Обеспечение ИБ. Управление доступом	47
8.1. Система ролевого управления доступом	47
8.1.1. Создание пользователя с назначенной ролью	47
8.1.2. Разблокировка или блокировка пользователя	50
8.1.3. Изменение роли пользователя	52

8.1.4.	<i>Изменение пароля пользователя</i>	54
8.1.5.	<i>Удаление пользователя</i>	55
8.2.	Ограничение доступа к интерфейсу администрирования	57
8.3.	Ограничение доступа к конфигурационным и временным файлам	57
8.4.	Ограничение доступа к интерфейсу просмотра журнала событий	58
8.5.	Настройка длительности периода неактивности для автоматической блокировки сессии	58
8.6.	Матрица доступа	59
8.7.	Удаленный доступ по SSH.....	62
8.8.	Удаленный доступ для POS протокола	64
9.	Обеспечение ИБ. Регистрация и учет событий ИБ	66
9.1.	Регистрация успешных/неуспешных попыток доступа	67
9.2.	Меры защиты журнала регистрации событий ИБ	68
10.	Обеспечение ИБ. Прочие сведения	70
10.1.	Информация о фактическом состоянии объектов аудита ИБ	70
10.2.	Сведения о сетевых параметрах	71
10.3.	Сведения о взаимодействии с сетью Интернет.....	72
10.4.	Сведения о хранении и передаче паролей (ключей).....	72
10.5.	Требования по обеспечению безопасности применения	73
ПРИЛОЖЕНИЕ А. Используемые сокращения		75
ПРИЛОЖЕНИЕ Б. История изменений в документе		76

1. ВВЕДЕНИЕ

Настоящий документ является руководством администратора программно-аппаратного комплекса «Модуль для модернизации МИБ 101» (далее по тексту – Модуль). Документ содержит базовую информацию о Модуле: его функциональность, запуск и завершение работы программного обеспечения Модуля, а также описание рабочего меню и средства организации работы.

Настоящий документ не затрагивает аспекты извлечения и монтажа Модуля в шкаф контроллера, подключения его к сетям электропитания и передачи информации. По данным вопросам обратитесь к руководству пользователя.

Модуль предназначен для модернизации контроллеров сопряжения оборудования АЗС различных марок и моделей «Gilbarco DOMS PSS 5000» с процессорной платой 505-й серии и контроллера «МАК 6000», в целях обеспечения поддержки современных операционных систем, браузеров на основе Chromium, соответствия встроенной операционной системы актуальным требованиям к информационной безопасности.

2. ОБЩИЕ СВЕДЕНИЯ

Модуль устанавливается в шкаф контроллера сопряжения, на место (взамен) штатного модуля «DCB-460» контроллера сопряжения «Gilbarco DOMS PSS 5000» или на место (взамен) штатного модуля «МК00» контроллера сопряжения «МАК 6000».

Современная операционная система Модуля встроенными средствами выполняет прозрачную трансляцию портов и протоколов, которые соответствуют актуальным требованиям к информационной безопасности информационной системы контроллера, и осуществляет перехват портов и протоколов, которые не соответствуют актуальным требованиям. Любые другие, неописанные порты и протоколы, включая недокументированные, операционная система Модуля отбрасывает (не пропускает между сетевыми интерфейсами). Перехваченные пакеты операционная система Модуля обрабатывает в соответствии с заложенным в нее алгоритмом.

3. ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ АДМИНИСТРАТОРА

Настоящее руководство предназначено для технических специалистов, обладающих базовыми знаниями и навыками по системному и прикладному администрированию, сетевым технологиям, информационной безопасности.

Допуск специалистов к выполнению работ с Модулем должен регулироваться внутренними документами эксплуатирующей организации.

4. ПОДГОТОВКА К РАБОТЕ

Перед началом работы необходимо выполнить определенные обязательные действия как на Контроллере, так и в информационной системе эксплуатирующей организации.

Необходимые действия обязательны для успешной интеграции Модуля в информационную систему эксплуатирующей организации. Указанные действия носят обратимый характер, что в случае выявления в процессе эксплуатации Модуля критических ошибок, позволит, на время устранения ошибок, оперативно откатиться к первоначальной конфигурации системы.

4.1. Конфигурирования локальных DNS

Администрирование Контроллера с Модулем осуществляется посредством веб-браузера по защищенному протоколу HTTPS. Чтобы подготовить веб-сервер Системы для обработки HTTPS-соединений, администратор должен получить и установить в систему сертификат открытого и закрытого ключа для каждой Системы, но перед этим прописать в локальном DNS сервере соответствие текущего ip-адреса Системы вымышленному доменному для каждой Системы имени локального домена.

Пример DNS записи может быть следующим:

```
192.168.1.54 mak6000.sbgroun.ru
```

4.2. Проверка конфигурации локальных DNS

Перед выпуском сертификатов следует убедиться, что прописанные DNS записи применились на нужных хостах. Для проверки можно, например, использовать команду ping:

```
D:\>ping mak6000.sbgrouр.ru

Обмен пакетами с mak6000.sbgrouр.ru [192.168.1.54] с 32 байтами данных:
Ответ от 192.168.1.54: число байт=32 время<1мс TTL=128
```

4.3. Выпуск сертификатов

Модуль поддерживает сертификаты ключей формата X.509. Для назначенного Системе доменного имени необходимо в локальном центре сертификации выпустить ключи в кодировке PEM, со следующими именами:

cert.pem – файл сертификата;

key.pem – файл ключа.

Действия администратора по выпуску сертификатов и их перевод в указанную кодировку требуют знаний, являющимися общедоступными и не описываются в настоящем руководстве.

4.4. Установка IP-адреса Контроллера

IP-адрес Контроллера должен иметь фиксированное значение по умолчанию – 10.10.10.100 и маску подсети 255.255.255.0.

Для установки IP-адреса Контроллера по умолчанию подключитесь к порту 41 Контроллера напрямую, минуя Модуль, и войдите в веб-интерфейс под учетной записью администратора.

В веб-интерфейсе раскройте меню 2 Installation --> 2.3 Communication Setup --> TCP/IP Setup, и впишите стандартные значения в соответствующие поля, затем нажмите кнопку Применить/ACCEPT:

IP Address

<input type="radio"/>	Obtain IP address automatically (using DHCP)
<input checked="" type="radio"/>	Specify an IP address
IP Address:	<input type="text" value="10.10.10.100"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="10.10.10.6"/>
MAC Address:	<input type="text" value="00-50-55-01-17-C6"/>

Установку IP-адреса Контроллера по умолчанию так же возможно произвести через клавиатуру платы центрального процессора Контроллера, минуя сетевое подключение к порту 41. За более подробной информацией обратитесь к руководству на Контроллер.

4.5. Установка стандартных паролей учетных записей Контроллера

Интеграция нового Модуля требует возврат паролей на Котроллере к установкам по умолчанию. По умолчанию должны быть установлены следующие пароли:

admin:password
host:password
manager:password
service:password

guest:password

Для установки заводских паролей подключитесь к порту 41 Контроллера напрямую, минуя Модуль, и войдите в веб-интерфейс под учетной записью администратора.

В веб-интерфейсе раскройте меню 2 Installation --> 2.4 System Profile --> 2.4.1 Password, откроется следующее меню:

Select user:

Enter old password

Enter new password

Enter new password again

OK

Выберите из выпадающего списка всех пользователей по очереди, и установите им заводской пароль по умолчанию – password. За более подробной информацией обратитесь к руководству на Контроллер.

5. НАЧАЛО РАБОТЫ

Управление Модулем и Контроллером, с установленным Модулем (далее по тексту совместно - Система), осуществляется оператором через веб-интерфейс с использованием следующих веб-браузеров актуальных версий:

- Google Chrome;
- Яндекс Браузер;
- Браузер Chromium-Gost;
- Спутник Браузер.

Разработчик не гарантирует полной работоспособности каждой отдельной версии различных браузеров, в связи с постоянно вносимыми изменениями разработчиками браузеров.

Для начала работы с требуется зайти на веб-страницу по IP-адресу Системы (IP-адрес, установленный на заводе-изготовителе по умолчанию – 192.168.2.1), ввести следующие логин и пароль:

`admin:$uperAdmin1!`

после чего произойдет автоматический переход в веб-консоль управления Системой.

При отсутствии действующего сертификата, загруженного в Модуль, и до момента загрузки в Модуль актуального сертификата, доступ к веб-странице производится по незащищенному протоколу HTTP. Процедура загрузки сертификата описана в текущем разделе далее по тексту.

Диалоговое окно входа в консоль изображено на снимке экрана:



Логин

admin

Пароль

.....

Войти

После прохождения процедуры аутентификации в Системе откроется главный экран, который визуально разделен на два блока. Сверху находится навигационное меню Модуля, под ним находится окно (фрейм) Модуля, в которое инкапсулирован интерфейс Контроллера. Главный экран Системы изображен на снимке экрана ниже:



PSS 5000 Service Menu

- ▶ 1 Information
- ▶ 2 Installation
- ▶ 3 Operation
- ▶ 4 Reset
- ▶ 5 Diagnostics
- ▶ W W & M

06.03.2025 15:14 UTC+3



[Администрирование](#)

[Настройки](#)

[О системе](#)

[admin](#)



PSS 5000 Service Menu

Select a function on the left.

Site: "61931270"

Program: 410-38-2.77

License Key Management Status:

EXTENDED_INFO: Offered
WD_ATC: Offered

Интерфейс Контроллера, инкапсулированный в окно Модуля, полностью его повторяет, за исключением некоторых функций, перенесенных в разделы управления Системой. Детальная информация о таких функциях содержится в настоящем руководстве в соответствующих разделах, пунктах и подпунктах.

Верхняя строка, предназначенная для управления функциями Системы, состоит из следующих блоков меню (слева на право):

1. Пиктограмма в виде изображения домика. При нажатии возвращает в главное меню Системы. В этом разделе меню обеспечивается доступ к веб-интерфейсу Контроллера.
2. Блок «Администрирование» предоставляет возможность доступа к журналу событий, управления пользователями, настройке парольной политики, настройки сокрытия конфигураций оборудования, настройки длительности сессии при неактивности Пользователя, настройки политики блокировки учетных записей, обновления программного обеспечения Контроллера, и др.
3. Блок «Настройки» предназначен для доступа к системным настройкам Модуля, таких как: настройка параметров сети, открытие доступа к Модулю по протоколу ssh, ручная установка даты и времени, установка часового пояса, настройка автоматической синхронизации с NTP-сервером, обновление прошивки Модуля, загрузка сертификатов и ключей, настройка доступа по портам, смена пароля суперпользователя, и др.

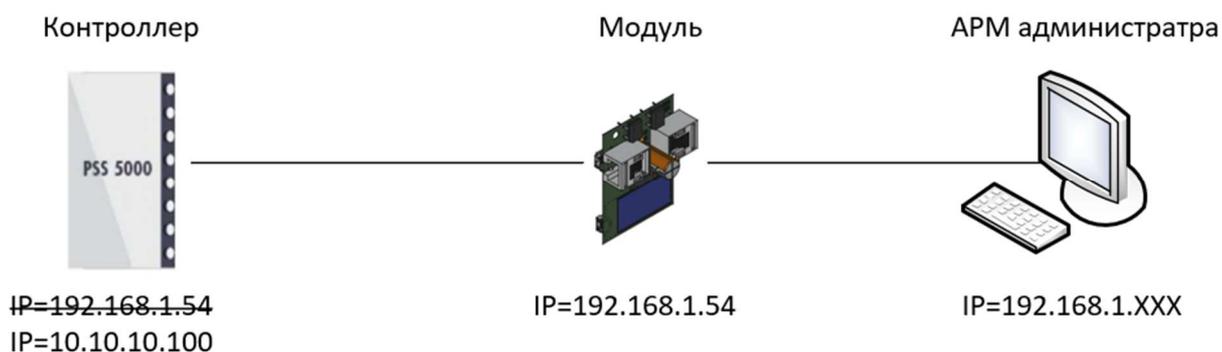
4. Блок «О системе» предназначен для отображения информации о Модуле, такой как: аппаратная версия модуля, серийный номер модуля, версия системного ПО, версия прикладного ПО, и др.
5. Блок %USER% (на снимке экрана – «Admin») предназначен для доступа к функции самостоятельной смены пароля текущего пользователя Системы.
6. Пиктограмма в виде изображения кружочка со стрелочкой. При нажатии происходит немедленное прекращение сессии текущего пользователя Системы.

Далее критически важно выполнить указанные в данном пункте действия, а именно: смена пароля Администратора, установка пароля Суперпользователя, загрузка сертификата и ключа, настройка IP-адреса.

5.1. Настройка IP-адреса

Системе требуется назначить IP-адрес, который был ранее назначен Контроллеру, до момента возврата к заводским настройкам IP-адреса Контроллера.

Допустим, что Контроллеру, до установки Модуля был назначен следующий IP-адрес: 192.168.1.54. В процессе модернизации Контроллера, его IP-адрес был возвращен к заводским значениям, а именно: 10.10.10.100. На данном шаге Модулю требуется назначить IP-адрес: 192.168.1.54. Для пояснения ниже приведена схема условной IP-адресации типовой информационной системы:



Для настройки IP-адреса из главного меню Системы перейдите в блок «Настройки», и введите пароль Суперпользователя. Пароль Суперпользователя по умолчанию отсутствует, при первом входе просто нажмите «Войти». Диалоговое окно входа в блок «Настройки» изображено на снимке экрана:

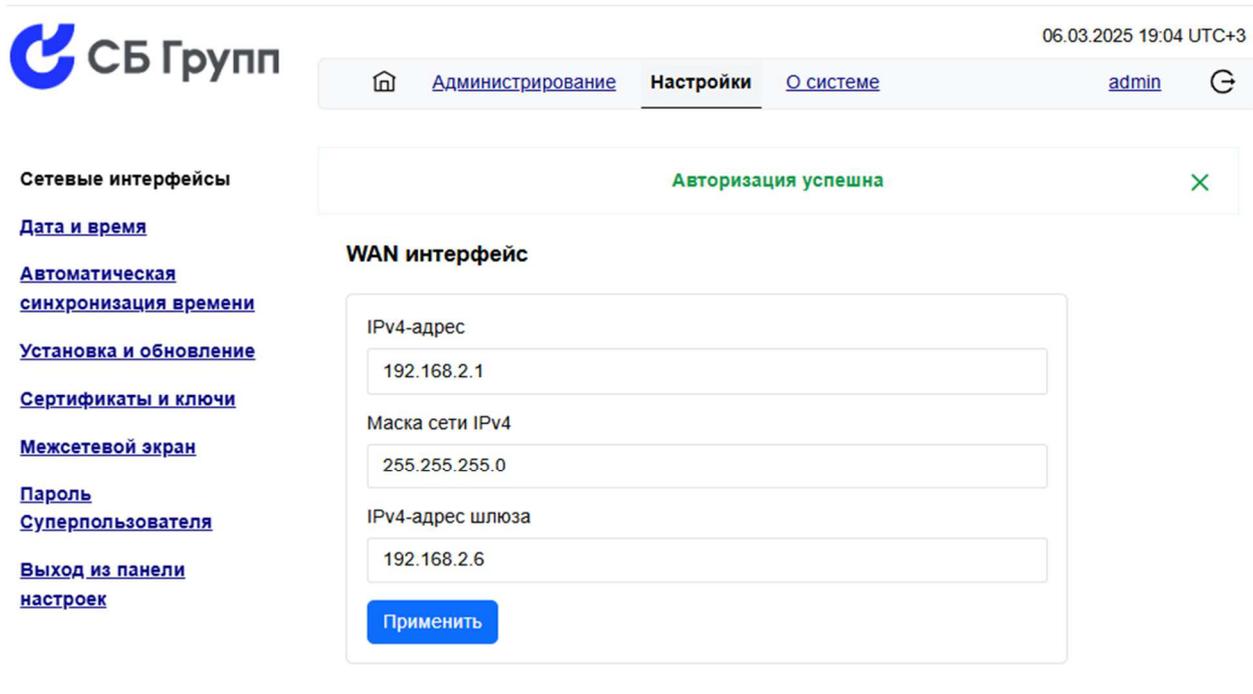
Вход в панель настроек

Логин

Пароль

Войти

В случае успешной авторизации в Модуле под учетной записью Суперпользователя вы попадаете в блок системных настроек Модуля:



06.03.2025 19:04 UTC+3

[Администрирование](#) **Настройки** [О системе](#) [admin](#)

Сетевые интерфейсы

[Дата и время](#)

[Автоматическая синхронизация времени](#)

[Установка и обновление](#)

[Сертификаты и ключи](#)

[Межсетевой экран](#)

[Пароль Суперпользователя](#)

[Выход из панели настроек](#)

Авторизация успешна

WAN интерфейс

IPv4-адрес
192.168.2.1

Маска сети IPv4
255.255.255.0

IPv4-адрес шлюза
192.168.2.6

Применить

Введите в соответствующее поле IP-адрес 192.168.1.54. При необходимости измените маску сети и пропишите шлюз. Нажмите кнопку «Применить» и закройте окно браузера.

Далее вход в Систему следует производить по локальному доменному имени. В настоящем документе, для примера, используется условное доменное имя – `mak6000.sbgroun.ru`.

5.2. Загрузка сертификата и ключа шифрования

Загрузка файлов сертификата и закрытого ключа требуется для обеспечения работы расширения протокола HTTP, применяемого для защиты трафика между веб-интерфейсом Системы и хостом, в целях повышения безопасности.

Загрузка сертификата (файл – `cert.pem`) и закрытого ключа (файл – `key.pem`) осуществляется через веб-интерфейс Системы. Для этого из главного меню Системы перейдите в блок «Настройки», и введите пароль Суперпользователя. Пароль Суперпользователя по умолчанию

отсутствует, при первом входе просто нажмите «Войти». Диалоговое окно входа в блок «Настройки» изображено на снимке экрана:

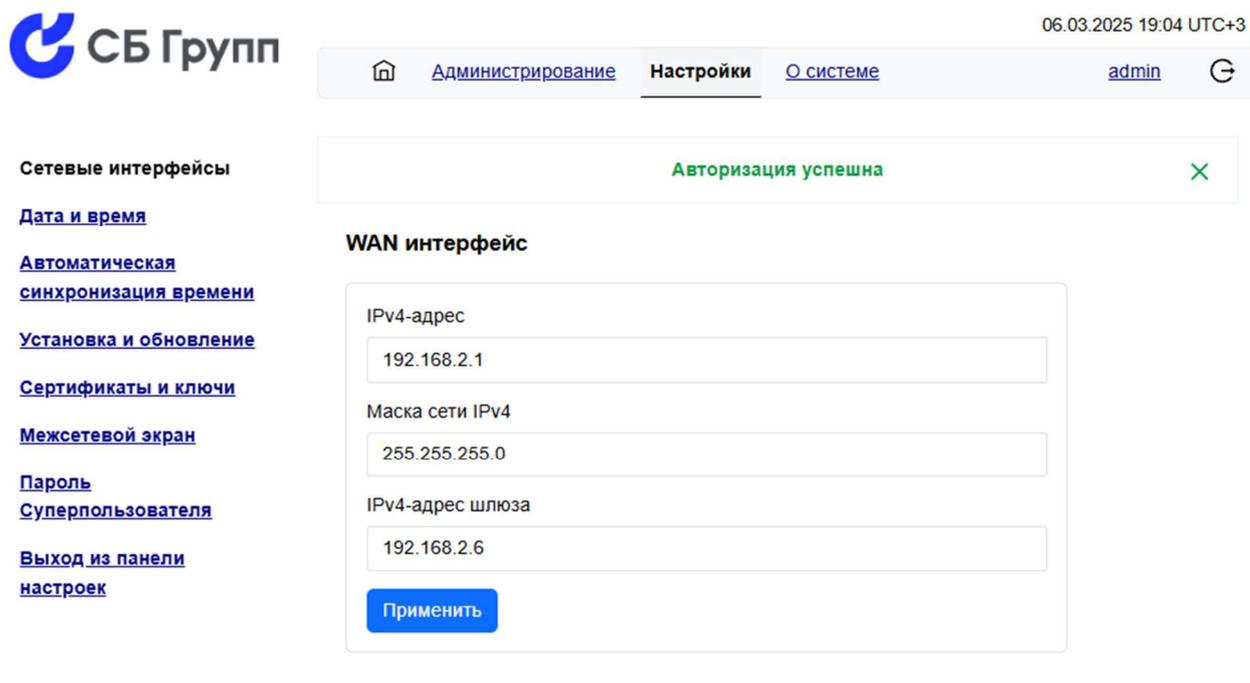
Вход в панель настроек

Логин

Пароль

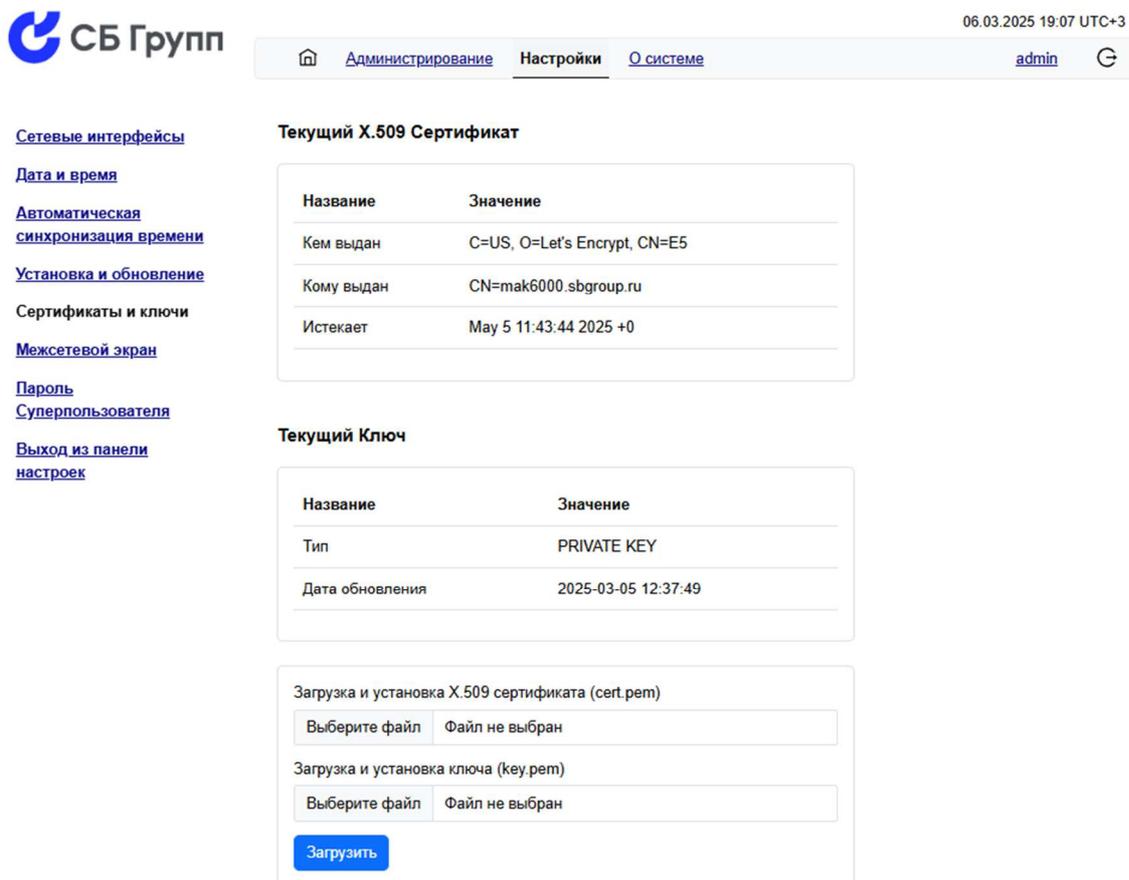
Войти

В случае успешной авторизации в Модуле под учетной записью Суперпользователя вы попадаете в раздел системных настроек Модуля:



С левой стороны расположено меню системных настроек Модуля. Нажмите в меню слева пункт «Сертификаты и ключи», после чего будет

осуществлен переход на страницу загрузки файлов сертификата, как показано на снимке экрана:



The screenshot shows the administration interface of the SB Group system. The top navigation bar includes the logo, the text 'СБ Групп', and the date '06.03.2025 19:07 UTC+3'. The main menu contains 'Администрирование', 'Настройки', and 'О системе'. The user is logged in as 'admin'. The left sidebar lists various system settings like 'Сетевые интерфейсы', 'Дата и время', 'Автоматическая синхронизация времени', 'Установка и обновление', 'Сертификаты и ключи', 'Межсетевой экран', 'Пароль Суперпользователя', and 'Выход из панели настроек'. The main content area is divided into two sections: 'Текущий X.509 Сертификат' and 'Текущий Ключ'. The 'Текущий X.509 Сертификат' section displays a table with the following data:

Название	Значение
Кем выдан	C=US, O=Let's Encrypt, CN=E5
Кому выдан	CN=mak6000.sbggroup.ru
Истекает	May 5 11:43:44 2025 +0

The 'Текущий Ключ' section displays a table with the following data:

Название	Значение
Тип	PRIVATE KEY
Дата обновления	2025-03-05 12:37:49

Below these tables, there are two file upload sections. The first is for 'Загрузка и установка X.509 сертификата (cert.pem)' with a 'Выберите файл' button and a 'Файл не выбран' status. The second is for 'Загрузка и установка ключа (key.pem)' with a 'Выберите файл' button and a 'Файл не выбран' status. A blue 'Загрузить' button is located at the bottom of these sections.

Нажмите на «выбрать файл» сначала сертификата (cert.pem), затем то же действие проделайте для файла закрытого ключа (key.pem), при этом указав на места расположения соответствующих файлов. Нажмите на кнопку «Загрузить».

Дождитесь появления надписи об успешной загрузке:

Файлы успешно загружены, ожидайте перезагрузки

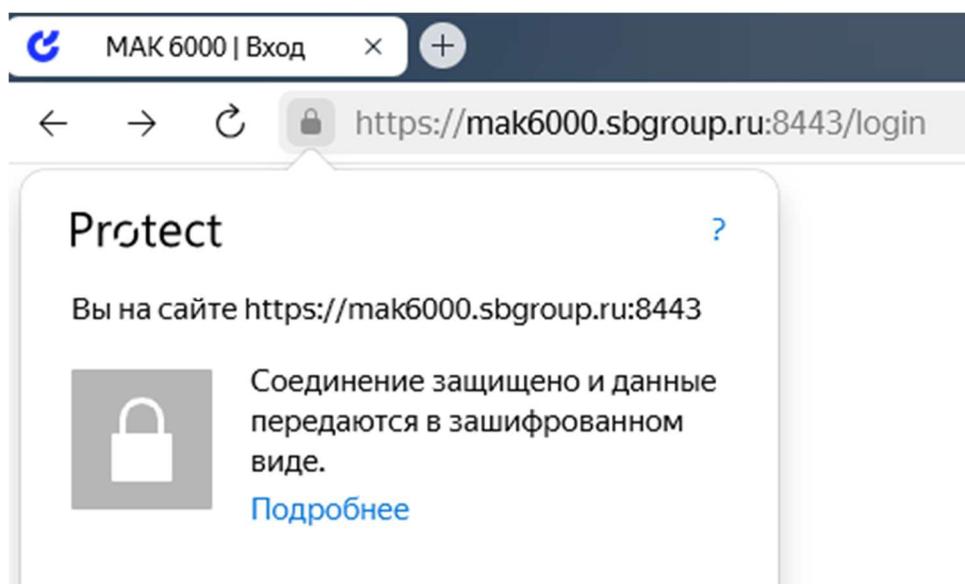


затем закройте браузер (не одно только окно, а все окна).

Откройте браузер снова и зайдите на веб-страницу Системы по локальному доменному имени. Теперь вход в веб-интерфейс будет осуществляться по протоколу защищенному HTTPS, пока сертификат

действителен. При необходимости замены сертификата проделайте повторно указанные в настоящем пункте действия.

В случае правильного выпущенного сертификата и его успешной загрузки в Модуль в строке авторизации будет отображаться протокол HTTPS, например так, как показано на снимке экрана:



5.3. Установка пароля Суперпользователя

Суперпользователь (root) это единственный и самый главный пользователь операционной системы Модуля. Под учетной записью Суперпользователя производятся системные настройки операционной системы Модуля, такие как: настройка IP-адреса, настройка встроенного межсетевого экрана, настройка удаленного доступа по протоколу ssh, обновление программного обеспечения, и пр.

В заводской конфигурации по умолчанию пароль Суперпользователя не установлен, поэтому крайне важно выполнить действия, указанные в настоящем пункте.

Для установки пароля Суперпользователя авторизуйтесь в Системе под учетной записью Администратора Системы, затем из главного меню Системы перейдите в блок «Настройки», в котором откроется диалоговое окно входа в панель настроек:

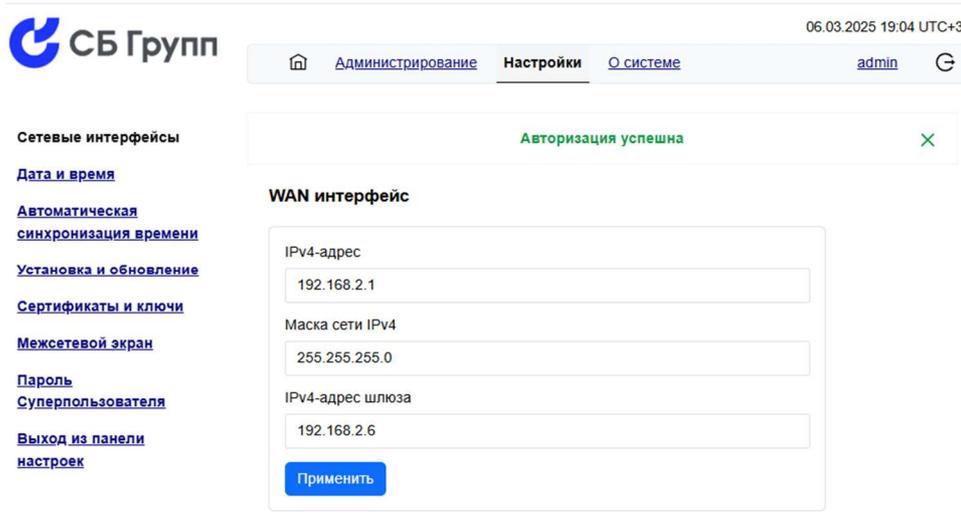
Вход в панель настроек

Логин

Пароль

Войти

Пароль Суперпользователя по умолчанию отсутствует, просто нажмите «Войти». Откроется раздел системных настроек Модуля:



СБ Групп 06.03.2025 19:04 UTC+3

Администрирование **Настройки** О системе admin

Сетевые интерфейсы

Дата и время

[Автоматическая синхронизация времени](#)

[Установка и обновление](#)

[Сертификаты и ключи](#)

[Межсетевой экран](#)

[Пароль Суперпользователя](#)

[Выход из панели настроек](#)

Авторизация успешна

WAN интерфейс

IPv4-адрес
192.168.2.1

Маска сети IPv4
255.255.255.0

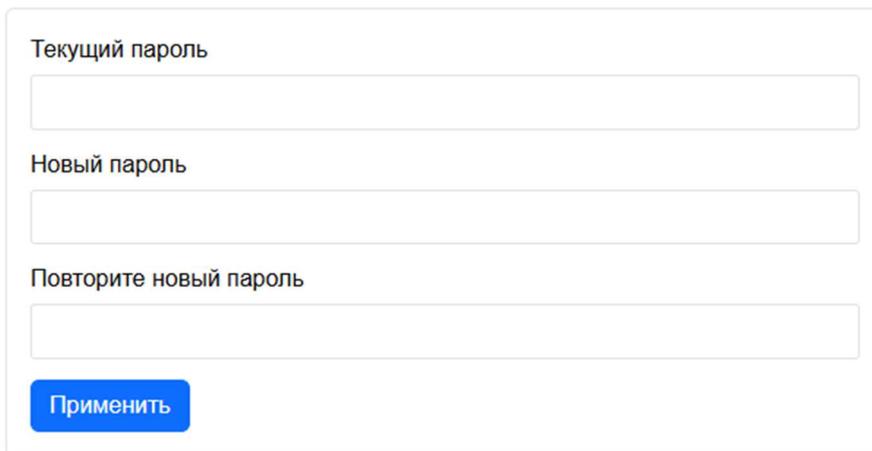
IPv4-адрес шлюза
192.168.2.6

Применить

С левой стороны расположено меню системных настроек Модуля. Нажмите в меню слева пункт «Пароль Суперпользователя», после чего

будет осуществлен переход на страницу смены Суперпользователя, как показано на снимке экрана:

Смена пароля суперпользователя



Текущий пароль

Новый пароль

Повторите новый пароль

Применить

Введите текущий пароль Суперпользователя (либо оставьте поле пустым, если делаете первичную установку пароля), введите новый пароль и повторите новый пароль в соответствующих строках. Нажмите кнопку «Применить».

Обязательно проверьте установку пароля Суперпользователя путем выхода из панели настроек, нажав на ссылку «Выход из панели настроек» в меню слева, затем снова войдите в блок «Настройки», но уже под установленным паролем.

5.4. Смена пароля Администратора Системы

Администратор Системы является главным пользователем Контроллера и прикладной части Модуля. Администратору системы доступны такие функции, как: доступ к журналу событий, управление пользователями, настройка парольной политики, настройка сокрытия конфигураций оборудования, настройка длительности сессии при

неактивности пользователя, настройка политики блокировки учетных записей, обновление программного обеспечения контроллера, и пр.

Для смены пароля Администратора Системы авторизуйтесь в Системе под учетной записью Администратора Системы, затем из главного меню Системы нажмите на гиперссылку «admin», которая расположена в верхней строке справа. Откроется меню редактирования профиля пользователя:

Профиль пользователя

ID	Имя	Роль
1000	admin	Admin

Старый пароль	<input type="password"/>
Новый пароль	<input type="password"/>
Подтверждение пароля	<input type="password"/>
<input type="button" value="Сохранить"/>	

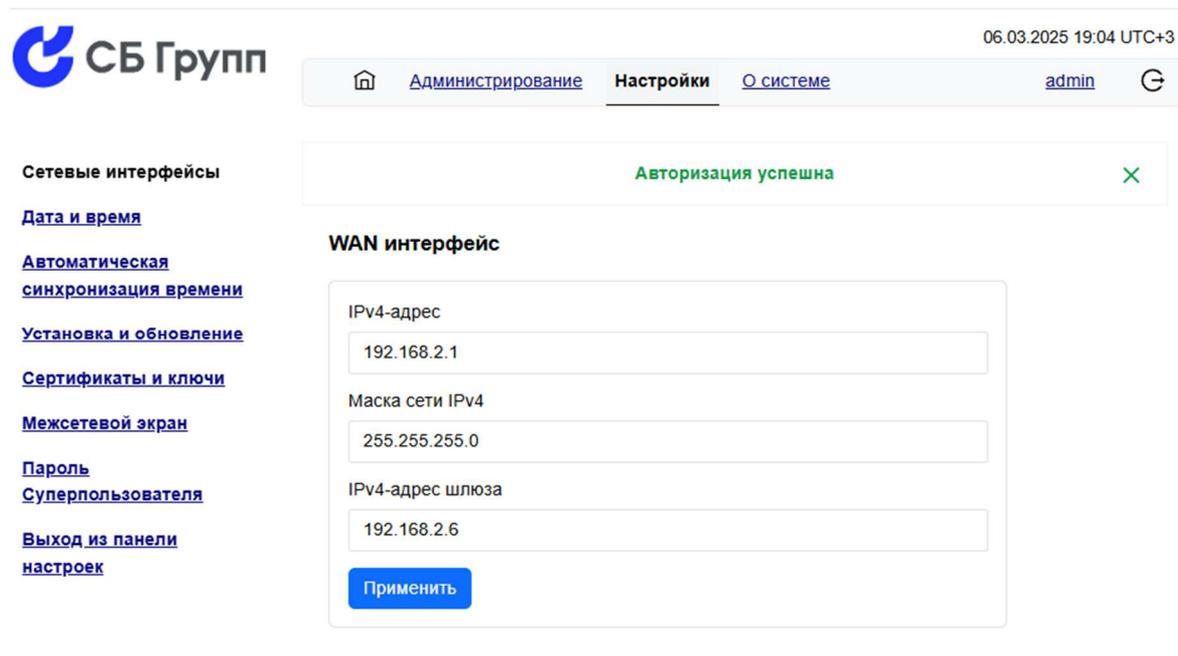
Введите в соответствующие поля текущий пароль, новый пароль и подтверждение нового пароля, затем нажмите кнопку «Сохранить». Далее необходимо выйти из Системы и авторизоваться повторно с новым паролем.

5.5. Синхронизация системного времени с сервером NTP

Модуль содержит функцию автоматической синхронизации системного времени с NTP сервером. Для настройки функции синхронизации авторизуйтесь в Системе под учетной записью

Администратора Системы, затем перейдите в блок «Настройки» и авторизуйтесь под учетной записью Суперпользователя.

После авторизации под учетной записью Суперпользователя откроется раздел системных настроек Модуля:



06.03.2025 19:04 UTC+3

СБ Групп

[Администрирование](#) **Настройки** [О системе](#) [admin](#)

Сетевые интерфейсы

- [Дата и время](#)
- [Автоматическая синхронизация времени](#)
- [Установка и обновление](#)
- [Сертификаты и ключи](#)
- [Межсетевой экран](#)
- [Пароль Суперпользователя](#)
- [Выход из панели настроек](#)

WAN интерфейс

IPv4-адрес

Маска сети IPv4

IPv4-адрес шлюза

Авторизация успешна

С левой стороны расположено меню системных настроек Модуля. Нажмите в меню слева ссылку «Автоматическая синхронизация времени», после чего будет осуществлен переход на страницу с настройками синхронизации системного времени по NTP.

[Сетевые интерфейсы](#)[Дата и время](#)[Автоматическая
синхронизация времени](#)[Установка и обновление](#)[Сертификаты и ключи](#)[Межсетевой экран](#)[Пароль](#)[Суперпользователя](#)[Выход из панели
настроек](#)**Автоматическая синхронизация времени**

Использовать ntp для синхронизации времени

1 Сервер NTP

2 Сервер NTP

3 Сервер NTP

Для активации функции синхронизации системного времени Модуля с NTP серверами поставьте галочку в чекбокс напротив «Использовать ntp для синхронизации времени».

Пропишите в соответствующие поля имена или IP-адреса NTP серверов. Модуль поддерживает работу с серверами NTP, в количестве до трех.

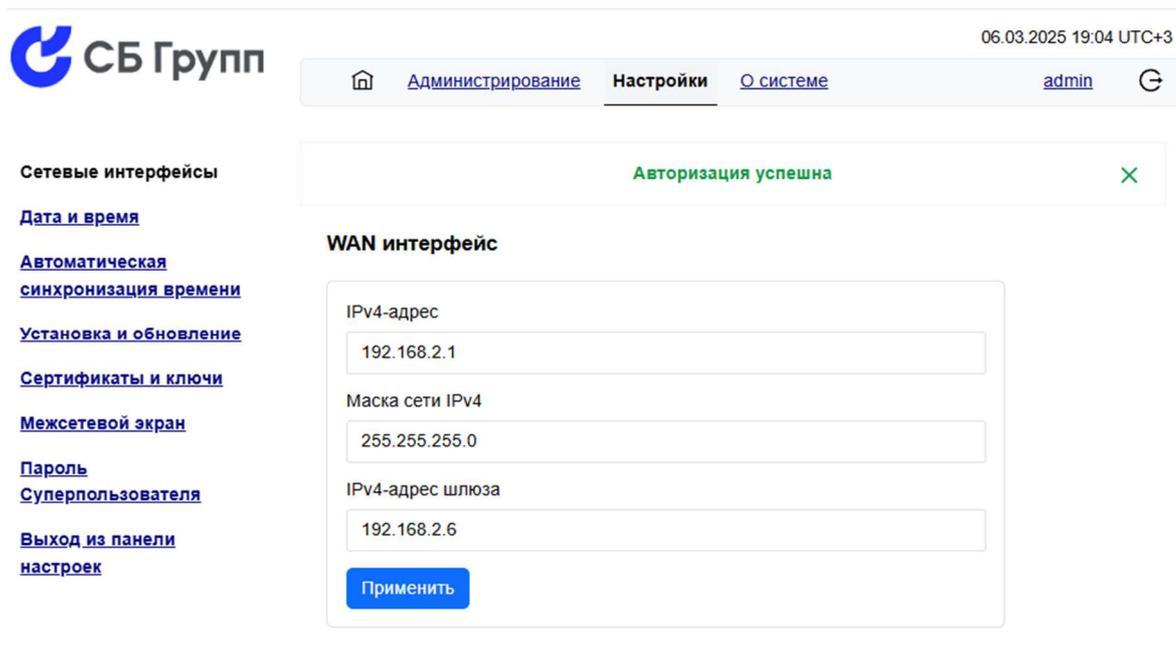
5.6. Ручная установка даты и времени

Для переключения функции синхронизации системного времени Модуля на встроенный модуль реального времени RTC, снимите галочку с чекбокса «Использовать NTP для синхронизации времени». Путь к странице, где находится эта галочка указан в предыдущем пункте.

Для ручной корректировки системного времени Модуля авторизуйтесь в Системе под учетной записью Администратора

Системы, затем перейдите в блок «Настройки» и авторизуйтесь под учетной записью Суперпользователя.

После авторизации под учетной записью Суперпользователя откроется раздел системных настроек Модуля:



The screenshot displays the administrative interface of the SB Group system. At the top left is the logo and name "СБ Групп". The top right shows the date and time: "06.03.2025 19:04 UTC+3". Below this is a navigation bar with links: "Администрирование", "Настройки" (highlighted), and "О системе". The user is logged in as "admin".

A green notification box at the top center states "Авторизация успешна" (Authorization successful). The main content area is titled "WAN интерфейс" (WAN interface) and contains three input fields:

- IPv4-адрес: 192.168.2.1
- Маска сети IPv4: 255.255.255.0
- IPv4-адрес шлюза: 192.168.2.6

A blue "Применить" (Apply) button is located at the bottom of the configuration area. On the left side, there is a sidebar menu with the following items:

- Сетевые интерфейсы
- Дата и время
- Автоматическая синхронизация времени
- Установка и обновление
- Сертификаты и ключи
- Межсетевой экран
- Пароль Суперпользователя
- Выход из панели настроек

С левой стороны расположено меню системных настроек Модуля. Нажмите в меню слева ссылку «Дата и время», после чего будет осуществлен переход на страницу с возможностью ручного ввода даты и времени.

[Сетевые интерфейсы](#)[Дата и время](#)[Автоматическая
синхронизация времени](#)[Установка и обновление](#)[Сертификаты и ключи](#)[Межсетевой экран](#)[Пароль
Суперпользователя](#)[Выход из панели
настроек](#)Текущий часовой пояс: Europe/Moscow
Смещение: UTC+3

Настройка часового пояса

Новый часовой пояс

Установка даты и времени вручную

Новая дата и время

Введите в советующее поле желаемые дату и время, и нажмите кнопку «Применить». Системные часы Модуля будут скорректированы, а встроенные часы реального времени принудительно синхронизируются с системным временем.

5.7. Установка часового пояса

Модуль содержит функцию настройки часового пояса. Для доступа к странице настройки часового пояса пройдите шаги из предыдущего пункта до нажатия на ссылку «Дата и время» и перейдите по ней, после чего будет осуществлен переход на страницу с возможностью корректировки часового пояса.

[Сетевые интерфейсы](#)[Дата и время](#)[Автоматическая
синхронизация времени](#)[Установка и обновление](#)[Сертификаты и ключи](#)[Межсетевой экран](#)[Пароль
Суперпользователя](#)[Выход из панели
настроек](#)Текущий часовой пояс: Europe/Moscow
Смещение: UTC+3

Настройка часового пояса

Новый часовой пояс

Установка даты и времени вручную

Новая дата и время

Нажмите на поле с указанием текущего часового пояса, после чего выпадет список доступных к выбору часовых поясов. Выберите желаемый часовой пояс либо по названию крупного населенного пункта, либо по корректировке относительно нулевой точки отсчета всемирного времени GMT, и нажмите кнопку «Применить».

Данные о выбранном часовом поясе сохраняются в конфигурационных файлах операционной системы Модуля.

6. ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Система обеспечивает возможность обновлять программное обеспечение трех типов: системное программное обеспечение Модуля, прикладное программное обеспечение Модуля и прошивку (firmware) Контроллера.

Обновление всех трех типов программного обеспечения Системы выполняется из веб-интерфейса Системы.

Информация об обновлениях программного обеспечения размещена на сайте производителя в информационно-телекоммуникационной сети Интернет по адресу:
https://sbgroup.ru/mib101_fw

Зарегистрированные пользователи Модуля с активным сертификатом на техническую поддержку получают от производителя рассылку по электронной почте о выходе новых версий программного обеспечения. Такие пользователи, в случае выявления производителем Модуля ошибок и уязвимостей в программном обеспечении, получают экстренную рассылку по электронной почте о найденных ошибках и уязвимостях в программном обеспечении, включая рекомендации по безопасной эксплуатации Системы, до момента выхода обновления программного обеспечения, устраняющее их.

6.1. Обновление прошивки Контроллера

Система предоставляет возможность обновления прошивки Контроллера посредством веб-интерфейса и с использованием одного из перечисленных браузеров актуальной версии: Google Chrome, Яндекс Браузер, Браузер Chromium-Gost или Спутник Браузер.

Для доступа к функции обновления прошивки Контроллера (firmware) авторизуйтесь в Системе под учетной записью Администратора Системы, затем из главного меню Системы перейдите в блок «Администрирование», откроется раздел «Администрирования Модуля».

Аудит[Пользователи](#)[РОС](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)**Аудит действий пользователя**

ID	Дата и время	Пользователь	Действие	Статус
bb753892-653d-4830-a713-6452d6364c6f	2025-03-12 09:30:30	admin	Вход в систему	Успешно
22f81ea2-4a5d-42aa-8f06-fbf16d345dec	2025-03-10 15:41:56	admin	Вход в систему	Успешно
ееcb54d0-f00a-43ec-9f3f-9ef8358dd210	2025-03-10 15:11:10	admin	Вход в систему	Успешно
721ea2ff-8fc9-471a-b7b2-716d41765e69	2025-03-07 11:24:35	admin	Вход в систему	Успешно

С левой стороны расположено меню административных настроек Модуля. Нажмите в меню слева на ссылку «Прошивка», после чего будет осуществлен переход на страницу функционала обновления программного обеспечения Контроллера, как показано на снимке экрана:

[Аудит](#)[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

История прошивок

Загрузить

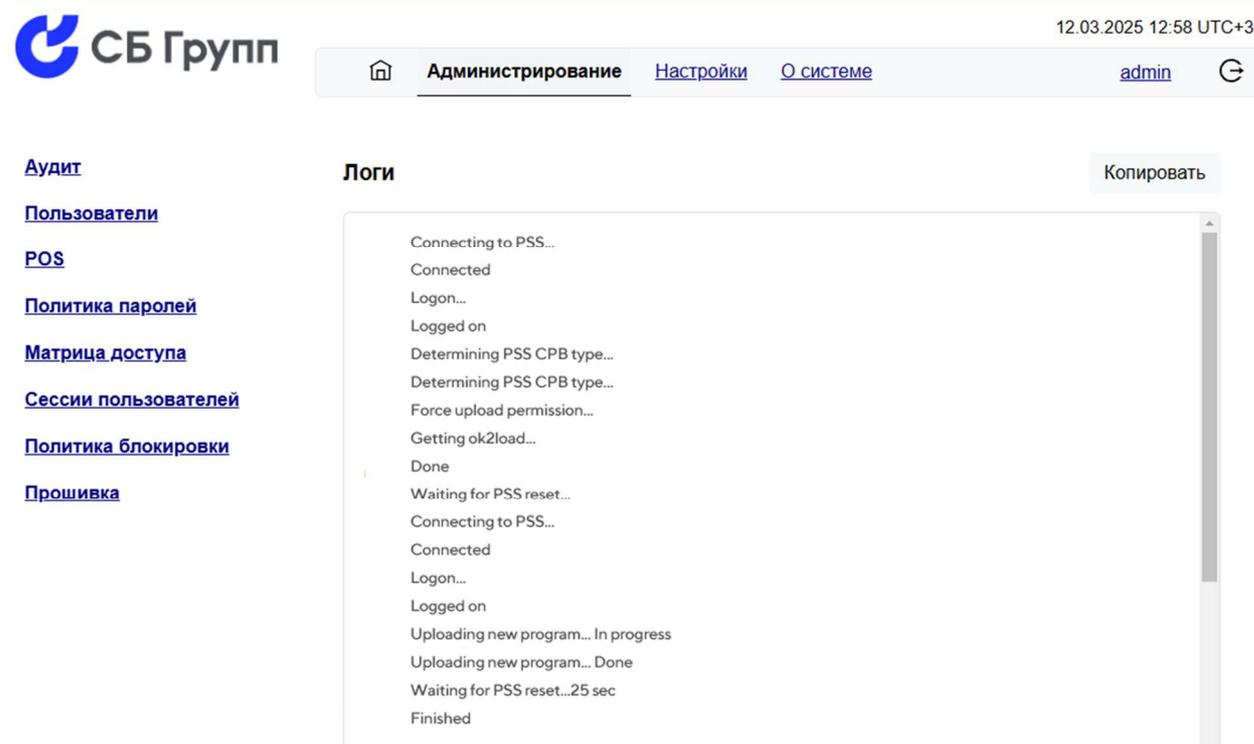
ID	Имя файла	Дата	Тип	Размер	Контрольная сумма	Статус
4	41038277.bin	2024-09-27 12:48:26	app	3407872	C2BF	Успешно Подробнее
3	41038277.bin	2024-09-27 10:13:33	app	3407872	D5D9	Успешно Подробнее
2	41038277_001.bin	2024-09-27 10:11:17	app	3407872	C8A7	Ошибка Подробнее
1	41038277_002.bin	2024-09-27 10:06:47	app	3407872	D5D9	Ошибка Подробнее

На странице отображается история обновлений прошивок, выполненных через веб-интерфейс Системы. Встроенным в Модуль функционалом обновления прошивки Контроллера предусмотрены следующие возможности:

- загрузка прошивки через веб-интерфейс браузера по безопасному протоколу https;
- расчет контрольной суммы прошивки;
- отказ от обновления Контроллера загруженной прошивкой, в случае несовпадения контрольной суммы;
- журналирование событий, связанных с действиями по обновлению прошивки, либо действиями по откату к старой версии прошивки;
- журналирование самого процесса прошивки;
- автоматический возврат к предыдущей версии прошивки, в случае неудачи процесса прошивки Контроллера загруженной прошивкой.

Подробная информация о ходе каждого процесса обновления прошивки Контроллера записывается и доступна к просмотру при

нажатию на кнопку «Подробнее» в конце каждой строки журнала истории прошивок. Пример такого журнала:



12.03.2025 12:58 UTC+3

Администрирование [Настройки](#) [О системе](#) [admin](#)

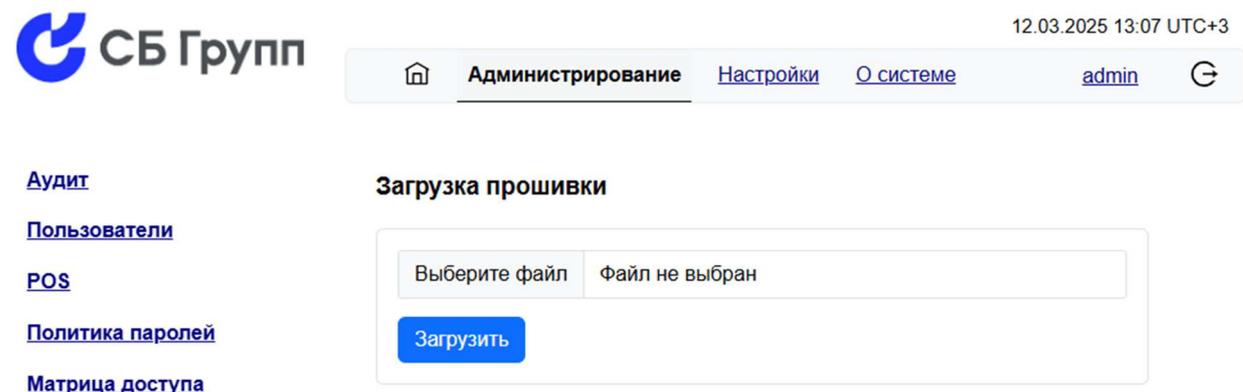
[Аудит](#)
[Пользователи](#)
[POS](#)
[Политика паролей](#)
[Матрица доступа](#)
[Сессии пользователей](#)
[Политика блокировки](#)
[Прошивка](#)

Логи Копировать

```
Connecting to PSS...
Connected
Logon...
Logged on
Determining PSS CPB type...
Determining PSS CPB type...
Force upload permission...
Getting ok2load...
Done
Waiting for PSS reset...
Connecting to PSS...
Connected
Logon...
Logged on
Uploading new program... In progress
Uploading new program... Done
Waiting for PSS reset...25 sec
Finished
```

Прошивка с максимальным значением поля «ID» и со статусом «Успешно» загружена в контроллер последней.

Для обновления прошивки Контроллера нажмите на кнопку «Загрузить», расположенную в правом верхнем углу окна страницы, откроется страница интерфейса загрузки прошивки:



12.03.2025 13:07 UTC+3

Администрирование [Настройки](#) [О системе](#) [admin](#)

[Аудит](#)
[Пользователи](#)
[POS](#)
[Политика паролей](#)
[Матрица доступа](#)

Загрузка прошивки

Выберите файл Файл не выбран

[Загрузить](#)

Нажмите в поле «Выберите файл» и затем укажите путь к *.bin файлу прошивки. Затем нажмите на кнопку «Загрузить». Начнется процесс прошивки. Обязательно дождитесь окончания процесса прошивки, не прерывайте его и не отключайте Контроллер.

[Аудит](#)[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

История прошивок

Идёт процесс обновления прошивки (Waiting for PSS reset...25 sec) 95% ...

ID	Имя файла	Дата	Тип	Размер	Контрольная сумма	Статус
5	41038280.bin	2025-03-12 10:09:38	app	3407872	9C28	В процессе Подробнее
4	41038277.bin	2024-09-27 12:48:26	app	3407872	C2BF	Успешно Подробнее
3	41038277.bin	2024-09-27 10:13:33	app	3407872	D5D9	Успешно Подробнее
2	41038277_001.bin	2024-09-27 10:11:17	app	3407872	C8A7	Ошибка Подробнее
1	41038277_002.bin	2024-09-27 10:06:47	app	3407872	D5D9	Ошибка Подробнее

По окончании успешного процесса прошивки отобразиться надпись «Прошивка устройства завершена». В таблице «История прошивок» появиться новая запись.

[Аудит](#)[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)Прошивка устройства завершена 

История прошивок

[Загрузить](#)

ID	Имя файла	Дата	Тип	Размер	Контрольная сумма	Статус
5	41038280.bin	2025-03-12 10:09:38	app	3407872	9C28	Успешно Подробнее
4	41038277.bin	2024-09-27 12:48:26	app	3407872	C2BF	Успешно Подробнее
3	41038277.bin	2024-09-27 10:13:33	app	3407872	D5D9	Успешно Подробнее
2	41038277_001.bin	2024-09-27 10:11:17	app	3407872	C8A7	Ошибка Подробнее
1	41038277_002.bin	2024-09-27 10:06:47	app	3407872	D5D9	Ошибка Подробнее

6.2. Обновление системного ПО Модуля

Обновление системного программного обеспечения Модуля может потребоваться в следующих случаях:

- найдены актуальные для реализации в Модуле уязвимости ядре или системных библиотеках операционной системы Linux;
- найдены актуальные для функций Модуля ошибки ядре или системных библиотеках операционной системы Linux;
- обновление прикладного программного обеспечения Модуля требует обновления ядра или системных библиотеках операционной системы Linux.

Для доступа к функции обновления системного программного обеспечения Модуля авторизуйтесь в Системе под учетной записью Администратора Системы, затем из главного меню Системы перейдите в блок «Настройки», откроется диалоговое окно входа в панель настроек:

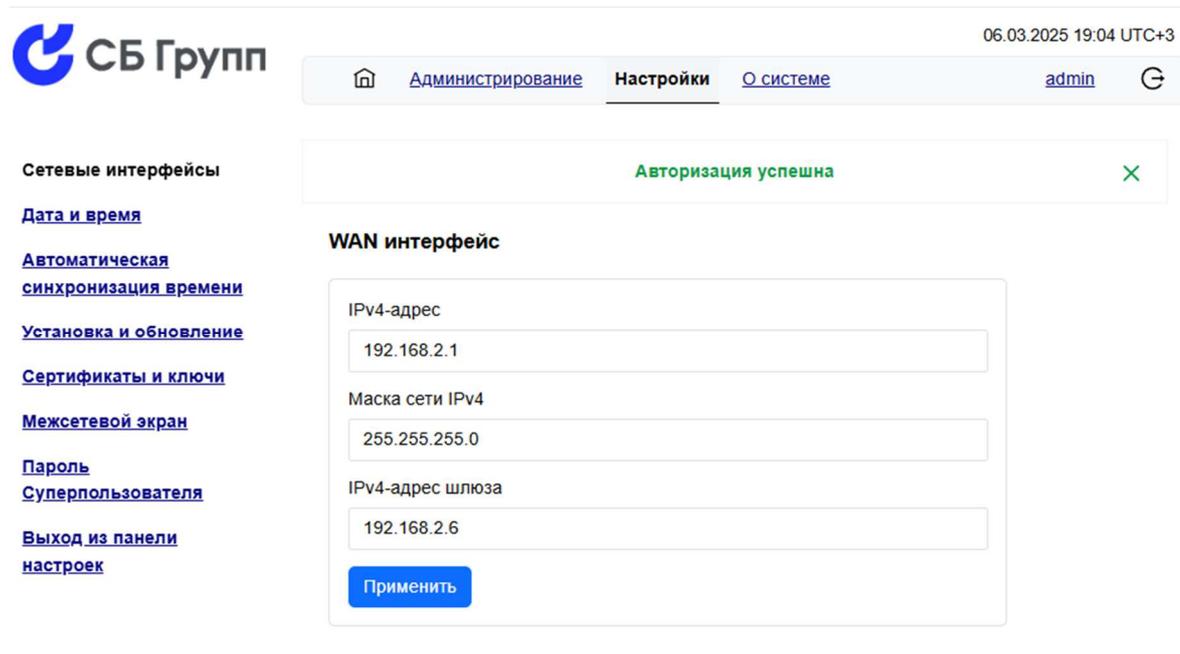
Вход в панель настроек

Логин

Пароль

Войти

Введите пароль Суперпользователя и нажмите «Войти».
Откроется раздел системных настроек Модуля.



С левой стороны расположено меню системных настроек Модуля. Нажмите в меню слева на ссылку «Установка и обновление», после чего будет осуществлен переход на страницу с информацией об текущих версиях системного и прикладного ПО Модуля и возможности их обновления, как показано на снимке экрана.

[Сетевые интерфейсы](#)[Дата и время](#)[Автоматическая
синхронизация времени](#)[Установка и обновление](#)[Сертификаты и ключи](#)[Межсетевой экран](#)[Пароль](#)[Суперпользователя](#)[Выход из панели
настроек](#)**Системное программное обеспечение**

Название	Значение
Версия системного ПО	22.03.5
Версия системных файлов	1555-r23902-50148a40d2
Версия фаерволла	2023-09-01-598d9fbb-1

Прикладное программное обеспечение

Название	Значение
Версия прикладного ПО	0.2.5
Дата сборки	23.10.2024 22:19 UTC+3

Обновление ПО

Обновление системного ПО	Обновление прикладного ПО
<input type="text" value="Выберите файл"/> <input type="text" value="Файл не выбран"/>	<input type="text" value="Выберите файл"/> <input type="text" value="Файл не выбран"/>
<input type="button" value="Загрузить"/>	<input type="button" value="Загрузить"/>

Для загрузки файла прошивки системного ПО модуля в нижнем левом углу нажмите в поле «Выберите файл» и затем укажите путь к файлу прошивки. Затем нажмите на кнопку «Загрузить». Начнется процесс прошивки. Обязательно дождитесь окончания процесса прошивки, не прерывайте его и не отключайте, и не перезагружайте Систему.

По окончании процесса прошивки Модуль перезагрузится автоматически. Для контроля результата обновления пройдите шаги настоящего пункта, до страницы «Установка и обновление» и убедитесь в том, что версии системного ПО Модуля были обновлены.

В случае возникновения ошибок на этапе обновления системного ПО Модуля произойдет автоматический откат к предыдущей версии.

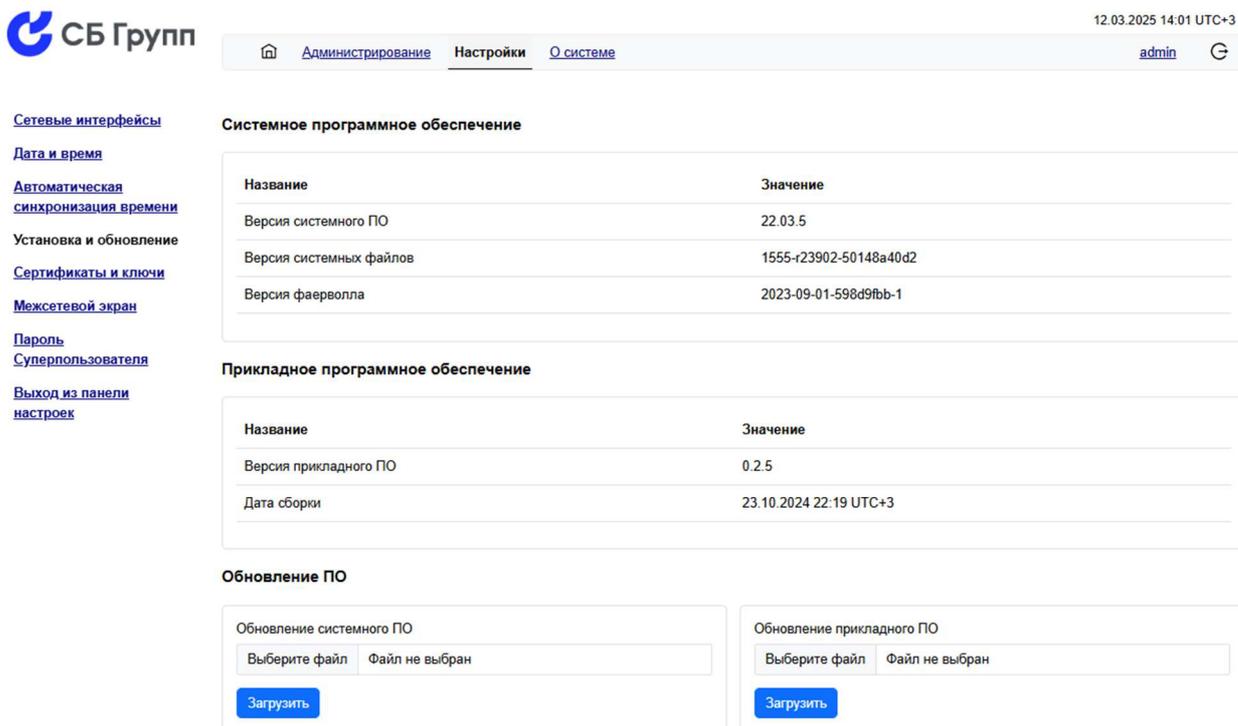
Если обновление не произошло, обратитесь в техническую поддержку производителя.

6.3. Обновление прикладного ПО Модуля

Обновление прикладного программного обеспечения Модуля может потребоваться в следующих случаях:

- добавлены новые функции в Модуль;
- найдены ошибки в функциях Модуля;
- доработаны, изменены, объединены функции Модуля;
- внесены изменения в интерфейс Модуля.

Для доступа к функции обновления прикладного программного обеспечения Модуля пройдите шаги в предыдущего пункта, до страницы «Установка и обновление».



The screenshot shows the administration interface for SB Group. The top navigation bar includes the logo, the text 'СБ Групп', and the date '12.03.2025 14:01 UTC+3'. The main menu has 'Администрирование', 'Настройки', and 'О системе'. The 'Настройки' section is active, showing a sidebar with links like 'Сетевые интерфейсы', 'Дата и время', 'Автоматическая синхронизация времени', 'Установка и обновление', 'Сертификаты и ключи', 'Межсетевой экран', 'Пароль Суперпользователя', and 'Выход из панели настроек'. The main content area is divided into three sections: 'Системное программное обеспечение' (System software), 'Прикладное программное обеспечение' (Application software), and 'Обновление ПО' (Software update). The 'Системное программное обеспечение' table lists: 'Версия системного ПО' (22.03.5), 'Версия системных файлов' (1555-r23902-50148a40d2), and 'Версия фаерволла' (2023-09-01-598d9fbb-1). The 'Прикладное программное обеспечение' table lists: 'Версия прикладного ПО' (0.2.5) and 'Дата сборки' (23.10.2024 22:19 UTC+3). The 'Обновление ПО' section has two panels: 'Обновление системного ПО' and 'Обновление прикладного ПО'. Both panels have a 'Выберите файл' field (currently showing 'Файл не выбран') and a 'Загрузить' button.

Для загрузки файла прошивки прикладного ПО Модуля в нижнем правом углу нажмите в поле «Выберите файл» и затем укажите путь к файлу прошивки. Затем нажмите на кнопку «Загрузить». Начнется процесс прошивки. Обязательно дождитесь окончания процесса

прошивки, не прерывайте его и не отключайте, и не перезагружайте Систему.

По окончании процесса прошивки Модуль перезагрузится автоматически. Для контроля результата обновления снова пройдите шаги предыдущего пункта, до страницы «Установка и обновление» и убедитесь в том, что версии прикладного ПО Модуля были обновлены.

В случае возникновения ошибок на этапе обновления прикладного ПО Модуля произойдет автоматический откат к предыдущей версии.

Если обновление не произошло, обратитесь в техническую поддержку производителя.

7. ОБЕСПЕЧЕНИЕ ИБ. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Встроенные средства информационной безопасности Системы, в части идентификации и аутентификации, обеспечивают основные требования к информационной безопасности Системы, например, такие как:

- для идентификации каждому пользователю назначается уникальный персональный идентификатор;
- доступ пользователей под локальной учетной записью осуществляется посредством аутентификации по паролю;
- обеспечивается защита обратной связи при вводе аутентификационной информации;
- все пароли, по умолчанию, для встроенных учетных записей имеют возможность замены;
- авторизация пользователей производится только после прохождения процедур идентификации и аутентификации.

7.1. Настройка парольной политики

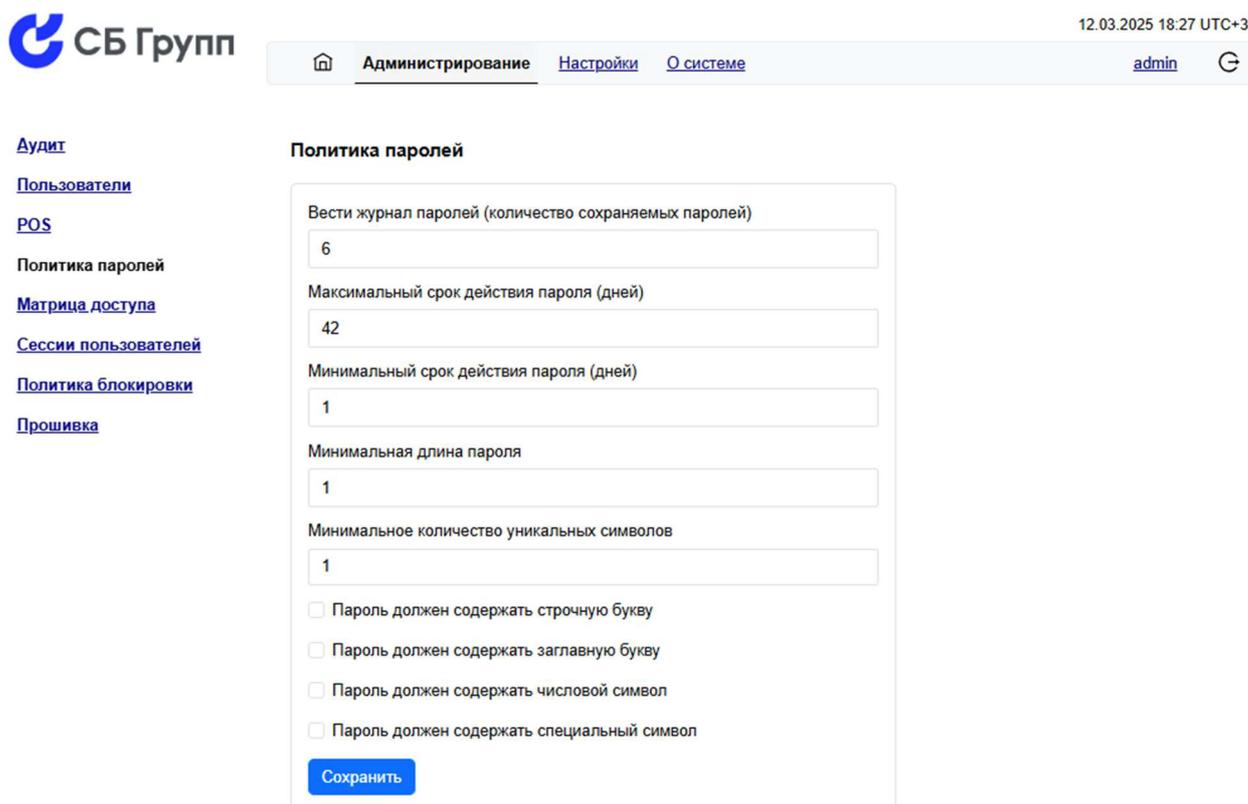
В Системе реализована функция определения парольной политики, позволяющая задать следующие требования к паролям пользователей:

- Журнал истории паролей. Ограничивает пользователей в повторяемости паролей. Значение определяет, через какое количество раз смены пароля пользователем разрешено повторение пароля;

- Максимальный срок действия пароля. Значение определяет, какое количество максимальное дней, с момента установки/смены пароль будет действителен;
- Минимальный срок действия пароля. Ограничивает пользователя в частой смене пароля. Значение определяет минимальное количество дней с момента установки или последней смены пароля пользователь сможет изменить свой пароль;
- Минимальная длина пароля. Значение определяет минимальное количество символов в задаваемом пользователем пароле;
- Минимальное количество уникальных символов. Значение определяет минимальное количество уникальных символов, в пароле, задаваемом пользователем;
- Требование «Пароль должен содержать строчную букву». Активный чекбокс устанавливает требование к содержанию во вводимом пользователем пароле хотя бы одной строчной буквы;
- Требование «Пароль должен содержать заглавную букву». Активный чекбокс устанавливает требование к содержанию во вводимом пользователем пароле хотя бы одной заглавной буквы;
- Требование «Пароль должен содержать числовой символ». Активный чекбокс устанавливает требование к содержанию во вводимом пользователем пароле хотя бы одной цифры;

- Требование «Пароль должен содержать специальный символ». Активный чекбокс устанавливает требование к содержанию во вводимом пользователем пароле хотя бы одного специального символа, например: \$@%#&.

Для настройки парольной политики авторизуйтесь в Системе под учетной записью Администратора Системы, затем из главного меню Системы перейдите в блок «Администрирование», далее в меню слева нажмите на ссылку «Политика паролей».



СБ Групп 12.03.2025 18:27 UTC+3

Администрирование [Настройки](#) [О системе](#) admin ↻

[Аудит](#)
[Пользователи](#)
[POS](#)
[Политика паролей](#)
[Матрица доступа](#)
[Сессии пользователей](#)
[Политика блокировки](#)
[Прошивка](#)

Политика паролей

Вести журнал паролей (количество сохраняемых паролей)

Максимальный срок действия пароля (дней)

Минимальный срок действия пароля (дней)

Минимальная длина пароля

Минимальное количество уникальных символов

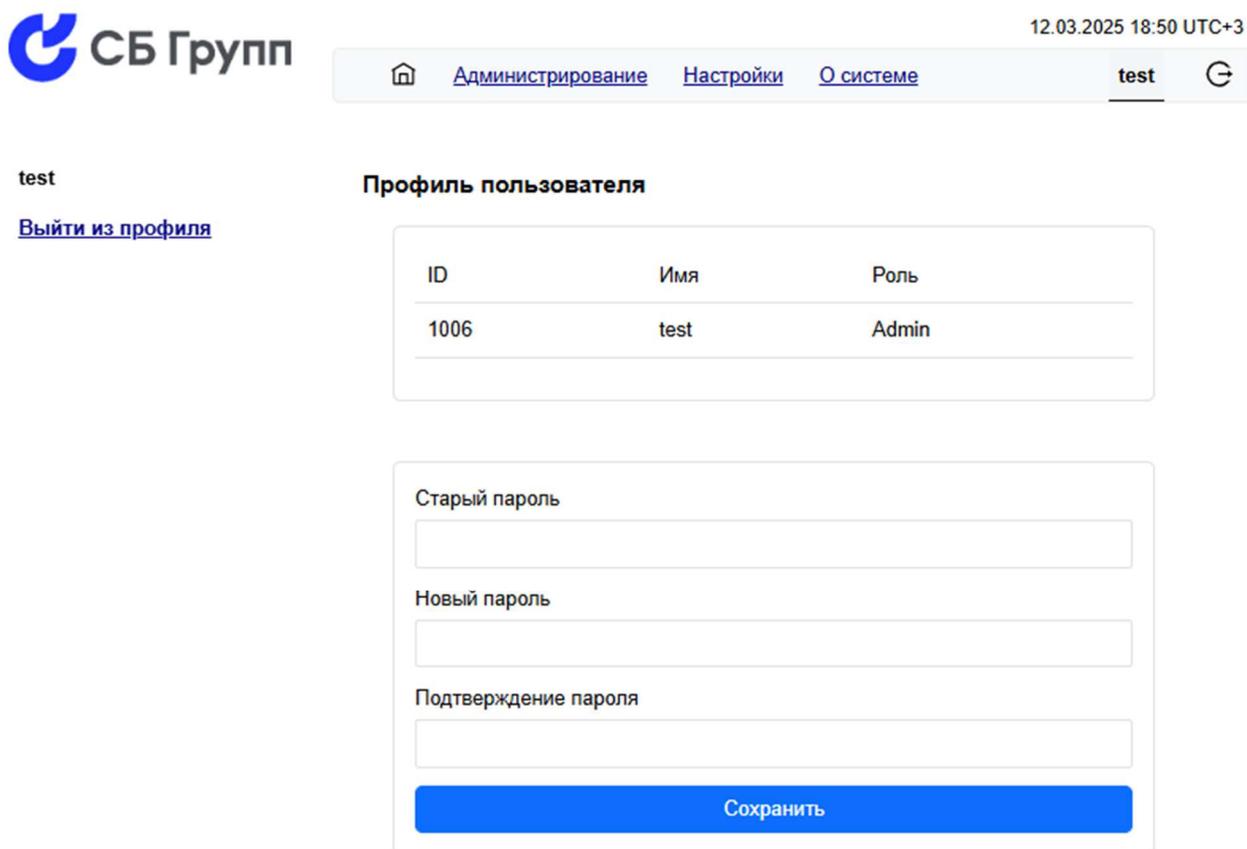
Пароль должен содержать строчную букву
 Пароль должен содержать заглавную букву
 Пароль должен содержать числовой символ
 Пароль должен содержать специальный символ

Введите в соответствующие поля значения и поставьте в нужные чекбоксы галочки, в соответствии с задаваемой парольной политикой. Затем нажмите кнопку «Сохранить». Парольная политика будет применена.

7.2. Самостоятельная смена пароля пользователем

В Системе реализована функция смены пароля пользователя, позволяющая выполнить процедуру смены пароля пользователем самостоятельно.

Для самостоятельной смены пароля пользователем авторизуйтесь в Системе под учетной записью Пользователя, затем в правой части главного меню Системы, рядом с пиктограммой «Выход», нажмите на отображаемое имя пользователя, после чего откроется страница смены пароля.



The screenshot shows the user profile page in the system interface. At the top left is the logo "СБ Групп". At the top right is the date and time "12.03.2025 18:50 UTC+3". Below the logo is the user name "test" and a link "Выйти из профиля". The main heading is "Профиль пользователя". Below it is a table with user information:

ID	Имя	Роль
1006	test	Admin

Below the table are three input fields for password change: "Старый пароль", "Новый пароль", and "Подтверждение пароля". At the bottom is a blue button labeled "Сохранить".

Введите в соответствующие поля текущий пароль, новый пароль и новый пароль ещё раз, затем нажмите кнопку «Сохранить».

7.3. Встроенные учетные записи

Система по умолчанию содержит следующие встроенные учетные записи:

- учётная запись Администратора Системы;
- учетная запись Суперпользователя;
- учетная запись POS протокола.

7.3.1. Учетная запись Администратора Системы

Учетная запись Администратора Системы является главной учетной записью Системы с ролью «admin». Данная учетная запись предназначена для администрирования прикладной части Системы.

Функционалом Модуля предусмотрена возможность блокировки и смены пароля учетной записи Администратора Системы.

При блокировке главной учетной записи Администратора Системы её разблокировка возможна только, если создана другая учетная запись с ролью «admin».

Список всех учетных записей прикладной части Системы доступен на странице «Пользователи» в блоке «Администрирование».

Для доступа к странице со списком пользователей авторизуйтесь в Системе под учетной записью Администратора Системы, затем из главного меню Системы перейдите в блок «Администрирование», откроется раздел администрирования Системы:

Аудит

[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

Аудит действий пользователя

ID	Дата и время	Пользователь	Действие	Статус
bb753892-653d-4830-a713-6452d6364c6f	2025-03-12 09:30:30	admin	Вход в систему	Успешно
22f81ea2-4a5d-42aa-8f06-fb16d345dec	2025-03-10 15:41:56	admin	Вход в систему	Успешно
eecb54d0-f00a-43ec-9f3f-9ef8358dd210	2025-03-10 15:11:10	admin	Вход в систему	Успешно
721ea2ff-8fc9-471a-b7b2-716d41765e69	2025-03-07 11:24:35	admin	Вход в систему	Успешно

С левой стороны расположено меню административных настроек Системы. Нажмите в меню слева на ссылку «Пользователи», после чего будет осуществлен переход на страницу со списком пользователей, с указанием уникального идентификатора, имени, ролью и статусом, как изображено на примере:

Аудит

[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

Пользователи

[+ Добавить](#)

ID	Логин	Роль	Статус	
1000	admin	Admin	Заблокирован	⚙
1001	host	Host	Активен	⚙
1002	manager	Manager	Активен	⚙
1003	service	Service	Заблокирован	⚙
1007	test	Admin	Активен	⚙

7.3.2. Учетная запись Суперпользователя

Учетная запись Суперпользователя является единственной учетной записью операционной системы Модуля. Данная учетная запись предназначена для администрирования системных функций операционной системы Модуля.

Под учетной записью Суперпользователя производится обновление системного и прикладного ПО Модуля, конфигурирование системных функций операционной системы Модуля, восстановление работоспособности Модуля путем переустановки прикладного ПО с потерей всех данных и настроек.

Функционалом Модуля предусмотрена возможность смены пароля учетной записи Суперпользователя. В целях безопасности функционалом Модуля ограничена возможность блокировки Суперпользователя.

В случае утери пароля Суперпользователя или блокировки учетной записи Суперпользователя восстановление Модуля до полностью исправного состояния возможно только в сервисном центре, авторизованном заводом-изготовителем.

Блокировка Суперпользователя, смена имени Суперпользователя, добавление/удаление других системных учетных записей выполняется стандартными средствами операционной системы Модуля, описание этих функций является общеизвестным и выходит за пределы настоящего руководства.

Список всех учетных записей операционной системы Модуля доступен штатными средствами встроенной операционной системы Модуля.

7.3.3. Учетная запись POS протокола

Учетная запись POS протокола является основной и единственной учетной записью, реализующей бизнес-функции Контроллера. Данная учетная запись предназначена для взаимодействия Контроллера с внешним оборудованием по POS протоколу. Учетная запись POS протокола не используется в административных либо прикладных функциях Модуля.

Функционалом Системы предусмотрена возможность смены пароля POS протокола. Функционалом Модуля, возможность блокировки учетной записи POS протокола реализована через ограничения сетевого доступа по портам, на которых работает POS протокол.

Для смены пароля учетной записи POS протокола авторизуйтесь в Системе под учетной записью Администратора Системы, затем из главного меню Системы перейдите в блок «Администрирование», откроется раздел администрирования Системы:

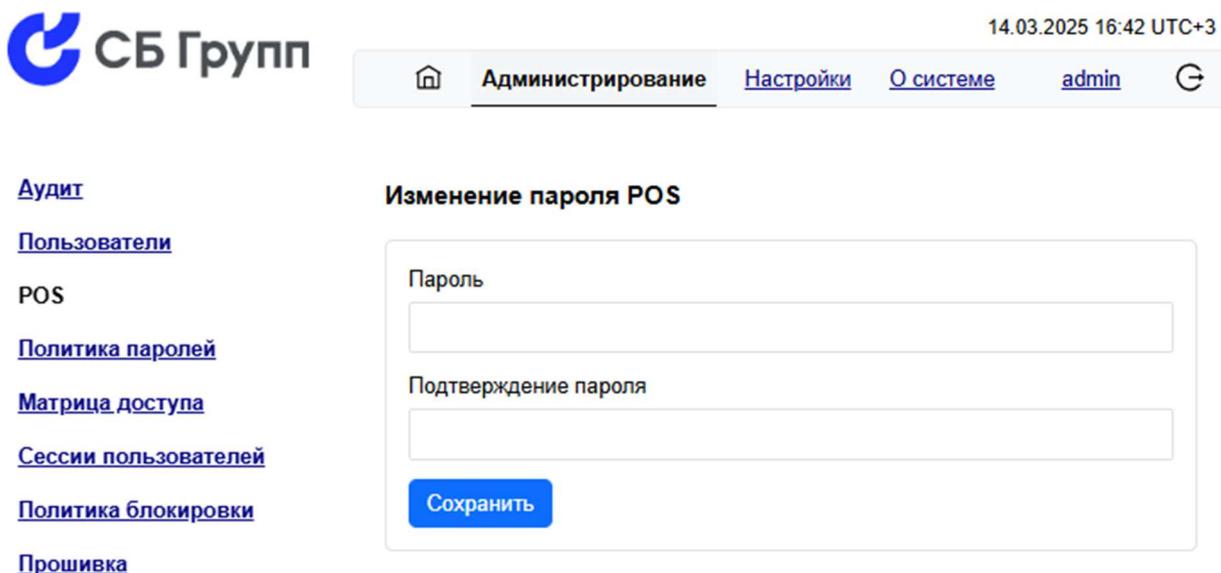
Аудит

[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

Аудит действий пользователя

ID	Дата и время	Пользователь	Действие	Статус
bb753892-653d-4830-a713-6452d6364c6f	2025-03-12 09:30:30	admin	Вход в систему	Успешно
22f81ea2-4a5d-42aa-8f06-fb16d345dec	2025-03-10 15:41:56	admin	Вход в систему	Успешно
eecb54d0-f00a-43ec-9f3f-9ef8358dd210	2025-03-10 15:11:10	admin	Вход в систему	Успешно
721ea2ff-8fc9-471a-b7b2-716d41765e69	2025-03-07 11:24:35	admin	Вход в систему	Успешно

С левой стороны расположено меню административных настроек Системы. Нажмите в меню слева на ссылку «POS», после чего будет осуществлен переход на страницу с функцией смены пароля POS протокола:



The screenshot shows the administrative interface of the SB Group system. At the top left is the SB Group logo. At the top right, the date and time are displayed as 14.03.2025 16:42 UTC+3. Below the logo and date is a navigation bar with the following items: a home icon, 'Администрирование' (Administration), 'Настройки' (Settings), 'О системе' (About system), and 'admin' with a refresh icon. On the left side, there is a vertical menu with the following items: 'Аудит' (Audit), 'Пользователи' (Users), 'POS', 'Политика паролей' (Password policy), 'Матрица доступа' (Access matrix), 'Сессии пользователей' (User sessions), 'Политика блокировки' (Lockout policy), and 'Прошивка' (Firmware). The main content area is titled 'Изменение пароля POS' (Change POS password). It contains two input fields: 'Пароль' (Password) and 'Подтверждение пароля' (Confirm password). Below the input fields is a blue button labeled 'Сохранить' (Save).

Функциональные особенности, заложенные в формат взаимодействия Контроллера с внешним оборудованием по POS протоколу таковы, что при смене пароля POS протокола не требуется вводить текущий пароль POS протокола.

8. ОБЕСПЕЧЕНИЕ ИБ. УПРАВЛЕНИЕ ДОСТУПОМ

Встроенные средства информационной безопасности Системы, в части управления доступом, обеспечивают основные требования к информационной безопасности Системы, например такие как:

- механизмы управления доступом реализованы на уровне пользовательского интерфейса;
- используется система ролевого управления доступом для управления правами доступа;
- реализован запрет на анонимное подключение к пользовательскому интерфейсу;
- по истечении периода неактивности для автоматической блокировки сессии, восстановление сессии осуществляется только после повторной аутентификации.

8.1. Система ролевого управления доступом

Для управления доступом в Системе реализована система ролевого управления доступом. Определение роли пользователя осуществляется на этапе его создания, путем выбора советующей роли.

8.1.1. Создание пользователя с назначенной ролью

Для создания пользователя авторизуйтесь в Системе под учетной записью Администратора Системы, затем из главного меню Системы перейдите в блок «Администрирование», откроется раздел администрирования Системы:

Аудит

[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

Аудит действий пользователя

ID	Дата и время	Пользователь	Действие	Статус
bb753892-653d-4830-a713-6452d6364c6f	2025-03-12 09:30:30	admin	Вход в систему	Успешно
22f81ea2-4a5d-42aa-8f06-fb16d345dec	2025-03-10 15:41:56	admin	Вход в систему	Успешно
eecb54d0-f00a-43ec-9f3f-9ef8358dd210	2025-03-10 15:11:10	admin	Вход в систему	Успешно
721ea2ff-8fc9-471a-b7b2-716d41765e69	2025-03-07 11:24:35	admin	Вход в систему	Успешно

С левой стороны расположено меню административных настроек Системы. Нажмите в меню слева на ссылку «Пользователи», после чего будет осуществлен переход на страницу со списком пользователей. В конфигурации Модуля, поступающего с завода, будет только один пользователь.

Аудит

[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

Пользователи

[+ Добавить](#)

ID	Логин	Роль	Статус
1000	admin	Admin	Активен 

Для добавления нового пользователя нажмите на кнопку «+Добавить» справа над списком пользователей. Откроется страница с функцией добавления нового пользователя.

[Аудит](#)[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

Создание пользователя

Имя пользователя	<input type="text" value="test"/>
Роль	<input type="text" value="manager"/>
Пароль	<input type="password" value="...."/>
Подтверждение пароля	<input type="password" value="...."/>
<input checked="" type="checkbox"/> Пользователь заблокирован	
<input type="button" value="Сохранить"/>	

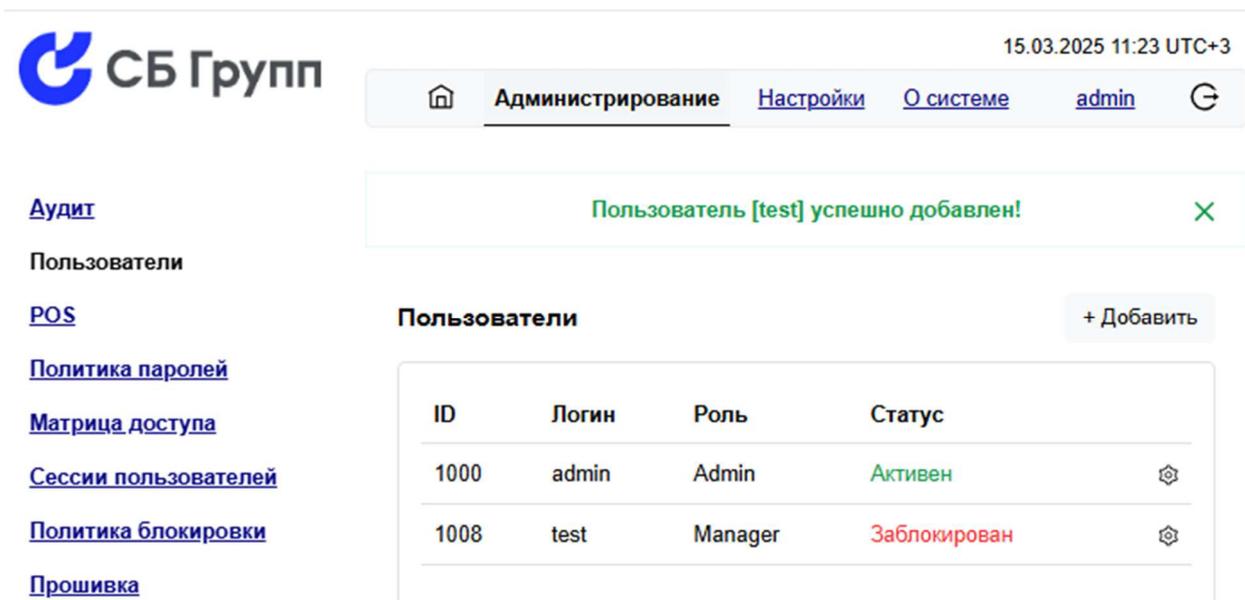
Введите имя пользователя, например «test». Назначьте роль создаваемому пользователю, например «manager». Введите пароль пользователя, затем введите его ещё раз повторно.

Политикой Модуля определено, что при создании новой учетной записи она автоматически заблокирована. Что бы создать учетную запись не заблокированной, снимите галочку, напротив пункта «Пользователь заблокирован».

Нажмите кнопку «Сохранить». Учетная запись нового пользователя с назначенной ролью создана.

8.1.2. Разблокировка или блокировка пользователя

Для разблокировки пользователя пройдите все этапы предыдущего подпункта до страницы пользователей. На странице будет присутствовать, созданный в предыдущем подпункте пользователь «test».



15.03.2025 11:23 UTC+3

Администрирование [Настройки](#) [О системе](#) [admin](#)

Пользователь [test] успешно добавлен!

Пользователи + Добавить

ID	Логин	Роль	Статус
1000	admin	Admin	Активен
1008	test	Manager	Заблокирован

Для разблокировки или блокировки пользователя, например «test» нажмите на колесико напротив соответствующего пользователя и выберите пункт «редактировать». Откроется страница с функцией редактирования свойств пользователя.

[Аудит](#)[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

Редактирование пользователя

Имя пользователя

test

Роль

manager

Пароль

Подтверждение пароля

 Пользователь заблокирован[Сохранить](#)

Поставьте или снимите (в зависимости от требуемых действий) галочку, напротив пункта «Пользователь заблокирован». Затем нажмите кнопку «Сохранить». Действия будут тут же применены.

[Аудит](#)[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

Данные пользователя с идентификатором [1008] успешно изменены! ✕

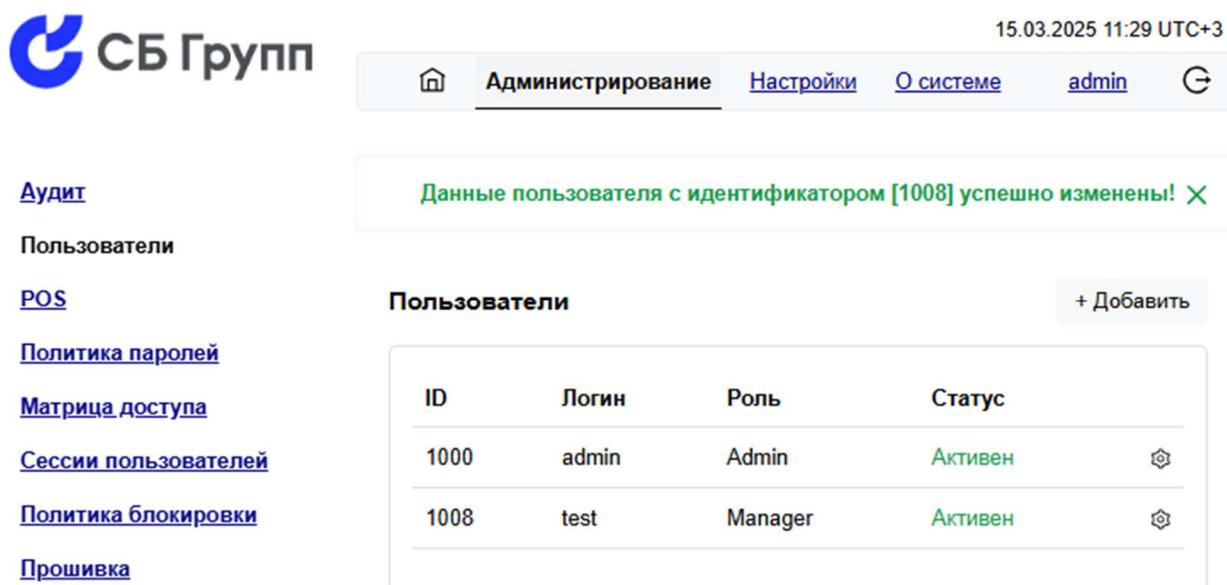
Пользователи

[+ Добавить](#)

ID	Логин	Роль	Статус	
1000	admin	Admin	Активен	
1008	test	Manager	Активен	

8.1.3. Изменение роли пользователя

Для изменения роли пользователя, например пользователя «test», пройдите все этапы первого подпункта до страницы пользователей. На странице будет присутствовать, созданный ранее пользователь «test».



15.03.2025 11:29 UTC+3

СБ Групп

Администрирование [Настройки](#) [О системе](#) [admin](#)

[Аудит](#)

[Пользователи](#)

[POS](#)

[Политика паролей](#)

[Матрица доступа](#)

[Сессии пользователей](#)

[Политика блокировки](#)

[Прошивка](#)

Данные пользователя с идентификатором [1008] успешно изменены! ✕

Пользователи [+ Добавить](#)

ID	Логин	Роль	Статус
1000	admin	Admin	Активен
1008	test	Manager	Активен

Для изменения роли пользователя, например «test» нажмите на колесико напротив соответствующего пользователя и выберите пункт «редактировать». Откроется страница с функцией редактирования свойств пользователя.

[Аудит](#)[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)**Редактирование пользователя**

Имя пользователя	<input type="text" value="test"/>
Роль	<input type="text" value="manager"/>
Пароль	<input type="password"/>
Подтверждение пароля	<input type="password"/>
<input type="checkbox"/> Пользователь заблокирован	
<input type="button" value="Сохранить"/>	

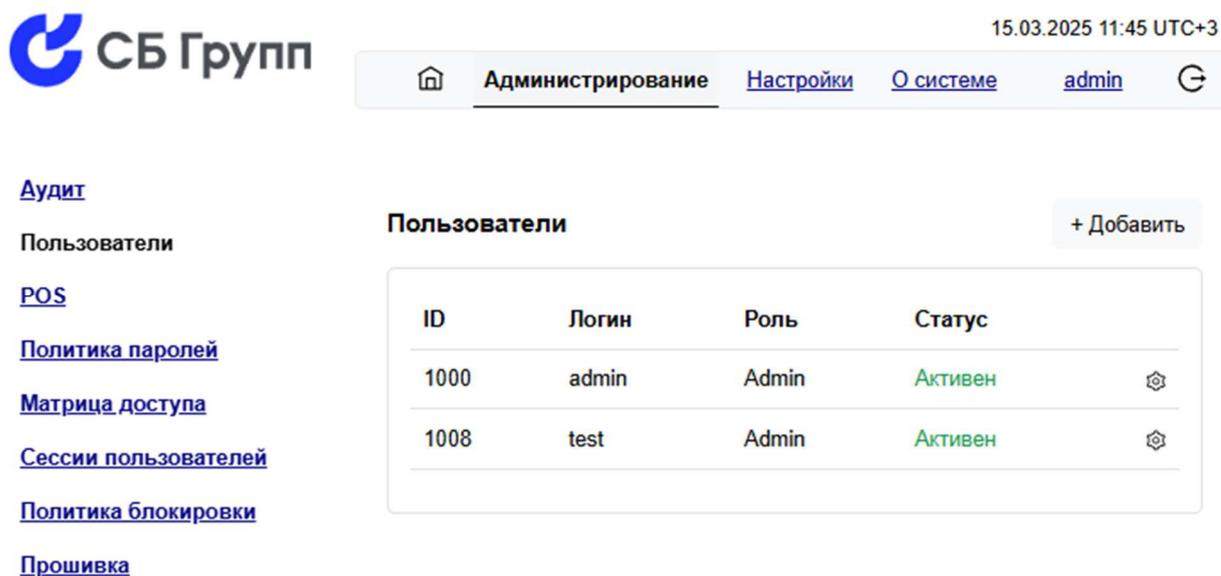
Текущая роль пользователя «manager». Для смены роли нажмите на «manager» и выберите другую роль, например «admin», затем нажмите кнопку «Сохранить». Действия будут тут же применены.

[Аудит](#)[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)**Пользователи**[+ Добавить](#)

ID	Логин	Роль	Статус	
1000	admin	Admin	Активен	
1008	test	Admin	Активен	

8.1.4. Изменение пароля пользователя

Для изменения пароля пользователя, например пользователя «test», пройдите все этапы первого подпункта до страницы пользователей. На странице будет присутствовать, созданный ранее пользователь «test».



15.03.2025 11:45 UTC+3

СБ Групп

Администрирование [Настройки](#) [О системе](#) [admin](#)

[Аудит](#)

[Пользователи](#)

[POS](#)

[Политика паролей](#)

[Матрица доступа](#)

[Сессии пользователей](#)

[Политика блокировки](#)

[Прошивка](#)

Пользователи + Добавить

ID	Логин	Роль	Статус
1000	admin	Admin	Активен
1008	test	Admin	Активен

Для смены пароля пользователя, например «test» нажмите на колесико напротив соответствующего пользователя и выберите пункт «редактировать». Откроется страница с функцией редактирования свойств пользователя.

[Аудит](#)[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)**Редактирование пользователя**

Имя пользователя	<input type="text" value="test"/>
Роль	<input type="text" value="admin"/>
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
<input type="checkbox"/> Пользователь заблокирован	
<input type="button" value="Сохранить"/>	

Введите в соответствующие поля новый пароль и подтверждение нового пароля ещё раз, затем нажмите кнопку «Сохранить». Действия будут тут же применены.

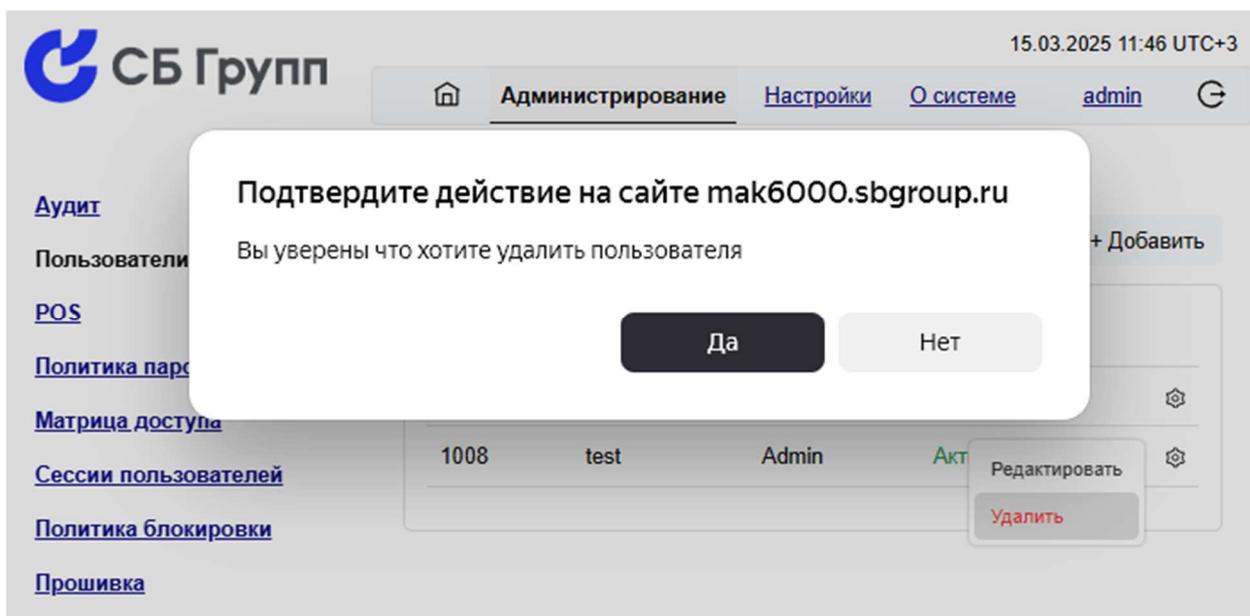
8.1.5. Удаление пользователя

Для удаления пользователя, например пользователя «test», пройдите все этапы первого подпункта до страницы пользователей. На странице будет присутствовать, созданный ранее пользователь «test».

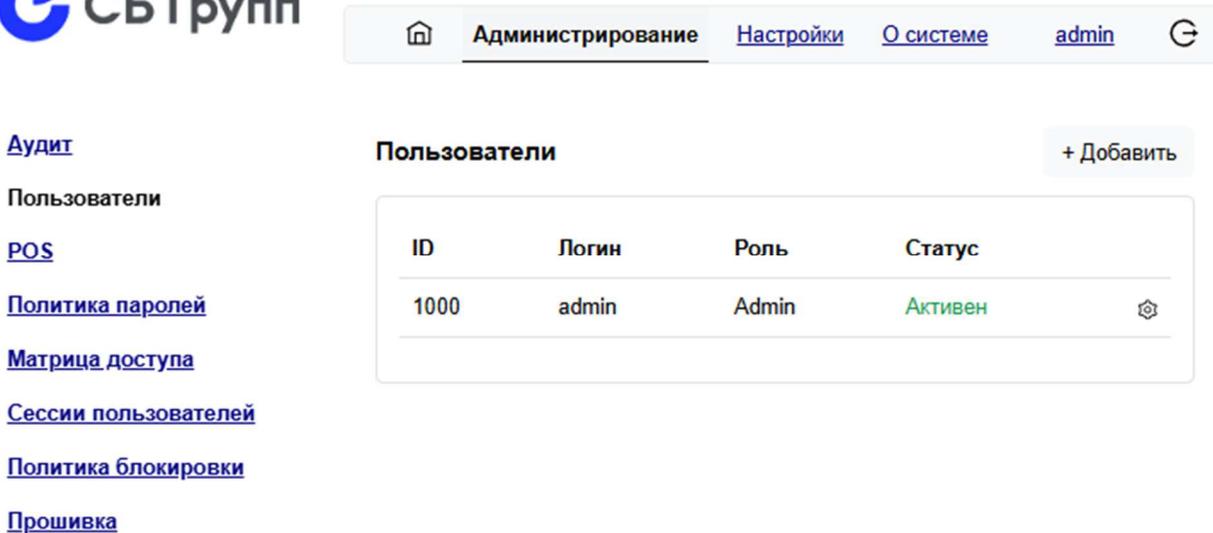
[Аудит](#)[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)**Пользователи**[+ Добавить](#)

ID	Логин	Роль	Статус	
1000	admin	Admin	Активен	
1008	test	Admin	Активен	

Для удаления пользователя, например «test» нажмите на колесико напротив соответствующего пользователя и выберите пункт «Удалить». Откроется всплывающее окно с функцией удаления пользователя. Необходимо подтвердить удаление пользователя.



После нажатия на кнопку «Да» действия, направленные на удаления пользователя «test» будут тут же выполнены.



[Аудит](#)

[Пользователи](#)

[POS](#)

[Политика паролей](#)

[Матрица доступа](#)

[Сессии пользователей](#)

[Политика блокировки](#)

[Прошивка](#)

Пользователи + Добавить

ID	Логин	Роль	Статус
1000	admin	Admin	Активен

8.2. Ограничение доступа к интерфейсу администрирования

В Системе доступ к интерфейсу администрирования Системы разрешен только пользователям Системы с назначенной ролью «admin».

Доступ к администрированию системных функций операционной системы Модуля разрешен только под учетной записью Суперпользователя.

8.3. Ограничение доступа к конфигурационным и временным файлам

Конфигурационные и временные файлы в Модуле расположены в реквизитах файловой системы операционной системы. Доступ к файловой системе операционной системы разрешен только под учетной записью Суперпользователя.

8.4. Ограничение доступа к интерфейсу просмотра журнала событий

Доступ к интерфейсу просмотра журнала событий в Системе разрешен только пользователям Системы с назначенной ролью «admin».

8.5. Настройка длительности периода неактивности для автоматической блокировки сессии

В Системе реализована функция автоматической блокировки сессии пользователя Системы по окончании заданного периода неактивности. Параметр периода неактивности является настраиваемой величиной.

Для изменения периода неактивности для автоматической блокировки сессии авторизуйтесь в Системе под учетной записью Администратора Системы, затем из главного меню Системы перейдите в блок «Администрирование», после чего откроется раздел администрирования Системы:



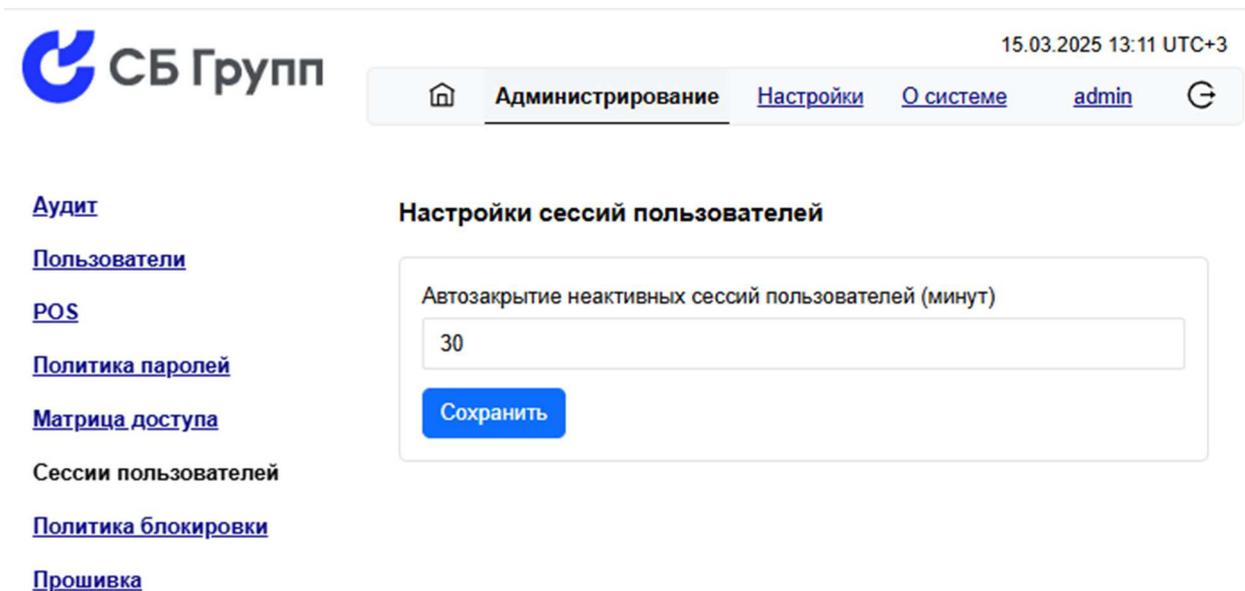
Аудит

[Пользователи](#)[РОС](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

Аудит действий пользователя

ID	Дата и время	Пользователь	Действие	Статус
bb753892-653d-4830-a713-6452d6364c6f	2025-03-12 09:30:30	admin	Вход в систему	Успешно
22f81ea2-4a5d-42aa-8f06-fbf16d345dec	2025-03-10 15:41:56	admin	Вход в систему	Успешно
ееcb54d0-f00a-43ec-9f3f-9ef8358dd210	2025-03-10 15:11:10	admin	Вход в систему	Успешно
721ea2ff-8fc9-471a-b7b2-716d41765e69	2025-03-07 11:24:35	admin	Вход в систему	Успешно

С левой стороны расположено меню административных настроек Системы. Нажмите в меню слева на ссылку «Сессии пользователей», после чего будет осуществлен переход на страницу с функционалом указания периода неактивности.



Введите в поле «Автозаккрытие неактивных сессий пользователей (минут)» нужное значение. Значение вводится в минутах. Затем нажмите кнопку «Сохранить». Внесенные изменения вступят в силу немедленно.

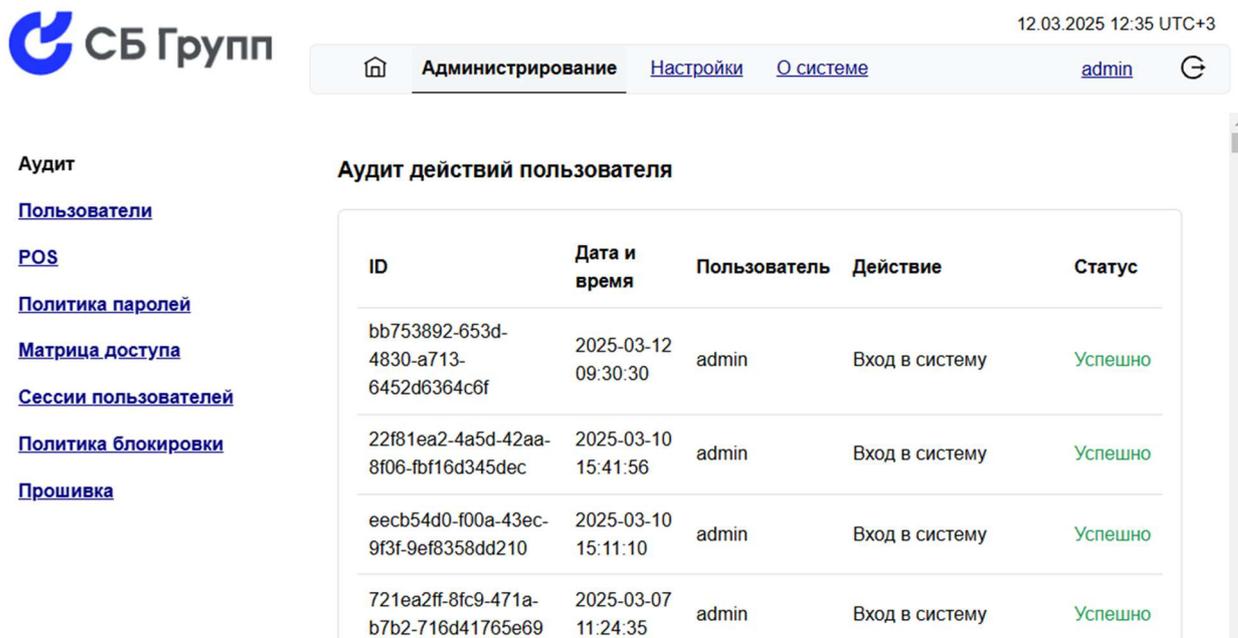
8.6. Матрица доступа

Страница «Матрица доступа» в Системе предназначена для реализации следующих функций:

- ограничение доступа к интерфейсу администрирования аппаратного обеспечения оборудования;
- скрытие конфигурации аппаратного обеспечения оборудования от Пользователей.

Для доступа к странице «Матрица доступа» авторизуйтесь в Системе под учетной записью Администратора Системы, затем из

главного меню Системы перейдите в блок «Администрирование», после чего откроется раздел администрирования Системы:



The screenshot shows the 'Администрирование' (Administration) section of the system. On the left is a navigation menu with links: Пользователи, РОС, Политика паролей, Матрица доступа, Сессии пользователей, Политика блокировки, and Прошивка. The main content area is titled 'Аудит действий пользователя' (User Action Audit) and contains a table with the following data:

ID	Дата и время	Пользователь	Действие	Статус
bb753892-653d-4830-a713-6452d6364c6f	2025-03-12 09:30:30	admin	Вход в систему	Успешно
22f81ea2-4a5d-42aa-8f06-fbf16d345dec	2025-03-10 15:41:56	admin	Вход в систему	Успешно
eecb54d0-f00a-43ec-9f3f-9ef8358dd210	2025-03-10 15:11:10	admin	Вход в систему	Успешно
721ea2ff-8fc9-471a-b7b2-716d41765e69	2025-03-07 11:24:35	admin	Вход в систему	Успешно

С левой стороны расположено меню административных настроек Системы. Нажмите в меню слева на ссылку «Матрица доступа», после чего будет осуществлен переход на страницу с функционалом, позволяющим установить ограничения доступа к интерфейсу администрирования аппаратного обеспечения оборудования и скрытие конфигурации аппаратного обеспечения оборудования от пользователей.

[Аудит](#)[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

Матрица доступа

	admin	host	manager	service	root	pos
Администрирование	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Настройки / SSH	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Информация о системе	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1. Information	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Installation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Operation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Reset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Diagnostics	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W W & M	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Сохранить](#)

Для ролей «admin» (главный Администратор Системы), root (Суперпользователь) и pos (пользователь POS протокола) изменить ограничения невозможно.

Пользователи под ролью «admin» всегда будут иметь доступ к интерфейсу администрирования аппаратного обеспечения оборудования и к конфигурации аппаратного обеспечения оборудования, за исключением доступа к операционной системе Модуля.

Пользователи под ролью «root» всегда будут иметь доступ только к интерфейсу администрирования операционной системы Модуля.

Так же невозможно открыть доступ пользователям с какой-либо ролью, за исключением роли «admin», к административной части Системы. А также невозможно открыть доступ пользователям с какой-либо ролью, за исключением роли «root», к настройкам операционной системы Модуля и к функции удаленного доступа по SSH.

Для всех остальных пользователей, с ролями «host», «manager» и «service» предоставляется возможность выборочного или полного сокрытия доступа к интерфейсу администрирования аппаратного обеспечения оборудования и к конфигурации аппаратного обеспечения оборудования, а именно:

- страница «Информация о системе» Системы;
- ветка «1. Information» Контроллера;
- ветка «2. Installation» Контроллера;
- ветка «3. Operation» Контроллера;
- ветка «4. Reset» Контроллера;
- ветка «5. Diagnostics» Контроллера;
- ветка «W W & M» Контроллера.

Для сокрытия доступа к требуемым страницам и веткам Системы установите галочки напротив соответствующих элементов и нажмите кнопку «Сохранить». Изменения будут приняты немедленно.

8.7. Удаленный доступ по SSH

Операционная система Модуля содержит встроенную функцию удаленного доступа протоколу SSH. Удаленный доступ по протоколу SSH предоставляется только к операционной системе Модуля.

Авторизация на доступ по протоколу SSH возможна только под учетной записью Суперпользователя.

Функция разрешения/блокировки удаленного доступа по протоколу SSH реализована в веб-интерфейсе Системы. Для доступа к функции из главного меню Системы перейдите в блок «Настройки» и введите пароль Суперпользователя.

Вход в панель настроек

Логин

Пароль

В случае успешной авторизации в Системе под учетной записью Суперпользователя вы попадаете в раздел системных настроек Модуля.



Сетевые интерфейсы

[Дата и время](#)[Автоматическая
синхронизация времени](#)[Установка и обновление](#)[Сертификаты и ключи](#)[Межсетевой экран](#)[Пароль](#)[Суперпользователя](#)[Выход из панели
настроек](#)

Авторизация успешна



WAN интерфейс

IPv4-адрес

Маска сети IPv4

IPv4-адрес шлюза

Сетевые службы WAN интерфейса

Удаленное управление (SSH Server)

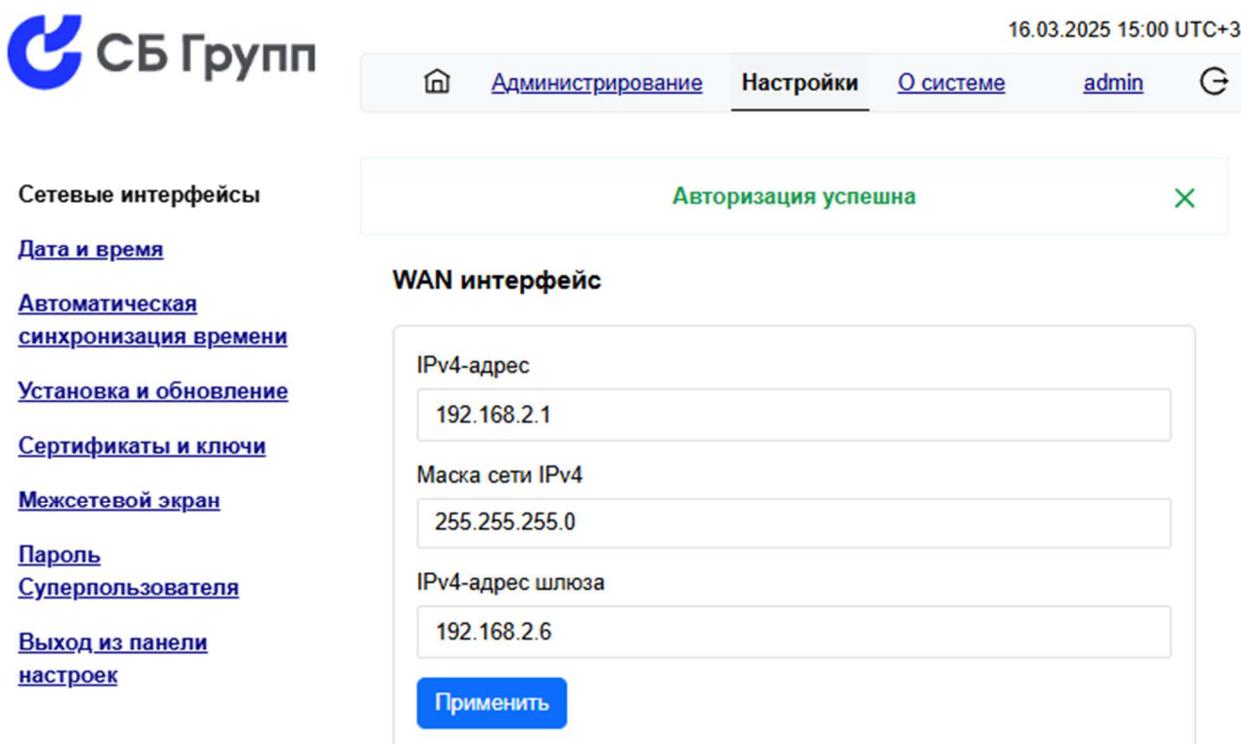
 Открыть доступ к утилите через внешний 22 порт

Для того, чтобы отключить удаленный доступ к операционной системе Модуля по протоколу SSH снимите галочку напротив функции «Открыть доступ к утилите через внешний 22 порт» (установленная галочка, наоборот, разрешает удаленный доступ по SSH).

8.8. Удаленный доступ для POS протокола

В Системе реализована функция проброса портов POS протокола на Контроллер. Управление доступом по портам протокола POS выведено в веб-интерфейс Системы.

Для доступа к странице управления удаленным доступом для портов POS протокола проделайте шаги из предыдущего пункта до момента успешной авторизации в блоке «Настройки».



СБ Групп 16.03.2025 15:00 UTC+3

[Администрирование](#) **Настройки** [О системе](#) [admin](#)

Сетевые интерфейсы

[Дата и время](#)

[Автоматическая синхронизация времени](#)

[Установка и обновление](#)

[Сертификаты и ключи](#)

[Межсетевой экран](#)

[Пароль Суперпользователя](#)

[Выход из панели настроек](#)

Авторизация успешна ✕

WAN интерфейс

IPv4-адрес
192.168.2.1

Маска сети IPv4
255.255.255.0

IPv4-адрес шлюза
192.168.2.6

[Применить](#)

С левой стороны расположено меню системных настроек Модуля. Нажмите в меню слева ссылку «Межсетевой экран», после чего будет

осуществлен переход на страницу с функционалом, позволяющим разрешить или запретить удаленный доступ к портам POS протокола.

[Сетевые интерфейсы](#)[Дата и время](#)[Автоматическая
синхронизация времени](#)[Установка и обновление](#)[Сертификаты и ключи](#)[Межсетевой экран](#)[Пароль
Суперпользователя](#)[Выход из панели
настроек](#)**Config redirect**

- Port 5001 Installation and other Supervised operations
- Port 5002 Unsolicited messages for Supervised operations
- Port 5003 Reserved for a Doms Fall Back Console
- Port 5004 Unsupervised operations
- Port 5005 Unsolicited messages for Unsupervised operations (transactions)
- Port 5006 Unsolicited messages for external payment server
- Port 5007 Interface to Payment Server (Reserved for)
- Port 5008 Transparent Security PIN PAD interface
- Port 5009 Interface to a remote Log Server

[Применить](#)

Установленная галочка напротив обозначения порта и его описания разрешает удаленный доступ. Что бы заблокировать удаленный доступ по какому-либо порту POS протокола снимите галочку напротив соответствующего порта и нажмите кнопку «Применить». Удаленный доступ по портам будет заблокирован немедленно.

9. ОБЕСПЕЧЕНИЕ ИБ. РЕГИСТРАЦИЯ И УЧЕТ СОБЫТИЙ ИБ

В Системе реализован функционал регистрации и учета событий информационной безопасности. Так же в Системе предусмотрен централизованный интерфейс для работы с журналами событий безопасности.

Удаленный доступ к журналу регистрации событий информационной безопасности реализован через веб-интерфейс. Удаленный доступ к странице с журналом регистрации событий информационной безопасности осуществляется с использованием веб-браузера.

Для доступа к странице журнала авторизуйтесь в Системе под учетной записью Администратора Системы, затем из главного меню Системы перейдите в блок «Администрирование». Откроется страница с журналом событий информационной безопасности.

Аудит

[Пользователи](#)[POS](#)[Политика паролей](#)[Матрица доступа](#)[Сессии пользователей](#)[Политика блокировки](#)[Прошивка](#)

Аудит действий пользователя

ID	Дата и время	Пользователь	Действие	Статус
bb753892-653d-4830-a713-6452d6364c6f	2025-03-12 09:30:30	admin	Вход в систему	Успешно
22f81ea2-4a5d-42aa-8f06-fb16d345dec	2025-03-10 15:41:56	admin	Вход в систему	Успешно
eecb54d0-f00a-43ec-9f3f-9ef8358dd210	2025-03-10 15:11:10	admin	Вход в систему	Успешно
721ea2ff-8fc9-471a-b7b2-716d41765e69	2025-03-07 11:24:35	admin	Вход в систему	Успешно

Функционалом Системы обеспечивается журналирование действий администратора, изменения конфигураций, а также следующих событий:

- вход в систему;
- вход в настройки;
- выход из системы;
- создание Пользователя;
- изменение параметров Пользователя;
- изменение привилегий Пользователя;
- удаление Пользователя.

Атрибутный состав событий, журнала событий информационной безопасности включает в себя следующие поля:

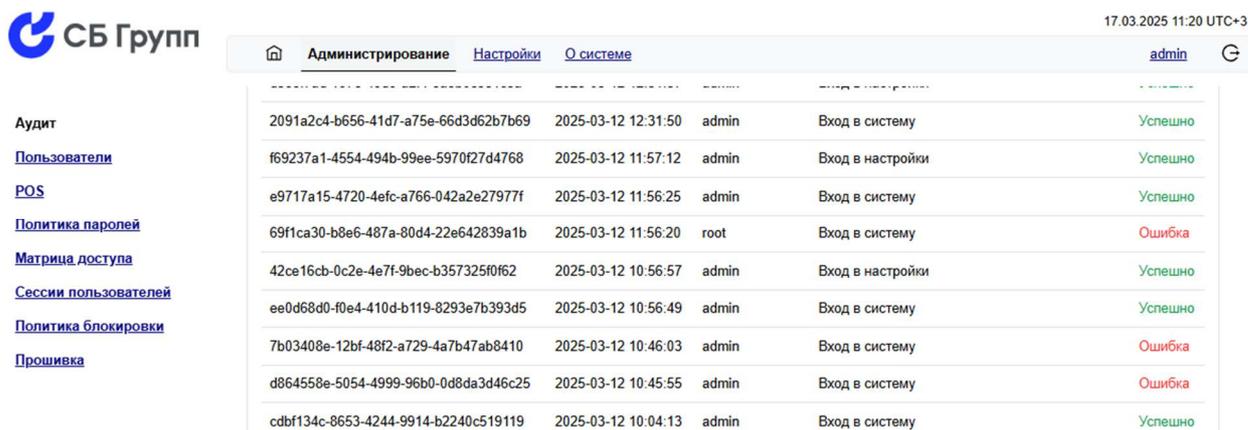
- дата возникновения события;
- время возникновения события;
- идентификатор события;
- наименование события;
- субъект операции;
- результат операции.

9.1. Регистрация успешных/неуспешных попыток доступа

В Системе реализован функционал регистрации успешных и неуспешных попыток доступа к оборудованию. Результат регистрации отображается в журнале регистрации событий информационной безопасности в графе «Статус».

Для просмотра журнала регистрации событий информационной безопасности выполните действия, указанные в настоящем разделе

выше, до момента, когда откроется страница с журналом событий информационной безопасности. Обратите внимание на графу «Статус», которая может выглядеть, например так:



The screenshot shows the administration interface of the SB Group system. At the top, there is a navigation bar with the SB Group logo, the text 'СБ Групп', and the date '17.03.2025 11:20 UTC+3'. Below the navigation bar, there are tabs for 'Администрирование', 'Настройки', and 'О системе'. The 'Администрирование' tab is active, and the 'admin' user is logged in. On the left side, there is a sidebar menu with links for 'Аудит', 'Пользователи', 'РОС', 'Политика паролей', 'Матрица доступа', 'Сессии пользователей', 'Политика блокировки', and 'Прошивка'. The main content area displays a table of events with the following columns: ID, Date and Time, User, Action, and Status.

ID	Дата и время	Пользователь	Действие	Статус
2091a2c4-b656-41d7-a75e-66d3d62b7b69	2025-03-12 12:31:50	admin	Вход в систему	Успешно
f69237a1-4554-494b-99ee-5970f27d4768	2025-03-12 11:57:12	admin	Вход в настройки	Успешно
e9717a15-4720-4efc-a766-042a2e27977f	2025-03-12 11:56:25	admin	Вход в систему	Успешно
69f1ca30-b8e6-487a-80d4-22e642839a1b	2025-03-12 11:56:20	root	Вход в систему	Ошибка
42ce16cb-0c2e-4e7f-9bec-b357325f0f62	2025-03-12 10:56:57	admin	Вход в настройки	Успешно
ee0d68d0-f0e4-410d-b119-8293e7b393d5	2025-03-12 10:56:49	admin	Вход в систему	Успешно
7b03408e-12bf-48f2-a729-4a7b47ab8410	2025-03-12 10:46:03	admin	Вход в систему	Ошибка
d864558e-5054-4999-96b0-0d8da3d46c25	2025-03-12 10:45:55	admin	Вход в систему	Ошибка
cdbf134c-8653-4244-9914-b2240c519119	2025-03-12 10:04:13	admin	Вход в систему	Успешно

Если в графе «Статус», интересующего вас события информационной безопасности, указан статус «Успешно», это означает, что функция Системы зарегистрировала успешную попытку доступа к оборудованию.

Если в графе «Статус», интересующего вас события информационной безопасности, указан статус «Ошибка», это означает, что функция Системы зарегистрировала неуспешную попытку доступа к оборудованию.

9.2. Меры защиты журнала регистрации событий ИБ

Журналы событий информационной безопасности хранятся в реквизитах файловой системы операционной системы Модуля, отдельно от журналов системных событий Модуля и Контроллера.

Доступ к журналам событий информационной безопасности для пользователей Системы (в рамках назначенных ролей и прав доступа), включая главного Администратора Системы возможен только на

чение. Данная конфигурация определена функционалом Системы и не имеет возможности редактирования.

Полный доступ к журналам событий информационной безопасности может получить только Суперпользователь. Суперпользователь имеет полный доступ к файловой системе операционной системы Модуля, в реквизитах которой хранятся журналы событий информационной безопасности.

10. ОБЕСПЕЧЕНИЕ ИБ. ПРОЧИЕ СВЕДЕНИЯ

В настоящем разделе описаны сведения о встроенных функциях информационной безопасности Системы, не вошедшие в другие разделы.

10.1. Информация о фактическом состоянии объектов аудита ИБ

Весь функционал Модуля расширения реализован в единственном приложении, работающим в среде операционной системы семейства Linux. Интерфейсом взаимодействия с администратором Системы является веб-браузер, работающий по защищенному протоколу HTTPS, запущенный на стандартном 443 порту.

Для оценки фактического состояния функционального приложения Модуля, в том числе для оценки фактического состояния встроенных средств информационной безопасности достаточно, например, убедиться в наличии ответа от Модуля по 443-порту.

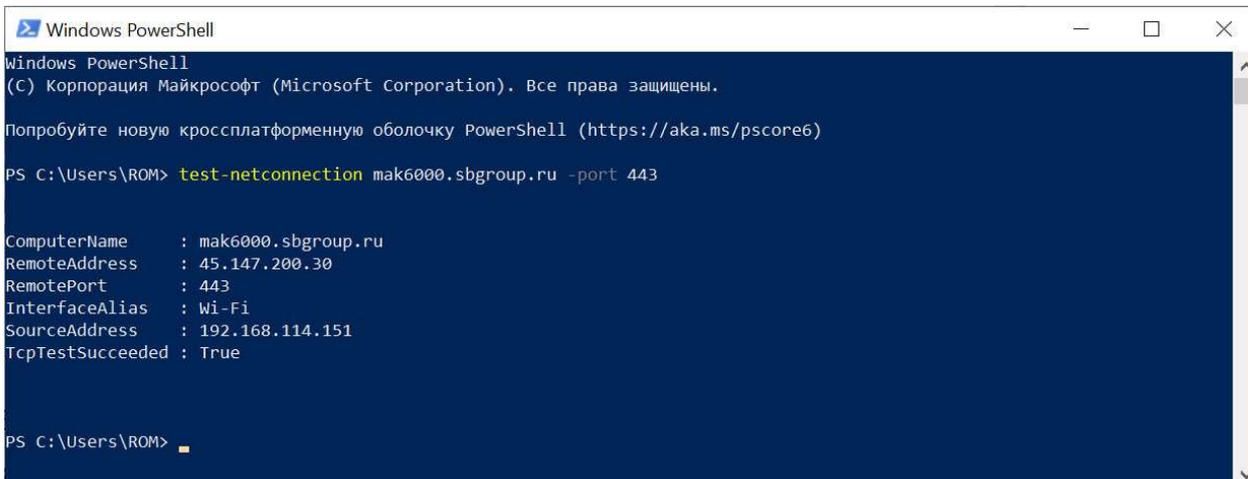
Например, для APM-а администратора с операционной системой Windows можно воспользоваться встроенным приложением автоматизации PowerShell.

Для этого запустите на APM-ме Администратора PowerShell и введите команду:

```
test-netconnection mak6000.sbgroupp.ru -port 443
```

, где: mak6000.sbgroupp.ru – локальное DNS имя Системы.

В случае подтверждения работоспособного состояния Модуля в среде PowerShell будут отображены следующие результаты:



```

Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)

PS C:\Users\ROM> test-netconnection mak6000.sbgroun.ru -port 443

ComputerName      : mak6000.sbgroun.ru
RemoteAddress     : 45.147.200.30
RemotePort        : 443
InterfaceAlias    : Wi-Fi
SourceAddress     : 192.168.114.151
TcpTestSucceeded  : True

PS C:\Users\ROM>
    
```

Значение «True» параметра «TcpTestSucceeded» подтверждает работоспособное состояние Модуля. Когда Модуль находится в неработоспособном состоянии, значение параметра «TcpTestSucceeded» будет отображено как «False».

10.2. Сведения о сетевых параметрах

Для функционирования Системы используются следующие протоколы и порты:

Протокол	Порты	Назначение
HTTP	80	Предназначен для первичной настройки Модуля расширения, либо для обновления сертификатов с истекшим сроком
HTTPS	443	Предназначен для администрирования Системы, взаимодействия пользователей с Системой
SSH	22	Предназначен для администрирования операционной системы Модуля расширения
POS	5001-5009*	Используется для взаимодействия Контроллера с внешними устройствами ¹

¹ За подробными сведениями о требованиях к портам POS протокола обратитесь к руководству на POS протокол.

10.3. Сведения о взаимодействии с сетью Интернет

В Системе отсутствуют неотключаемые функции взаимодействия с сетью Интернет, в том числе в части управления лицензиями.

Для полнофункциональной работы Системы не требуется предоставление доступа в сеть Интернет.

10.4. Сведения о хранении и передаче паролей (ключей)

Пароли пользователей Системы хранятся в базе данных, которая в свою очередь расположена в реквизитах файловой системы операционной системы Модуля. Пароли хранятся в виде уникального битового массива, сформированного по алгоритму хеширования HMAC SHA512.

Пароли пользователей операционной системы Модуля хранятся в реквизитах файловой системы операционной Системы Модуля в хешированном виде.

Пароли пользователей Контроллера хранятся в реквизитах файловой системы Контроллера в хешированном виде.

Доступ к веб-интерфейсу взаимодействия с Системой как для пользователей, так и для администратора осуществляется по защищённому протоколу HTTPS.

Доступ к консольному интерфейсу администрирования операционной системы Модуля осуществляется по защищенному протоколу SSH.

10.5. Требования по обеспечению безопасности применения

Для безопасности эксплуатации Системы и программного обеспечения должны выполняться организационно-технические и административные требования. К ним относятся требования по:

- физическому размещению Системы;
- установке ПО на Систему;
- средствам защиты от НСД к ОС и управлению Системы;
- обеспечению бесперебойного режима работы Системы.

При размещении Системы в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются сведения, составляющие государственную тайну или конфиденциального характера, данные Системы должны иметь соответствующее разрешение.

Размещение, специальное оборудование, охрана и режим в помещении, в котором устанавливается Система для эксплуатации (далее – помещение), должны обеспечивать:

- безопасность информации, Системы и ключевых документов;
- невозможность доступа к Системе лиц, не допущенных к работе с Системой, к аппаратным и программным средствам Системы, к эксплуатационной документации и ключевым документам Системы, к просмотру процедур работы с Системой;
- исключение кражи компонентов Системы.

Подготовка Системы к работе осуществляется в соответствии с требованиями эксплуатационной документации.

Порядок допуска в помещение определяется внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры организации, использующей Систему.

Помещение оборудуется средствами, препятствующими несанкционированному доступу в помещение, например, такими как: охранная сигнализация, прочные входные двери, надежные замки или иные средства.

Устанавливаемый руководителем организации порядок охраны помещения должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.

Должны быть предприняты меры, препятствующие несанкционированному вскрытию шкафа Системы, то есть шкаф должен быть опечатан. Наряду с этим допускается применение других средств контроля доступа к Системе.

Должны быть предприняты меры, которые определяются внутренней инструкцией, исключающие несанкционированный доступ к Системе лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе с Системой.

Администратор безопасности должен периодически проводить контроль сохранности пломб шкафа Системы с занесением результатов проверки в журнал.

Порядок действий при обнаружении несанкционированного вскрытия шкафа Системы должен определяться регламентами организации, эксплуатирующей Систему, и быть прописан во внутренних инструкциях.

ПРИЛОЖЕНИЕ А. ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

Термин	Расшифровка
Контроллер	Контроллер сопряжения «Gilbarco DOMS PSS 5000» или контроллер сопряжения «МАК 6000»
Модуль	Модуль «МИБ 101», предназначенный для модернизации контроллеров сопряжения «Gilbarco DOMS PSS 5000» или «МАК 6000»
Система	Модернизированный контроллер сопряжения «Gilbarco DOMS PSS 5000» или модернизированный контроллер сопряжения «МАК 6000»
Администратор Системы	Пользователи с ролью «admin» в прикладной части прошивки Модуля и прошивки Контроллера
Пользователь Системы	Пользователи с ролью, отличной от «admin» в прикладной части прошивки Модуля и прошивки Контроллера
Суперпользователь	Пользователь с ролью «root» в системной части прошивки Модуля

ПРИЛОЖЕНИЕ Б. ИСТОРИЯ ИЗМЕНЕНИЙ В ДОКУМЕНТЕ

Версия документа	Внесенные изменения
1.0	Выполнены стилистика и форматирование документа