



ООО «ИТРИУМ СПб»

**Видеоинформационная консоль  
«ВИК»**

**Руководство пользователя**

**Санкт – Петербург**

**2016**

# Содержание

<b>1</b>	<b>ОПИСАНИЕ ИЗДЕЛИЯ .....</b>	<b>3</b>
1.1	Назначение изделия .....	3
1.2	Выполняемые функции.....	4
1.3	Условия работы.....	4
<b>2</b>	<b>МОНТАЖ ИЗДЕЛИЯ .....</b>	<b>5</b>
2.1	Крепежные элементы, габаритные и установочные размеры.....	5
2.2	Питание устройства .....	5
2.3	Подключение к сети Ethernet.....	6
<b>3</b>	<b>НАСТРОЙКА ИЗДЕЛИЯ .....</b>	<b>8</b>
3.1	Подключение к интерфейсу .....	8
3.2	Базовое конфигурирование.....	9
3.3	Настройка ВИК .....	12
3.4	Проверка настроек.....	12
3.5	Создание резервной копии.....	13
<b>4</b>	<b>ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ .....</b>	<b>13</b>
4.1	Режимы работы изделия .....	13
4.2	Режим «Терминал» .....	13
<b>5</b>	<b>ГАРАНТИИ ИЗГОТОВИТЕЛЯ .....</b>	<b>18</b>
<b>6</b>	<b>СВЕДЕНИЯ ОБ ИЗГОТОВИТЕЛЕ .....</b>	<b>18</b>
<b>7</b>	<b>ПРИЛОЖЕНИЯ .....</b>	<b>19</b>

# 1 ОПИСАНИЕ ИЗДЕЛИЯ

## 1.1 Назначение изделия

- 1.1.1 Видеоинформационная консоль «ВИК» – это IP-консоль интерактивного управления подсистемами охранной, пожарной сигнализации и СКУД КСБ НЕЙРОСС.
- 1.1.2 По способу взаимодействия с пользователем, «ВИК» относится к классу так называемых информационных сенсорных киосков. В отличие от специализированных компьютерных и программных средств обеспечения работы операторов и диспетчерских служб, информационные сенсорные киоски являются многопользовательскими устройствами, предоставляющими «условно каждому» простой, интуитивно понятный интерфейс доступа к типовым информационным сервисам.
- 1.1.3 По функциональному назначению, «ВИК» может использоваться в качестве устройства постановки/снятия с охраны или как «индикационная панель», отображающая информацию КСБ и также предоставляющая функции управления. Традиционно, эти функции выполнялись с помощью специализированных устройств с кнопочными клавиатурами, LCD и фиксированными светодиодными индикаторами, подключёнными к охранным и пожарным панелям.
- 1.1.4 IP-консоль «ВИК» предоставляет пользователю современный интерактивный интерфейс доступа к функциям системы в целом, а не к конкретному контроллеру или панели.
- 1.1.5 Конструктивно ВИК представляет собой планшетный компьютер, предназначенный для установки на стены или встраивания в иные конструкции. Конструктивные исполнения и требования к дизайну могут согласовываться на этапе проектирования соответствующих систем. В связи с особенностями применения (физическая безопасность), используются планшетные компьютеры с Ethernet-подключением, а не с типовым для планшетов и традиционных информационных сенсорных киосков — Wi-Fi. По тем же резонам на планшетах устанавливается ОС Linux, а не Android. Необходимую функциональность и информационное взаимодействие ВИК с КСБ, в том числе с контроллерами и ПО ITRIUM, обеспечивает устанавливаемое на планшеты ПО НЕЙРОСС.

## **1.2 Выполняемые функции**

- 1.2.1 Контролирует состояние связи и обеспечивает синхронизацию данных с другими узлами сети, в том числе с другими устройствами «ВИК», «Борей», «КБУ-1», комплексной системой безопасности ITRIUM;
- 1.2.2 Ведет журналирование событий в энергонезависимой памяти;
- 1.2.3 Предоставляет пользовательский интерфейс конфигурирования и мониторинга состояний и управления посредством веб-браузера;
- 1.2.4 Обеспечивает идентификацию по пин-коду (с защитой от подбора кода с помощью интерактивной скремблированной клавиатуры) и интерфейс навигации по охраняемым объектам.
- 1.2.5 Изделие обеспечивает взаимное обнаружение устройств в «своём» сетевом домене, передаёт команды управления другим устройствам домена, контролирует и отображает текущее состояние зон и разделов охранной сигнализации, точек доступа, предоставляет видеоданные.
- 1.2.6 Совместно с «Борей», «ВИК» обеспечивает автономное компьютерное автоматизированное рабочее место мониторинга и управления охранно-тревожной сигнализацией и доступом.

## **1.3 Условия работы**

- 1.3.1 Подключение изделия к информационной сети производится через порт Ethernet с возможностью маршрутизации сетевого трафика.
- 1.3.2 Питание изделия может осуществляться:
  - От источников постоянного тока 12 В (9 — 27 В) (блоков резервного питания). В качестве источника питания рекомендуется применять блок резервного питания БРП-12 «ЯСЕНЬ» ТУ 4372-020-59497651-2008;
  - Посредством PoE (Power over Ethernet — технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными, через стандартную витую пару в сети Ethernet), предоставляется по заказу;
  - От сети ~220 В, 50 Гц с использованием блока питания в комплекте поставки.
- 1.3.3 Изделие предназначено для использования в температурном диапазоне от +5 до +55 °С и рассчитано на круглосуточный режим работы.

## 2 МОНТАЖ ИЗДЕЛИЯ

### 2.1 Крепежные элементы, габаритные и установочные размеры

2.1.1 Изделие монтируется на стену с помощью крепежных планок, входящих в комплект поставки. Планки продеваются в специальные отверстия на корпусе изделия и крепятся к корпусу с помощью винтов, входящих в комплект поставки. Предусмотрена специальная наклейка на стену с обозначением места расположения крепежных элементов. Разъемы для подключения к информационной сети, подачи питания и USB-устройств расположены на задней панели изделия (рисунок 1)

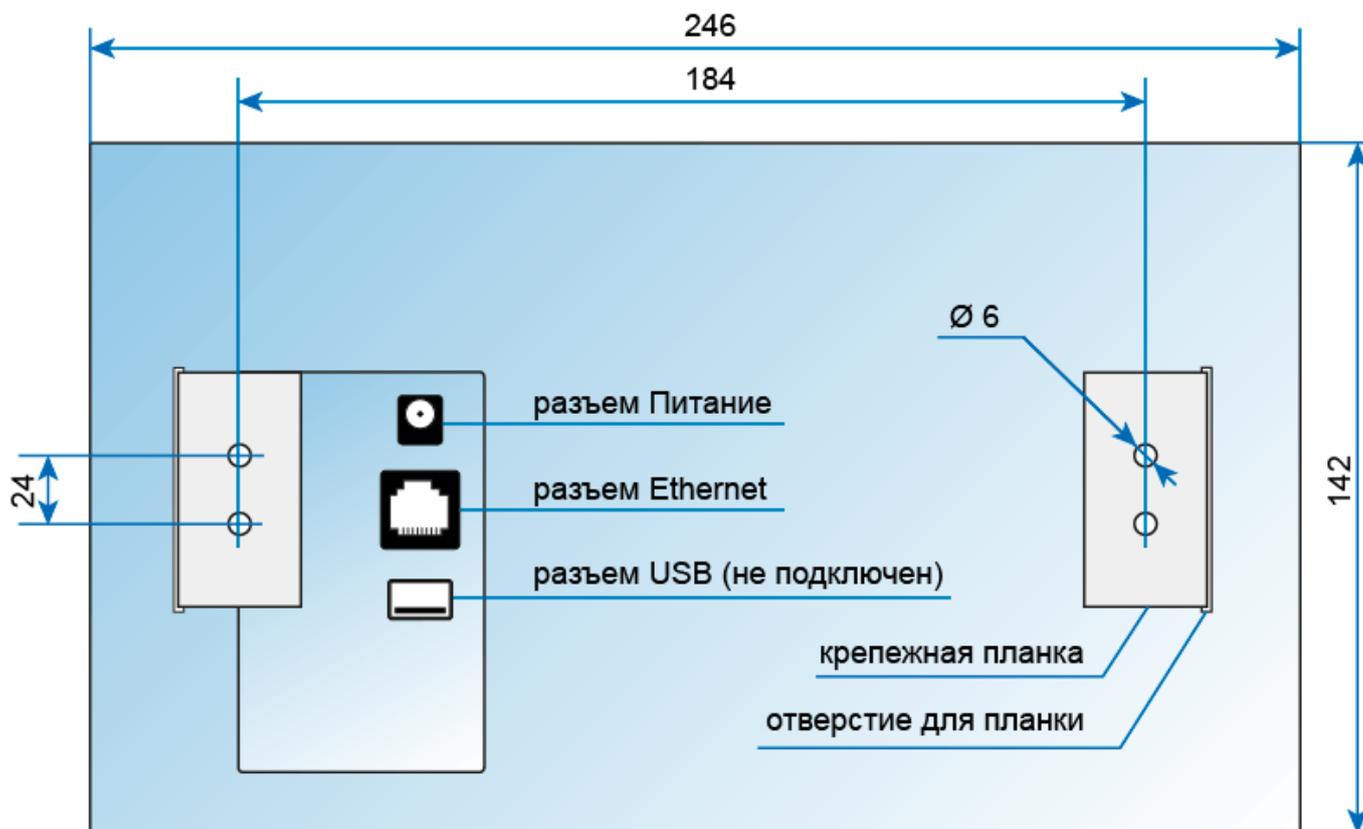


Рисунок 1 – Крепежные элементы, габаритные и установочные размеры изделия

### 2.2 Питание устройства

2.2.1 Схема подключения питания от источника постоянного тока 9 – 27 В приведена на рисунке 2.

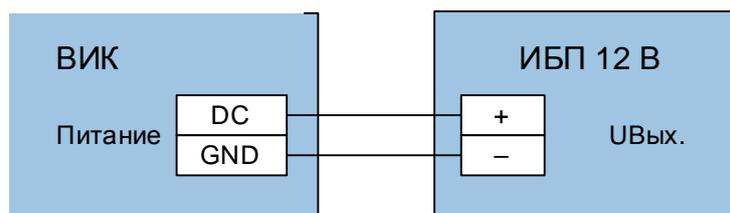


Рисунок 2 – Схема подключения источника бесперебойного питания (ИБП)

2.2.2 Схема подключения питания посредством витой пары сети Ethernet приведена на рисунке 5.

## 2.3 Подключение к сети Ethernet

2.3.1 При подключении питания посредством источника бесперебойного питания, благодаря встроенному сетевому коммутатору и наличию двух разъемов Ethernet на плате «Борей», возможно прямое последовательное соединение нескольких устройств «Борей», одного «ВИК» и конфигурационного компьютера (рисунок 3), также возможно создание сетевой инфраструктуры с использованием коммутатора (рисунок 4).

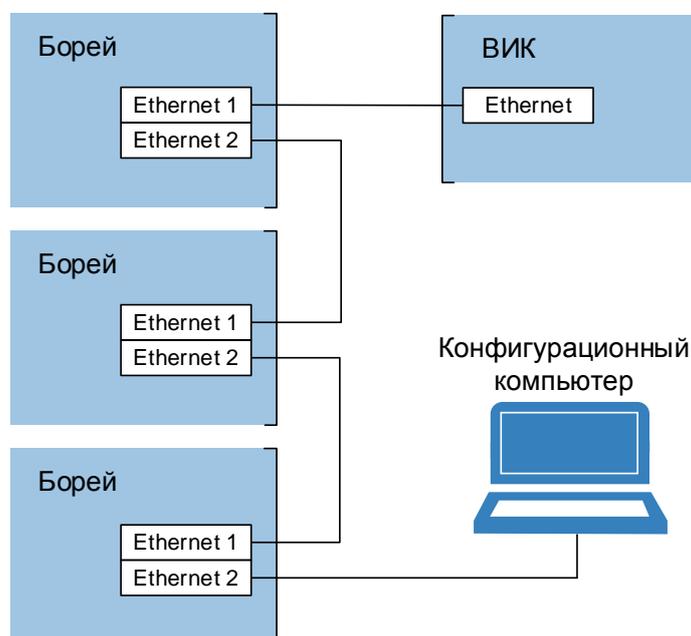


Рисунок 3 — Схема подключения устройств к сети Ethernet. «Коммутируемая IP-шина»

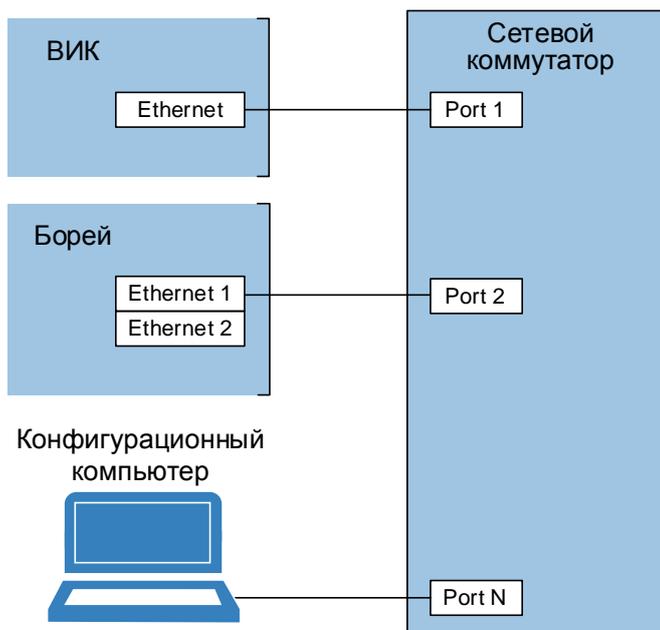


Рисунок 4 – Схема подключения устройств к сети Ethernet. Классический вариант

2.3.2 При использовании технологии PoE, устройства «ВИК» подключаются к сети через PoE инжектор (рисунок 5) и сетевой коммутатор. При этом компьютер для первоначального конфигурирования можно подключить напрямую с использованием второго порта Ethernet устройства «Борей».

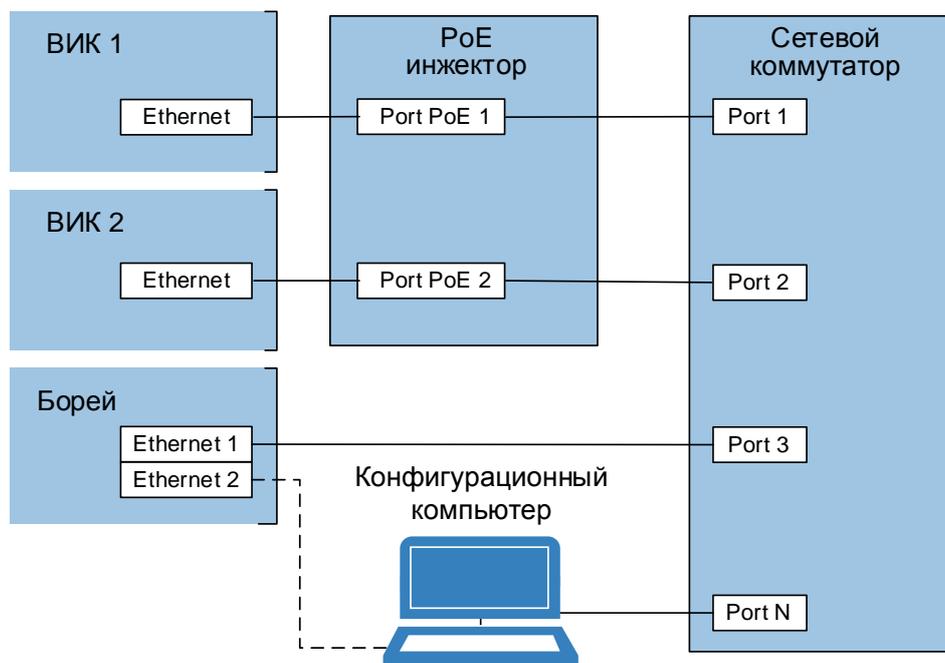


Рисунок 5 — Схема подключения устройств к сети Ethernet с использованием PoE инжектора

### 3 НАСТРОЙКА ИЗДЕЛИЯ

#### 3.1 Подключение к интерфейсу

3.1.1 **Внимание:** Если перед вскрытием упаковки изделие находилось в условиях отрицательных температур, то перед включением изделия его необходимо выдержать при комнатной температуре не менее 4-х часов!

3.1.2 **Выполните последовательно следующие действия:**

3.1.2.1 Подключите устройство к источнику питания.

3.1.2.2 Подключите устройство к компьютеру посредством разъема Ethernet. Настройте сетевое подключение компьютера на работу в диапазоне IP-адресов **192.168.1.XXX** и подсети **255.255.255.0**.

3.1.2.3 Включите питание устройства. Проконтролируйте ток потребления с помощью амперметра. По световым индикаторам на разъёме Ethernet компьютера убедитесь в наличии сетевого соединения.

3.1.2.4 Не более чем через 120 секунд после подачи питания на дисплее устройства должно отображаться окно приветствия, что свидетельствует об успешной загрузке встроенного программного обеспечения прибора и готовности прибора к работе (рисунок 6).



Рисунок 6 — Окно приветствия

3.1.2.5 Подключитесь к веб-интерфейсу прибора. Для этого запустите программу Google Chrome, Mozilla Firefox, Microsoft Edge, Internet Explorer или Apple Safari и в строке адреса введите **192.168.1.100** (см. раздел [Вход в веб-интерфейс](#)). Введите имя пользователя **root** и пароль **root**.

## 3.2 Базовое конфигурирование

- 3.2.1 Перейдите в раздел [Конфигурация узлов](#). В разделе [Основные настройки](#) перейдите к вкладке Мастер-пароль, смените пароль **root**, заданный по умолчанию, на новый (см. раздел [Смена мастер-пароля](#));
- 3.2.2 Перейдите к разделу [Сетевые параметры](#). При необходимости, смените ip-адрес, шлюз, задайте сетевые маршруты, перейдите к вкладке **Дополнительно** и в поле **Домен НЕЙРОСС** укажите латинскими буквами домен НЕЙРОСС (дополнительную информацию о доменах см. в разделе [Понятие домена НЕЙРОСС](#)).

**Внимание:** Если после сохранения новых сетевых параметров устройство стало недоступным, измените настройки сетевого подключения компьютера и выполните подключение к веб-интерфейсу по новому IP-адресу. Если был изменен мастер-пароль, авторизацию следует проходить под новым паролем.

Домены НЕЙРОСС предназначены для обеспечения взаимодействия нескольких устройств, образующих сеть НЕЙРОСС («Борей», «ВИК», «Игнис», ITRIUM, ONVIF IP-камер). Взаимное обнаружение устройств сети НЕЙРОСС производится в пределах заданных в сетевых настройках доменов. Если какое-то устройство (прибор или компьютер с ITRIUM® не «виден» в списке устройств, скорее всего, он принадлежит другой сети или другому домену/доменам.

**Примечание:** После смены домена НЕЙРОСС необходимо выполнить перезагрузку устройства (см. раздел [Перезагрузка прибора](#)).

- 3.2.3 Настройте параметры даты и времени на устройстве (см. раздел [Дата и время](#)). Наилучшим выбором является синхронизация по NTP-серверу (IP-адрес из локальной сети или Интернет).
- 3.2.4 Проверьте сетевую видимость устройств «Борей» и «ВИК»: устройства должны принадлежать одной подсети и одному домену НЕЙРОСС.
- 3.2.5 Выполните синхронизацию «ВИК» с другими устройствами сети НЕЙРОСС, необходимую для обеспечения взаимодействия.
- Перейдите в раздел **Сеть** (рисунок 7), проверьте, что устройства синхронизированы по времени (состояние **Норма**, отсутствует знак рассинхронизации времени ). Выберите «ВИК» и устройство-источник данных («Борей»). Нажмите на кнопку **Синхронизация данных**.

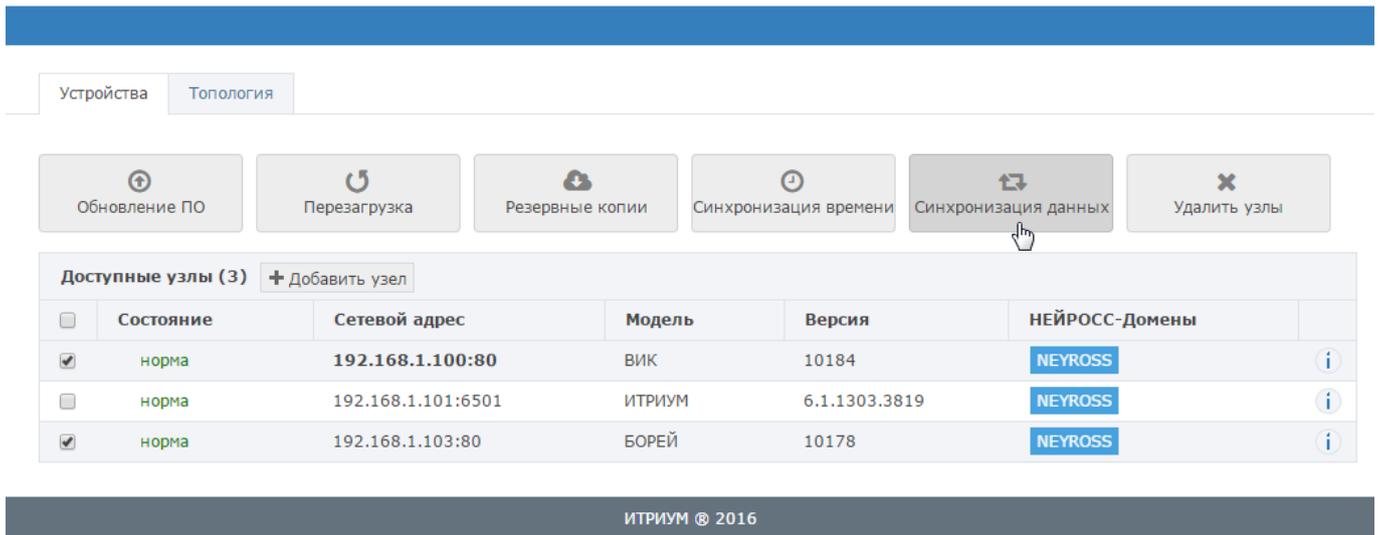


Рисунок 7 — Окно приложения Сеть

- В окне **Синхронизация данных** (рисунок 8) выберите **Синхронизировать вручную**.



Рисунок 8 — Выбор способа синхронизации данных

- Чтобы оценить текущий статус данных, в левом столбце выберите тип данных для сравнения. В основной части окна иконками будет показано текущее состояние (рисунок 9).

**Примечание:** Щелчком левой клавиши мыши по блоку **Легенда** можно раскрыть описание обозначений статусов синхронизации. Наведением указателя мыши по имени статуса, можно ознакомиться с дополнительным описанием.

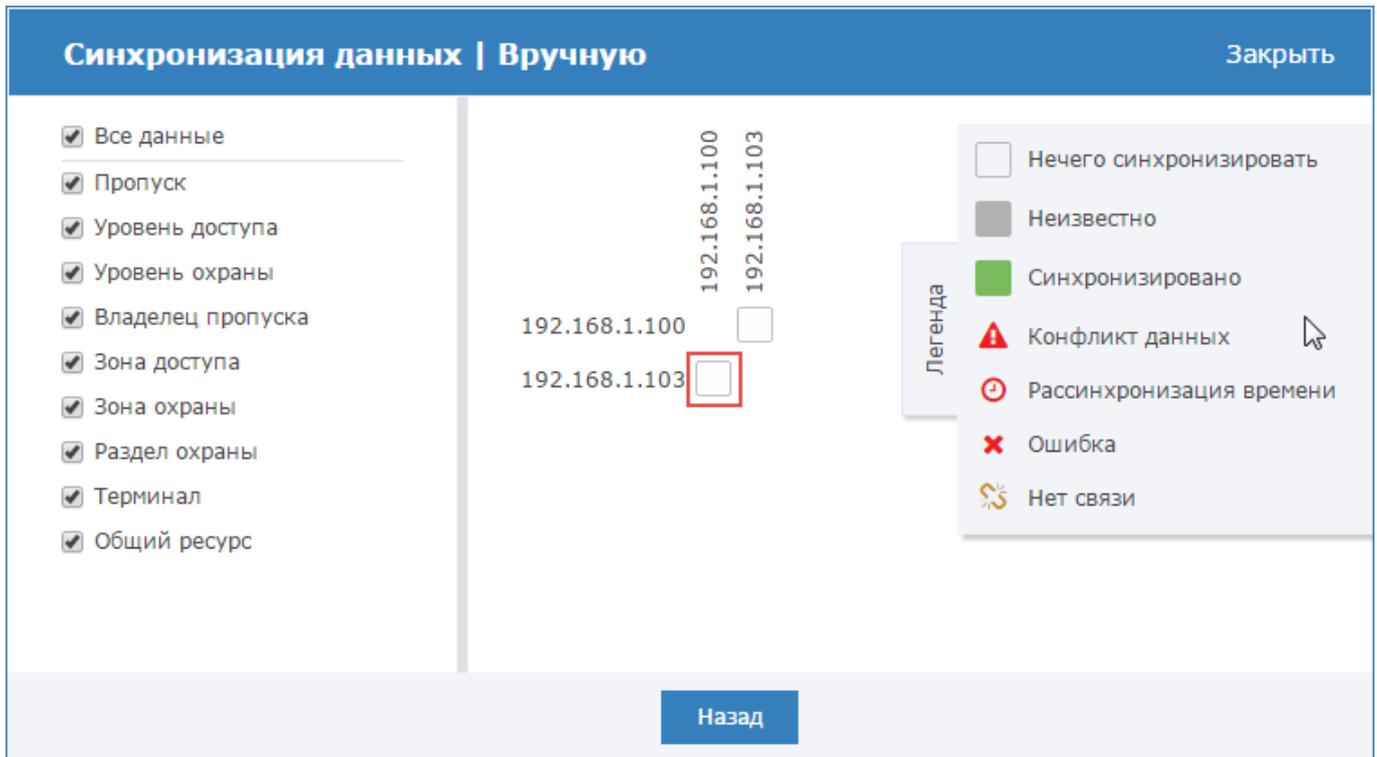


Рисунок 9 — Состояние синхронизации данных между узлами

- Для синхронизации данных нажмите в требуемой ячейке и в следующем окне с помощью стрелок влево/вправо выберите направление и выполните синхронизацию по всем типам данных (рисунок 10).

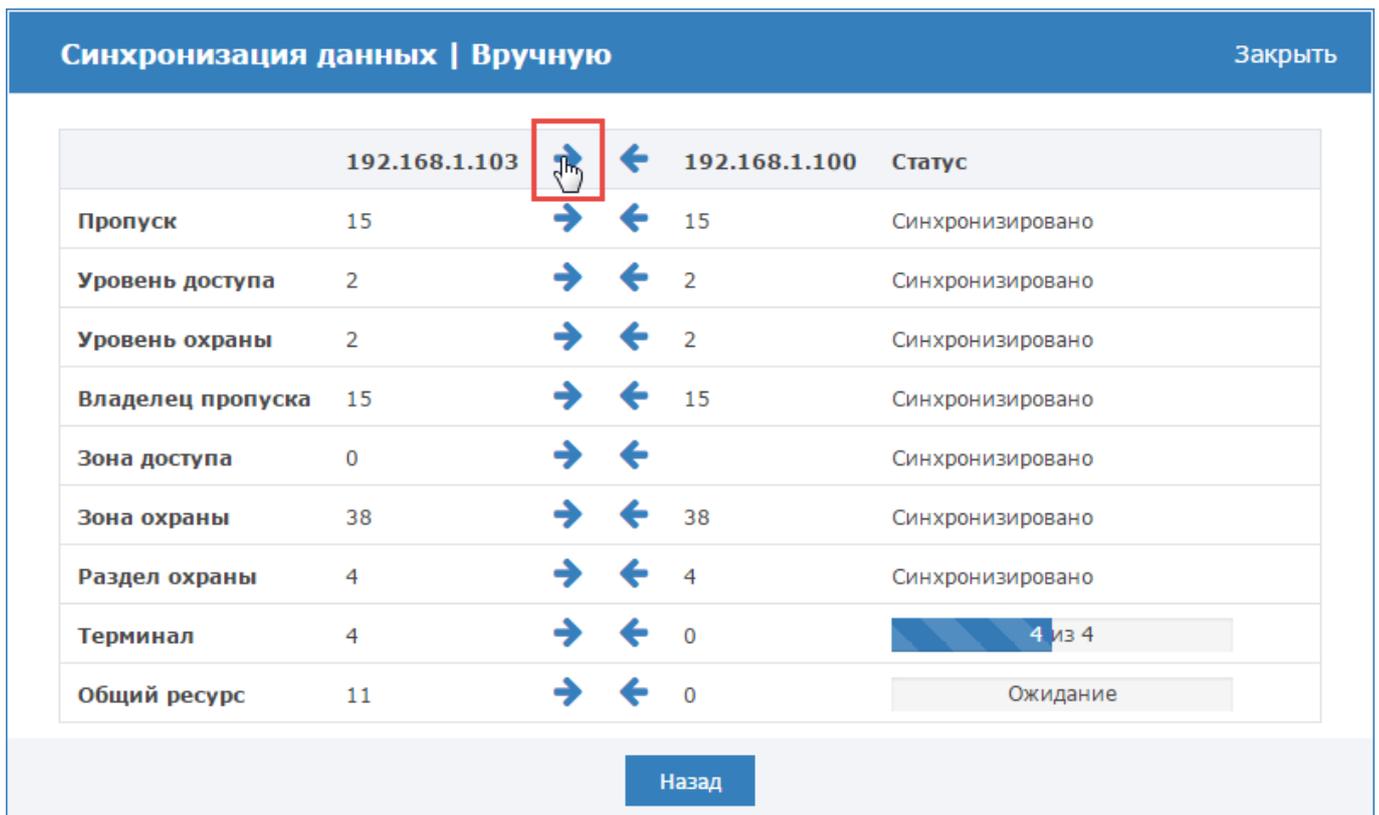


Рисунок 10 — Синхронизация данных по типам

- Закройте окно синхронизации данных.

**Примечание:** По завершении синхронизации данных, в узел «ВИК» будут загружены также облачные учетные записи сети НЕЙРОСС. При авторизации в интерфейсе под облачной учетной записью вы сможете конфигурировать все устройства сети и выполнять групповые операции из раздела **Сеть** (см. приложение [Сеть](#)). Рекомендуется выйти из интерфейса (см. раздел [Выход из веб-интерфейса](#)) и авторизоваться под «облачной» учетной записью.

### 3.3 Настройка ВИК

#### 3.3.1 Настройка режима работы.

3.3.1.1 В разделе [Раздел Конфигурация узлов](#) — [Настройки ВИК](#) задайте режим работы устройства «Терминал».

- В поле **Режим работы** выберите из раскрывающегося списка значение **Терминал**;
- В поле **Точка доступа** выберите из раскрывающегося списка точку доступа, если требуется выполнять авторизацию по карте, или задайте значение **нет**, если авторизация будет проводиться только пин-коду.
- Сохраните изменения и перезапустите «ВИК» (см. раздел [Перезагрузка прибора](#)).

3.3.1.2 В разделе [Терминалы](#) укажите список разделов сигнализации, которыми можно управлять с данного устройства (см. раздел [Настройка терминала](#)) и и перезапустите «ВИК» (см. раздел [Перезагрузка прибора](#)).

### 3.4 Проверка настроек

Здесь перечислены используемые ресурсы системы, параметры которых должны быть настроены. Проверьте, настроены ли:

3.4.1 Параметры шлейфов сигнализации (см. документ «Прибор управления доступом и охранной сигнализации сетевой «Борей» Руководство по эксплуатации КМУР.425723.125 РЭ»).

3.4.2 Параметры точки доступа (при необходимости авторизации с помощью карты (см. документ «Прибор управления доступом и охранной сигнализации сетевой «Борей» Руководство по эксплуатации КМУР.425723.125 РЭ»).

3.4.3 Разделы сигнализации (см. [Разделы охранной сигнализации](#)).

3.4.4 Уровень доступа пропуска, который разрешает доступ по точке (при необходимости авторизации с помощью карты; см. раздел [Настройка уровней доступа](#)).

3.4.5 Уровень охраны пропуска, заданы права на постановку/снятие разделов сигнализации (см. раздел [Настройка уровней охраны](#)).

3.4.6 Пропуск(а), для которого задан:

- Уровень доступа (при необходимости авторизации с помощью карты),
- Уровень охраны,
- Пин-код (при необходимости авторизации по пин-коду),
- Для владельца пропуска задано ФИО и фото (для отображения на экране постановки/снятия).

Описание процедур настройки приведено в приложении [Бюро пропусков](#).

- 3.4.7 В разделе Терминалы «ВИК'у» как точке доступа заданы права на управление разделами сигнализации .
- 3.4.8 Пересечение множества «привязанных» к «ВИК» разделов с множеством разделов, заданных уровнем охраны пропуски, не должно быть пустым.

### 3.5 Создание резервной копии

- 3.5.1 Создайте резервную копию настроек «ВИК». Для этого в разделе [Конфигурация узлов](#) — [Основные настройки](#) перейдите к вкладке **Управление** и в блоке **Резервные копии** нажмите на кнопку **Создать** (см. раздел [Резервные копии](#)).

Прибор готов к использованию!

## 4 ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ

### 4.1 Режимы работы изделия

- 4.1.1 **Выключено.** В этом режиме на экране «ВИК» отображается приветственное сообщение с приглашением выполнить настройку устройства.
- 4.1.2 **Терминал.** В этом режиме на экране «ВИК» отображается приглашение выполнить идентификацию для получения доступа к управлению разделами охранной сигнализации. В зависимости от настроек пропуски, идентификацию можно выполнить по карте, по пин-коду, по карте или пин-коду, по карте и пин-коду. После прохождения процедуры идентификации пользователю представляется информация о текущем состоянии разделов и зон охранной сигнализации и средства управления разделами/зонами. Список разделов ограничен уровнем охраны пропуски и правами точки доступа на управление разделами.
- 4.1.3 **Индикационная панель.** В этом режиме на экране отображается индикационная панель. Каждый индикатор панели окрашен цветом в соответствии с состоянием «привязанных» к нему зон и разделов охранной сигнализации. Предоставляются средства управления зонами и разделами.

### 4.2 Режим «Терминал»

В данном режиме «ВИК» реализует функции постановки на охрану и снятия с охраны разделов сигнализации с возможностью визуального контроля текущего состояния разделов и составляющих их зон охранной сигнализации.

#### 4.2.1 Стартовое окно

На рисунке 11 изображено стартовое окно приложения с приглашением приложить карту или прикоснуться к экрану. Авторизация в терминале осуществляется посредством предъявления идентификатора на считыватель точки доступа или ввода пин-кода.

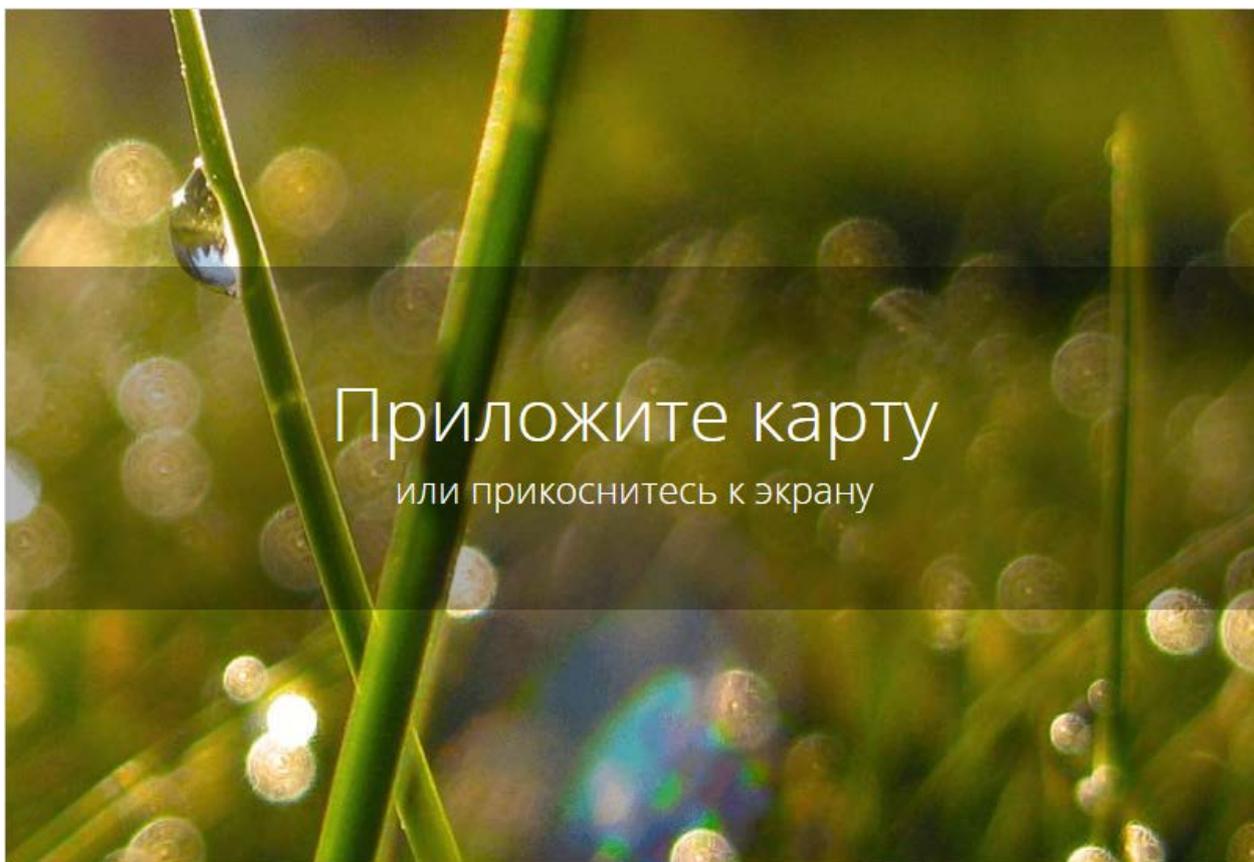


Рисунок 11 — Терминал. Стартовое окно

#### 4.2.2 Порядок работы

Выполните следующую последовательность шагов:

1. Приложите валидную карту или прикоснитесь к экрану для ввода пин-кода.
  - Если была выбрана авторизация по пин-коду, наберите код (рисунок 12) и нажмите **Подтвердить**.

**Внимание:** Во избежание считывания следов пальцев с экрана планшета, используется интерактивная скремблированная клавиатура: расположение цифр на клавиатуре каждый раз меняется.

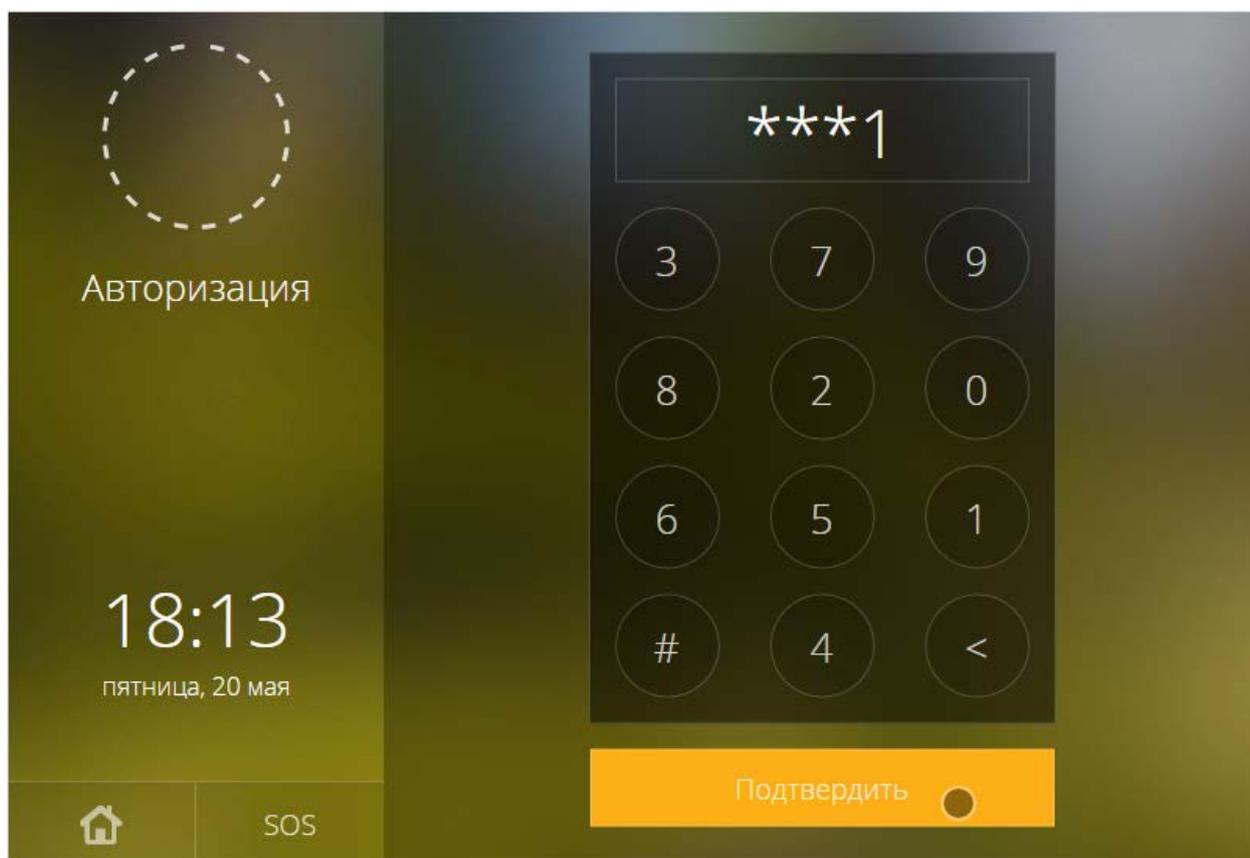


Рисунок 12 — Цифровая панель для ввода пин-кода

- При авторизации по карте на экране отобразится сообщение «Коснитесь чтобы начать работу» (рисунок 13). Касание необходимо для прерывания транзакции по точке доступа и перехода к управлению охраной. Если будет начата транзакция (например, открыта дверь), сеанс управления охраной будет заблокирован, отобразится стартовое окно (рисунок [11](#)). Коснитесь экрана.

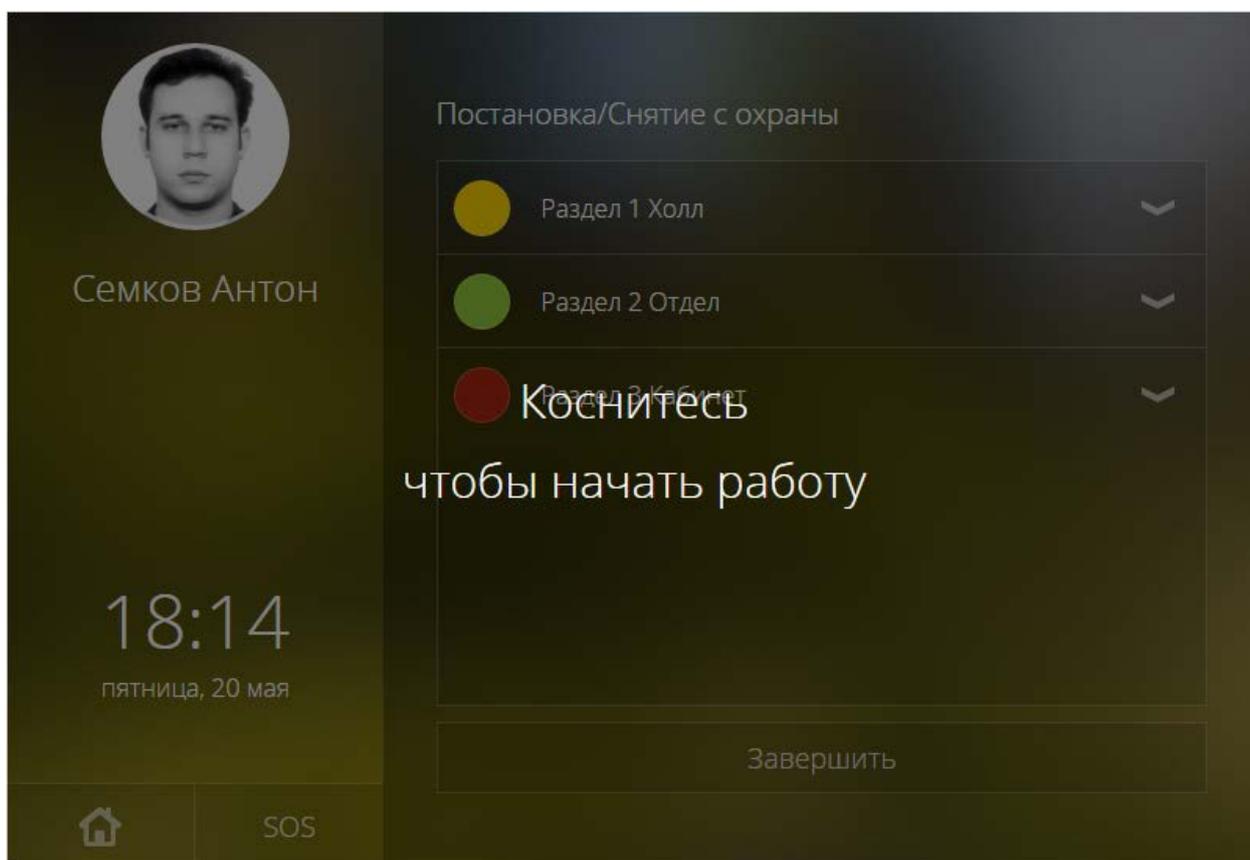


Рисунок 13 — Авторизация по карте. Требуется подтверждение

2. Будет отображен список разделов сигнализации, доступных к управлению с данной точки доступа по данному пропуску (рисунок 14). Цветом обозначается текущее состояние раздела (таблица 1).

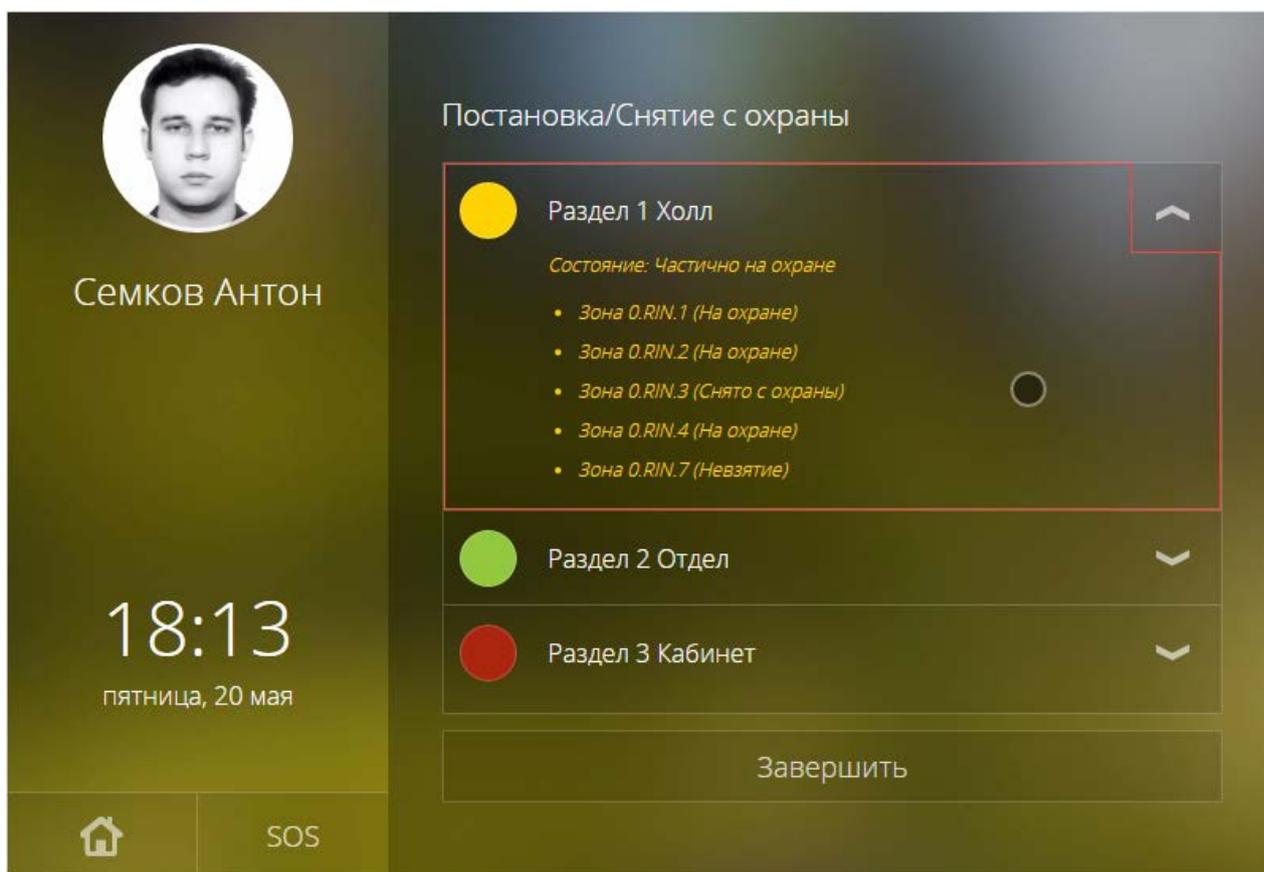


Рисунок 14 — Список разделов сигнализации для управления охраной

Таблица 1. Состояния разделов сигнализации

Обозначение	Состояние раздела
Зеленый	На охране
Желтый	Частично на охране
Красный	Тревога
Бесцветный	Снято с охраны Неисправность

- Для отображения/скрытия списка зон раздела используйте кнопки  и  соответственно.
- Для управления разделом нажмите в области его заголовка: если раздел на охране, он будет снят с охраны; если раздел снят с охраны, будет предпринята попытка постановки на охрану. Дополнительную информацию см. в разделе [Смена состояний зон и разделов при постановке на охрану](#). Процедура постановки/снятия может занять некоторое время, в течение выполнения которой будет отображаться индикатор  (рисунок 15).

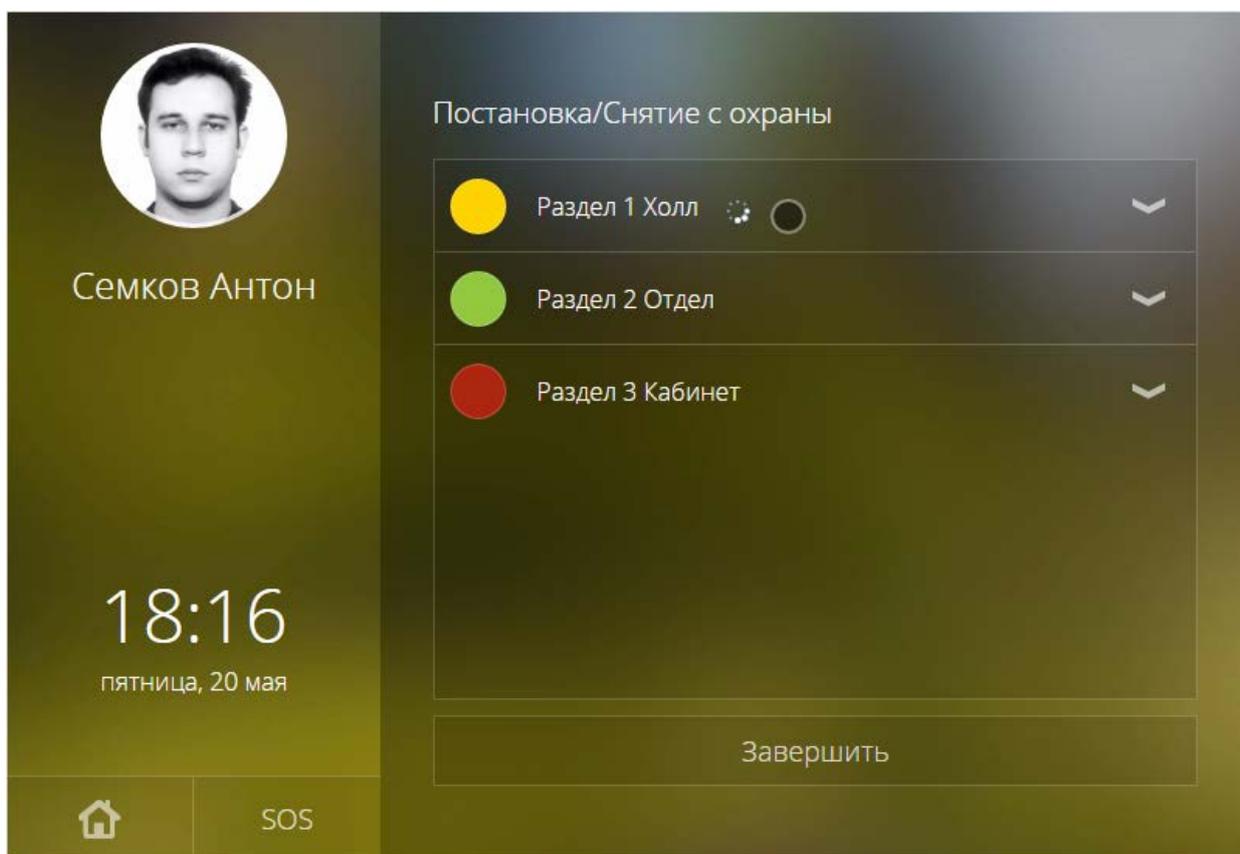


Рисунок 15 — Индикатор выполнения процедуры постановки/снятия

3. По завершению нажмите на кнопку **Завершить** или **Домой**.

## 5 ГАРАНТИИ ИЗГОТОВИТЕЛЯ

Изготовитель гарантирует соответствие прибора приемно-контрольного управления доступом и охранной сигнализации «Борей» техническим требованиям при соблюдении потребителем правил транспортирования, хранения и эксплуатации.

Гарантийный срок эксплуатации — 12 месяцев, но не более 24 месяцев со дня отгрузки. Срок службы — 5 лет.

## 6 СВЕДЕНИЯ ОБ ИЗГОТОВИТЕЛЕ

ООО «ИТРИУМ СПб», 194100, г. Санкт-Петербург, ул. Харченко, д.5, Литер А.

Тел./факс: (812) 960–06–13.

E-mail: [interop@itrium.ru](mailto:interop@itrium.ru); <http://www.itrium.ru>

## **7 ПРИЛОЖЕНИЯ**

Пользовательский интерфейс

Настройка устройства

Настройка общих ресурсов сети

Сеть

Бюро пропусков

Фотоидентификация

Журнал событий

Журнал аудита

Состояния элементов прибора

Администрирование прибора

## ПРИЛОЖЕНИЕ 1. ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС

Устройство «ВИК» предоставляет административный интерфейс, предназначенный для обеспечения удаленного конфигурирования всех устройств подсети, способных обмениваться данными в стандарте ONVIF, а также в рамках веб-приложений обеспечиваются функции терминала постановки/снятия и индикационной панели. Поддерживается работа в нескольких доменах, предназначенных для изолирования/группировки нескольких устройств.

Административный интерфейс позволяет:

1. Обнаруживать и конфигурировать следующие устройства подсети: «Борей», «Борей-Т», «Игнис», ВИК, компьютеры с ПО ИСБ ITRIUM, ip-камеры.
2. Конфигурировать уровни и режимы доступа, зоны и разделы охранной сигнализации, выполнять постановку зон и разделов на охрану и снятие с охраны, выполнять сброс тревог и др.
3. Синхронизировать данные между устройствами сети, в том числе — пропуска ITRIUM.
4. Подготавливать, создавать и учитывать пропуска в системах пропускного режима.
5. Проводить мониторинг состояния устройств и событий на устройстве.
6. В рамках приложения «Фотоидентификация», позволяет просматривать «живое» видео с камер видеонаблюдения и события доступа.
7. Выполнять групповое обновление программного обеспечения («прошивки») приборов, создавать резервные копии настроек и многое другое.

Пользовательское приложение «Терминал» позволяет:

1. Выполнять авторизацию по карте и/или пин-коду.
2. Проводить мониторинг состояний разделов и зон охранной сигнализации и выполнять постановку разделов на охрану и снятие с охраны. При этом доступ к управлению разделами и зонами ограничивается уровнем охраны пропуска. Если задана «привязка» к точке доступа, доступ к управлению разделами ограничивается также правами выбранной точки доступа.

Пользовательское приложение «Индикационная панель» позволяет:

1. Проводить непрерывный мониторинг состояния зон и разделов охранной сигнализации, получать суммарную информацию по числу тревог, неисправностей и пр., просматривать видеоданные с «привязанной камеры», выполнять команды постановки/снятия и сброса тревог.

Авторизация в приложении «Индикационная панель» осуществляется по пин-коду. Доступ к управлению зонами/разделами ограничивается составом индикаторов панели.

Доступ к веб-интерфейсу осуществляется с любого мобильного или стационарного ПК посредством веб-браузера Google Chrome, Mozilla Firefox, Internet Explorer, Safari или др. через пользовательский интерфейс, предоставляемый встроенным веб-сервером IP-прибора «Борей».

Для входа в интерфейс необходимо ввести в адресной строке браузера IP-адрес прибора и нажать клавишу **Ввод (Enter)**.

Предустановленные сетевые параметры:

IP-адрес: **192.168.1.100**

Маска подсети: **255.255.255.0**

## 1. Вход в веб-интерфейс

**Примечание 1:** Для доступа к интерфейсу необходимо настроить сетевое подключение вашего компьютера или планшета для работы в диапазоне IP-адресов устройства «Борей».

Для подключения к веб-интерфейсу контроллера:

1. Запустите веб-браузер.
2. В адресной строке браузера введите ip-адрес устройства и нажмите **Ввод** (Enter).

Предустановленные сетевые параметры:

IP-адрес: **192.168.1.100**

Маска подсети: **255.255.255.0**

3. Введите данные авторизации.

Предустановленные данные авторизации для базового конфигурирования прибора:

Имя пользователя **root**

Пароль: **root**

**Примечание 2:** Пароль учетной записи root рекомендуется изменить, см. раздел [Смена мастер-пароля](#)). Для управления общими ресурсами и конфигурирования других устройств сети, необходимо воспользоваться «облачной» учетной записью (см. раздел [Пользователи, роли и права](#)).

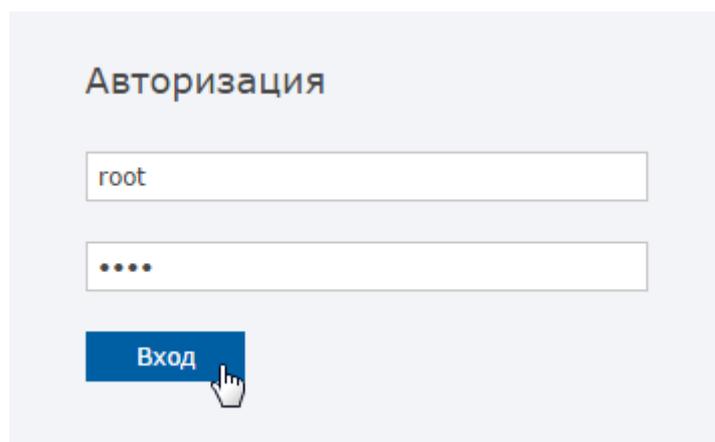


Рисунок 16 — Веб-интерфейс. Окно авторизации.

Если данные введены корректно, отобразится рабочий стол (рисунок [18](#)).

**Примечание 3:** В случае, если доступа к веб-интерфейсу нет:

- Проверьте наличие физического сетевого подключения;
- Настройте сетевое подключение компьютера или планшета для работы в диапазоне IP-адресов и подсети устройства.
- Проверьте отсутствие конфликта IP-адресов устройств, для этого отключите устройство от локальной сети, затем перейдите к интерфейсу командной строки и выполните команду **ping [IP-адрес]**, например, **ping 192.168.1.100**.

**Примечание 4:** При входе в веб-интерфейс с компьютера/планшета, на котором уже проводилась работа с прибором другой версии прошивки, требуется провести очистку кеша браузера вне зависимости от того, выводится ли экран предупреждения (рисунок 17).

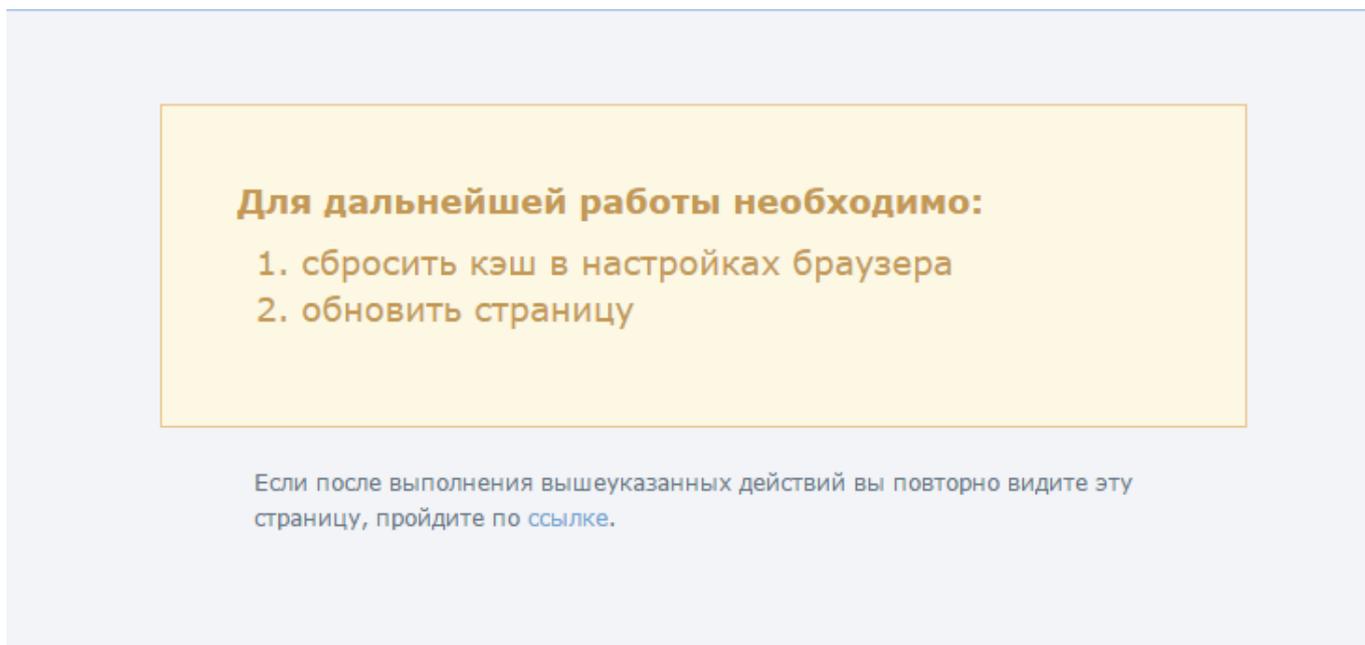


Рисунок 17 — Предупреждение о необходимости очистки кеша браузера

**Примечание 5:** Настройка контроллера осуществляется с любого мобильного или стационарного ПК посредством веб-браузера Google Chrome, Mozilla Firefox, Microsoft Edge, Internet Explorer или Apple Safari.

Необходимо использовать одну из последних двух версий перечисленных браузеров.

Корректная работа в других браузерах или с устаревшими версиями не гарантируется!

Перед выполнением пусконаладки настоятельно рекомендуется установить наиболее «свежую» версию браузера.

## 2. Окно веб-интерфейса. Рабочий стол

Рабочий стол (рисунок 18) предназначен для доступа ко всем функциям веб-приложения, содержит два блока элементов:

1. Блок **Программы** содержит перечень прикладных программ:

- **Бюро пропусков** – реализует функции Бюро пропусков (см. приложение [Бюро пропусков](#));
- **Фотоидентификация** – реализует функции подтверждения доступа на основе просмотра фото-/видеоданных (см. приложение [Фотоидентификация](#));
- **Журнал событий** – реализует функции просмотра журнала событий всей системы в целом с возможностью фильтрации по дате и времени, источнику события

и др. и последующего экспорта в текстовый файл (см. приложение [Журнал событий](#)).

2. Блок **Обслуживание** содержит перечень приложений по настройке и обслуживанию приборов и общих ресурсов системы:

- Приложение **Конфигурация узлов** – предоставляет функционал задания индивидуальных настроек каждого прибора/узла системы, с возможностью перехода к настройкам других узлов (см. [Настройки](#));
- Приложение **Пользователи, роли и права** – предоставляет функционал настройки пользователей и прав доступа к системе (см. раздел [Пользователи, роли и права](#));
- Приложение **Журнал аудита** – предназначено для выгрузки log-файлов с целью передачи производителю (см. приложение [Журнал аудита](#));
- Приложение **Сеть** – предназначено для управления взаимодействием различных узлов сети, выполнения процедур синхронизации данных, группового обновления программного обеспечения (прошивки), создания резервных копий и др. (см. приложение [Администрирование прибора](#)).
- Приложение **Разделы сигнализации** – предоставляет функционал конфигурирования разделов (см. [Разделы охранной сигнализации](#));
- Приложение **Терминалы** – предоставляет функционал конфигурирования терминалов (см. раздел [Терминалы](#));
- Приложение **Зоны доступа** – предназначено для конфигурирования зон доступа с целью организации контроля повторного прохода;
- Приложение **Настройка видеорегистраторов** – предназначено для задания параметров видеорегистраторов (в настоящий момент недоступно).

Для перехода к программе или приложению, щелкните левой клавишей мыши по требуемому элементу. Для прокрутки рабочего стола используйте колесико мыши, ползунок или функцию перелистывания при просмотре на сенсорном устройстве.

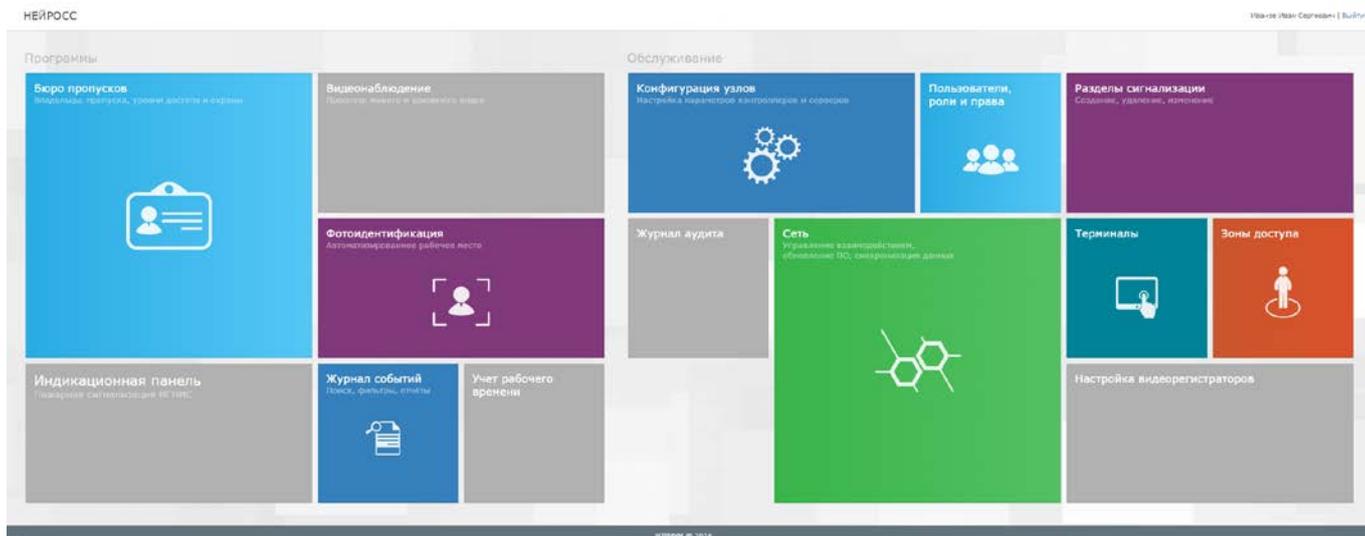


Рисунок 18 — Рабочий стол

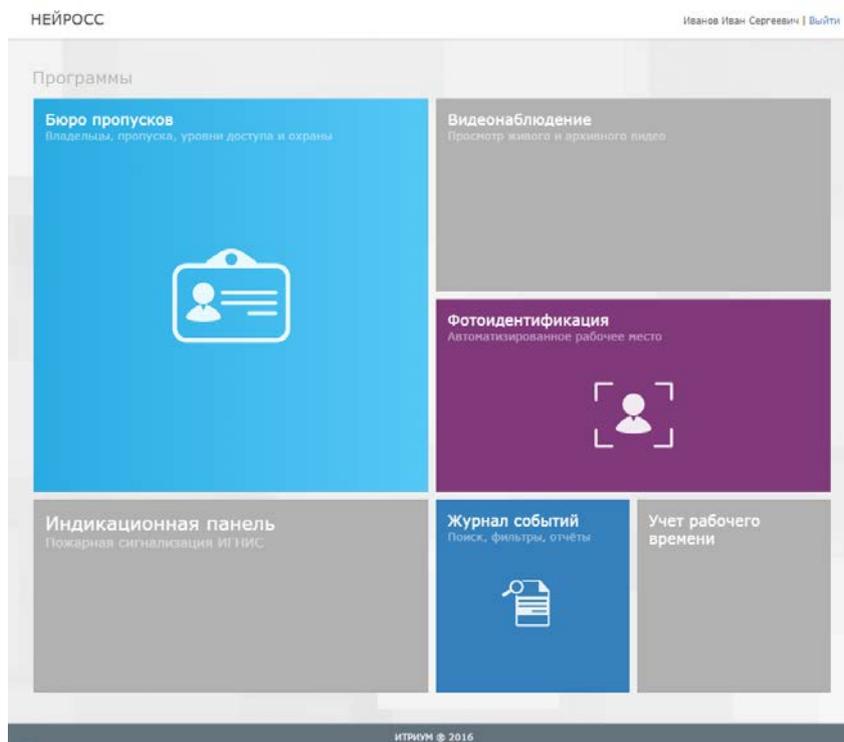


Рисунок 19 — Рабочий стол. Блок **Программы**

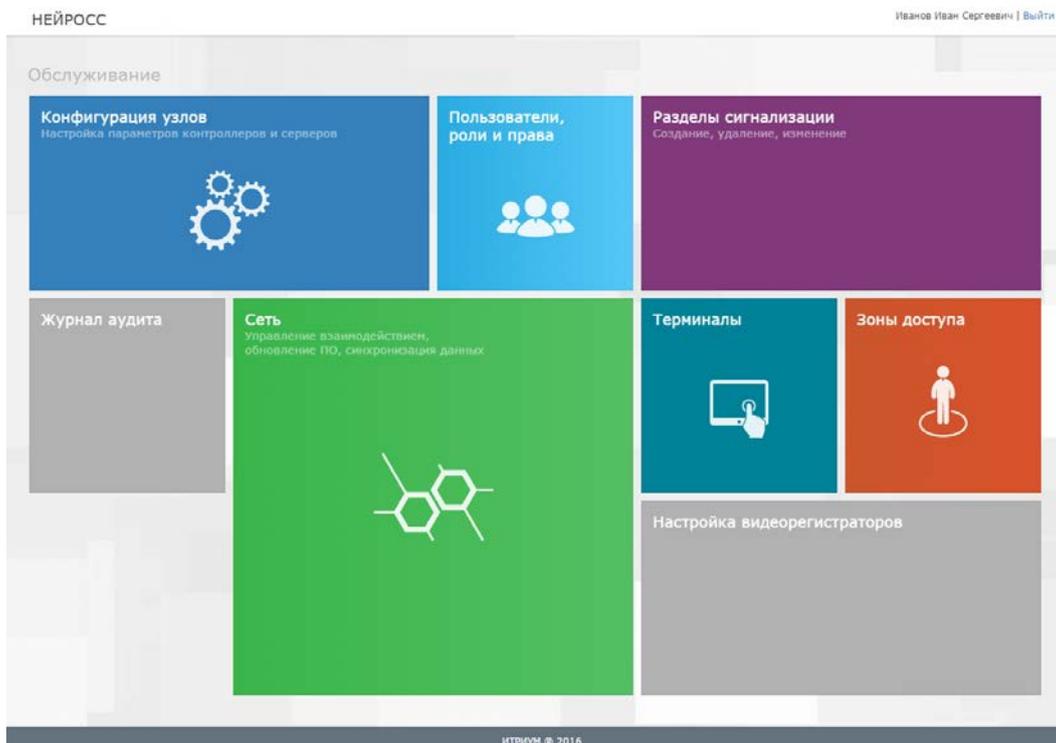


Рисунок 20 — Рабочий стол. Блок **Обслуживание**

Ярким цветом обозначены элементы доступных к выбору программ и приложений, недоступные элементы отображены серым цветом.

**Примечание:** Доступ к программам и приложениям определяется ролью пользователя (см. раздел [Пользователи, роли и права](#)).

Для возврата к рабочему столу после перехода к программе/приложению используйте ссылку [Рабочий стол](#) в заголовке окна (рисунок 21).

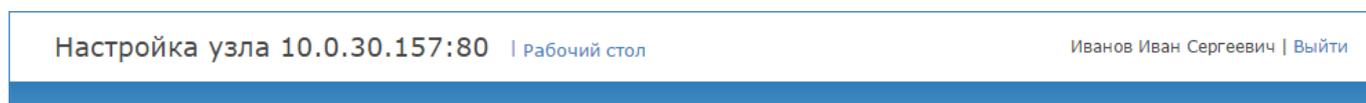


Рисунок 21 — Пример заголовка окна приложения

### 3. Раздел Конфигурация узлов

Для доступа к настройкам прибора, по его ip-адресу выполните вход в веб-интерфейс (см. раздел [Вход в веб-интерфейс](#)) и перейдите к разделу **Конфигурация узлов**.

Раздел **Конфигурация узлов** содержит левое вертикальное меню со списком разделов настроек текущего устройства. Справа отображается список полей настройки выбранного раздела (подробнее о настройках устройства см. приложение [Настройки](#)).

Для перехода к конфигурированию других устройств/узлов сети:

- Нажмите в области серой панели со стрелкой  в левой части окна (рисунок 22). Отобразится скрытое ранее окно со списком доступных устройств, отсортирован-

ным по группам (БОРЕЙ, ИТРИУМ, ВИК, ИГНИС, Камеры и др.) (рисунок 23). Справа в строке устройства указана текущая версия программного обеспечения (прошивки) устройства.

- Щелкните левой клавишей мыши по IP-адресу требуемого устройства.

**Внимание:** Учетная запись **root** предназначена для первичной настройки устройства. Для работы с «облачными» сервисами, в том числе для конфигурирования других узлов сети, необходимо авторизоваться под учетной записью из раздела [Пользователи, роли и права](#).

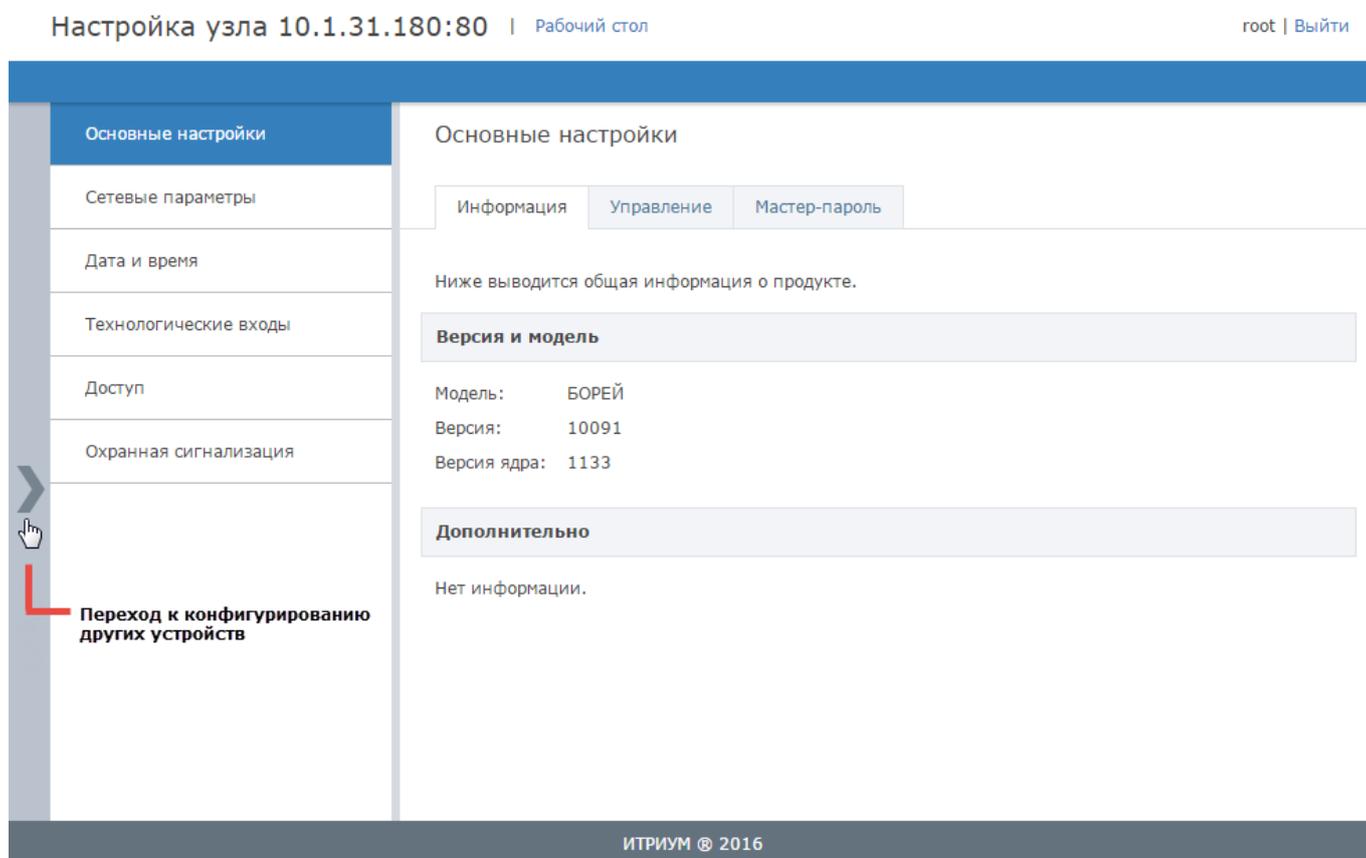


Рисунок 22 — Окно конфигурирования устройства

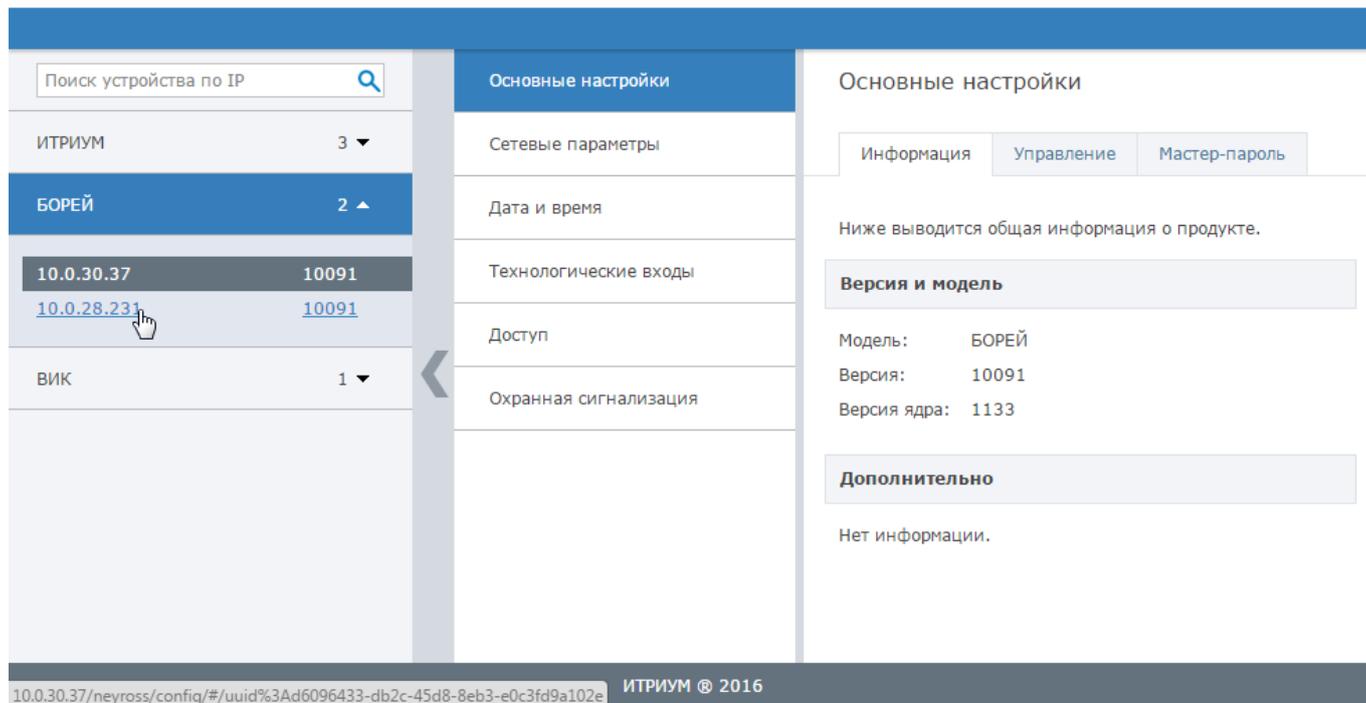


Рисунок 23 — Окно конфигурирования со списком устройств

#### 4. Выход из веб-интерфейса

Для выхода из веб-интерфейса нажмите на ссылку **Выйти** в правом верхнем углу экрана интерфейса (рисунок 24).

Иванов Иван Сергеевич | [Выйти](#)

Рисунок 24 — Выход из веб-интерфейса

Выход из программы с помощью закрытия браузера является некорректным, так как другой пользователь может воспользоваться данными авторизации, сохраненным в cookies-файлах браузера.

## ПРИЛОЖЕНИЕ 2. НАСТРОЙКИ УСТРОЙСТВА

### 1. Основные настройки

Раздел **Основные настройки** предназначен для уточнения версии прошивки и ядра, для создания резервных копий настроек прибора, смены мастер-пароля и пр. Перейдите к разделу [Конфигурация узлов](#) — **Основные настройки**.

На вкладке **Информация** указана текущая версия прошивки программных средств и ядра прибора, которая может пригодится для обращения в техподдержку.

Вкладка **Управление** содержит инструментарий программной перезагрузки прибора, обновления прошивки программных средств, а также создания резервных копий и восстановления данных из имеющейся резервной копии.

Вкладка **Мастер-пароль** предназначена для задания нового пароля учётной записи **root** (мастер-пароля).

**Примечание:** Для группового управления устройствами: сброса настроек и перезапуска, обновления версии прошивки и синхронизации данных предназначен раздел **Сеть** интерфейса. Для доступа к инструментам раздела необходимо авторизоваться под «облачной» учётной записью (см. раздел [Пользователи, роли и права](#)). Под учётной записью **root** возможно управление только тем устройством, под ip-адресом которого выполнен вход в интерфейс, и только с помощью инструментария из раздела **Основные настройки**.

### Перезагрузка прибора

С точки зрения программных средств, прибор «ВИК» – это полноценный компьютер, работающий под управлением операционной системы семейства Linux. В случае изменения сетевых параметров прибора, привязки с доменам НЕЙРОСС и проч., а также если устройство «зависло», необходимо перезагрузить прибор. Перезагрузка может быть выполнена аппаратно или удаленно с помощью программных средств.

При наличии доступа к веб-интерфейсу возможен программный перезапуск прибора:

1. В разделе [Конфигурация узлов](#) — **Основные настройки** перейдите к вкладке **Управление** и нажмите на кнопку **Перезагрузка**.
2. В списке устройств сети выберите требуемое устройство(а), нажмите на кнопку **Перезагрузка**.
3. Будет выполнена перезагрузка. По окончании нажмите на кнопку **Закреть** (рисунок 25).



Рисунок 25 — Перезагрузка

### Обновление программных средств

Обновление программных средств (прошивки) прибора осуществляется из файла архива формата **TAR.GZ**.

Выполните следующие шаги:

1. В разделе [Конфигурация узлов](#) — **Основные настройки** перейдите к вкладке **Управление**.
2. В блоке **Обновление программных средств** (рисунок 26) в поле **Файл обновления** укажите файл архива программных средств, нажмите на кнопку **Обновить**.

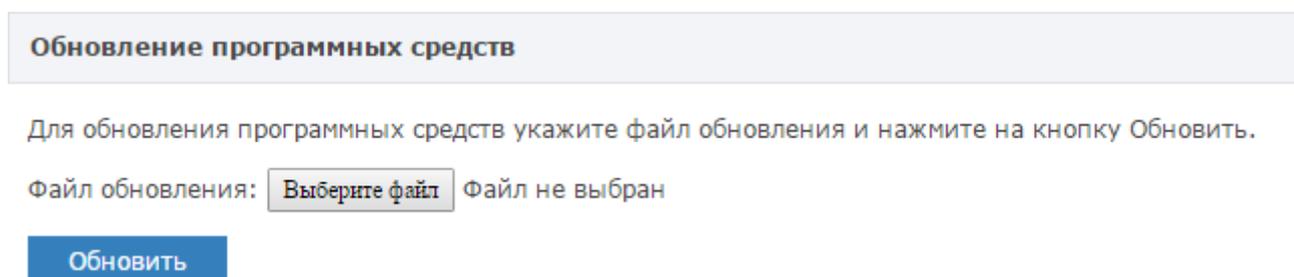


Рисунок 26 — Кнопка **Обновление ПО**

3. Будет выполнена процедура обновления программного обеспечения с последующей перезагрузкой. По завершении нажмите на кнопку **Закреть** (рисунок 7.27).

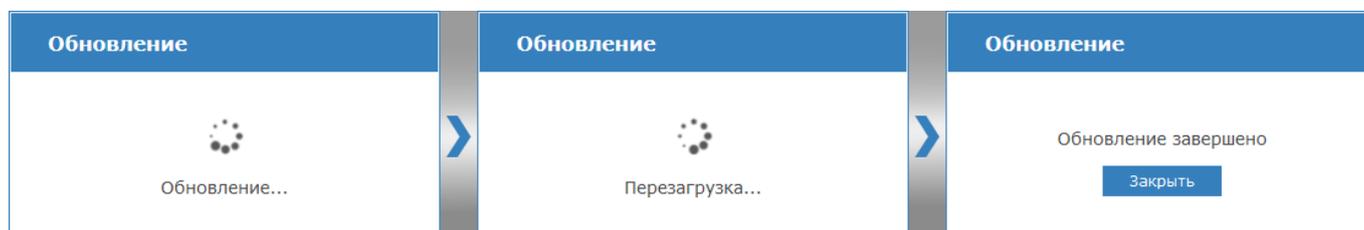


Рисунок 7.27 — Три шага обновления программных средств

4. После обновления, для работы с веб-интерфейсом выполните очистку кеша браузера.

**Инструкция для Google Chrome:** В меню **Настройки** выберите **История**, нажмите **Очистить историю...**, выберите **Файлы Cookie...** и **Изображения и другие файлы, сохраненные в кеше**. Нажмите **Очистить историю**.

При использовании других браузеров, смотрите документацию от производителя.

## Резервные копии

Посредством веб-интерфейса можно создать резервную копию настроек прибора и программного обеспечения (прошивки) прибора, выполнить восстановление из резервной копии, выполнить сброс настроек в заводские установки.

1. В разделе [Конфигурация узлов](#) — **Основные настройки** перейдите к вкладке **Управление**.
2. В блоке **Резервные копии** (рисунок 7.28) нажмите на кнопку **Создать**.

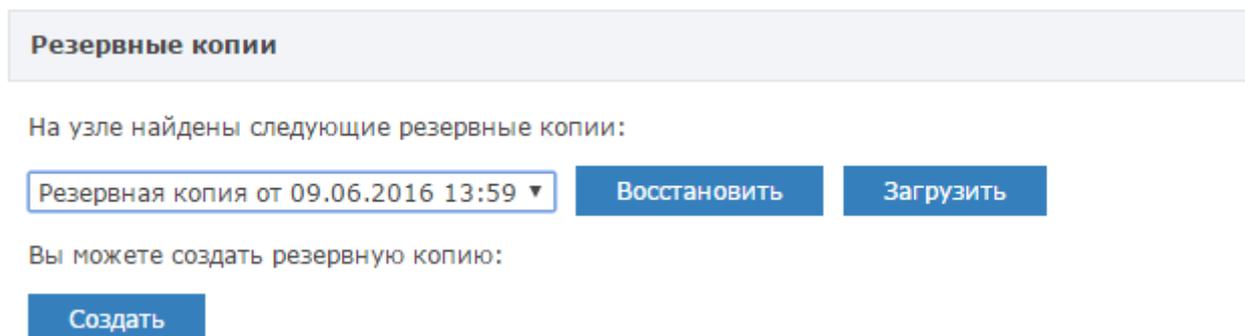


Рисунок 7.28 — Кнопка **Обновление ПО**

3. Будет выполнена процедура создания резервной копии. Ранее созданная резервная копия будет затерта. В процессе создания копии будет выполнен перезапуск программных средств устройств. По завершении нажмите на кнопку **Заккрыть** (рисунок 7.29).

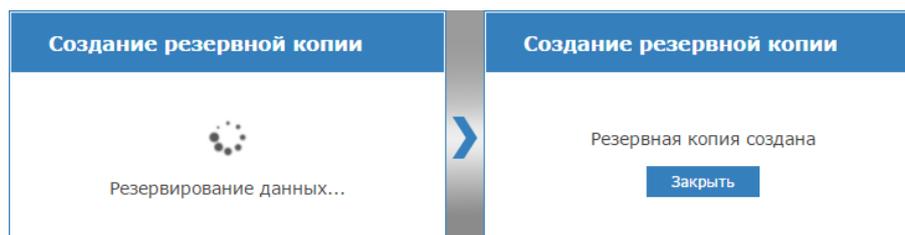


Рисунок 7.29 — Процедура создания резервной копии

По команде **Восстановление** выполняется восстановление данных из ранее созданной резервной копии.

**Внимание:** Если после создания резервной копии было выполнено обновление программного обеспечения устройства, после восстановления прошивка прибора будет замена версией, сохраненной в резервной копии.

По команде **Загрузить** выполняется загрузка файла резервной копии в папку загрузок браузера.

## Смена мастер-пароля

На данной вкладке можно задать новый пароль учетной записи **root**, предназначенной для первичного конфигурирования устройства, под IP-адресом которого выполнен вход в интерфейс (пароль по умолчанию – **root**).

**Внимание:** В целях безопасности рекомендуется изменить пароль учетной записи **root**.

Для смены пароля учетной записи **root**:

1. Перейдите к вкладке **Мастер-пароль**.
2. В поле **Пароль** введите новый пароль.
3. В поле **Повторите пароль** повторите ввод пароля.

**Примечание:** После смены пароля, при входе в веб-интерфейс следует вводить: в поле **Имя пользователя** – **root**, в поле **Пароль** – новый пароль.

Чтобы иметь возможность редактировать параметры других устройств сети и управлять ими, необходимо авторизоваться под «облачной» учетной записью. Дополнительную информацию см. в разделе [Пользователи, роли и права](#).

## 2. Сетевые параметры

Задание сетевых параметров необходимо для:

- Доступа к контроллеру по сети Ethernet с целью конфигурирования, мониторинга состояния и управления прибором;
- Предотвращения возможного конфликта IP-адресов, так как адрес по умолчанию (указан на корпусе прибора) может быть занят другим устройством;
- Обеспечения взаимодействия с другими устройствами сети, поддерживающими протокол ONVIF, в том числе другими устройствами «Борей», «КБУ-1», «Игнис», «ВИК», ip-камерами, а также с системами комплексного мониторинга и управления, и интегрированной системой безопасности ITRIUM® путем передачи пакетов сообщений по Ethernet или GSM-каналу.

Настройка контроллера осуществляется с любого мобильного или стационарного ПК посредством веб-браузера Google Chrome, Mozilla Firefox, Microsoft Edge, Internet Explorer или Safari.

**Для смены сетевых параметров:**

1. Выполните подключение к веб-интерфейсу прибора, для этого в адресной строке браузера введите ip-адрес прибора. IP-адрес по умолчанию указан на корпусе прибора.

**Примечание:** Более подробную информацию подключению к веб-интерфейсу см. в разделе [Вход в веб-интерфейс](#).

2. В разделе [Конфигурация узлов](#) — **Сетевые параметры**:

- На вкладке **Ethernet** задайте параметры сетевого интерфейса **Ethernet** (таблица 2). Нажмите на кнопку **Сохранить**.

Таблица 2 — Настройки сетевых параметров. Вкладка **Ethernet**

Параметр	Диапазон значений	Значение по умолчанию	Примечание
MAC-адрес	MAC-адрес в формате FF-FF-FF-FF-FF-FF	-	Уникальный идентификатор сетевого оборудования. Информационное поле.
Основной адрес	ip-адрес	Указано на корпусе прибора	Введите IP-адрес, по которому будет выполняться подключение к устройству.
Основной шлюз	ip-адрес шлюза		Укажите основной сетевой шлюз устройства.
Маска основного адреса	маска подсети	255.255.255.0	Укажите маску подсети, в которой будет находиться устройство.

- При использовании модема, на вкладке **GSM** задайте параметры беспроводной точки доступа по GSM-модему (см. таблицу 3). Параметры интерфейса **PPP0** будут сконфигурированы автоматически при подключении модема. Нажмите на кнопку **Сохранить**.

**Примечание:** Поля **Наличие модема**, **Наличие сигнала** и **Уровень сигнала** являются информационными и предназначены для индикации наличия соединения с модемом, наличия и уровня сигнала.

Таблица 3 — Настройки сетевых параметров. Вкладка **GSM**.

Параметр	Диапазон значений	Значение по умолчанию	Примечание
APN	текст	gmz.nw	Введите имя точки доступа в сети GSM для модема.
Имя пользователя APN	текст		Введите имя пользователя для точки доступа, указанной в поле <b>APN</b> .
Пароль пользователя APN	текст		Введите пароль пользователя, указанного в поле <b>Имя пользователя APN</b> для точки доступа, указанной в поле <b>APN</b> . Имя и пароль пользователя используется для защиты соединения через GSM-модем.
<b>Модем</b>			
Наличие модема	да/нет		Информационные поля, предназначены для указания наличия связи с модемом, наличия и уровня сигнала.
Наличие сигнала	да/нет		
Уровень сигнала	число		

Параметр	Диапазон значений	Значение по умолчанию	Примечание
<b>Расширенные настройки</b>			
Таймаут потери связи (сек.)	число	300	Введите временной интервал в секундах ожидания ответа от устройства на запросы наличия связи. Если по истечении данного интервала времени не получен ни один ответ, фиксируется потеря связи по модему.
Интервал между пингами (сек.)	число	10	Введите временной интервал в секундах между отправкой запросов (посылок) к устройству с целью проверки наличия связи.
Количество пингов в посылке (шт.)	число	3	Введите количество пинг-запросов, отправляемых на <b>Адрес для тестирования связи</b> .
Режим модема Huawei		GPRS_ONLY	Введите режим работы модема.
Адрес для тестирования связи		10.20.10.1	Введите ip-адрес, на который устройство будет слать пакеты для определения наличия связи. Используется для удаленного контроля соединения GSM-модема с сетью. Если указанный адрес будет не доступен, устройство определит "зависание" модема и перезагрузит его.

- При необходимости задания статических маршрутов, перейдите в вкладке **Маршруты**. На данной вкладке задаются статические маршруты передачи пакетов извещений, адресованных в сети, не принадлежащие заданным интерфейсам **Ethernet** и **PPP0**. Маршруты позволяют однозначно задать предпочитаемый интерфейс для передачи пакета. Адресом назначения может выступать адрес компьютера или сети, параметр **Шлюз** не обязателен. При определении пути маршрутизации для очередного пакета, система сначала будет искать его среди записей вида компьютер — компьютер (сетевая маска 255.255.255.255), затем среди записей вида подсеть — компьютер (в порядке уменьшения сетевой маски), и, наконец, в записи вида 0.0.0.0 компьютер (сетевая маска 0.0.0.0 означает всю сеть).

Чтобы задать статические маршруты:

- Нажмите на кнопку **Добавить** .
- Задайте параметры маршрута (см. таблицу 4).
- При необходимости, создайте новый маршрут.
- Нажмите на кнопку **Сохранить**.

Таблица 4 — Настройки сетевых параметров. Вкладка **Маршруты**

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Адрес	ip-адрес		Введите IP-адрес сервера назначения или адрес сети назначения.
Шлюз	ip-адрес		Введите адрес сервера – маршрутизатора другой сети, доступного по Ethernet или GSM-каналу.
Маска подсети	маска подсети		Введите маску сети назначения. При необходимости указания единичного узла сети, введите <b>255.255.255.255</b> .
Интерфейс	eth0 ppp0	eth0	Выберите из списка введите предпочитаемый интерфейс передачи пакетов.

- Вкладка **Дополнительно** содержит информацию о принадлежности данного прибора (узла) к домену **NEYROSS**. Устройства «Борей», «КБУ-1», «ВИК» и др. осуществляют обмен событиями и синхронизацию распределённых ресурсов только в рамках своих доменов.

Таблица 5 — Настройки сетевых параметров. Вкладка **Дополнительно**

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Домен НЕЙРОСС	имя домена (любые символы) при использовании нескольких доменов, их имена указывается через запятую и пробел	уникальный домен, сгенерированный на основе его идентификатора (например, <b>NEYROSS-a2581d2d-86af-447a-8e4c-64e8e9a3cc54</b> )	Домен НЕЙРОСС – это закрытая для внешнего доступа группа устройств, взаимодействие осуществляется только внутри группы/домена. Устройство может принадлежать нескольким доменам, при этом на устройство возрастает нагрузка по приёму/передаче пакетов устройств разных доменов. Поле <b>Домен НЕЙРОСС</b> не может быть пустым. Значение поля по умолчанию — NEYROSS. При необходимости смены домена, указания нескольких доменов, введите имена доменов через запятую.
Строгий режим фильтрации доменов	да/нет	нет	Определяет «видны» ли в сети узлы, не принадлежащие доменам (например, – IP-камеры). «Да» означает, что не видны, «нет» - не «видны».

**Внимание:** Настоятельно не рекомендуется изменять другие настройки данной вкладки. Изменения дополнительных сетевых параметров может привести к невозможности обмена данными с другими устройствами сети (в том числе ПО ИСБ ITRIUM®).

### 3. Дата и время

Настройки даты и времени необходимы для фиксации точного времени и хронологии событий в **Журнале событий** (см. приложение [Журнал событий](#)), а также для обеспе-

чения синхронизации между несколькими устройствами (см. раздел [Синхронизация данных между узлами НЕЙРОСС](#)).

Для указания даты и времени:

1. Перейдите к веб-интерфейсу, выберите раздел [Конфигурация узлов](#)— **Дата и время**.
2. В поле **Временная зона** из раскрывающегося списка выберите требуемую временную зону.
3. Выберите режим задания временных параметров: **Ручной** (ручной ввод или синхронизация с локальным временем на компьютере или планшете) или **Автоматический** (синхронизация по NTP-серверу).
4. Если выбран **Ручной** режим: введите дату и время или нажмите на кнопку **Выставить локальное**. Если выбран **Автоматический** режим, введите адрес NTP-сервера и нажмите **Синхронизировать**.
5. Нажмите на кнопку **Сохранить**.

**Внимание:** Для обеспечения взаимодействия устройств и компьютеров с ПО ИСБ ITRIUM® необходимо, чтобы все узлы сети были синхронизированы по времени. Для этого рекомендуется использовать режим автоматической синхронизации по NTP-серверу (в качестве NTP-сервера может выступать любой компьютер с ITRIUM®). Проверить текущее состояние синхронизации можно в разделе **Сеть** (дополнительную информацию см. в разделе [Веб-приложение «Сеть»](#)).

Синхронизация времени на всех устройствах сети НЕЙРОСС может быть выполнена двумя способами:

- **Посредством ПО ITRIUM®:** в программе «Администратор системы» в окне частных свойств элемента **Служба НЕЙРОСС** установить флаг в поле **NTP сервер** и сохранить изменения. Не позднее пяти минут на всех устройствах домена будет выбран **Автоматический режим**, в качестве NTP-сервера будет указан ip-адрес компьютера с ITRIUM®.
- **Посредством веб-интерфейса:** в разделе **Сеть** выбрать устройства, нажать на кнопку **Синхронизация времени** и ввести адрес NTP-сервера. При этом настройки в разделе **Дата и время** изменены не будут, будет выполнена разовая процедура синхронизации. Дополнительную информацию см. в разделе [Синхронизация времени на узлах НЕЙРОСС](#).

## 4. Настройки ВИК

Данный раздел предназначен для задания режима работы устройства «ВИК» (см. раздел [Режимы работы изделия](#)). По умолчанию, устройство находится в режиме **Отключено**, на экране «ВИК» отображается сообщение о необходимости настройки узла.

## Настройка ВИК в режим Терминал

Чтобы настроить ВИК в режим работы «Терминал» для выполнения функций просмотра состояния разделов и зон охранной сигнализации и управления разделами, выполните:

- В поле **Режим работы** выберите из раскрывающегося списка значение **Терминал**;
- В поле **Точка доступа** выберите из раскрывающегося списка точку доступа, если требуется выполнять авторизацию по карте, или задайте значение **нет**, если авторизация будет проводиться только пин-коду.
- Сохраните изменения и перезапустите «ВИК» (см. раздел [Перезапуск прибора](#)).

## ПРИЛОЖЕНИЕ 3. НАСТРОЙКА ОБЩИХ РЕСУРСОВ СЕТИ

### 1. Пользователи, роли и права

Учётные записи пользователей необходимы для авторизации в веб-интерфейсе. Каждая учётная запись имеет роль, которая определяет права пользователя. Учётная запись **root** предназначена является «заводской» и предназначена для первичного конфигурирования устройства. Первоначальный пароль учетной записи **root** (так называемый мастер-пароль), заданный по умолчанию – **root** – должен быть в целях безопасности изменен. Это можно сделать в разделе **Конфигурация узлов — Основные настройки** (см. раздел [Основные настройки](#)).

Чтобы иметь возможность редактировать параметры других устройств сети и управлять ими, необходимо:

1. Создать новую, «облачную» учетную запись (инструкцию см. ниже);
2. [Выйти из веб-интерфейса](#) и авторизоваться под новой учетной записью.

**Примечание 1** — Если в сети присутствует только одно устройство, «облачную» учетную запись создавать не обязательно, так как она нужна для конфигурирования нескольких устройств сети и выполнения функций раздела **Сеть** интерфейса (см. приложение [Сеть](#)).

**Примечание 2** — При добавлении нового устройства в уже существующую сеть НЕЙРОСС с настроенными «облачными» учётными записями, для загрузки учётных записей в память нового узла сети необходимо выполнить синхронизацию данных (см. раздел [Синхронизация данных между узлами НЕЙРОСС](#)).

Чтобы создать новую учетную запись, выполните следующую последовательность шагов:

1. Выполните подключение к веб-интерфейсу контроллера посредством учетной записи **root** и перейдите в раздел **Пользователи, роли и права**.
2. На вкладке **Роли** создайте роль пользователя. Для этого:
  - Нажмите кнопку **Добавить** ;
  - В отобразившемся окне (рисунок 30) задайте права новой роли (если вы хотите создать полнофункциональную роль, выберите **Все**) и нажмите на кнопку **Создать**.

**Добавить роль** Заккрыть

Название

Права  Все

- Журнал событий / Использование приложения
- Бюро пропусков / Управление пропусками
- Бюро пропусков / Управление уровнями доступа
- Бюро пропусков / Управление уровнями охраны
- Фотоидентификация / Использование приложения
- Видеонаблюдение / Использование приложения
- Общее / Обслуживание
- Управление пользователями и ролями

**Создать**

Рисунок 30 — Окно добавления роли пользователя

- Новая роль добавится в список ролей (рисунок 31). Роль можно удалить или отредактировать с помощью кнопок, расположенных в строке роли.

Пользователи **Роли**

Название	Права	Действия
<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>
administrator	Общее / Обслуживание	<input type="button" value="✎"/> <input type="button" value="-"/>

+ Добавить новую роль  
✎ - Удалить роль  
✎ Редактировать роль

Рисунок 31 — Список ролей

- На вкладке **Пользователи** создайте новую учётную запись. Для этого:
  - Нажмите на кнопку **Добавить**;
  - В отобразившемся окне (рисунок 32) введите данные нового пользователя, в поле **Роль** выберите из списка созданную на предыдущем этапе роль, нажмите на кнопку **Создать**.

Рисунок 32 — Окно добавление новой учётной записи пользователя

- Новая учётная запись пользователя добавится в список **Пользователи** (рисунок 33). Роль можно удалить или отредактировать с помощью кнопок, расположенных в строке роли.

Пользователи							Роли	
Фамилия	Имя	Отчество	Логин	Роль	Пароль	Действия		
Иванов	Иван	Сергеевич	admin	administrator	****			

— Добавить новую роль  
 — Удалить роль  
 — Редактировать роль

Рисунок 33 — Список пользователей интерфейса НЕЙРОСС

Чтобы **удалить** учетную запись, нажмите на кнопку в строке данной учетной записи.

Чтобы **отредактировать** параметры учетной записи, нажмите на кнопку в строке учетной записи и измените требуемые данные (рисунок 34).

Пользователи							Роли	
Фамилия	Имя	Отчество	Логин	Роль	Пароль	Действия		
Иванов	Иван	Сергеевич	admin	administrator				

Рисунок 34 — Окно редактирования параметров учётной записи пользователя

**Примечание:** Редактирование имени пользователя (логина) запрещено. При необходимости изменения логина, удалите учетную запись и создайте новую с требуемыми данными.

## 2. Разделы охранной сигнализации

Разделы охранной сигнализации предназначены для группового мониторинга состояний и управления зонами охранной сигнализации «Борей», «Тополь-3» и «КБУ-1». Раздел объединяет несколько охранных зон в единый объект мониторинга и управления. Разделы могут группироваться в разделы более высокого уровня (возможно построение иерархии разделов), при этом тревожные состояния подразделов будут наследоваться. Список возможных состояний разделов охранной сигнализации приведен в разделе [Состояния разделов охранной сигнализации](#).

Для начала работы с разделами, перейдите к веб-интерфейсу прибора (см. раздел [Окно веб-интерфейса. Рабочий стол](#)) и выберите пункт **Разделы сигнализации**.

Окно конфигурирования разделов охранной сигнализации (рисунок 35) разделено на две вертикальные области: слева задается номер и наименование раздела, справа к разделу добавляются охранные зоны. Если разделы ранее не конфигурировались, отобразится пустое окно.

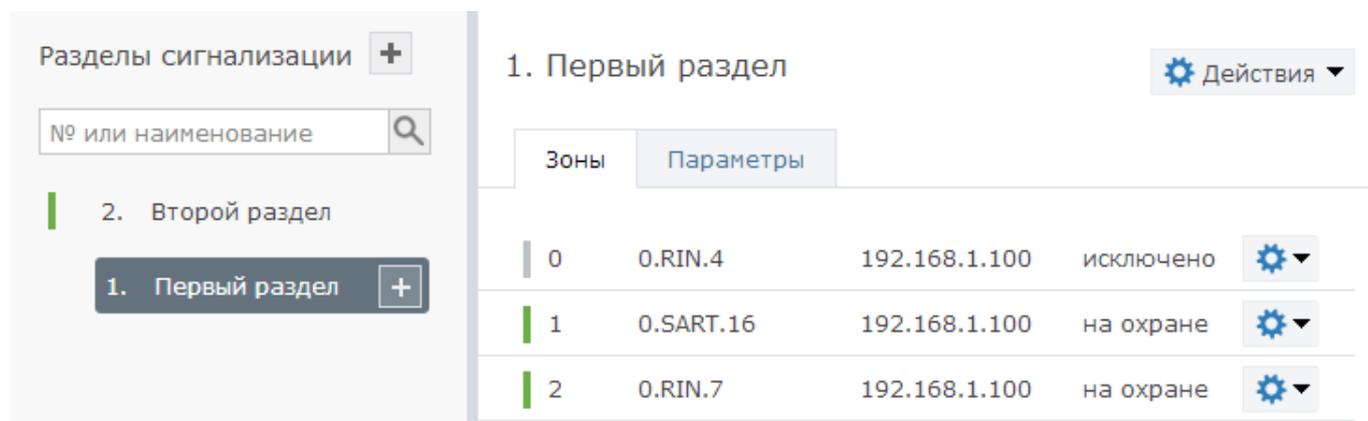


Рисунок 35 — Окно конфигурирования разделов

### Создание раздела

1. Создайте пустой раздел, для этого:

- В столбце **Разделы сигнализации** нажмите на кнопку .
- Укажите номер раздела и его название (рисунок 36). Нажмите на кнопку .

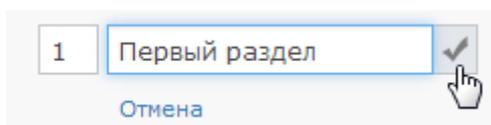


Рисунок 36 — Добавление раздела

2. Добавьте зоны в раздел, для этого:

- В окне справа, предназначенном для отображения списка зон раздела, нажмите на кнопку **Действия**  **Действия** ▾, выберите команду **Добавить зоны** (рисунок 37).

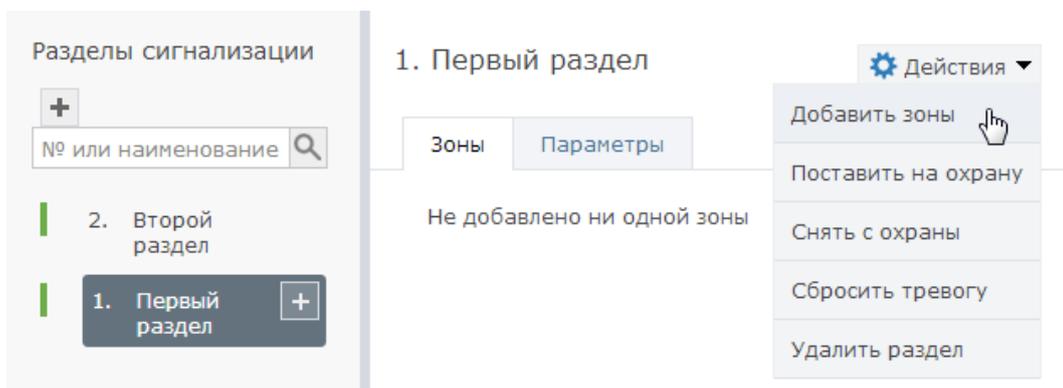


Рисунок 37 — Добавление охранных зон в раздел

- В отобразившемся окне в поле **Устройство** введите IP-адрес устройства, зоны которого вы хотите добавить в раздел. Из списка зон устройства отметьте флажком требуемые зоны. Если какая-то зона добавлена по ошибке, её можно удалить, нажав на кнопку [ x ] в таблице **Список выбранных зон** (рисунок 38).

**Примечание:** Возможно добавление только свободных зон (зон, которые не входят ни в один раздел). В раздел могут входить зоны различных контроллеров «КБУ-1» и «Борей».

- Далее при необходимости можно выбрать зоны другого устройства, для этого в строке поиска устройства введите IP-адрес и выберите зоны уже этого устройства.

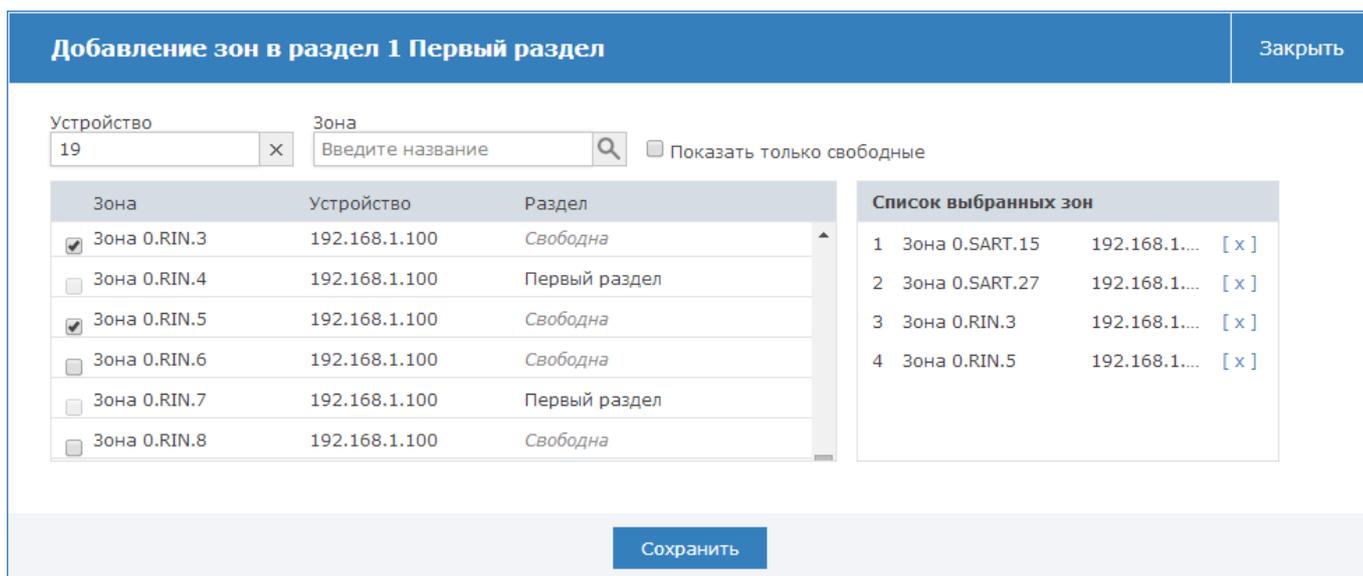


Рисунок 38 — Добавление охранных зон в раздел

- Нажмите на кнопку **Сохранить**.

### Перенос раздела

При необходимости построения сложной иерархии разделов возможен перенос уже созданного раздела в другой в качестве дочернего, выполните следующие действия:

1. В списке разделов сигнализации нажмите на левую клавишу мыши в области имени раздела, который требуется переместить.
2. Удерживая левую клавишу мыши, перенесите «раздел» к области имени раздела, который будет родительским разделом. Область имени родительского раздела выделится серой пунктирной линией (рисунок 39).
3. Отпустите клавишу мыши. Дерево разделов обновится с учетом перенесенного раздела.

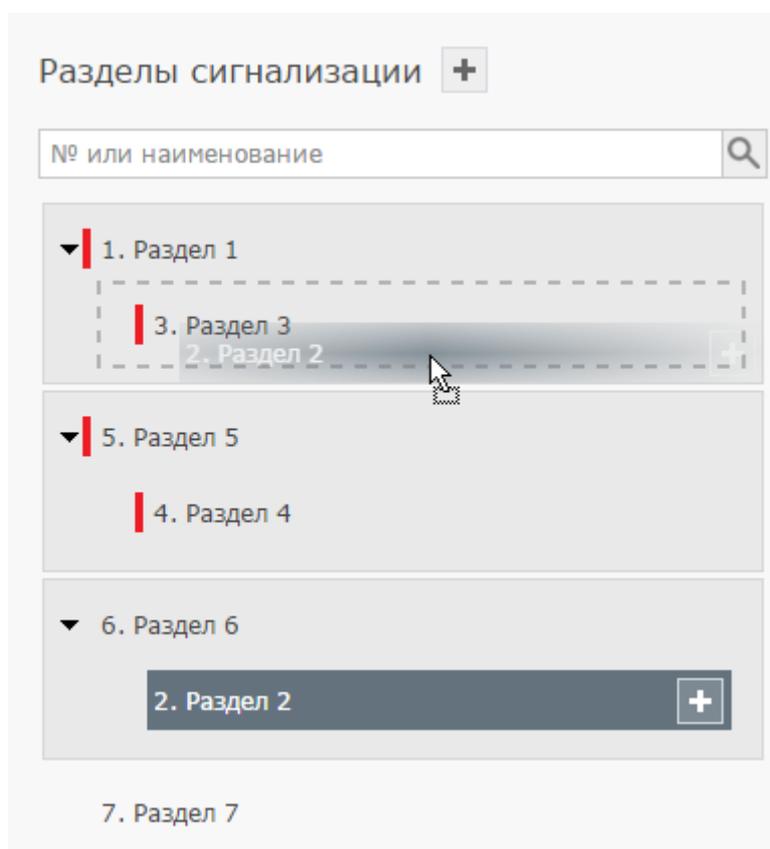


Рисунок 39 — Процедура переноса раздела

### Удаление раздела

1. В столбце **Разделы сигнализации** нажмите на кнопку выберите раздел, который требуется удалить.
2. В окне справа, предназначенном для отображения списка зон раздела, нажмите на кнопку **Действия**  **Действия** ▼, выберите команду **Удалить раздел**.

### Команды управления разделами и зонами

Средствами веб-интерфейса или ПО ИСБ ITRIUM® может осуществляться: постановка зоны/раздела на охрану, снятие зоны/раздела с охраны, сброс тревог зо-

ны/раздела, удаление зоны/раздела, добавление зон в раздел. Описание команд управления см. в таблице [6](#).

#### **Веб-интерфейс. Доступ к командам управления раздела:**

1. Перейдите к списку разделов. Инструкцию по переходу к списку разделов см. в разделе **Создание раздела**.
2. В списке разделов выберите требуемый раздел.
3. Нажмите на кнопку **Действия**  **Действия** ▼ в правом верхнем углу окна и выберите требуемую команду.

#### **Веб-интерфейс. Доступ к командам управления зоной:**

1. Перейдите к разделу **Охранная сигнализация** настроек прибора.
2. В списке зон выделите требуемую зону.
3. В строке зоны, команду над которой требуется выполнить, нажмите на кнопку  ▼ и выберите требуемую команду.

#### **ITRIUM®. Доступ к командам управления разделами/зонами:**

1. В программе «Администратор системы» выберите в дереве элементов **Сеть IP-устройств — Охранная сигнализация НЕЙРОСС — Разделы охранной сигнализации НЕЙРОСС**, выберите требуемый элемент и откройте контекстное меню элемента.
2. Если в программе «Администратор мониторинга» предварительно были размещены элементы, соответствующие разделам или зонам, в программе «Мониторинг» выберите требуемый элемент и откройте контекстное меню элемента.

Таблица 6 — Команды управления разделами/зонами

Группа команд	Название команды	Описание
Команды управления разделами	Добавить зоны	Добавление зон к разделу (см. <a href="#">Создание раздела</a> ).
	Поставить на охрану	Команда постановки раздела на охрану. Будет предпринята попытка постановки всех зон раздела на охрану. <ul style="list-style-type: none"> <li>• Все зоны раздела в состоянии [Норма] будут поставлены на охрану.</li> <li>• Зоны в состоянии [Тревога] перейдут в состояние [Невзятие] и при восстановлении шлейфа будут автоматически поставлены на охрану.</li> </ul> Если некоторые зоны раздела находятся в тревожном состоянии, раздел перейдет в состояние [Частично на охране]. Если некоторые зоны раздела находятся в неисправном состоянии, состояние зон и раздела не изменится ([Неисправно]) *.
	Снять с охраны	Команда снятия раздела с охраны. Будет предпринята попытка снятия с охраны каждой зоны раздела. См. описание команды снятия зоны с охраны.
	Сбросить тревогу	Команда сброса тревожного состояния раздела, не меняя охранного состояния раздела. Будет предпринята попытка сброса тревоги каждой зоны раздела.
	Удалить раздел	Команда удаления раздела. Все зоны раздела становятся свободными и доступными для добавления в другие разделы
Команды управления зонами	Удалить зону	Команда удаления зоны из раздела. Зона становится свободной и доступной для добавления в другие разделы.
	Поставить на охрану	Команда постановки зоны на охрану.
	Снять с охраны	Команда снятия зоны с охраны. Команда не доступна, если в настройках зоны в поле <b>Режим контроля</b> задано <b>Охрана 24 часа</b> . Если в настройках зоны в поле <b>Длительная охрана</b> задано <b>Да</b> , попытка снятия зоны с охраны приведет к формированию тревожного сообщения и состояние охраны не изменится.
	Сбросить тревогу	Команда сброса тревожного состояния зоны, не меняя её охранного состояния. После выполнения команды тревога номинально сбрасывается, шлейф заново опрашивается, если физическое состояние шлейфа не изменилось, тревожное состояние зоны сохраняется.

\* Дополнительную информацию см. в разделе [Смена состояний зон и разделов при постановке на охрану](#).

### 3. Терминалы

Раздел «Терминалы» предназначен для задания списка разделов охранной сигнализации, доступных для управления с помощью конкретной точки доступа/считывателя или устройства «ВИК». Права пользователя на постановку/снятие определяется уровнем охраны пропуски (см. раздел [Настройка уровней охраны](#)).

Для настройки терминалов, перейдите к веб-интерфейсу прибора (см. раздел [Окно веб-интерфейса. Рабочий стол](#)) и выберите пункт **Терминалы**. Предварительно необходимо сконфигурировать разделы сигнализации (см. [Разделы охранной сигнализации](#)).

Страница раздела разделена на две области. Слева отображается список точек доступа системы, справа — список сконфигурированных разделов сигнализации (рисунок 40).

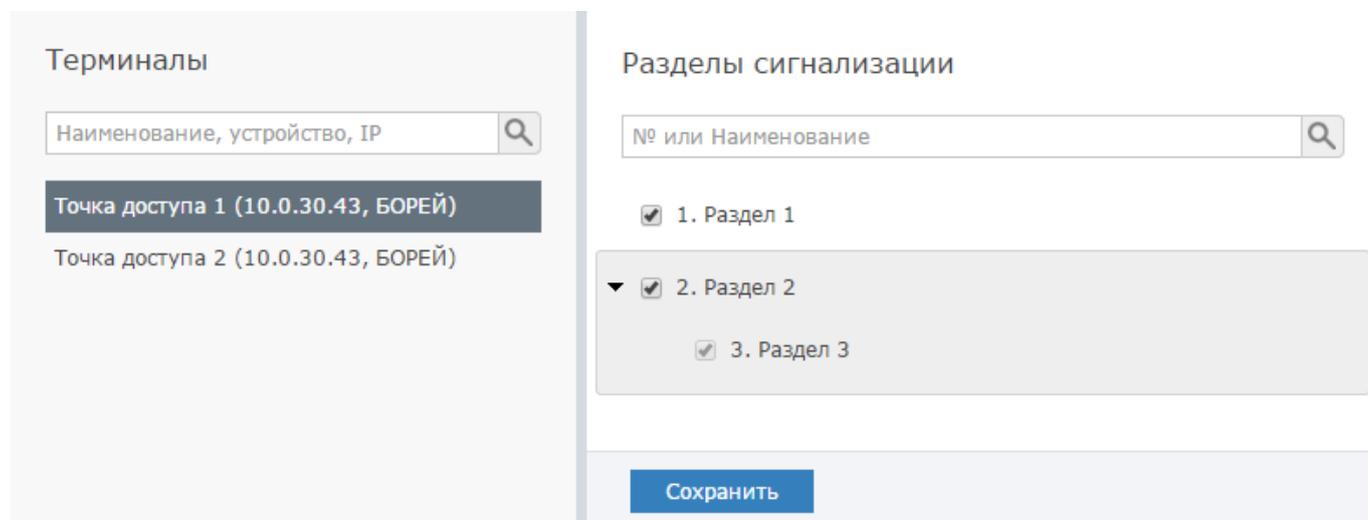


Рисунок 40 — Страница раздела «Разделы сигнализации»

### Настройка терминала

Выполните следующую последовательность шагов:

1. В окне **Терминалы** выделите требуемую точку доступа или устройство «ВИК».
2. В окне **Разделы сигнализации** определите набор разделов, которыми разрешено управлять посредством точки доступа, путем установки флажков в соответствующих полях.
3. Нажмите на кнопку **Сохранить**.

## ПРИЛОЖЕНИЕ 4. СЕТЬ

### Понятие сети НЕЙРОСС

Устройства «Борей», «ВИК», «ИГНИС», компьютеры с ПО ИСБ ITRIUM, ONVIF IP-камеры образуют сеть НЕЙРОСС и предназначены для построения комплексной системы безопасности НЕЙРОСС.

В основу сети НЕЙРОСС заложены такие общие ресурсы, как учетные записи пользователей, уровни и режимы доступа, разделы охранной сигнализации, терминалы, зоны доступа, пропуска и многое другое.

Сеть НЕЙРОСС образуют устройства, способные ответить на запрос WS-Discovery (WSD, Web Services Dynamic Discovery — a multicast discovery protocol to locate services on a local network). После получения ответа на запрос WSD, устройству отсылаются запросы по протоколу ONVIF — запрос информации об узле, его возможности, сервисы, также запрашивается текущее время на устройстве. Запрос времени необходим, так как, при наличии расхождения, синхронизировать данные между узлами невозможно.

Настройка общих ресурсов и синхронизация данных осуществляется посредством веб-интерфейса на основе прав учётной записи пользователя. Синхронизация данных между устройствами сети может быть выполнена автоматически от устройства-источника к устройствам-приёмникам, так и вручную по каждому типу данных между двумя устройствами.

Устройство, входящее в сеть НЕЙРОСС называется **узлом** сети НЕЙРОСС или **узлом НЕЙРОСС**.

**Внимание:** Взаимное сетевое обнаружение узлов НЕЙРОСС осуществляется в пределах домена НЕЙРОСС (см. раздел **Понятие домена НЕЙРОСС**).

### Понятие домена НЕЙРОСС

Домен НЕЙРОСС — это символическое обозначение закрытой для внешнего доступа группы узлов НЕЙРОСС. Взаимное сетевое обнаружение осуществляется только внутри «своего» домена.

Первоначально каждому узлу НЕЙРОСС присвоен уникальный домен, сгенерированный на основе его идентификатора (вида **NEYROSS-a2581d2d-86af-447a-8e4c-64e8e9a3cc54**). В процессе первоначальной настройки или в любое время впоследствии узлы могут быть сгруппированы по доменам.

#### Основные постулаты:

- «Видимость» узлов НЕЙРОСС обеспечивается только в пределах заданного в его настройках домена.
- Узел может принадлежать нескольким доменам, в этом случае он является связующим узлом между изолированными группами устройств, получает мультикасто-

вые сообщения «своих» доменов и транслирует их в группы. При этом нагрузка на узел возрастает.

- Значение домена для узла может быть в любой момент изменено.
- Перевод узла в новый домен/домены осуществляется после перезапуска программных средств (см. раздел [Перезапуск](#)).

## Рекомендации по настройке доменов НЕЙРОСС

1. В крупных системах узлы рекомендуется объединять в домены (группы) по территориальному, функциональному или нагрузочному критерию. Например, контроллеры проходной или входной группы объединяются в один домен, а контроллеры внутренних помещений в другой. Или, например, контроллеры каждого этажа объединяются в свой домен. Другой пример: контроллеры, через которые интенсивно осуществляется доступ (каждые 3-4 секунды) объединяются в один домен, а контроллеры с низкой нагрузкой в другой.
2. Система не ограничивает количество доменов, таким образом достигается оптимизация информационного обмена контроллеров друг с другом.
3. Узел ITRIUM (при использовании в системе) должен входить во все домены системы. Для этого в настройках «Службы НЕЙРОСС» необходимо через запятую указать имена всех используемых в системе доменов, сохранить изменения и перезапустить службу.

## Веб-приложение «Сеть»

Приложение «Сеть» предназначено для проверки состояния связи с устройством, состояний синхронизации времени и данных между устройствами и выполнения операций обновления ПО, перезагрузки, резервного копирования. Окно приложения содержит список устройств сети, принадлежащих домену (доменам) текущего устройства (устройства, с IP-адреса которого выполнен вход в интерфейс) (рисунок 41).

В верхней части окна раздела размещены инструменты раздела: [Обновление ПО узлов НЕЙРОСС](#), [Перезагрузка узлов НЕЙРОСС](#), [Резервные копии узлов НЕЙРОСС](#), [Синхронизация времени на узлах НЕЙРОСС](#), [Синхронизация данных между узлами НЕЙРОСС](#), [Удаление узлов НЕЙРОСС](#). Для выполнения операции требуется выделить требуемые узлы и выбрать соответствующий инструмент.

**Примечание:** Если кнопка инструмента не активна, значит в списке выбранных устройств есть устройство, указанное действие над которым невозможно (например, обновление программного обеспечения сервера ITRIUM осуществляется на компьютере ITRIUM средствами операционной системы).

Устройства
Топология

Панель инструментов раздела Сеть


  
Обновление ПО


  
Перезагрузка


  
Резервные копии


  
Синхронизация времени


  
Синхронизация данных


  
Удалить узлы

Доступные узлы (47) + Добавить узел

<input type="checkbox"/>	Состояние	Сетевой адрес	Модель	Версия	НЕЙРОСС-Домены	i
<input checked="" type="checkbox"/>	норма	10.0.28.231:80	БОРЕЙ	10158	Itrium-Borey-1 stand2	i
<input checked="" type="checkbox"/>	норма	<b>10.0.30.37:80</b>	БОРЕЙ	10158	Itrium-Borey-1	i
<input type="checkbox"/>	нет связи	10.1.29.11:6501	ИТРИУМ	6.1.1303.3819	Itrium-Borey-1	i
<input type="checkbox"/>	норма	10.1.29.11:2911	ИТРИУМ	6.1.1308.3866	AKPP10 Itrium-Borey-1 NEYROSS-70-only kbu stand2	i
<input type="checkbox"/>	нет связи	10.1.29.26:6501	ИТРИУМ	6.1.1303.3819	Itrium-Borey-1 NEYROSS-Lena	i
<input type="checkbox"/>	нет связи	10.1.30.3:6502	ВИК	9999	Itrium-Borey-1	i
<input type="checkbox"/>	норма	10.1.31.96:80	SNC-CH280	1.85.00		i
<input type="checkbox"/>	норма	10.1.31.98:80	SNC-CH280	1.85.00		i
<input type="checkbox"/>	норма	10.1.31.99:80	SNC-CH280	1.85.00		i
<input type="checkbox"/>	норма	10.1.31.100:80	SNC-CH280	1.85.00		i
<input type="checkbox"/>	норма	10.1.31.101:80	SNC-RH164	1.85.00		i
<input type="checkbox"/>	норма <span style="color: red;">○</span>	10.1.31.147:80	B47	A1D-500-V6.10.25-AC		i
<input type="checkbox"/>	норма <span style="color: red;">○</span>	10.1.31.150:80	WV-SP306	2.13		i
<input type="checkbox"/>	норма <span style="color: red;">○</span>	10.1.31.151:80	WV-SP509	1.62		i
<input type="checkbox"/>	нет связи <span style="color: red;">○</span>	10.1.31.152:80	WV-SF135	2.12		i
<input type="checkbox"/>	норма <span style="color: red;">○</span>	10.1.31.163:80	SNO-6084R	1.00_130412		i
<input type="checkbox"/>	нет связи	10.1.31.165:80	CAM2311P	V2.4.C09		i
<input type="checkbox"/>	норма	10.1.31.166:80	CAM2321	V2.2.E02		i
<input type="checkbox"/>	норма <span style="color: red;">○</span>	10.1.31.180:80	CMNC-200(PoE)	V1.211R04-T200		i

ИТРИУМ © 2016

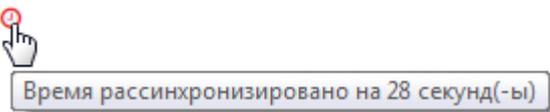
Рисунок 41 — Окно раздела Сеть

При строгом режиме фильтрации доменов, в списке будут «видны» только те устройства, которые принадлежат домену (доменам) текущего устройства. При нестрогом режиме фильтрации будут «видны» также узлы, не принадлежащие доменам (например, – IP-камеры). Домен и режим фильтрации для узла настраиваются в разделе **Конфигурация узлов – Сетевые параметры** (см. раздел [Сетевые параметры](#)).

В столбце **Состояние** указано состояние связи с устройством (таблица 7).

Таблица 7 — Список состояний узлов

Состояние	Обозначение	Описание
Норма	норма	Узел ответил на все запросы, интервал расхождения времени с текущим устройством – менее 5 секунд.

Рассинхронизация времени		Узел ответил на все запросы, интервал расхождения более 5 сек. Точная величину можно просмотреть при наведении указателя мыши на ячейку. Необходимо синхронизировать время на устройстве (см. раздел <a href="#">Синхронизация данных между узлами НЕЙРОСС</a> ).
Нет связи		С узлом потеряна связь.
Неизвестно		Узел ответил только на WSD-запрос.

Необходимым требованием успешной синхронизации данных между узлами сети является синхронизация устройств по времени. Допустимый интервал расхождения – 5 сек. При превышении данного порога, требуется выполнить синхронизацию времени.

### Обновление ПО узлов НЕЙРОСС

Выполните следующие шаги:

1. Перейдите к веб-интерфейсу прибора, выберите раздел **Сеть**.
2. В списке устройств сети выберите требуемое устройство(а), нажмите на кнопку **Обновление ПО** (рисунок 42).



Рисунок 42 — Кнопка **Обновление ПО**

3. После обновления программного обеспечения устройства, для работы с веб-интерфейсом, выполните очистку кеша браузера.

**Инструкция для Google Chrome:** В меню **Настройки** выберите **История**, нажмите **Очистить историю...**, выберите **Файлы Cookie...** и **Изображения и другие файлы, сохраненные в кеше**. Нажмите **Очистить историю**.

При использовании других браузеров, смотрите документацию от производителя.

### Перезагрузка узлов НЕЙРОСС

При наличии доступа к веб-интерфейсу возможна программная перезагрузка приложения:

1. Перейдите к веб-интерфейсу прибора, выберите раздел **Сеть**.
2. В списке устройств сети выберите требуемое устройство(а), нажмите на кнопку **Перезагрузка** (рисунок 43).

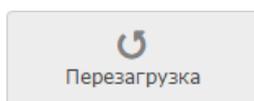


Рисунок 43 — Кнопка **Перезагрузка**

3. В окне подтверждения повторно нажмите на кнопку **Перезагрузить**.
4. По окончании процесса перезагрузки отобразится информационное окно (рисунок 44). Нажмите на кнопку **Закреть**.

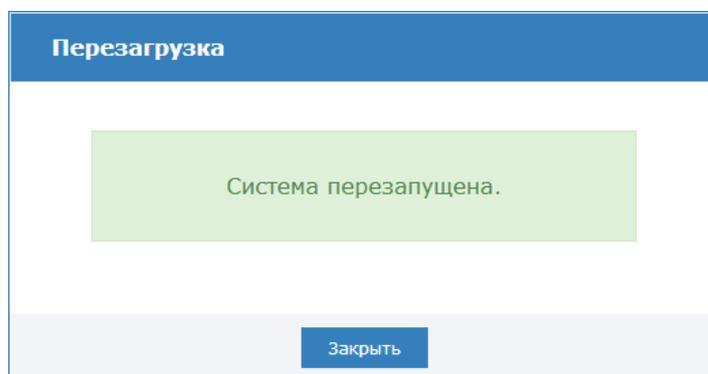


Рисунок 44 — Окно подтверждения завершения перезагрузки

### **Резервные копии узлов НЕЙРОСС**

Посредством веб-интерфейса можно создать резервную копию настроек прибора и программного обеспечения (прошивки) прибора, выполнить восстановление из резервной копии, выполнить сброс настроек в заводские установки.

1. Перейдите к веб-интерфейсу прибора, выберите раздел **Сеть**.
2. В списке устройств сети выберите требуемое устройство(а), нажмите на кнопку **Резервные копии** (рисунок 45).



Рисунок 45 — Кнопка **Резервные копии**

3. Выберите требуемую команду (рисунок 46).

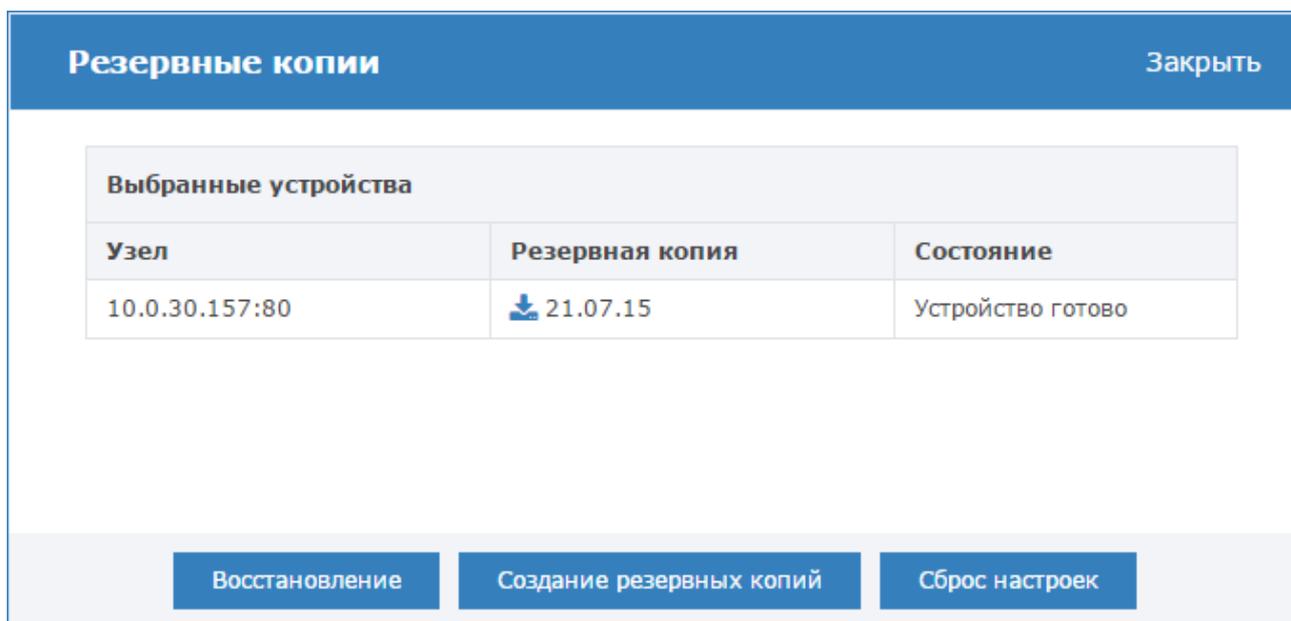


Рисунок 46 — Работа с резервными копиями

По команде **Создание резервных копий** выполняется создание резервных копий выбранных устройств. Ранее созданная резервная копия будет затерта.

В резервной копии содержится программное обеспечение (прошивка) прибора и все данные, настраиваемые пользователем (сетевые параметры, дата/время, параметры точек доступа, охранных зон и др.).

По команде **Сброс настроек** выполняется очистка всех данных, заданных пользователем и возврат к заводским настройкам.

**Внимание:** IP-адрес устройства также будет заменен на адрес, указанный на корпусе прибора. Доступ к контроллеру будет возможен только по данному IP-адресу и из подсети **255.255.255.0**.

По команде **Восстановление** выполняется восстановление данных из ранее созданной резервной копии.

**Внимание:** Если после создания резервной копии было выполнено обновление программного обеспечения устройства, в процессе восстановления прошивка прибора будет замена версией, сохраненной в резервной копии.

### Синхронизация времени на узлах НЕЙРОСС

Необходимым условием обеспечения взаимодействия нескольких устройств сети НЕЙРОСС является синхронизация устройств по времени.

Отсутствие расхождений по времени на узлах «Борей», «КБУ-1», «ВИК» и др. можно обеспечить настройками текущего времени на каждом устройстве (дополнительную информацию см. в разделе [Дата и время](#)) или средствами «Службы НЕЙРОСС».

Примечание: Параметры даты и времени на узле ITRIUM следует устанавливать средствами операционной системы Windows (**Панель управления — Дата и время**).

В разделе **Сеть** может быть выполнена разовая процедура синхронизации времени на устройствах «Борей», «КБУ-1», «ВИК», для этого выполните следующую последовательность шагов:

1. Перейдите к веб-интерфейсу прибора, выберите раздел **Сеть**.
2. В списке устройств сети выберите требуемое устройство(а), нажмите на кнопку **Синхронизация времени** (рисунок 47).



Рисунок 47 — Кнопка **Синхронизация времени**

3. В отобразившемся окне введите адрес NTP-сервера. Нажмите на кнопку **Синхронизировать**.

В процессе выполнения будет отображаться текущий статус (рисунок 48).

Скриншот окна «Синхронизация времени» с заголовком «Синхронизация времени» и кнопкой «Закреть» в правом верхнем углу. В центре таблицы отображается прогресс синхронизации: «Синхронизация времени (5 из 6)». Таблица содержит следующие данные:

Узел	Расхождение по времени ⓘ	Статус
172.16.207.3:80	0	✓ Завершено
172.16.207.4:80	-207	✓ Завершено
172.16.207.5:80	0	✓ Завершено
172.16.207.6:80	0	✓ Завершено
172.16.207.7:80	1156	✓ Завершено
172.16.207.8:80	-1	Выполнение..

В нижней части окна находится кнопка «Синхронизировать».

Рисунок 48 — Окно синхронизации времени

### **Синхронизация данных между узлами НЕЙРОСС**

Обязательным условием успешного взаимодействия узлов сети (таких как «Борей», «КБУ-1», «ВИК», компьютеров с ПО ИСБ ITRIUM и др.) является синхронизация данных.

Под данными понимается набор элементов конфигурации системы ОПС и СКУД - пропусков, владельцев пропусков, уровней доступа, уровней охраны, зон доступа (для контроля повторного прохода), зон охраны, зон и разделов охраны, терминалов, также общий ресурс - роли и пользователи.

**Внимание:** Синхронизация данных невозможна, если узлы не синхронизированы по времени (см. раздел [Синхронизация времени на узлах НЕЙРОСС](#)).

Существует два способа синхронизации данных: ручной и автоматический. При автоматической синхронизации данные одного или нескольких узлов заменяются данными узла-источника (выполняется под «облачной» учётной записью, см. раздел [Пользователи, роли и права](#)). При выборе ручного способа можно выполнить количественное сравнение данных двух узлов и выполнить синхронизацию по какому-либо одному типу данных. При этом по типу данных любой узел может выступать как в качестве источника, так и в качестве приёмника (получателя).

**Примечание:** На узле-приёмнике данные выбранного типа заменяются данными узла-источника (конкатенация данных не производится).

Выполните следующую последовательность шагов:

1. Перейдите к веб-интерфейсу прибора, выберите раздел **Сеть**.
2. Выберите узлы, данные которых требуется синхронизировать и нажмите на кнопку **Синхронизация данных** (рисунок 49).

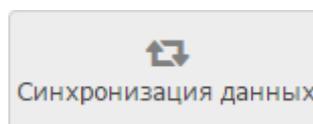
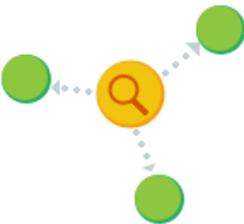


Рисунок 49 — Кнопка **Синхронизация данных**

3. Выберите требуемый способ синхронизации (рисунок 50).

Синхронизация данныхЗакреть

**Автоматическая синхронизация**



Выберите этот режим для синхронизации данных всех выбранных узлов с одного эталонного источника. В результате синхронизации данные выбранного узла будут загружены во все остальные узлы.

Выбрать источник

**Ручное управление**



Ручной режим предназначен для опытных пользователей. Он позволяет просмотреть статус синхронизации данных всех выбранных узлов в форме матрицы и управлять синхронизацией отдельных типов данных.

Синхронизировать вручную

Рисунок 50 — Выбор способа синхронизации данных

- Для синхронизации по одному узлу-источнику нажмите на кнопку **Выбрать источник**, в новом окне выберите из раскрывающегося списка IP-адрес источника и нажмите на кнопку **Экспортировать данные**.
- Для сравнения данных по группам: **Пропуск, Уровень доступа, Уровень охраны, Владелец пропуска, Зона доступа, Зона охраны, Раздел охраны, Терминал, Общий ресурс**, – нажмите на кнопку **Синхронизировать вручную**.
- Чтобы оценить текущий статус данных, в левом столбце выберите тип данных для сравнения. В основной части окна иконками будет показано текущее состояние (рисунок 51).

**Примечание:** Щелчком левой клавиши мыши по блоку **Легенда** можно раскрыть описание обозначений статусов синхронизации. Наведением указателя мыши по имени статуса, можно ознакомиться с дополнительным описанием.

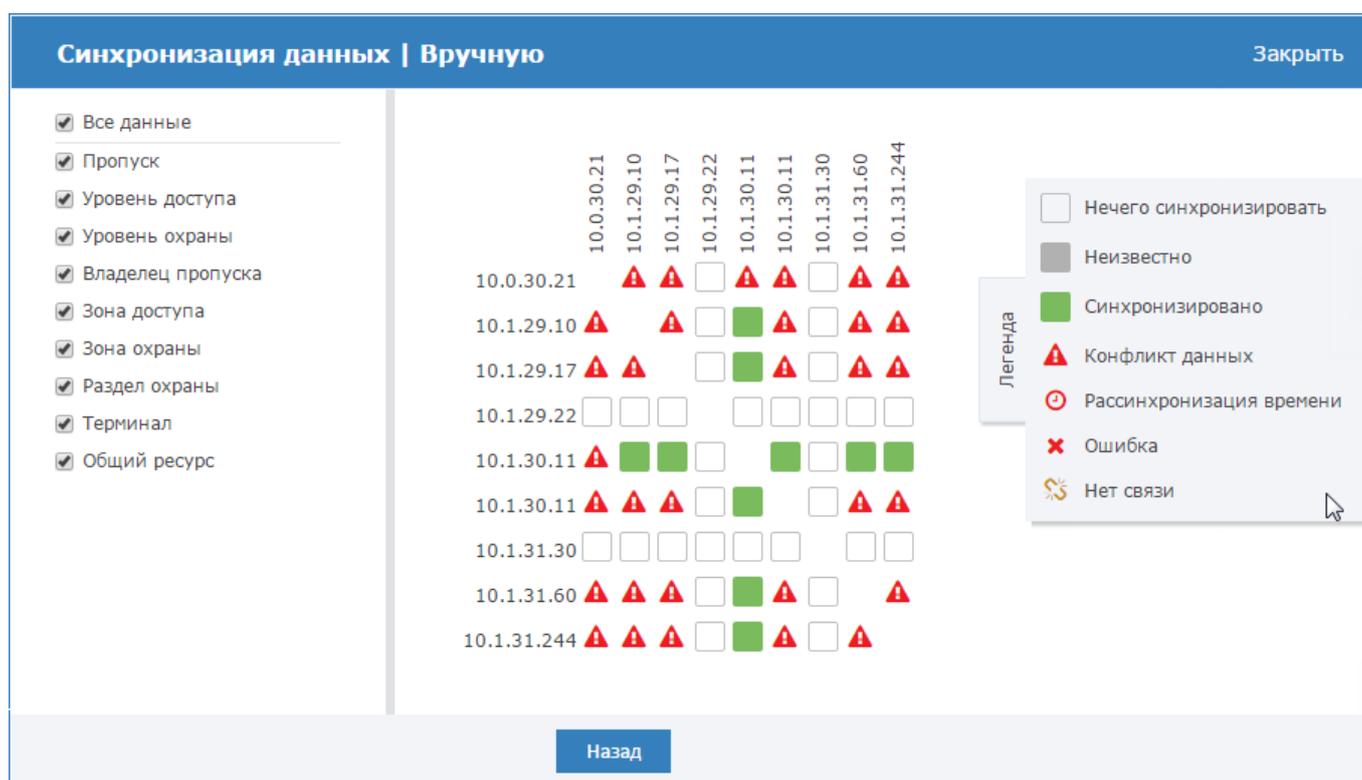


Рисунок 51 — Состояние синхронизации данных между узлами

- Для синхронизации данных, выберите любую пару узлов (нажмите в требуемой ячейке таблицы и в следующем окне с помощью стрелок влево и вправо выполните синхронизацию по требуемым типам данных (рисунок 52)).

Синхронизация данных   Вручную					Закреть
	10.0.30.43	→ ←	10.1.29.26	Статус	
Пропуск	10256	→ ←	10256	Синхронизировано	
Уровень доступа	8	→ ←	8	Синхронизировано	
Уровень охраны	3	→ ←	3	Синхронизировано	
Владелец пропуска	10256	→ ←	10256	Синхронизировано	
Зона доступа	5	→ ←	5	Синхронизировано	
Зона охраны	72	→ ←	72	Синхронизировано	
Раздел охраны	9	→ ←	9	Синхронизировано	
Терминал	2	→ ←	0	Конфликт	
Общий ресурс	4	→ ←	2	Конфликт	

**Назад**

Рисунок 52 — Синхронизация данных по типам

- Для выбора другой пары узлов для синхронизации нажмите на кнопку **Назад**.

### Удаление узлов НЕЙРОСС

Если какой-то узел удален из сети НЕЙРОСС, для удаления его из списка узлов необходимо выполнить процедуру удаления узла:

1. Перейдите к веб-интерфейсу прибора, выберите раздел **Сеть**.
2. В списке устройств сети выберите требуемое устройство(а), нажмите на кнопку **Удалить узлы** (рисунок 47).

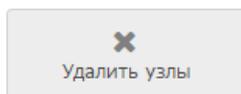


Рисунок 53 — Кнопка **Синхронизация времени**

Примечание 1 — Если был удалён узел, доступный в сети, то при получении ответа на WSD-запрос узел будет возвращен в список устройств (подробнее см. в разделе [Понятие сети НЕЙРОСС](#)).

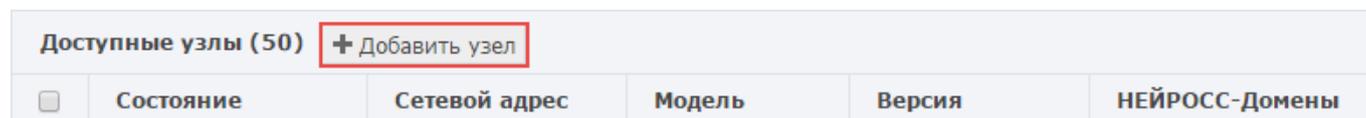
Примечание 2 — Чтобы удалить недоступный узел из списка всех узлов сети, необходимо повторить процедуру удаления на каждом из устройств.

## Добавление узлов НЕЙРОСС

Поиск узлов НЕЙРОСС производится автоматически путем отправки широковещательного WSD-запроса (см. раздел [Понятие сети НЕЙРОСС](#)).

В некоторых случаях необходимо добавить узел вручную. Для этого выполните следующую последовательность шагов:

1. Перейдите к веб-интерфейсу прибора, выберите раздел **Сеть**.
2. Нажмите на кнопку **Добавить узел**, расположенную в заголовке таблицы списка устройств (рисунок 54).



Доступные узлы (50) <span style="border: 1px solid red; padding: 2px;">+ Добавить узел</span>					
<input type="checkbox"/>	Состояние	Сетевой адрес	Модель	Версия	НЕЙРОСС-Домены

Рисунок 54 — Заголовок таблицы списка устройств сети НЕЙРОСС

3. Выберите, хотите ли вы добавить узел НЕЙРОСС (прибор «Борей», «КБУ-1», «Девизор», «ВИК», сервер ITRIUM) или ONVIF-камеру.
4. Укажите ip-адрес и учётные данные для доступа к узлу НЕЙРОСС (root/мастер-пароль или данные «облачной» учётной записи на устройстве) или адрес Onvif Device Service для камеры, следуйте инструкциям мастера.

## ПРИЛОЖЕНИЕ 5. БЮРО ПРОПУСКОВ

Веб-приложение «Бюро пропусков» предназначено для просмотра и конфигурирования данных пропусков. Каждому пропуску назначается уровень доступа, также может быть задан уровень охраны. Номер карты и код предприятия пропуска может быть считан с помощью выбранного считывателя. Данные пропусков, уровней доступа и уровней охраны автоматически синхронизируются между контроллерами «Борей», КБУ-1, «ВИК», ПО ИСБ ITRIUM®.

База данных пропусков является общей для всей системы в целом. При создании пропуска средствами веб-интерфейса какого-либо устройства «Борей», «КБУ-1», «ВИК», а также из ПО ИСБ ITRIUM®, данные автоматически обновляются во всех контроллерах сети и в ITRIUM®.

Для перехода в Бюро пропусков, перейдите на **Рабочий стол** (см. раздел [Окно веб-интерфейса. Рабочий стол](#)) и выберите пункт **Бюро пропусков**.

Окно приложения «Бюро пропусков» (рисунок 55) содержит три вкладки:

- **Пропуска** — вкладка предназначена для поиска и редактирования пропусков в системе, а также для создания новых пропусков;
- **Уровни доступа** — вкладка предназначена для создания, просмотра и редактирования уровней доступа в системе;
- **Уровни охраны** — вкладка предназначена для создания, просмотра и редактирования уровней охраны.

Пропуска | Уровни доступа | Уровни охраны

Поиск

Номер карты

Код предприятия

PIN

Фамилия

Имя

Отчество

Найти

Создать новый

Создать на основе

Редактировать

Удалить

◀ Задайте критерии и начните поиск

ИТРИУМ © 2014

Рисунок 55 — Окно Бюро пропусков

### Создание пропуска

Чтобы создать новый пропуск, выполните следующую последовательность шагов:

1. На вкладке **Пропуска** нажмите на кнопку **Создать новый**.
2. В окне добавления пропуска выберите из раскрывающегося списка тип пропуска (рисунок 57) и введите данные владельца пропуска (рисунок 56).

Пропуска | Уровни доступа | Уровни охраны

Поиск | Пропуск №142/32633: Постоянный

Владелец | Карта | Действия ▾

Фамилия \*  
Семков

Имя \*  
Антон

Отчество \*  
Викторович

Подразделение  
Центр управления проектами

Должность  
Директор центра

Табельный номер  
II-AK 163

К карте → | Сохранить

Рисунок 56 — Окно создания нового пропуска. Вкладка **Владелец**

Новый пропуск:

- Постоянный
- Временный
- Разовый**
- Транспортный

Рисунок 57 — Выбор типа пропуска

3. Загрузите фото для пропуска. Для этого:

- Нажмите на кнопку **Загрузить фото**.
- Укажите на файл с изображением.
- В открывшемся окне редактора (рисунок 58) поверните и измените, если требуется, границы фотографии, отцентрируйте при помощи перетаскивания видимой области. Нажмите на кнопку **Сохранить**.



Рисунок 58 — Окно редактора изображения пропуска

4. Перейдите к вкладке **Карта** или нажмите на кнопку **К карте** (рисунки 56 и 59).

Пропуска | Уровни доступа | Уровни охраны

Поиск

Пропуск №142/32633: Постоянный

Владелец | Карта | Действия



Постоянный

Загрузить фото

Карта

32633

Код предприятия

142

ПИН

1234

ПИН для прохода под принуждением

2341

Период действия

ДД-ММ-ГГГГ — ДД-ММ-ГГГГ

Уровень доступа

1. Вездеход

Уровень охраны

1. Основной уровень охраны

К владельцу | Сохранить

Рисунок 59 — Окно создания нового пропуска. Вкладка **Карта**

5. В полях **Карта** и **Код предприятия** введите номер и код карты соответственно.

**Примечание:** Эти данные могут быть считаны с карты. Для этого:

- Нажмите на кнопку **Считать номер с карты** .
- В отобразившемся окне выберите из раскрывающегося списка требуемый считыватель, нажмите на кнопку **Далее**. Выбранный считыватель будет заблокирован.
- Поднесите карту. Данные номера и кода карты будут считаны и подставлены в соответствующие поля формы.
- Нажмите на кнопку **Завершить** или **Считать другую карту**, если считать данные другой карты.

6. Если будет осуществляться идентификация по пинкоду, в поле **ПИН** задайте пинкод карты. Если будет выполняться контроль прохода под принуждением, заполните поле ниже.

7. Задайте период действия, если требуется.

8. В поле **Уровень доступа** выберите из раскрывающегося списка уровень доступа (порядок настройки уровней доступа представлен в разделе [Настройка уровней доступа](#)).

- Если данному пропуску требуются права на управление разделами сигнализации при помощи считывателя, в поле **Уровень охраны** выберите из раскрывающегося списка уровень охраны (порядок настройки уровней охраны представлен в разделе [Настройка уровней охраны](#)).
- Нажмите на кнопку **Сохранить**.

### Поиск пропуска

Чтобы **найти все пропуска в системе**, на вкладке **Пропуска** бюро пропусков нажмите на кнопку **Найти**.

Чтобы **найти пропуска по определенным критериям**, введите данные в форму поиска и нажмите на кнопку **Найти**. Данные номера карты и кода предприятия могут быть введены вручную или считаны с пропуска (с помощью кнопки **Считать номер с карты**



### Редактирование пропуска

Чтобы отредактировать данные пропуска, найдите требуемый пропуск (см. раздел [Поиск пропуска](#)). Далее выделите требуемый пропуск и нажмите на кнопку **Редактировать**, или откройте форму пропуска двойным щелчком.

Кнопка  предназначена для очистки всех полей пропуска.

### Сброс зоны АРВ

Если в точке доступа осуществляется контроль повторного прохода в жестком режиме, при нарушении режима прохода (предъявлении карты на считыватель другой зоны) произойдет отказ в доступе. Для решения данной проблемы предусмотрен механизм сброса текущей зоны:

- Перейдите к приложению «Бюро пропусков»
- Выполните поиск пропуска.
- В таблице пропусков, в поле **Зона АРВ** требуемого пропуска нажмите на кнопку  **Сбросить зону** (рисунок 60).

Пропуска						
	Тип	ФИО	Зона АРВ		№ карты	Пин
	Постоянный	Пропуск 1 Лена Лена	2. Зона 2		32633	
	Постоянный	Пропуск 2 Лена Лена	Нет			

Рисунок 60 — Окно списка пропусков

## Настройка уровней доступа

Уровень доступа назначается пропуску и определяет, в какое время и по каким точкам доступа разрешается проход.

Настройка уровней доступа осуществляется в приложении «Бюро пропусков». Для перехода в Бюро пропусков, перейдите на **Рабочий стол** и выберите пункт **Бюро пропусков**, далее перейдите к вкладке **Уровни доступа**.

Окно конфигурирования уровней доступа (рисунок 61) разделено на три вертикальные области: слева задается номер и имя уровня доступа, по центру указываются временные интервалы, в течение которых проход разрешен. Справа выбираются точки доступа устройства НЕЙРОСС: «Борей», «КБУ-1», «ВИК».

Уровни доступа +

Номер, наименование

- 1. Уровень доступа Основной
- 2. Уровень доступа Охранник
- 4. Уровень доступа Техник

Временная зона +

09:00:00 — 18:59:59

Пн Вт Ср Чт Пт Сб Вс Все

10:00:00 — 12:59:59

Пн Вт Ср Чт Пт Сб Вс Все

Точки доступа

Устройство, IP, ТД

- Все
- 10.0.30.37(BOREJ) Точка доступа 1
- 10.0.30.37(BOREJ) Точка доступа 2
- 192.168.1.100(BO... Точка доступа 1
- 192.168.1.100(BO... Точка доступа 2
- 10.1.31.213(BOREJ) Точка доступа 1
- 10.1.31.213(BOREJ) Точка доступа 2

Сохранить

Рисунок 61 — Окно конфигурирования уровней доступа

Если уровни доступа ранее не конфигурировались, отобразится пустое окно (рисунок 62).

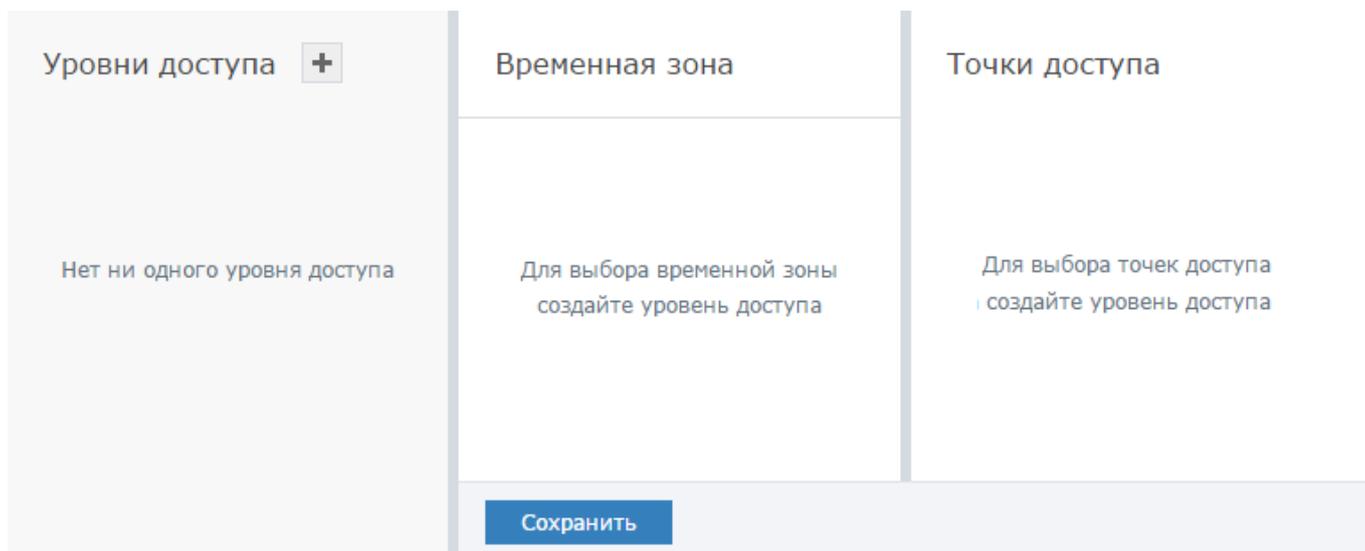


Рисунок 62 — Окно конфигурирования уровней доступа. Не создано ни одного уровня

Чтобы добавить уровень доступа, выполните следующую последовательность шагов:

1. В столбце **Уровень доступа** нажмите на кнопку **Добавить уровень доступа**.
2. Укажите номер и наименование уровня доступа (рисунок 63). Нажмите на кнопку .

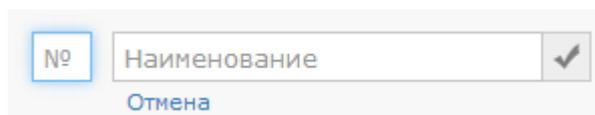


Рисунок 63 — Добавление уровня доступа

3. В столбце **Временная зона** (рисунок 64) укажите временной интервал и дни недели, в течение которых разрешен проход. Часы, минуты, секунды начала/окончания временного интервала можно вписать вручную или выбрать с помощью дополнительного инструмента, который можно открыть по кнопке . Дни недели выбираются щелчком левой клавишей мыши. При необходимости выбора всех дней недели, нажмите на кнопку **Все**.



Рисунок 64 — Добавление временного интервала

4. При необходимости добавления к этому уровню доступа нового временного интервала, нажмите на кнопку **Добавить временную зону** и задайте параметры новой зоны.

5. В столбце **Точки доступа** выберите точки доступа, проход по которым разрешен для данного уровня доступа. Можно осуществлять поиск точки доступа по IP-адресу контроллера, его названию или названию точки доступа.
6. Нажмите на кнопку **Сохранить**.
7. При необходимости создания нового уровня доступа, повторите действия пп. 1. - 6.
8. Впоследствии параметры уровней доступа могут быть изменены, для этого перейдите в окно конфигурирования уровней доступа, слева выберите требуемый уровень (или воспользуйтесь поиском по номеру или наименованию), измените временные интервалы или точки доступа, нажмите на кнопку **Сохранить**.

### Настройка уровней охраны

Уровень охраны назначается пропуску и определяет:

- список разделов сигнализации и разрешенное действие (постановка и/или снятие) по каждому разделу,
- период времени, в течение которого разрешается работа с разделами сигнализации.

**Примечание:** Один пропуск может обладать правами постановки/снятия в нескольких точках доступа. Для каждой точки доступа необходимо предварительно задать список разделов сигнализации, с которыми может работать точка доступа (порядок «привязки» разделов к точке доступа описан в разделе [Терминалы](#)).

Список разделов для управления определяется пересечением множества «привязанных» к точке доступа разделов с множеством разделов, заданных уровнем охраны пропуска (рисунок 65).

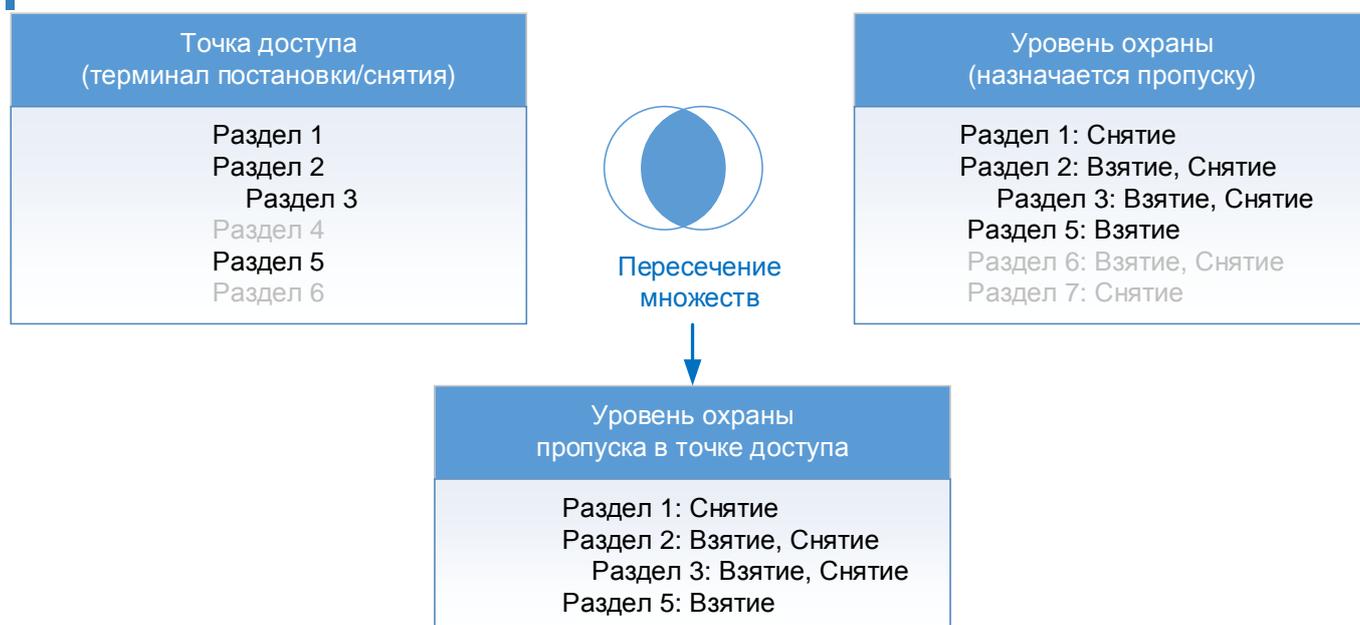


Рисунок 65 — Уровень охраны пропуска в точке доступа

Настройка уровней охраны осуществляется в приложении «Бюро пропусков». Для перехода в Бюро пропусков, перейдите на **Рабочий стол** и выберите пункт **Бюро пропусков**, далее перейдите к вкладке **Уровни охраны**.

Окно конфигурирования уровней охраны (рисунок 66) разделено на три вертикальные области: слева задается номер и имя уровня охраны, по центру выбираются разделы сигнализации и разрешенные действия, справа указываются временные интервалы, в течение которых разрешено управление разделами.

Уровни охраны +

Номер, наименование 🔍

1. Уровень охраны ✕

Разделы сигнализации

Номер, наименование 🔍

Раздел 1  
 Взятие  Снятие

▼  Раздел 2  
 Взятие  Снятие

Раздел 3  
 Взятие  Снятие

Раздел 4

Раздел 5  
 Взятие  Снятие

Раздел 6  
 Взятие  Снятие

Раздел 7  
 Взятие  Снятие

Временная зона +

09:00:00 ⌚ – 18:59:59 ⌚ ✕

Пн Вт Ср Чт Пт Сб Вс Все

10:00:00 ⌚ – 12:00:00 ⌚ ✕

Пн Вт Ср Чт Пт Сб Вс Все

Сохранить

Рисунок 66 — Окно конфигурирования уровней охраны

Если уровни охраны ранее не конфигурировались, отобразится пустое окно (рисунок 67).

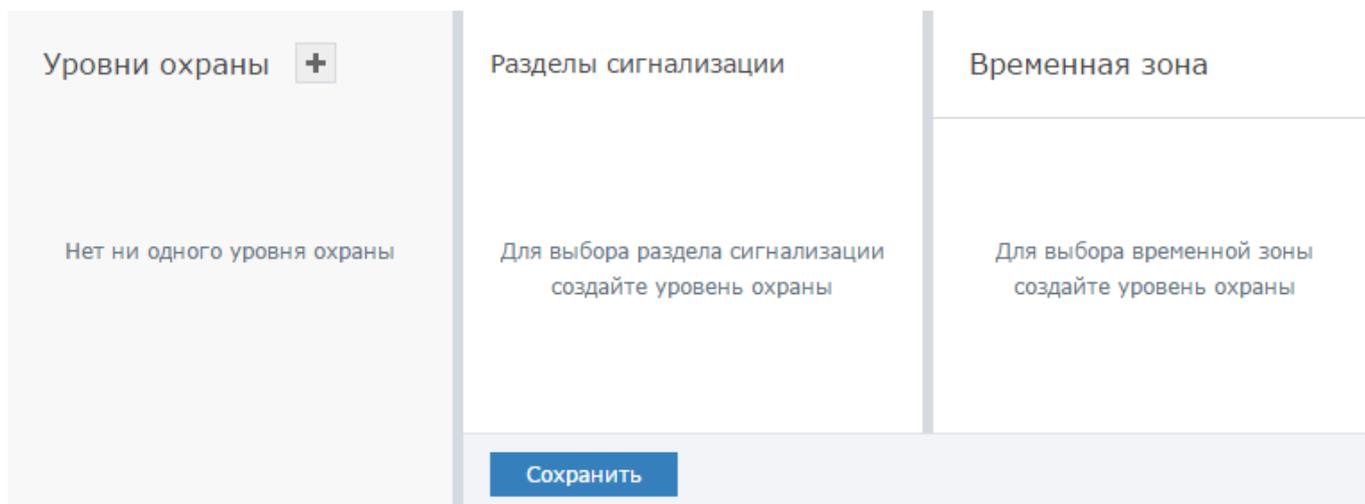


Рисунок 67 — Окно конфигурирования уровней охраны. Не создано ни одного уровня

Чтобы добавить уровень охраны, выполните следующую последовательность шагов:

1. В столбце **Уровни охраны** нажмите на кнопку  **Добавить уровень охраны**.
2. Укажите номер и наименование уровня охраны (рисунок 68). Нажмите на кнопку .

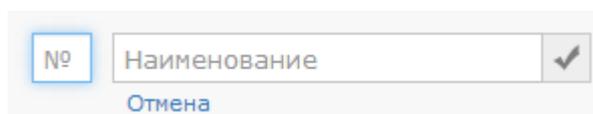


Рисунок 68 — Добавление уровня охраны

3. В столбце **Разделы сигнализации** выберите разделы сигнализации и разрешенные действия с разделами.

**Примечание:** Список разрешенных действий отображается после выбора раздела. При выборе действия (например, взятие раздела под охрану) для родительского раздела, данное действие автоматически выбирается для всех дочерних разделов. Можно осуществлять поиск раздела по его номеру или наименованию.

4. В столбце **Временная зона** (рисунок 69) укажите временной интервал и дни недели, в течение которых разрешен проход. Часы, минуты, секунды начала/окончания временного интервала можно вписать вручную или выбрать с помощью дополнительного инструмента, который можно открыть по кнопке . Дни недели выбираются щелчком левой клавишей мыши. При необходимости выбора всех дней недели, нажмите на кнопку **Все**.



Рисунок 69 — Добавление временного интервала

5. При необходимости добавления к этому уровню охраны нового временного интервала, нажмите на кнопку **+** **Добавить временную зону** и задайте параметры новой зоны.
6. Нажмите на кнопку **Сохранить**.
7. При необходимости создания нового уровня охраны, повторите действия пп.1. 1. - 6.
8. Впоследствии параметры уровней охраны могут быть изменены, для этого перейдите в окно конфигурирования уровней охраны, слева выберите требуемый уровень (или воспользуйтесь поиском по номеру или наименованию), измените список разделов, разрешенные действия или временные интервалы, нажмите на кнопку **Сохранить**.

## ПРИЛОЖЕНИЕ 6. ФОТОИДЕНТИФИКАЦИЯ

Приложение «Фотоидентификация» предназначено для подтверждения личности владельца пропуска в системе контроля доступа и позволяет:

- Проводить мониторинг событий доступа с одновременным просмотром фото-/видеоданных с «привязанной» камеры;
- Выполнять подтверждение или запрет доступа.

Окно приложения разделено на две области:

- Слева расположена область ленты событий системы доступа (рисунок 70);
- Основное окно поделено на области, в каждой из которых отображаются события по выбранной точке доступа (рисунок 71). При наличии «привязанной» камеры, в случае запроса доступа отображается «живое видео».

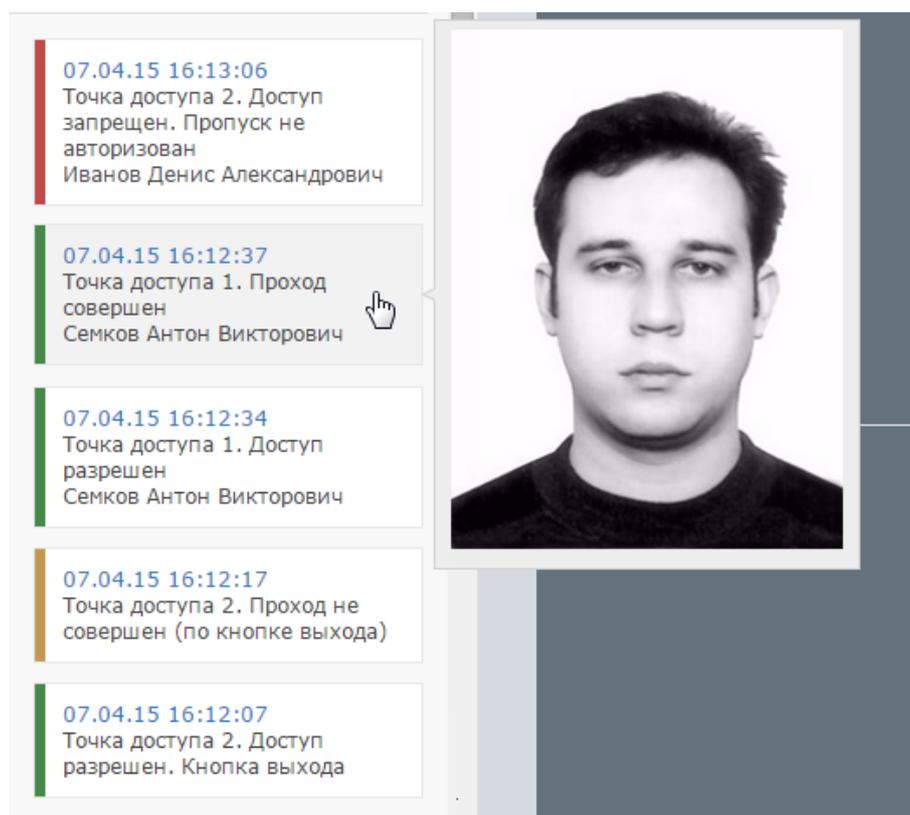


Рисунок 70 — Лента событий приложения «Фотоидентификация»

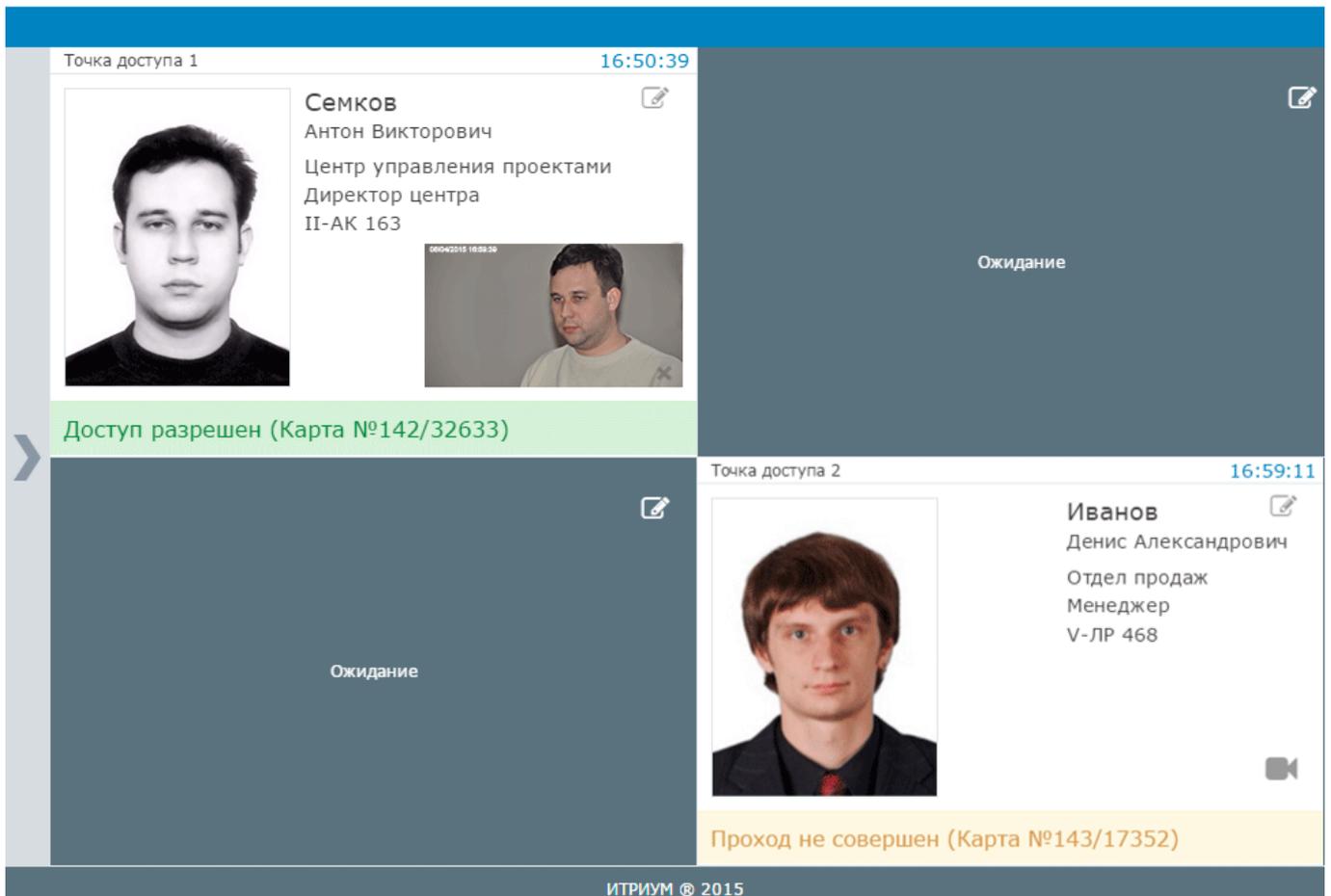


Рисунок 71 — Основное окно приложения «Фотоидентификация»

## ПРИЛОЖЕНИЕ 7. ЖУРНАЛ СОБЫТИЙ

Приложение **Журнал событий** реализует функции просмотра журнала событий всей системы в целом с возможностью фильтрации по дате и времени, источнику события, узлу системы, пропуску и др. и последующего экспорта в текстовый файл.

Приложение содержит две вкладки: **«Живой» журнал** и **Поиск**.

На вкладке **Живой журнал** события отображаются в режиме реального времени и могут быть отфильтрованы по типу, источнику, пропуску или узлу сети. Кнопка **Очистить** позволяет очистить экран для более удобного просмотра поступающих событий (при этом события не удаляются, их можно отобразить с помощью инструментов вкладки **Поиск**).

Инструменты вкладки **Поиск** позволяют отобразить события за определённый период времени с возможностью их фильтрации по заданным критериям. Дату и время начала и окончания временного интервала, за который будет проводиться поиск событий, можно вписать в поля **Дата начала** и **Дата окончания** вручную в формате **ДД-ММ-ГГГГ ЧЧ:ММ:СС**, например **19-05-2016 10:17:38** или выбрать с помощью дополнительного инструмента:

- по кнопке  можно перейти к инструменту задания даты,
- затем по кнопке  можно перейти к указанию момента времени (рисунок 72).

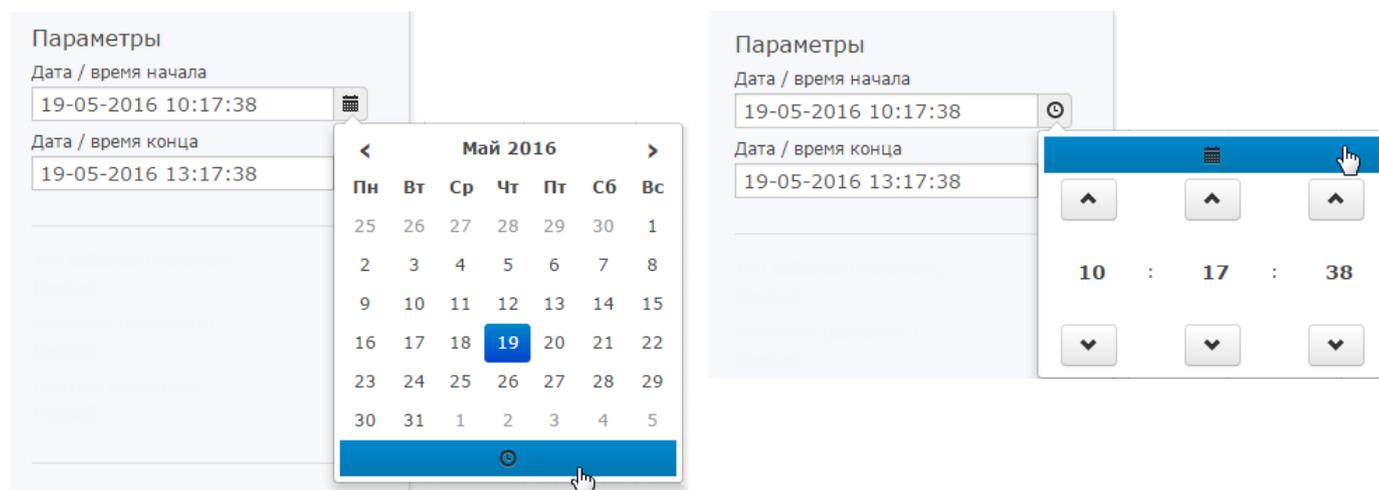


Рисунок 72 — Добавление временного интервала

По завершению поиска, список событий можно экспортировать в формат **CSV** для редактирования в MS Excel и др. программах. Для экспорта нажмите на кнопку  (рисунок 73).

Поиск завершён  (найдено 659 из 661 событий до 19.05.16 14:41:23)

Дата	Время	Заголовок	Источник	Карта	Субъект
19.05.16	14:26:17	Проход совершен	Точка доступа 1	4614 / 12000	Семков Антон Виктор..
19.05.16	14:26:17	Изменилось состояние двери	Точка доступа 1	-	-
19.05.16	14:26:16	Изменилось состояние замка	Точка доступа 1	-	-
19.05.16	14:26:16	Изменилось состояние двери	Точка доступа 1	-	-
19.05.16	14:26:15	Изменилось состояние замка	Точка доступа 1	-	-
19.05.16	14:26:15	Изменилось состояние точки доступа	Точка доступа 1	-	-
19.05.16	14:26:15	Доступ разрешен	Точка доступа 1	4614 / 12000	Семков Антон Виктор..
19.05.16	13:16:41	На охране, раздел Раздел 1	/alarm/section/1c54e...	-	-
19.05.16	13:16:41	Зона 'Зона 0.RIN.1' поставлена на ох...	Зона 0.RIN.1	-	-
19.05.16	13:16:41	Зона 'Зона 0.RIN.1' перешла в состоя...	Зона 0.RIN.1	-	-
19.05.16	13:14:24	Частично на охране, раздел Раздел 1	/alarm/section/1c54e...	-	-
19.05.16	13:13:42	Зона 'Зона 0.RIN.4' поставлена на ох...	Зона 0.RIN.4	-	-
19.05.16	13:13:42	Зона 'Зона 0.RIN.4' перешла в состоя...	Зона 0.RIN.4	-	-

Рисунок 73 — Список событий за заданный период времени

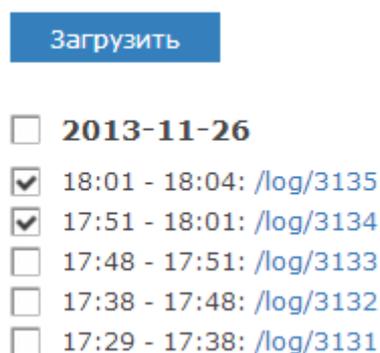
## ПРИЛОЖЕНИЕ 8. ЖУРНАЛ АУДИТА

**Внимание:** Раздел **Журнал аудита** временно неактивен.

В разделе **Журнал аудита** отображаются ссылки на отладочные файлы устройства (лог-файлы). Файлы упорядочены по времени создания в порядке убывания и предназначены для отслеживания внутренней работы прибора, отладки отсылок извещений, наличия связи прибора с подписчиками и т.д. Информация данного раздела предназначена, в основном, только разработчикам.

Чтобы скачать требуемый файл, нажмите на ссылку с идентификатором файла. Скачивание начнется незамедлительно.

Чтобы скачать несколько файлов, отметьте флажками требуемые файлы и нажмите на кнопку **Загрузить** (рисунок 74). Скачивание начнется незамедлительно. Выбранные файлы будут сформированы в архив формата **.tar.gz**.



Загрузить

- 2013-11-26**
- 18:01 - 18:04: /log/3135
- 17:51 - 18:01: /log/3134
- 17:48 - 17:51: /log/3133
- 17:38 - 17:48: /log/3132
- 17:29 - 17:38: /log/3131

Рисунок 74 — Список лог-файлов

Чтобы скачать лог-файлы за сутки / несколько суток, отметьте флажками требуемые даты и нажмите на кнопку **Загрузить**.

## ПРИЛОЖЕНИЕ 9. СОСТОЯНИЯ ЭЛЕМЕНТОВ ПРИБОРА

### 1. Состояния охранных зон

Таблица 8

Состояние	Описание
Снято с охраны, Норма*	Состояние по умолчанию. Зона готова к постановке на охрану.
На охране	Зона поставлена на охрану, тревог нет.
Тревога*	<ul style="list-style-type: none"> <li>Тревога в зоне на охране;</li> <li>Тревога в снятой с охраны зоне (формируется, если в настройках зоны в поле <b>Тревога в снятой с охраны зоне</b> задано <b>Да</b>);</li> <li>Короткое замыкание или обрыв шлейфа в зоне с режимом контроля <b>Охрана 24 часа</b>.</li> </ul>
Невзятие	Предпринята попытка постановки на охрану зоны в состоянии [Тревога]. При восстановлении шлейфа, зона будет поставлена на охрану.
Обрыв шлейфа*	Неисправное состояние зоны, обрыв шлейфа сигнализации (формируется только для зон, образуемых радиальными шлейфами сигнализации (название по-умолчанию <b>Зона 0.RIN.1 – Зона 0.RIN.8</b> )). Если в настройках зоны в поле <b>Режим контроля</b> указано <b>Охрана 24 часа</b> , формируется состояние [Тревога].
Короткое замыкание*	Неисправное состояние зоны, короткое замыкание (формируется только для зон, образуемых радиальными шлейфами сигнализации (название по-умолчанию <b>Зона 0.RIN.1 – Зона 0.RIN.8</b> )). Если в настройках зоны в поле <b>Режим контроля</b> указано <b>Охрана 24 часа</b> , формируется состояние [Тревога].
Неисправность*	Неисправное состояние зоны (формируется только для зон, образуемых адресными шлейфами сигнализации АМ-06 (название по-умолчанию <b>Зона 0.SART.0 – Зона 0.SART.29</b> )).
Отключена	Зона отключена. В поле <b>Режим контроля</b> задано <b>Исключена</b> .
Потеря связи	Потеряна связь со шлейфом (формируется только для зон, образуемых адресными шлейфами сигнализации АМ-06 (название по-умолчанию <b>Зона 0.SART.0 – Зона 0.SART.29</b> )).
Неизвестно	Логическое состояние связи с устройством «Борей», «КБУ-1», зона которого объединена в раздел охранной сигнализации (только для мониторинга состояния разделов).

\* Состояния зоны [Норма], [Тревога], [Обрыв шлейфа], [Короткое замыкание], [Неисправность] связаны с физическим состоянием шлейфа.

### 2. Состояния разделов охранной сигнализации

Таблица 9

Состояние	Описание
Снято с охраны	Состояние по умолчанию. Все зоны раздела в состоянии [Снято с охраны, Норма]. Раздел готов к постановке на охрану.

Состояние	Описание
На охране	Раздел поставлен на охрану, нет тревог или неисправностей ни в одной зоне раздела.
Частично на охране	Раздел поставлен на охрану, некоторые зоны находятся в состояниях [Невзятие]. Нет тревог или неисправностей ни в одной зоне раздела.
Тревога	Одна или несколько зон раздела находятся в состоянии [Тревога]. Имеет наивысший приоритет.
Неисправность	Одна или несколько зон раздела находятся в одном из состояний: [Потеря связи], [Короткое замыкание], [Обрыв шлейфа] или [Неисправность]. Нет ни одной зоны в состоянии [Тревога].

### 3. Смена состояний зон и разделов при постановке на охрану

Таблица 10

Состояние до выполнения команды постановки на охрану		Состояние после выполнения команды постановки на охрану	
Зона	Раздел	Зона	Раздел
Снято с охраны, Норма	Снято с охраны	На охране	На охране
<ul style="list-style-type: none"> <li>Снято с охраны, норма (если в настройках зоны в поле Тревога в снятой с охраны зоне установлено Нет, но физическое состояние шлейфа [Тревога]);</li> <li>Тревога (если в настройках зоны в поле Тревога в снятой с охраны зоне установлено Да и физическое состояние шлейфа [Тревога]).</li> </ul>	<ul style="list-style-type: none"> <li>Снято с охраны (если в настройках зоны в поле Тревога в снятой с охраны зоне установлено Нет),</li> <li>Тревога (если в настройках хотя бы одной зоны раздела в поле Тревога в снятой с охраны зоне установлено Да)</li> </ul>	Невзятие	Частично на охране
<ul style="list-style-type: none"> <li>Тревога (если в настройках зоны в поле Тревога в снятой с охраны зоне установлено Да и физическое состояние шлейфа [Тревога]).</li> </ul>	<ul style="list-style-type: none"> <li>Тревога</li> </ul>	Состояние зоны не меняется, постановка на охрану не выполняется	Состояние раздела не меняется, постановка на охрану не выполняется.

Состояние до выполнения команды постановки на охрану		Состояние после выполнения команды постановки на охрану	
Зона	Раздел	Зона	Раздел
<p>Для радиальных шлейфов (название по умолчанию <b>Зона 0.RIN.1–Зона 0.RIN.8</b>):</p> <ul style="list-style-type: none"> <li>• <b>Обрыв шлейфа,</b></li> <li>• <b>Короткое замыкание;</b></li> </ul> <p>Для шлейфов S-ART (название по умолчанию <b>Зона 0.SART.–Зона 0.RIN.29</b>):</p> <ul style="list-style-type: none"> <li>• <b>Неисправность;</b></li> <li>• <b>Потеря связи;</b></li> </ul> <p>Для зон прибора, связь с которым потеряна</p> <ul style="list-style-type: none"> <li>• <b>Неизвестно</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>Неисправность</b></li> </ul>	Состояние зоны не меняется, постановка на охрану не выполняется	Состояние раздела не меняется, постановка на охрану не выполняется

**Пояснение:** Если хотя бы одна зона раздела находится в состоянии [Тревога], раздел также находится в состоянии [Тревога]. Если нет зон в тревожном состоянии, но есть зоны в состояниях [Короткое замыкание], [Обрыв шлейфа], [Неисправность], [Потеря связи], [Неизвестно], то раздел находится в состоянии [Неисправность]. При выполнении команды постановки на охрану зоны в состояниях [Короткое замыкание], [Обрыв шлейфа], [Неисправность], [Потеря связи], состояние зоны и, соответственно, раздела не меняется. При выполнении команды постановки на охрану зоны, физическое состояние шлейфа которой [Тревога], зона переходит в состояние [Невзятие] с автоматической постановкой на охрану при сбросе тревоги или восстановлении шлейфа. Описание состояний разделов/зон дано в разделах [Состояния охранных зон](#), [Состояния разделов охранной сигнализации](#).

## ПРИЛОЖЕНИЕ 10. АДМИНИСТРИРОВАНИЕ ПРИБОРА

### 1. Перезапуск прибора

#### Аппаратный перезапуск

Если устройство «зависло» и получить доступ к интерфейсу не удаётся, может потребоваться аппаратный перезапуск прибора, который может быть выполнен отключением и восстановлением питания прибора.

#### Перезагрузка приложения

При наличии доступа к веб-интерфейсу возможна программная перезагрузка приложения:

- При авторизации под учётной записью **root** возможна перезагрузка только того прибора, по IP-адресу которого выполнен вход в интерфейс. Перезагрузка осуществляется по команде из раздела **Конфигурация узлов — Основные настройки** (см. раздел [Перезагрузка прибора](#));
- При авторизации под «облачной» учётной записью с правами обслуживания (см. раздел [Пользователи, роли и права](#)) возможна перезагрузка одновременно нескольких устройств по команде из раздела интерфейса **Сеть** (см. раздел [Перезагрузка узлов НЕЙРОСС](#)).

### 2. Обновление программного обеспечения (прошивки) прибора

Средства пользовательского интерфейс позволяют выполнять обновление прошивки как одного узла, так и группы однотипных узлов:

- При авторизации под учётной записью **root** возможно обновление только того прибора, по IP-адресу которого выполнен вход в интерфейс. Обновление осуществляется по команде из раздела **Конфигурация узлов — Основные настройки** (см. раздел [Обновление программных средств](#));
- При авторизации под «облачной» учётной записью с правами обслуживания (см. раздел [Пользователи, роли и права](#)) возможно обновление одновременно нескольких однотипных узлов НЕЙРОСС по команде из раздела интерфейса **Сеть** (см. раздел [Обновление ПО узлов НЕЙРОСС](#)).

### 3. Резервные копии

- При авторизации под учётной записью **root** возможно создание резервной копии данных только того прибора, по IP-адресу которого выполнен вход в интерфейс. Резервная копия создаётся по команде из раздела **Конфигурация узлов — Основные настройки** (см. раздел [Резервные копии](#));

- При авторизации под «облачной» учётной записью с правами обслуживания (см. раздел [Пользователи, роли и права](#)) возможно создание резервных копий одновременно нескольких узлов НЕЙРОСС по команде из раздела интерфейса **Сеть** (см. раздел [Резервные копии узлов НЕЙРОСС](#)).