

РЭ 4372-126-80484710-2016



**ИТРИУМ®**

ООО «ИТРИУМ СПб»

**Прибор управления доступом  
и охранной сигнализации сетевой  
«ЯРС»**

**Руководство по эксплуатации  
КМУР.425723.126 РЭ**

Листов 206

Санкт – Петербург  
2018

## Содержание

<b>1 ОПИСАНИЕ И РАБОТА</b> .....	<b>11</b>
<b>1.1 Описание и работа изделия</b> .....	<b>11</b>
1.1.1 Назначение изделия .....	11
1.1.2 Технические характеристики изделия .....	12
1.1.2.1 Устойчивость к климатическим и механическим воздействиям .....	12
1.1.2.2 Условия работы .....	12
1.1.2.3 Электропитание изделия .....	12
1.1.2.4 Подключение изделия.....	13
1.1.3 Состав и комплектация изделия .....	15
1.1.3.1 Состав изделия.....	15
1.1.3.2 Комплектация изделия .....	17
1.1.3.3 Информация для заказа.....	17
1.1.3.4 Устройство и работа изделия .....	18
1.1.3.5 Маркировка и пломбирование .....	21
1.1.4 Упаковка прибора.....	22
<b>1.2 Описание и работа составных частей изделия</b> .....	<b>23</b>
1.2.1 Описание и работа контроллера «ЯРС» .....	23
1.2.1.1 Общие сведения о контроллере «ЯРС».....	23
1.2.1.2 Описание контроллера «ЯРС» .....	23
1.2.1.2.1 Технические характеристики изделия .....	23
1.2.1.2.2 Описание состояний индикаторов .....	25
1.2.1.2.3 Питание изделия.....	25
1.2.1.2.4 Шлейфы сигнализации .....	26
1.2.1.2.5 Дополнительные входы.....	27
1.2.1.2.6 Выходы управления.....	27
1.2.1.2.7 Конструкция изделия .....	28
1.2.1.2.8 Режимы индикации считывателей.....	30
1.2.1.3 Взаимодействие с внешним оборудованием .....	32
1.2.1.3.1 Взаимодействие с Handkey-II.....	32
1.2.2 Описание и работа коммуникационных модулей .....	33
1.2.2.1 Общие сведения о коммуникационных модулях .....	33
1.2.2.2 Конструкция коммуникационных модулей .....	33
1.2.3 Описание и работа модуля «M2».....	35
1.2.3.1 Общие сведения о модуле «M2» .....	35
1.2.3.2 Описание модуля «M2».....	35
1.2.3.2.1 Технические характеристики изделия .....	35
1.2.3.2.2 Шлейфы сигнализации .....	37
1.2.3.2.1 Дополнительные входы.....	39
1.2.3.2.2 Выходы управления.....	39

1.2.3.2.3	Питание изделия.....	39
1.2.3.2.4	Конструкция изделия.....	39
1.2.4	Описание и работа модуля «МДС».....	41
1.2.4.1	Общие сведения о модуле «МДС».....	41
1.2.4.2	Описание модуля «МДС».....	42
1.2.4.2.1	Технические характеристики изделия .....	42
1.2.4.2.2	Шлейфы сигнализации .....	43
1.2.4.2.3	Питание изделия.....	44
1.2.4.2.4	Конструкция изделия.....	44
<b>2</b>	<b>ИСПОЛЬЗОВАНИЕ ПО НАЗНАЧЕНИЮ .....</b>	<b>46</b>
<b>2.1</b>	<b>Эксплуатационные ограничения.....</b>	<b>46</b>
2.1.1	Меры безопасности при подготовке изделия.....	46
2.1.2	Осмотр изделия.....	46
<b>2.2</b>	<b>Подготовка изделия к использованию .....</b>	<b>47</b>
2.2.1	Подготовка к работе одного (первого) устройства .....	47
2.2.2	Добавление устройства к сети НЕЙРОСС .....	51
2.2.3	Обновление программных средств.....	52
2.2.4	Подготовка к работе с турникетом .....	54
2.2.5	Подготовка к работе с Handkey-II.....	54
<b>2.3</b>	<b>Использование изделия .....</b>	<b>55</b>
2.3.1	Предоставление доступа.....	55
2.3.1.1	Дежурный режим .....	55
2.3.1.2	Режим «Разблокировано».....	56
2.3.1.3	Режим «Заблокировано».....	57
2.3.2	Управление зонами и разделами охранной сигнализации .....	57
2.3.2.1	Управление разделами с помощью считывателя.....	57
<b>3</b>	<b>ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ .....</b>	<b>58</b>
<b>3.1</b>	<b>Общие указания и меры безопасности .....</b>	<b>58</b>
<b>3.2</b>	<b>Порядок технического обслуживания изделия .....</b>	<b>58</b>
<b>3.3</b>	<b>Проверка работоспособности изделия.....</b>	<b>59</b>
<b>4</b>	<b>ХРАНЕНИЕ .....</b>	<b>59</b>
<b>5</b>	<b>ТРАНСПОРТИРОВАНИЕ .....</b>	<b>59</b>
<b>6</b>	<b>УТИЛИЗАЦИЯ .....</b>	<b>60</b>
<b>7</b>	<b>ГАРАНТИИ ИЗГОТОВИТЕЛЯ .....</b>	<b>60</b>

<b>8</b>	<b>СВЕДЕНИЯ ОБ ИЗГОТОВИТЕЛЕ .....</b>	<b>60</b>
<b>9</b>	<b>ПРИЛОЖЕНИЯ .....</b>	<b>61</b>
	<b>Приложение 1. Габаритные и установочные размеры изделия .....</b>	<b>62</b>
	<b>Приложение 2. Линии связи .....</b>	<b>66</b>
	Понятие LonWorks .....	66
	Топология сети LonWorks.....	66
	<b>Приложение 3. Схемы внешних подключений.....</b>	<b>69</b>
	<b>1. Разъёмы платы электроники .....</b>	<b>69</b>
	<b>2. Подключение устройства к источнику питания.....</b>	<b>71</b>
	<b>3. Подключение к сети Lonworks.....</b>	<b>72</b>
	<b>4. Схемы подключения внешнего оборудования.....</b>	<b>72</b>
	Подключение GSM-модема .....	72
	Подключение к сети Ethernet .....	73
	Подключение шлейфов охранной сигнализации .....	75
	Подключение считывателей .....	75
	Подключение замковых устройств.....	78
	Подключение дверных контактов и кнопок выхода .....	81
	Подключение турникета .....	82
	Подключение картоприёмника.....	83
	Подключение Handkey-II .....	85
	<b>Приложение 4. Сеть НЕЙРОСС .....</b>	<b>87</b>
	Понятие сети НЕЙРОСС .....	87
	Понятие домена НЕЙРОСС .....	87
	<b>Приложение 5. Пользовательский интерфейс.....</b>	<b>89</b>
	<b>1. Мастер первого запуска.....</b>	<b>90</b>
	<b>2. Вход в веб-интерфейс .....</b>	<b>95</b>
	<b>3. Рабочий стол.....</b>	<b>96</b>
	<b>4. Конфигурация узлов .....</b>	<b>100</b>
	<b>5. Выход из веб-интерфейса .....</b>	<b>102</b>
	<b>Приложение 6. Настройки узла.....</b>	<b>103</b>
	<b>1. Основные настройки .....</b>	<b>103</b>
	Перезагрузка узла .....	103
	Обновление программных средств .....	104
	Резервные копии .....	105
	Смена мастер-пароля .....	106

<b>2. Сетевые параметры</b> .....	<b>106</b>
Основные сетевые параметры .....	107
Параметры GSM .....	108
Сетевые маршруты .....	110
Дополнительные сетевые параметры .....	110
<b>3. Дата и время</b> .....	<b>111</b>
Установка даты и времени вручную .....	111
Синхронизация по NTP-серверу .....	111
<b>4. Технологические входы</b> .....	<b>112</b>
<b>5. Точки доступа</b> .....	<b>113</b>
Тестирование правильности настройки точки доступа .....	122
<b>6. Зоны сигнализации</b> .....	<b>123</b>
Тестирование правильности настройки зон .....	125
<b>7. Модули расширения</b> .....	<b>125</b>
Добавление M2/МДС .....	126
Настройка M2/МДС .....	127
Замена M2/МДС .....	136
Удаление M2/МДС .....	136
Восстановление конфигурации M2/МДС .....	137
<b>8. Интеграция с Handkey-II</b> .....	<b>137</b>
<b>Приложение 7. Настройка общих ресурсов сети</b> .....	<b>140</b>
<b>1. Пользователи, роли и права</b> .....	<b>140</b>
<b>2. Охранная сигнализация</b> .....	<b>143</b>
Разделы сигнализации .....	143
Команды управления разделами и зонами .....	146
Реле управления .....	148
<b>3. Терминалы</b> .....	<b>150</b>
Настройка терминала .....	151
<b>4. Зоны доступа</b> .....	<b>151</b>
Создание зон доступа .....	152
<b>Приложение 8. Сеть</b> .....	<b>153</b>
Обновление ПО узлов НЕЙРОСС .....	155
Перезагрузка узлов НЕЙРОСС .....	156
Резервные копии узлов НЕЙРОСС .....	157
Синхронизация времени на узлах НЕЙРОСС .....	158
Синхронизация данных между узлами НЕЙРОСС .....	159

Удаление узлов НЕЙРОСС .....	162
Добавление узлов НЕЙРОСС .....	162
Создание кольцевой топологии узлов НЕЙРОСС .....	163
<b>Приложение 9. Бюро пропусков .....</b>	<b>165</b>
Создание пропуска .....	166
Поиск пропуска .....	169
Сброс зоны АРВ.....	170
Настройка уровней доступа .....	170
Настройка уровней управления.....	172
<b>Приложение 10. Фотоидентификация .....</b>	<b>177</b>
<b>Приложение 11. События .....</b>	<b>179</b>
<b>Приложение 12. Журнал аудита.....</b>	<b>181</b>
<b>Приложение 13. ПО ИСБ ITRIUM®.....</b>	<b>182</b>
<b>1. Настройка «Службы НЕЙРОСС».....</b>	<b>182</b>
<b>2. Команды управления.....</b>	<b>191</b>
<b>3. Настройка доступа в ПО ИСБ ITRIUM .....</b>	<b>192</b>
Уровни доступа.....	193
Уровни управления.....	194
Настройка режимов доступа .....	195
Команды управления точками доступа .....	197
<b>4. Загрузка данных в НЕЙРОСС.....</b>	<b>197</b>
<b>Приложение 14. Состояния элементов прибора.....</b>	<b>200</b>
<b>1. Состояния технологических входов .....</b>	<b>200</b>
<b>2. Состояния охранных зон .....</b>	<b>200</b>
<b>3. Состояния разделов охранной сигнализации .....</b>	<b>201</b>
<b>4. Смена состояний зон и разделов при постановке на охрану.....</b>	<b>202</b>
<b>5. Состояния точек доступа .....</b>	<b>203</b>
<b>Приложение 15. Администрирование узла.....</b>	<b>204</b>
<b>1. Сброс настроек .....</b>	<b>204</b>
<b>2. Перезапуск узла .....</b>	<b>204</b>
Аппаратный перезапуск .....	204
Перезагрузка программных средств.....	204
<b>3. Обновление программных средств (прошивки) прибора.....</b>	<b>204</b>
Обновление узла .....	204
Обновление LON-модулей.....	205

4. Резервные копии .....	206
--------------------------	-----

Настоящее руководство по эксплуатации содержит сведения о назначении, выполняемых функциях, принципе работы, конструкции, характеристиках и комплектации прибора управления доступом и охранной сигнализации сетевой «ЯРС», необходимые для правильной его эксплуатации, транспортирования, хранения и обслуживания.

Для настройки и обслуживания изделия специальная подготовка не требуется.

В соответствии с «Порядком проведения сертификации в РФ» для продукции, реализуемой изготовителем в течение срока действия сертификатов, они действительны при поставке, монтаже, эксплуатации и т.п. в течение срока службы изделия, указанном в паспорте на изделие.



## Список используемых терминов

**веб-интерфейс прибора/устройства (веб-интерфейс, веб-интерфейс НЕЙРОСС)** – веб-приложение (программа) в контроллере, предоставляющее пользовательский интерфейс конфигурирования устройств (контроллеров «ЯРС» и подключённых модулей), мониторинга состояния охранных зон и разделов, постановки на охрану, снятия с охраны, сброса тревог и другие функции; доступ к веб-приложению осуществляется посредством браузера по IP-адресу;

**односторонняя точка доступа** – считыватель у двери при входе в зону доступа, датчик состояния двери, кнопка выхода, управляемый замок;

**двусторонняя точка доступа** – считыватель у двери при входе в зону доступа, датчик состояния двери, считыватель у двери при выходе из зоны доступа, управляемый замок;

**ЕСПИ (единый стандартизованный протокол извещения системы мониторинга объектов)** – спецификация требований информационного взаимодействия в системах мониторинга объектов;

**зона охранной сигнализации (охранная зона, зона, ОЗ)** – логическое понятие; при изменении состояния шлейфа сигнализации формирует соответствующее извещение;

**идентификатор (идентификационный признак)** — номер, штрих-код, QR-код и т.п. пропуска, ПИН-код, биометрические параметры (такие как рука/палец/сетчатка/лицо и/или вес), гос. номер транспортного средства; содержится в базе данных;

**извещатель** – принятое в системах охранной и пожарной сигнализации наименование датчиков, реагирующих на различные физические воздействия: световые, электромагнитные, тепловые, механические, химические и прочие, и формирующих электрические сигналы, воспринимаемые соответствующими электронными устройствами;

**узел НЕЙРОСС (устройство НЕЙРОСС)** — специализированный функциональный контроллер, работающий под управлением программных средств интеграции и управления безопасностью НЕЙРОСС®, обеспечивающий горизонтальное (межконтроллерное) и вертикальное (с системами верхнего уровня) информационное взаимодействие в IP-сетях, и предназначенный для построения комплексной системы безопасности НЕЙРОСС;

**пропуск** — основание для разрешения доступа на территорию, на объект, в помещение, в некоторую зону или зоны доступа; содержит идентификатор (идентификационный признак);

**раздел охранной сигнализации (охранный раздел, раздел)** – логическое понятие; используется для группового мониторинга состояния охранных зон; в раздел объединяются зоны, возможно, физически подключённые к разным устройствам; разделы могут объединяться в другие разделы, формируя иерархию разделов;

**считыватель** — средство (устройство, аппаратно-программный комплекс/система), автоматически считывающее идентификационный признак; может быть составным – например, считыватель бесконтактных карт, в который встроена клавиатура;

**шлейф сигнализации (шлейф, ШС, ШОС, охранный шлейф)** – электрическая цепь питания, получения информации от извещателей и контроля их состояния.

### **Список принятых сокращений**

**АС** – переменный ток;

**DC** – постоянный ток;

**NTP (Network Time Protocol)** – сетевой протокол для синхронизации внутренних часов компьютера (контроллера);

**OASIS (Organization for the Advancement of Structured Information Standards)** — международный консорциум, разрабатывающий и внедряющий открытые стандарты электронного бизнеса и веб-сервисов;

**ONVIF (Open Network Video Interface Forum)** — международный форум и отраслевой стандарт, определяющий протоколы взаимодействия устройств IP-видеонаблюдения, СКУД и других сетевых устройств и сервисов;

**W3C (World Wide Web Consortium)** — мировой консорциум Интернет, разрабатывающий спецификации открытых стандартов информационного взаимодействия в локальных и глобальных сетях;

**ИБП** – источник бесперебойного питания;

**КЗ** – короткое замыкание;

**ПО** – программное обеспечение;

**ПЦН** – пункт централизованного наблюдения;

**СКУД** – система контроля и управления доступом;

**ОТС** – система охранной сигнализации.

# 1 ОПИСАНИЕ И РАБОТА

## 1.1 Описание и работа изделия

### 1.1.1 Назначение изделия

Изделие представляет собой IP-прибор приёмно-контрольный управления доступом и охранной сигнализации «ЯРС» (далее – «ЯРС», прибор, изделие) и предназначено для контроля и управления доступом в помещения малых, средних и крупных объектов, а также охраны зданий и сооружений от несанкционированного проникновения

Прибор может использоваться как автономно, так и в составе систем контроля и управления доступом и охранно-тревожной сигнализации.

Благодаря встроенному сетевому коммутатору, приборы «ЯРС» способны непосредственно взаимодействовать друг с другом и объединяться в единые системы СКУД/ОТС неограниченного количественного, территориального и географического масштаба; обладают способностью интегрироваться с комплексной системой безопасности ITRIUM, а также с устройствами, совместимыми со спецификациями ONVIF.

Наличие унифицированного интерфейса для подключения вторичных коммуникационных линий TP/FT-10 (LonWorks), RS-485 и RS-232 допускает гибкую функциональную конфигурацию.

Встроенный в прибор веб-сервер предоставляет единый интерфейс настройки, мониторинга и управления, который может выступать для пользователя в качестве «одного окна» доступа ко всем ресурсам системы.

При работе совместно с ИСБ ITRIUM® позволяет проводить мониторинг событий и состояний системы охранно-тревожной сигнализации, сбрасывать тревоги, выполнять постановку и снятие объектов с охраны, а также осуществлять управление пропусками и уровнями доступа из среды ITRIUM и строить отчёты.

Для передачи информации во внешние системы используется проводное Ethernet-соединение или GSM-модем (COM или USB).

По конструктивному исполнению прибор относится к многокомпонентным приборам, обладает свойством модульности и расширяемости и рассчитан на круглосуточную работу.

За счёт модулей «М2», «МДС», подключаемых по вторичной коммуникационной линии Lonworks, прибор обеспечивает:

- управление до 128 (64x2) шт. односторонними точками доступа или до 64 двусторонними, из них 2 односторонние точки доступа или одна двусторонняя на «борту» «ЯРС»;
- охранную сигнализацию до 512 (64x8) контролируемых шлейфов, из них 8 — на «борту» «ЯРС»;
- до 506 (2+63x8) управляемых реле, из них 2 – на борту «ЯРС»;
- возможность расширения существующей системы за счёт увеличения количества точек доступа и шлейфов сигнализации;

- обслуживание территориально-распределённых объектов протяжённостью до 2,7 км на один прибор (в случае использования двух экземпляров прибора — до 5,5 км (2700 + 100 + 2700 м), 100 м — максимальная протяжённость Ethernet-соединения;
- широкие возможности по настройке работы шлюзов.

Прибор поддерживает различные типы считывателей, может работать с ID-картами разных форматов, за счёт мощного процессора и большой ёмкости памяти — хранить базу данных пропусков ёмкостью свыше 300 000 записей. Прибор обеспечивает подключение считывателей, многопороговых шлейфов сигнализации и кнопок тревожно-вызывной сигнализации, управление исполнительными устройствами посредством релейных выходов и приём дискретных сигналов. В рамках подсети обеспечивается взаимное сетевое обнаружение и автоматическая синхронизация данных: пропусков, уровней и режимов доступа, данных о текущем местоположении для обеспечения контроля повторного прохода, состоянии точек доступа, зон, разделов и пр. Прибор выполняет автоматическое конфигурирование параметров LON-соединения, избавляя пользователя от необходимости использования дополнительных средств и изучения технической стороны вопроса.

## **1.1.2 Технические характеристики изделия**

### **1.1.2.1 Устойчивость к климатическим и механическим воздействиям**

По устойчивости к климатическим воздействиям изделие относится к группе исполнения С3 ГОСТ Р 52931-2008. При этом рабочий диапазон температуры окружающего воздуха равен  $-10^{\circ}\text{C} \div +50^{\circ}\text{C}$ , а верхнее значение относительной влажности равно 95% при  $+35^{\circ}\text{C}$  и более низких температурах, без конденсации влаги. В особо оговорённых при заказе случаях, изделие может быть изготовлено для рабочего диапазона температуры окружающего воздуха  $+5^{\circ}\text{C} \div +50^{\circ}\text{C}$ .

По устойчивости к механическим воздействиям изделие относится к группе исполнения L2 ГОСТ Р 52931-2008.

Прибор является пожаробезопасным при правильной установке, монтаже и техническом обслуживании.

### **1.1.2.2 Условия работы**

Изделие рассчитано на непрерывную круглосуточную работу и применяется в помещениях и/или уличных шкафах с регулируемыми климатическими условиями или в закрытых помещениях жилых и производственных зданий и сооружений.

### **1.1.2.3 Электропитание изделия**

Питание изделия осуществляется от внешних источников постоянного тока (блоков резервного питания БРП). Алгоритм работы входов питания, включая контроль наличия

питания, соответствует требованиям ГОСТ Р 53325-2009. Дополнительную информацию см. в разделе [Подключение устройства к источнику питания](#).

#### 1.1.2.4 Подключение изделия

Подключение изделия к информационной сети производится через порт Ethernet. Встроенный коммутатор Ethernet позволяет использовать последовательное подключение устройств «ЯРС» — образовывать так называемую коммутируемую IP-шину. Для этого предусмотрен второй порт Ethernet. При подключении в топологии типа «кольцо» осуществляется резервирование канала передачи данных. Также допускается подключение в произвольной топологии. Дополнительную информацию см. в разделе [Подключение к сети Ethernet](#).

Для подключения дополнительного оборудования (в том числе GSM-модема) предусмотрены интерфейсы RS-232 и USB. Для подключения модулей доступа и сигнализации предусмотрен интерфейс LonWorks.

##### **Интерфейс для связи устройств «ЯРС» между собой и с внешним оборудованием (АРМ, прочие СБТ)**

Количество интерфейсов	2
Тип интерфейса	Ethernet 10/100Base-T
Тип канала передачи	Витая пара (UTP Cat.5)

##### **Интерфейсы для работы с дополнительными внешними устройствами (модемом и проч.)**

Тип интерфейса	RS-232	USB
Количество интерфейсов	1	2

##### **Для работы с СОМ-портовым модемом дополнительно предусмотрен управляемый выход питания с защитой от КЗ**

Нагрузочная способность выхода питания	22 В при 0,4 А
Уровень ограничения тока КЗ	0,75 А

##### **Интерфейс для связи с модулями доступа и сигнализации (при установленном модуле подключения TP/FT-10)**

Количество интерфейсов	1
Тип интерфейса	ANSI / EIA – 709.1 (LonWorks)
Тип канала передачи	Витая пара (TP/FT-10)
Количество устройств в одной физической подсети	Не более 63 (1 адрес занимает сам «ЯРС»)
Топология	Шинная или произвольная

<p>Предельные длины линий связи, выполненной кабелем Belden 8471</p>	<p>Длина линии связи с шинной топологией и максимальной длиной ответвления не более 3 м: не более 2700 м;  Длина линии связи со свободной топологией между самыми удалёнными узлами (при длине линии связи между смежными узлами не более 400 м): не более 500 м.</p>
--	---

**Интерфейс для связи с внешними устройствами  
(при установленном модуле подключения RS-232)**

Тип интерфейса	RS-232
Количество интерфейсов	1

**Интерфейс для связи с внешними устройствами  
(при установленном коммуникационном модуле RS-485)**

Тип интерфейса	RS-485
Количество интерфейсов	1
Тип канала передачи	Витая пара (UTP Cat.5)

### **1.1.3 Состав и комплектация изделия**

#### **1.1.3.1 Состав изделия**

В состав прибора «ЯРС» входят следующие компоненты:

- Прибор управления доступом и охранной сигнализации сетевой «ЯРС» ТУ 4372-126-80484710-2016 (КМУР.425723.126 ТУ) - центральный прибор, состоящий из платы электроники с SD-картой памяти и корпуса;
- Сменный коммуникационный модуль TP/FT-10 Lonworks;
- Модуль доступа и охранной сигнализации «М2»;
- Модуль доступа и охранной сигнализации «МДС»;
- Сменный коммуникационный модуль подключения интерфейса RS-232;
- Сменный коммуникационный модуль подключения интерфейса RS-485.

Структурная схема системы охранно-тревожной сигнализации (СОТС) и системы контроля и управления доступом (СКУД) «ЯРС» приведена на рисунке 1.1.

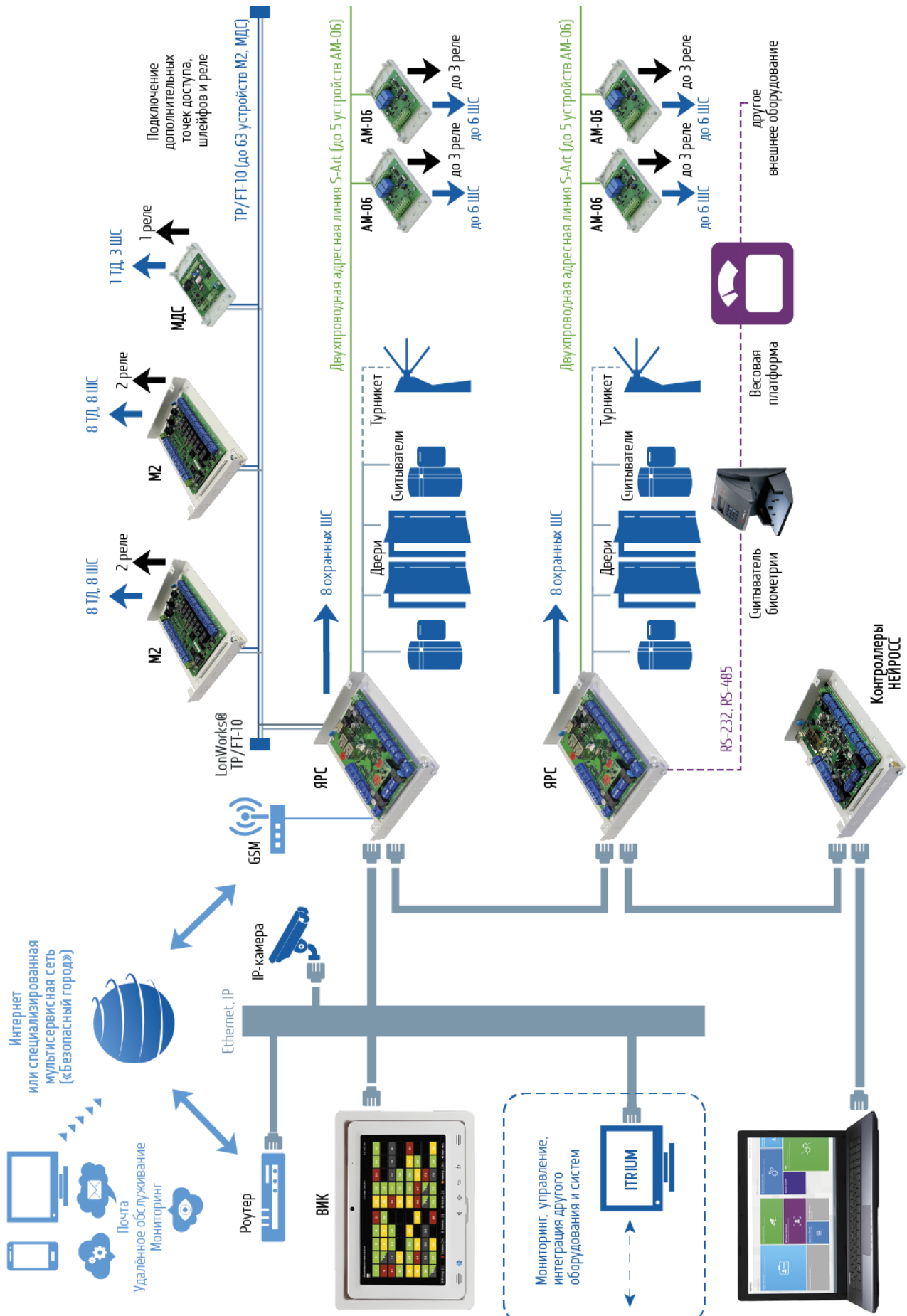


Рисунок 1.1 – Структурная схема СОТС и СКУД «ЯРС»



### 1.1.3.2 Комплектация изделия

Прибор может поставляться в любой комплектации.

### 1.1.3.3 Информация для заказа

По желанию заказчика возможна поставка произвольного количества компонентов прибора. В коде заказа количество поставляемых приборов «ЯРС», модулей «М2», «МДС» и сменных коммуникационных модулей указывается отдельно.

Поставка прибора «ЯРС» возможна в металлическом или пластиковом корпусе, а также без корпуса, возможно уличное исполнение и исполнение для использования в условиях помещения. Поэтому в записи для заказа прибора указывается код исполнения прибора в формате **П.ХХХ.УУУ** или **У.ХХХ.УУУ**. Буквенный индекс «П» обозначает исполнение для помещения (использование при температуре  $+5 \div +50$  и влажности 95% при  $35^{\circ}\text{C}$  без конденсации влаги), «У» – уличное исполнение (использование при температуре  $-40 \div +60$  и влажности 95% при  $35^{\circ}\text{C}$  без конденсации влаги). Буквенный индекс указывается перед кодом корпуса («ХХХ») и разделяется точкой. В случае необходимости поставки прибора без корпуса, вместо «ХХХ» указывается «000». «УУУ» - тип сменного коммуникационного модуля подключения интерфейса. В случае необходимости поставки прибора без сменного коммуникационного модуля, вместо «УУУ» указывается «000».

#### **Примеры записи заказа прибора «ЯРС»:**

Пример записи заказа прибора в корпусе 075 ( $+5 \div +50$ ) со сменным коммуникационным модулем подключения интерфейса Lonworks:

«Прибор управления доступом и охранной сигнализации сетевой ЯРС ТУ 4372-126-80484710-2016 (КМУР.425723.126 ТУ) исп. П.075.LON».

Пример записи заказа прибора в корпусе 041 ( $-10 \div +50$ ) со сменным коммуникационным модулем подключения интерфейса RS-232:

«Прибор управления доступом и охранной сигнализации сетевой ЯРС ТУ 4372-126-80484710-2016 (КМУР.425723.126 ТУ) исп. У.041.232».

Пример записи заказа прибора в корпусе 041 ( $-10 \div +50$ ) со сменным коммуникационным модулем подключения интерфейса RS-485:

«Прибор управления доступом и охранной сигнализации сетевой ЯРС ТУ 4372-126-80484710-2016 (КМУР.425723.126 ТУ) исп. У.041.485».

Пример записи заказа прибора без корпуса ( $+5 \div +50$ ) и без сменных модулей:

«Прибор управления доступом и охранной сигнализации сетевой ЯРС ТУ 4372-126-80484710-2016 (КМУР.425723.126 ТУ) исп. П.000.000».

### **Пример записи заказа сменных коммуникационных модулей:**

«Сменный коммуникационный модуль TP/FT-10 ТУ 4372-126-80484710-2016 (КМУР.425723.126 ТУ)»,

«Сменный коммуникационный модуль RS-232 ТУ 4372-126-80484710-2016 (КМУР.425723.126 ТУ)»,

«Сменный коммуникационный модуль RS-485 ТУ 4372-126-80484710-2016 (КМУР.425723.126 ТУ)».

Поставка модуля «М2» возможна в металлическом или пластиковом корпусе, а также без корпуса, возможно уличное исполнение и исполнение для использования в условиях помещения. Поэтому в записи для заказа модуля указывается код исполнения прибора в формате **П.ХХХ** или **У.ХХХ**. Буквенный индекс «П» обозначает исполнение для помещения (использование при температуре +5 ÷ +50 и влажности 95% при 35°С без конденсации влаги), «У» – уличное исполнение (использование при температуре –40 ÷ +60 и влажности 95% при 35°С без конденсации влаги). Буквенный индекс указывается перед кодом корпуса («ХХХ») и разделяется точкой.

### **Пример записи заказа модуля доступа и сигнализации «М2»:**

Пример записи заказа модуля «М2» в корпусе 075 (+5 ÷ +50):

«Модуль доступа и охранной сигнализации М2 ТУ 4372-131-35521209-2017 (КМУР.425723.131 ТУ) исп. П.075»

Пример записи заказа модуля доступа и сигнализации «М2» в корпусе 041 (-40 ÷ +60):

«Модуль доступа и охранной сигнализации М2 ТУ 4372-131-35521209-2017 (КМУР.425723.131 ТУ) исп. У.041»

### **Пример записи заказа модуля доступа и сигнализации «МДС»:**

«Модуль доступа и охранной сигнализации МДС ТУ 4372-132-35521209-2017 (КМУР.425723.132 ТУ)».

#### **1.1.3.4 Устройство и работа изделия**

Прибор предназначен для построения системы контроля и управления доступом и охранной сигнализации и выполняет следующие функции:

- Контролирует состояние входа неисправности блока резервного питания и датчика вскрытия корпуса;
- Посредством сменных коммуникационных модулей предоставляет интерфейсы TP/FT-10 (Lonworks), RS-232, RS-485;

- Контролирует физическое состояние собственных шлейфов охранной сигнализации, а также шлейфов модулей «М2» и «МДС» посредством интерфейса TP/FT-10 (Lonworks), формирует состояние охранных зон, позволяет объединить несколько зон в разделы и отображать состояния разделов. Контролирует состояние точек доступа, дверных контактов, замков и считывателей, в том числе — модулей «М2» и «МДС». При изменении контролируемых параметров формирует соответствующие извещения;
- Обеспечивает ручное и автоматическое управление точками доступа и реле, постановку и снятие разделов и зон с охраны;
- Ведёт журналирование событий в энергонезависимой памяти;
- Предоставляет пользовательский интерфейс конфигурирования, мониторинга и управления посредством веб-браузера;
- Обеспечивает передачу извещений о событиях по сети Ethernet или с помощью модемного соединения;
- Обеспечивает синхронизацию данных с другими узлами сети, в том числе с другими приборами «ЯРС»;
- Обеспечивает взаимодействие с программным обеспечением интегрированных систем безопасности ITRIUM®.

В части контроля доступа прибор обеспечивает:

- Управление двумя односторонними или одной двусторонней точкой доступа, а также точками доступа модулей «М2» и «МДС»;
- Идентификацию по карте, по карте или пин-коду, по карте и пинкоду, по биометрическим параметрам;
- Автоматическую блокировку/разблокировку точки доступа при возникновении тревоги в разделе охранной сигнализации или при постановке/снятии с охраны разделов;
- Управление реле при возникновении тревоги охранной сигнализации (с настраиваемыми режимами работы реле);
- Контроль прохода под принуждением;
- Контроль повторного прохода (antipassbak);
- Проход по правилу N-лиц.

Прибор является самодостаточным и может работать при условии отсутствия связи с другими устройствами сети: проводить мониторинг состояний и управление охранными зонами и точками доступа.

При подключении к сети способен обеспечивать взаимную синхронизацию данных с другими узлами сети НЕЙРОСС, причём синхронизация инициируется контроллером, на котором произошли изменения: контроллер формирует сетевые запросы ко всем смежным

узлам сети с информацией о времени и характере изменения. Другие узлы сети получают этот запрос и обновляют собственные данные. Если в момент обновления связь с каким-либо узлом была прервана, при восстановлении связи «потерянный» узел сам инициирует запросы на получение информации об изменениях.

### **Состояния зон и разделов охранной сигнализации**

На основе физического состояния шлейфов, состояния связи с «М2» и «МДС», а также состояния охраны, зоне присваивается одно из следующих состояний:

- [Снято с охраны, норма],
- [На охране],
- [Тревога],
- [Невзятие],
- [Обрыв шлейфа],
- [Короткое замыкание],
- [Неисправность],
- [Потеря связи].

Состояние [Тревога] имеет наивысший приоритет; может фиксироваться до ручного сброса тревоги.

Все состояния неисправности ([Обрыв шлейфа], [Короткое замыкание], [Неисправность]), имеют второй по значимости приоритет; сбрасываются автоматически при устранении причины. Если в настройках зоны отключён контроль неисправности, то состояния [Обрыв шлейфа] и [Короткое замыкание] не формируются.

Состояние [Невзятие] является промежуточным, при устранении причины возникновения тревоги переходит в состояние [На охране].

Состояние [Потеря связи] формируется для зон шлейфов модулей «М2», «МДС» при потере с ними связи.

Подробнее о состояниях охранных зон см. в разделе [Состояния охранных зон](#).

Охранные зоны логически объединяются в разделы. В каждый раздел могут входить зоны, физически подключённые к различным контроллерам «НЕЙРОСС», адресным расширителям «АМ-06» и модулям «М2», «МДС». Каждой зоне присваивается номер (целое число). На основе состояний зон раздела формируется состояние самого раздела. Предусмотрены следующие состояния:

- [Снято с охраны],
- [На охране],
- [Частично на охране],

- [Тревога],
- [Неисправность].

Состояние [Тревога] имеет наивысший приоритет; формируется, если хотя бы одна зона раздела находится в тревожном состоянии. Состояние [Неисправности] имеет второй по значимости приоритет; формируется, если хотя бы одна зона раздела находится в одном из состояний [Обрыв шлейфа], [Короткое замыкание], [Неисправность], [Потеря связи]. Состояние [Частично на охране] формируется, если хотя бы одна зона раздела находится в состоянии [Невзятие], а остальные зоны находятся в нормальном состоянии.

Подробнее о состояниях разделов см. в разделе [Состояния разделов охранной сигнализации](#).

### **Состояния точек доступа**

Состояния точек доступа формируются независимо друг от друга. Предусмотрены следующие состояния:

- [Ожидание идентификации],
- [Проход разрешён, ожидание прохода],
- [Взлом двери],
- [Удержание двери],
- [Заблокирована],
- [Разблокирована] (свободный проход),
- [Отказано в доступе].

Состояния [Заблокирована] и [Разблокирована] инициируются пользователем автоматически (при тревоге в заданной зоне) или вручную. Состояния [Взлом двери] и [Удержание двери] формируются в зависимости от состояния дверного контакта и этапа совершения прохода. Другие состояния формируются в зависимости от состояния считывателя.

Подробнее о состояниях точек доступа см. в разделе [Состояния точек доступа](#).

#### **1.1.3.5 Маркировка и пломбирование**

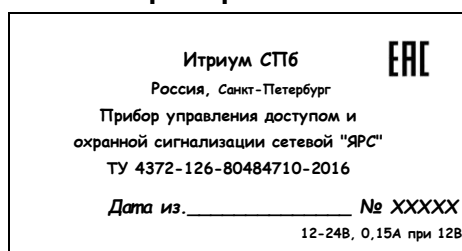
Маркировка устройств в составе прибора соответствует конструкторской документации. Маркировка потребительской и транспортной тары соответствует требованиям ГОСТ 14192-96.

На корпусе устройства указаны:

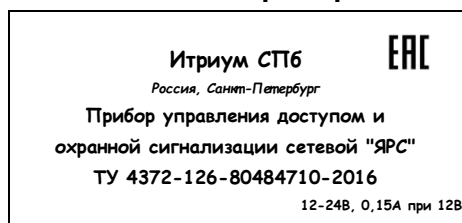
- Наименование и местонахождение (город) предприятия-изготовителя;
- Наименование или условное обозначение устройства;
- ТУ на изготовление устройства.

Пример маркировки:

### Прибор «ЯРС»



### Упаковка прибора



#### 1.1.4 Упаковка прибора

Упаковка прибора, технической и товарно-сопроводительной документации соответствует требованиям ГОСТ 26828-86 и производится в потребительскую тару — картонную коробку. В каждую коробку вложен паспорт на изделие.

## 1.2 Описание и работа составных частей изделия

### 1.2.1 Описание и работа контроллера «ЯРС»

#### 1.2.1.1 Общие сведения о контроллере «ЯРС»

Контроллер «ЯРС» является основным устройством прибора. Это полностью автономное устройство, которое может использоваться для обеспечения работоспособности двух односторонних точек доступа или одной двусторонней, а также контролировать восемь шлейфов охранной сигнализации, подключаемых непосредственно плате контроллера. При использовании модуля подключения TP/FT-10 способен контролировать до 63 модулей «М2» (две точки доступа, 8 шлейфов сигнализации и 10 реле на один модуль). На основе данных пропусков, пин-кодов и уровней доступа, хранящихся в базе данных, контроллер самостоятельно принимает решение о разрешении доступа. Ёмкость базы данных пропусков позволяет хранить свыше 100 тысяч записей.

Контроллер предоставляет интерфейс прямого подключения нескольких устройств между собой посредством Ethernet-соединения, предоставляет единый веб-интерфейс для конфигурирования, мониторинга состояний и управления другими устройствами в рамках IP-сети.

Контроллер способен обеспечивать взаимную синхронизацию данных с другими узлами сети НЕЙРОСС, в том числе данных пропусков и уровней доступа, состояний точек доступа, зон и разделов охранной сигнализации, а также обеспечивает управление световыми и звуковыми индикаторами считывателей.

Контроллер может использоваться в температурном диапазоне от  $-10$  до  $+50$  °С, и предназначен для установки как в помещении, так и на улице, и рассчитан на круглосуточный режим работы.

#### 1.2.1.2 Описание контроллера «ЯРС»

##### 1.2.1.2.1 Технические характеристики изделия

**Сетевые интерфейсы: Линия подключения к сети НЕЙРОСС и прочим СВТ**

Количество интерфейсов	2
Тип интерфейса	Ethernet 10/100Base-T
Тип канала передачи	Витая пара (UTP Cat.5)

**Дополнительные интерфейсы**

**Линии подключения COM- или USB-модема и других устройств**

Тип интерфейса	RS-232*	USB тип «А»
Количество интерфейсов	2	2
Тип канала передачи	Витая пара (UTP Cat.5)	–

\* Для работы с COM-портовым модемом дополнительно предусмотрен управляемый выход питания с защитой от КЗ

### Подключение карты памяти

Тип интерфейса	SD mini
Количество интерфейсов	1

### Шлейфы сигнализации

Тип шлейфа, количество	Многopороговый резистивный: 8
Номинальные сопротивления резисторов шлейфов сигнализации	$3\pm 5\%$ кОм и $510\pm 5\%$ Ом, 0,125 Вт

### Устройства идентификации

Количество интерфейсов	2
Тип устройства идентификации	Считыватель радиочастотных карт или идентификаторов Touch Memory
Тип интерфейса	Wiegand/1-Wire

### Дополнительные входы

Назначение	Дискретный вход сигнала неисправности внешнего источника питания	Дискретный вход сигнала неисправности аккумулятора
Тип сигнала	«Сухой контакт» или оптронный ключ	
Количество	1	1

### Выходы управления

Тип выходов	Контакты электромеханических реле	
Количество выходов	2	
Номинальный коммутируемый ток, А	Переменный ток (при 125 В)	Постоянный ток (при 30 В)
	1	2
Максимальное коммутируемое напряжение, В	Переменный ток	Постоянный ток
	250	220
Количество контактных групп каждого реле (О, НР, НЗ)	1	

### Органы индикации

Тип индикаторов	Индикаторы световые светодиодные
Количество индикаторов	3: Питание (красный), Работа (зелёный), Коммуникация с сопроцессором (зеленый)

### Питание

Напряжение питания, В	12 ÷ 24 постоянный ток
Ток потребления (не более), А	0,4 при напряжении 12 В 0,2 при напряжении 24 В
Количество входов питания	1

### Дополнительные выходы питания

Назначение	Питание считывателей	Питание COM-модема
Напряжение питания, В	9	12 ÷ 24 (входное питание)



Ток потребления (не более), А	0,5 (суммарно)	0,7
Количество выходов питания	2	1

#### Параметры корпуса

Код исполнения корпуса	Степень защиты корпуса	Габаритные размеры (ДхШхВ), мм	Масса прибора в корпусе (не более), кг
075	IP22	200x150x35	1,05
041	IP65	222x146x55	1,15
000	–	165x110x30	0,35

#### Код исполнения

Код исполнения	Т °С	Относительная влажность (верхний предел)
П.ХХХ*	+5 ÷ +50	95% при 35 °С, без конденсации влаги
У.ХХХ*	-50 ÷ +50	95% при 35 °С, без конденсации влаги

\* ХХХ – код корпуса. В случае, если устройство поставляется без корпуса, на месте «ХХХ» записывается «000».

#### 1.2.1.2.2 Описание состояний индикаторов

На плате устройства предусмотрено три световых индикатора для индикации наличия питания устройства, контроля его работоспособности и состояния коммуникации с сопроцессором.

Таблица 1.1

Световой индикатор, цвет, обозначение на плате	Работа
<b>ПИТАНИЕ</b> , красный, <b>PW</b>	<b>Включен:</b> система питания в норме. <b>Выключен:</b> нет питания или проблема в системе питания.
<b>РАБОТА</b> , зелёный, <b>АСТ</b>	<b>Включен:</b> устройство не работает/зависло. <b>Мигает с частотой 0.5 Гц:</b> Загрузка ядра и прикладного приложения успешно завершена. Устройство работает. <b>Выключен:</b> устройство не работает/зависло.
<b>Состояние коммуникации с сопроцессором</b> , зелёный, <b>VD32</b>	<b>Светится прерывисто:</b> коммуникационный обмен между основным процессором и сопроцессором в нормальном состоянии. Любой другой режим работы означает неисправность коммуникации.

#### 1.2.1.2.3 Питание изделия

На плате устройства предусмотрен один вход для подключения источника питания постоянного тока 12 – 24 В ± 10%.

Напряжение питания постоянного тока	10,8 – 28 В
Максимальный потребляемый ток	200 мА (при напряжении 12 В) 400 мА (при напряжении 24 В)

В качестве источника питания рекомендуется применять блок резервного питания БРП-12 «ЯСЕНЬ» ТУ 4372-020-59497651-2008.

#### 1.2.1.2.4 Шлейфы сигнализации

##### Радиальные шлейфы

На плате «ЯРС» предусмотрены входы для подключения восьми двухпроводных радиальных шлейфов; тип «многопороговый резистивный». Питание каждого осуществляется постоянным током 0,5 мА.

Физические состояния контролируемой цепи:

- [Норма],
- [Тревога],
- [Короткое замыкание],
- [Обрыв].

Диаграмма порогов состояний при контроле цепи нагрузки приведена на рисунке 1.2 (в скобках указаны значения АЦП с учётом 15% температурного дрейфа источника тока в промышленном диапазоне  $-40 \div +70^{\circ}\text{C}$ ).

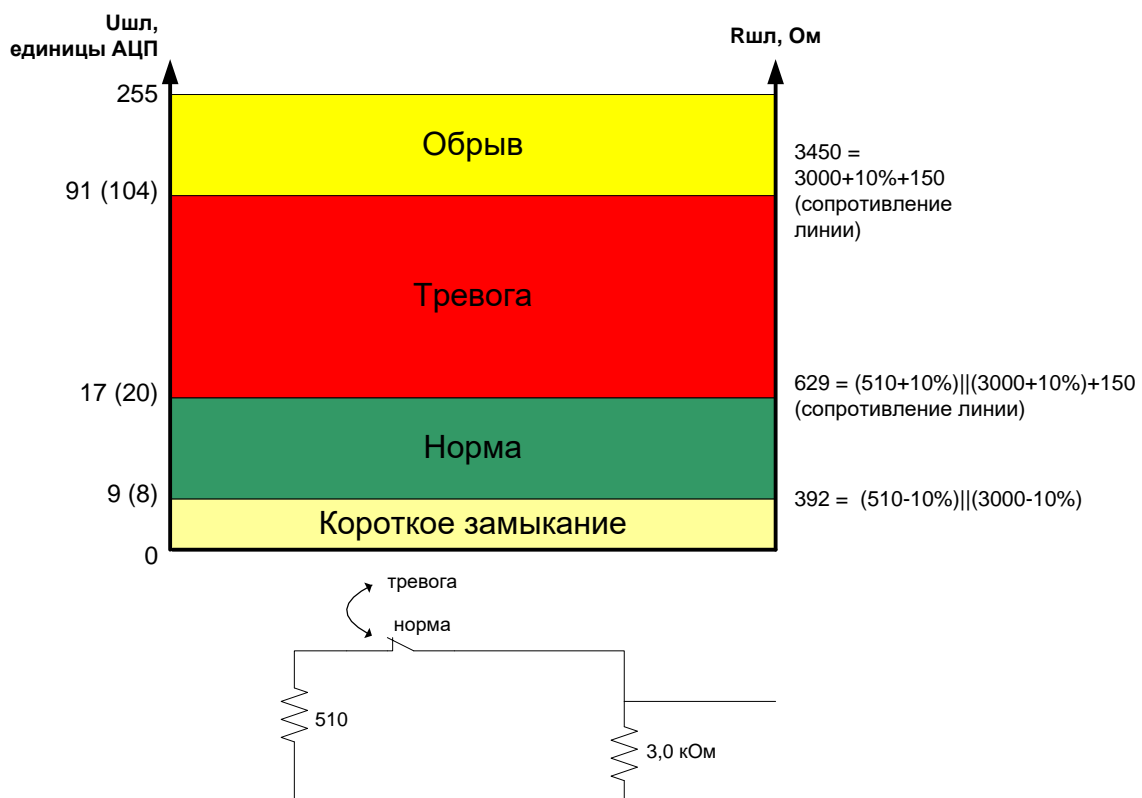


Рисунок 1.2 — Диаграмма порогов состояний при контроле цепи нагрузки

Предусмотрена работа в режиме «сухого контакта» (без контроля неисправности). При этом в качестве порогов состояний «замкнуто» ([Норма]) и «разомкнуто» ([Тревога]) используются границы состояний [Короткое замыкание] + [Норма] и [Тревога] + [Обрыв] соответственно. Диаграмма приведена на рисунке 1.3.

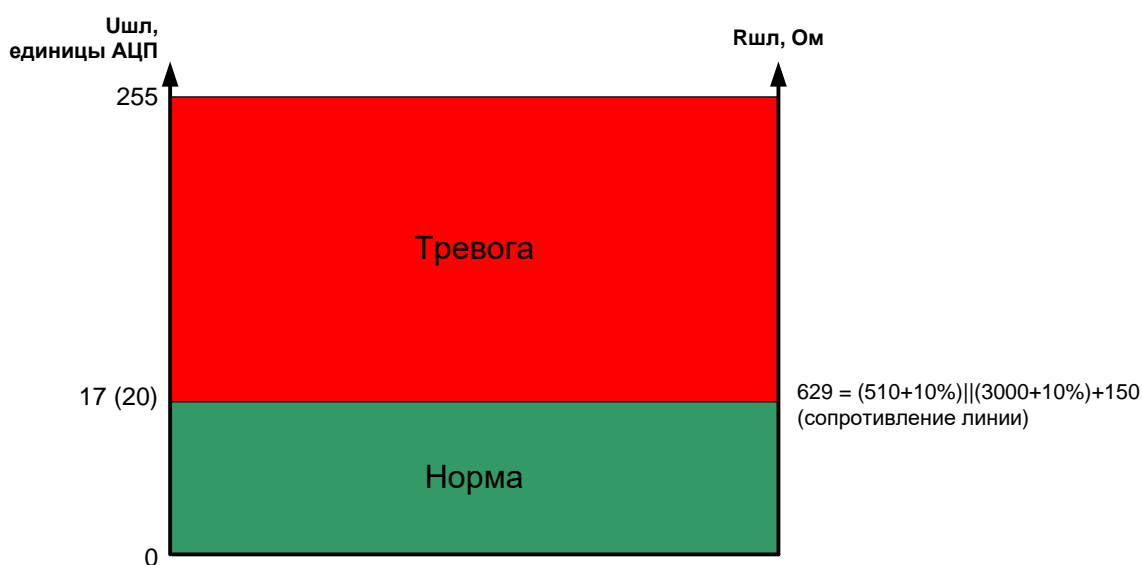


Рисунок 1.3 — Диаграмма порогов состояний без контроля цепи нагрузки

#### 1.2.1.2.5 Дополнительные входы

Дискретный вход «Неисправность ИП» (PF, DI1). Вход предназначен для приёма сигнала о неисправности внешнего источника питания. Данный вход используется в случае, когда питание устройства осуществляется от бесперебойного источника питания, который самостоятельно выполняет функции контроля исправности первичного источника питания и формирования дискретного сигнала о возникшей неисправности в виде замыкания контактов механического или оптореле.

Дискретный вход «Неисправность аккумулятора» (AF, DI2). Вход предназначен для приёма сигнала о неисправности аккумулятора источника питания. Данный вход используется в случае, когда питание устройства осуществляется от бесперебойного источника питания, который самостоятельно выполняет функции контроля исправности аккумулятора и формирования дискретного сигнала о возникшей неисправности в виде замыкания контактов механического или оптореле.

#### 1.2.1.2.6 Выходы управления

На плате устройства предусмотрено 2 релейных выхода для управления замковыми устройствами.

### 1.2.1.2.7 Конструкция изделия

Прибор представляет собой конструктивно законченное изделие, состоящее из платы электроники и корпуса из металла или пластика.

Пластиковый корпус имеет степень защиты IP65. Он состоит из основания и крышки. Крышка фиксируется в закрытом состоянии при помощи винтов. Основание корпуса оснащено отверстиями для крепления к стене. Внутри корпуса закреплена металлическая пластина, на которую при помощи стоек устанавливается плата электроники. Для подвода проводов предусмотрены гермовводы (6 штук).

Металлический корпус имеет степень защиты IP21. Он также состоит из основания и крышки, закрепляемой винтами. В основании расположено отверстие, предназначенное для ввода проводов при подключении прибора.

Габаритные и установочные размеры платы и корпусов приведены в разделе [Габаритные и установочные размеры изделия](#).

На плате прибора расположена кнопка **MODE**, используемая для сброса настроек прибора, и кольцевой выключатель с подпружиненным плунжером, используемый в качестве датчика вскрытия корпуса (тампера). Также на плате расположены винтовые колодки для подключения интерфейсов RS-232, питания, винтовые колодки дополнительных дискретных входов. Для подключения по интерфейсу Ethernet 10/100Base-T предусмотрены два разъёма; для подключения по интерфейсу USB – разъем типа «А». Также на плате электроники расположен разъем для подключения microSD Card и разъем для подключения сменных коммуникационных модулей.

Внешний вид платы электроники контроллера «ЯРС» представлен на рисунке 1.4.

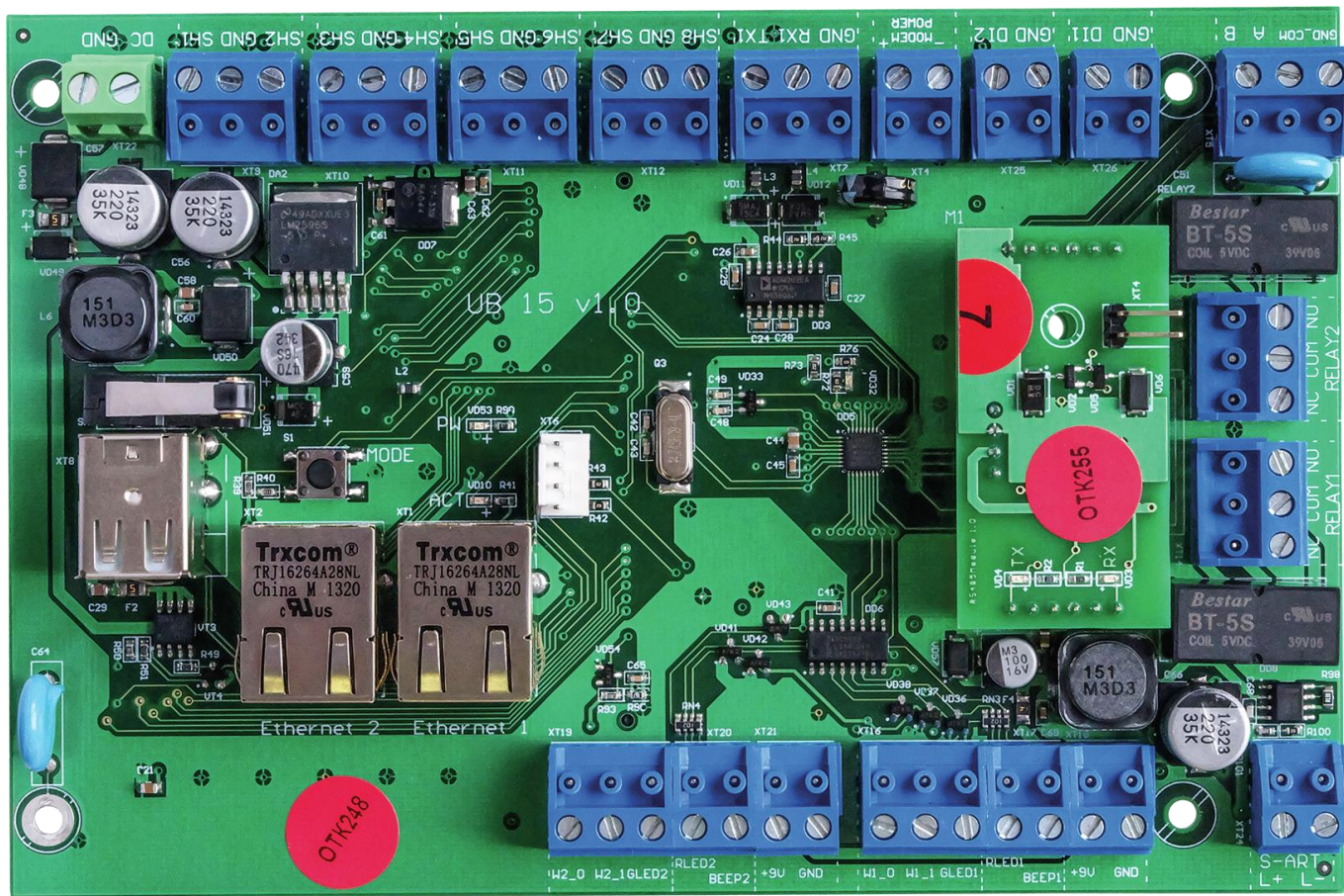


Рисунок 1.4 – Плата электроники контроллера «ЯРС». Внешний вид

Расположение разъемов платы представлено на рисунке 1.5. Описание разъемов представлено в разделе [Разъемы платы электроники](#).

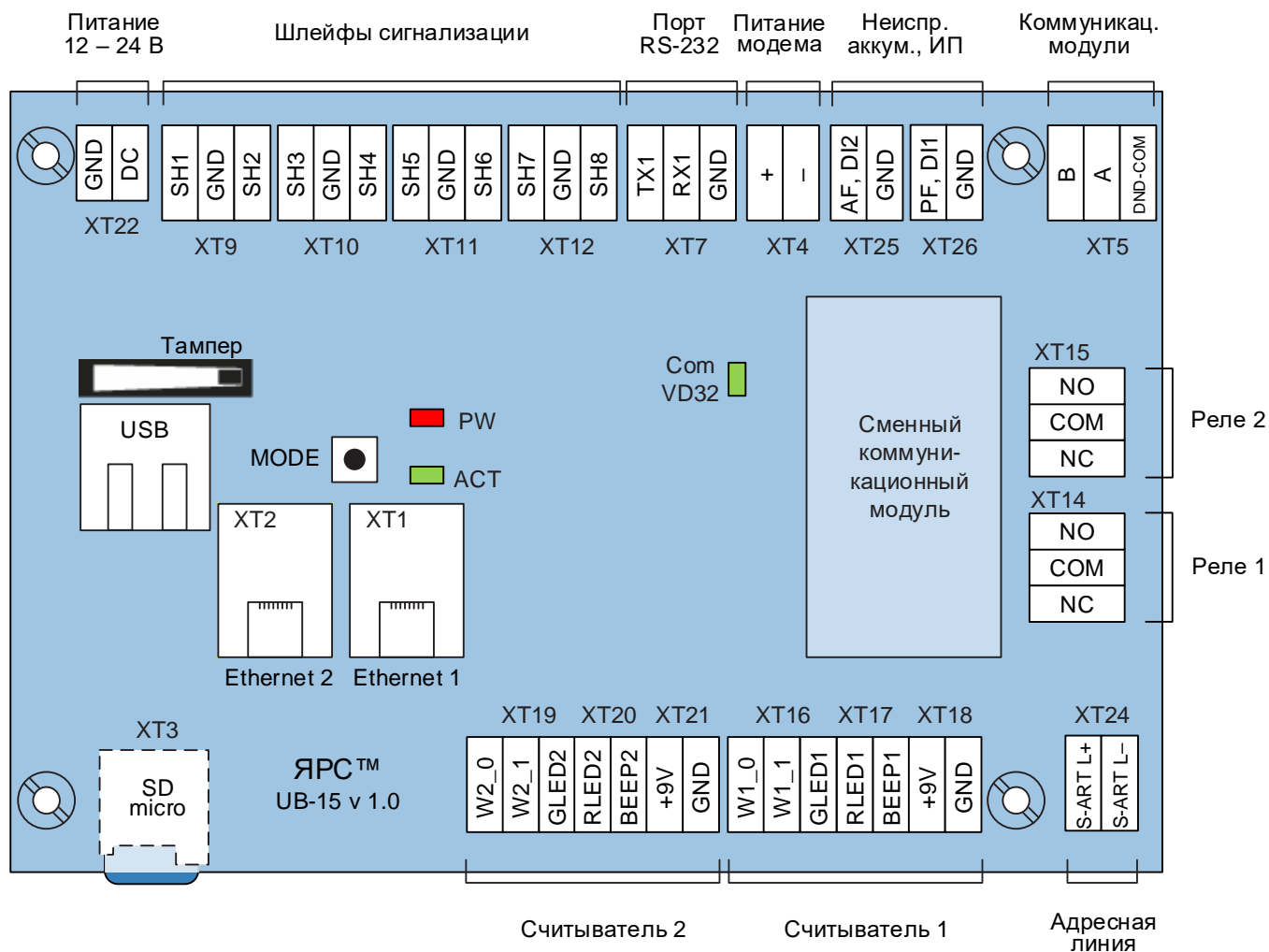


Рисунок 1.5 – Плата электроники контроллера «ЯРС». Схема расположения разъёмов

### 1.2.1.2.8 Режимы индикации считывателей

Контроллер «ЯРС», а также модули «М2» и «МДС» осуществляют управление индикаторами подключенных к ним считывателей. Тип индикаторов и их количество указано в таблице 1.2. Режимы индикации перечислены в таблице 1.3.

Таблица 1.2 – Индикаторы считывателей

Тип индикатора	Количество
Индикатор световой (светодиодный)	2 (цвет красный и цвет зелёный)
Индикатор звуковой (бипер)	1

Таблица 1.3 – Режимы индикации

Фаза	Состояние точки доступа/раздела сигнализации*	Режимы работы индикаторов		
		Красный световой индикатор	Зелёный световой индикатор	Звуковой индикатор
1	Ожидание идентификации	Мигает с частотой 1 Гц	Выключен	Выключен

Фаза	Состояние точки доступа/раздела сигнализации*	Режимы работы индикаторов		
		Красный световой индикатор	Зелёный световой индикатор	Звуковой индикатор
2 – 3	Проход разрешён, ожидание прохода; Проход	Выключен	Включён на время ожидания открытия двери (ЯРС) Мигает с частотой 1 Гц (М2, МДС);	Выключен
4	Взлом двери	Включён	Выключен	Включён
5	Удержание двери	Включён	Выключен	Включён
6	Заблокировано	Включён	Выключен	Выключен
7	Разблокировано: свободный проход	Выключен	Включён	Выключен
8	Заблокировано: взлом	Включён	Выключен	Включён
9	Отключено	Включён	Выключен	Выключен
10	Отказано в доступе	Включён в течение 3 с	Выключен	Включён в течение 3 с
12	Ожидание идентификации последующих лиц при проходе по правилу N-лиц	Мигает с частотой 2 Гц (0,5 с)	Мигает с частотой 2 Гц (0,5 с)	Выключен
13	Ожидания подтверждения от оператора	Выключен	Мигает с частотой 2 Гц (0,5 с)	Выключен
14	Подготовка к постановке на охрану	Выключен	Мигает с частотой 4 Гц (0,25 с)	Выключен
15	Взятие на охрану	Мигает с частотой 2 Гц (0,5 с) в течение 3 с	Выключен	Выключен
16	Невзятие на охрану	Включён в течение 3 с	Выключен	Включён в течение 3 с
17	На охране, Норма (аналогично 6. Заблокировано)	Включён	Выключен	Выключен
18	На охране, Тревога	Мигает неравномерно. Включается на 1,25 с через 0,25 с	Выключен	Выключен
19	Снятие с охраны	Выключен	Мигает с частотой 4 Гц (0,25 с) в течение 3 с	Выключен

Фаза	Состояние точки доступа/раздела сигнализации*	Режимы работы индикаторов		
		Красный световой индикатор	Зелёный световой индикатор	Звуковой индикатор
20	Невозможность снятия (есть зона в режиме <b>Контроль 24 часа</b> )	Включён в течение 3 с	Выключен	Выключен

\* Описание состояний представлены в разделах [Состояния точек доступа](#), [Состояния разделов охранной сигнализации](#), [Смена состояний зон и разделов при постановке на охрану](#).

Фазы 14-20 относятся к управлению разделами охранной сигнализации с помощью считывателя. Дополнительную информацию см. в разделе [Управление разделами с помощью считывателя](#).

### 1.2.1.3 Взаимодействие с внешним оборудованием

#### 1.2.1.3.1 Взаимодействие с Handkey-II

Прибор приёмно-контрольного управления доступом и охранной сигнализации «ЯРС» в версии «М» может использоваться для организации точек доступа, оснащённых биометрическими сканерами геометрии руки HANDKEY II.

Биометрические сканеры геометрии кисти руки HANDKEY II производства компании Recognition Systems выделяются среди прочих биометрических систем по следующим показателям:

- Минимальными ошибками первого и второго рода;
- Минимальным размером файла биометрических данных;
- Невозможностью компрометирования носителя фиксируемого биометрического признака.

Взаимодействие HANDKEY II с контроллерами «ЯРС» расширяет возможности как КСБ НЕЙРОСС, так и самих сканеров:

- Благодаря хранению данных в контроллере «ЯРС», биометрическая база данных становится практически неограниченной;
- База данных владельцев карт СКУД НЕЙРОСС расширяется биометрическими данными;
- HANDKEY II «в связке» с «ЯРС» может использоваться без дополнительного «внешнего» ПО.

Сканер HANDKEY II подключается к прибору «ЯРС» посредством сменных коммуникационных модулей подключения RS-232/RS-485, через порт RS-232 или включается в общую с прибором «ЯРС» локальную сеть Ethernet.

Все данные владельца пропуска (в том числе биометрические) хранятся в базе данных прибора «ЯРС». Первоначальная запись шаблона геометрии руки реализуется с помощью трёхразового сканирования кисти руки сотрудника и усреднения полученной



информации в бюро пропусков ITRIUM. В дальнейшем пропуска ITRIUM загружаются в «ЯРС», и идентификация проводится автономно.

Порядок идентификации:

1. Владелец пропуска предъявляет карту считывателю, подключённому к контроллеру. По карте из базы данных «ЯРС» вычитывается биометрический шаблон владельца и передаётся в HANDKEY II;
2. Владелец кладёт кисть руки на панель сканера. В случае успешной аутентификации (сравнение геометрии руки владельца с биометрическим шаблоном), HANDKEY II отправляет данные в «ЯРС», который разрешает проход или отказывает в доступе.

Биометрический контроль доступа на основе HANDKEY II может также применяться для автоматизации шлюзовых кабин и тамбур-шлюзов.

## **1.2.2 Описание и работа коммуникационных модулей**

### **1.2.2.1 Общие сведения о коммуникационных модулях**

Наличие унифицированного интерфейса для подключения вторичных коммуникационных линий TP/FT-10 (LonWorks), RS-485 и RS-232 допускает гибкую функциональную конфигурацию и позволяет реализовать дополнительные решения:

- Контроллер шлюзовых кабин и агрегированных тамбур-шлюзов;
- Узел интеграции биометрических и других сторонних систем.

Модуль подключения TP/FT-10 (NeuronModule) предоставляет интерфейс Lonworks для подключения модулей M2 и MDC (всего до 63 модулей), что позволяет расширить систему на базе одного устройства «ЯРС»: до 500 датчиков (извещателей, шлейфов), исполнительных устройств или до 120 точек доступа. Для настройки точек доступа, шлейфов и реле специальные средства конфигурирования сетей Lonworks не требуются. Настройка и управление осуществляется посредством веб-интерфейса устройства или ПО ИСБ ITRIUM®.

Модуль подключения RS-232 (RS232Module) предоставляет гальваноизолированный интерфейс RS-232, который может быть использован для подключения внешних систем контроля и управления доступом, охранно-пожарной сигнализации. В этом случае устройство «ЯРС» может выступать в качестве узла интеграции этих систем.

Модуль подключения RS-485 (RS485Module) предоставляет гальваноизолированный полудуплексный интерфейс RS-485 для подключения биометрических систем и другого внешнего оборудования.

### **1.2.2.2 Конструкция коммуникационных модулей**

Конструктивно коммуникационные модули представляют собой мезонинную плату, подключаемую параллельно плате прибора «ЯРС» с помощью двух разъёмов по 6

контактов в каждом. Одновременно может быть подключено не более одного коммуникационного модуля.

Внешний вид модуля подключения TP/FT-10 (NeuronModule) приведён на рисунке 1.6. Внешний вид модулей подключения RS-232 (RS232Module) и RS-485 (RS485Module) идентичен и приведён на рисунке 1.7.

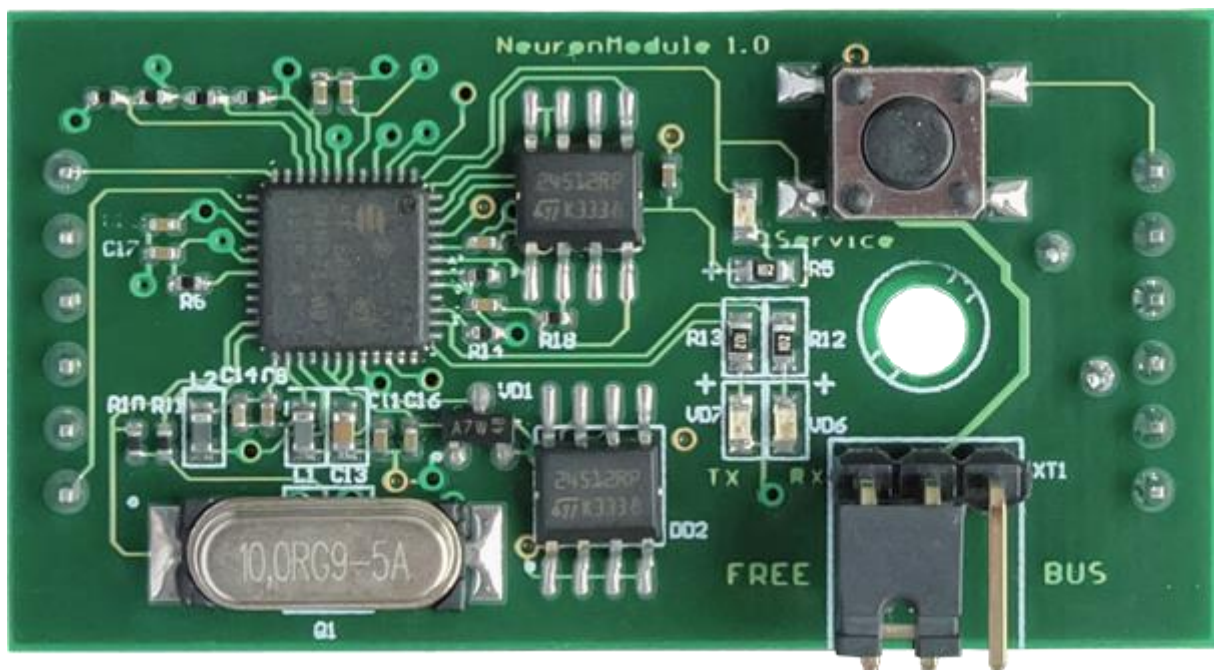


Рисунок 1.6 — Внешний вид мезонинной платы подключения интерфейса TP/FT-10

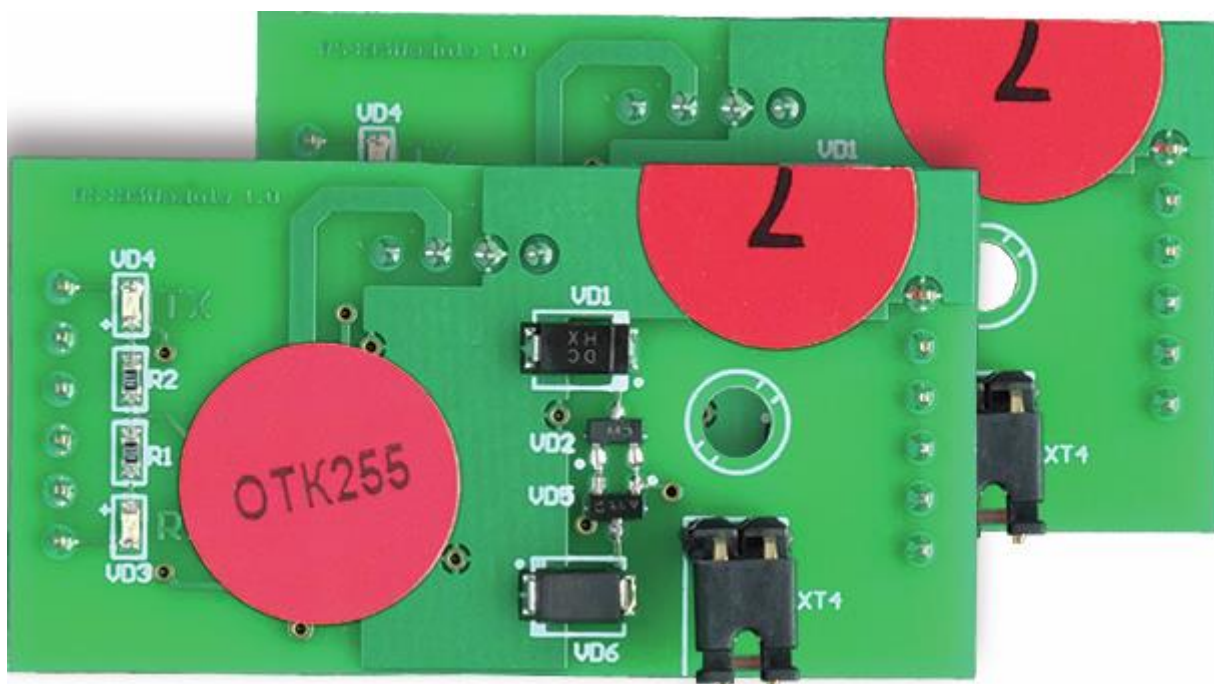


Рисунок 1.7 — Внешний вид мезонинных плат подключения интерфейсов RS-232/RS-485

### 1.2.3 Описание и работа модуля «М2»

#### 1.2.3.1 Общие сведения о модуле «М2»

Модуль доступа и охранной сигнализации «М2» предназначен для использования в качестве прибора приёмно-контрольного в системах управления доступом и охранно-тревожной сигнализации малых, средних и крупных объектов.

Модуль подключается к прибору «ЯРС» посредством двухпроводной линии LonWorks и расширяет количество точек доступа, шлейфов сигнализации и реле, управляемых прибором «ЯРС». Модуль обеспечивает управление двумя односторонними или одной двусторонней точкой доступа, восемью шлейфами сигнализации и восемью реле. К одному «ЯРС» может быть подключено до 63 модулей «М2».

Встроенная согласующая нагрузка с возможностью выбора используемой топологии сети Lonworks упрощает монтаж прибора. Переключатель питания считывателей позволяет расширить диапазон поддерживаемых типов ридеров.

Настройка модуля осуществляется посредством веб-интерфейса, предоставляемого прибором «ЯРС»; средства конфигурирования LonWorks-сетей не требуются.

В штатном режиме требуется наличие постоянной связи с «ЯРС», на котором хранится полная база данных. Поведение модуля в случае аварийного разрыва связи с «ЯРС», настраивается. Модуль «М2» может работать в режиме запрета доступа, либо использовать локальный энергонезависимый буфер, в котором хранятся данные последних 1200 предъявленных валидных карт: до восстановления связи с головным контроллером, доступ по всем картам из буфера будет разрешён.

Модуль рассчитан на круглосуточную работу. Питание модуля осуществляется от внешних источников постоянного тока (блоков резервного питания).

#### 1.2.3.2 Описание модуля «М2»

##### 1.2.3.2.1 Технические характеристики изделия

**Сетевые интерфейсы:** для связи с «ЯРС», другими модулями «М2» и «МДС»

Количество интерфейсов	1
Тип интерфейса	ANSI / EIA – 709.1 (LonWorks)
Тип канала передачи	Витая пара (TP/FT-10)

##### Шлейфы сигнализации

Количество шлейфов	8 (2 шлейфа также используются в качестве датчиков состояния дверей — дверных контактов)
Тип ШС	Многопороговый резистивный
Количество проводников в ШС	2
Номинальное значение сопротивлений резисторов ШС	3±5% кОм и 510±5% кОм, 0,125 Вт

Определяемые прибором состояния с двумя установленными оконечными резисторами	«Норма», «Тревога», «Обрыв», «Короткое замыкание»
Тип выходного сигнала извещателя, подключаемого к оконечному элементу ШС	«сухой контакт»

### Устройства идентификации

Количество интерфейсов	2
Тип устройства идентификации	Считыватель радиочастотных карт или идентификаторов Touch Memory
Тип интерфейса	Wiegand (до 64 бит)

Режимы индикации считывателей «ЯРС» и «М2» сходны и приведены в разделе [Режимы индикации считывателей](#).

### Дополнительные входы

Назначение	Количество, тип
Управление замком посредством кнопки выхода при одностороннем контроле прохода	2, кнопка открытия двери
Получение сигнала о неисправности источника питания	1, сухой контакт или оптронный ключ

### Выходы управления

Тип выходов	Контакты электромеханических реле		Оптореле
	Переменный ток	Постоянный ток	
Количество выходов	2		8
Тип контактной группы реле	Переключение		Нормально-разомкнутые
Максимальный коммутируемый ток, А	Переменный ток (при 125 В)	Постоянный ток (при 30 В)	0,1
	1	2	
Максимальное сопротивление контакта включённого реле, Ом	–		25
Максимальное коммутируемое напряжение, В	Переменный ток	Постоянный ток	250
	250	230	
Количество контактных групп каждого реле (О, НР, НЗ)	1		-

### Органы индикации

Тип индикаторов	Индикаторы световые светодиодные
Количество индикаторов	5 (служебные)

### Питание модуля

Напряжение питания, В	10,8 – 28 постоянный ток
Ток потребления (не более), А	0,2 при напряжении 12 В
Количество входов питания	1

### Дополнительные выходы питания

Назначение выходов	Питание считывателей
Напряжение питания, В	9/входное питание — тип питания задаётся установкой перемычки
Ток потребления (не более), А	0,35/0,75
Количество выходов питания	2

### Параметры корпуса

Код исполнения корпуса	Степень защиты корпуса	Габаритные размеры (ДхШхВ), мм	Масса прибора в корпусе (не более), кг
075	IP22	200x150x35	1
041	IP65	222x146x55	1,15
000	—	165x11x0x30	0,35

#### 1.2.3.2.2 Шлейфы сигнализации

На плате «М2» предусмотрены входы для подключения восьми двухпроводных радиальных шлейфов, тип «многопороговый резистивный». Питание каждого осуществляется постоянным током 0,5 мА.

Физические состояния контролируемой цепи:

- [Норма],
- [Тревога],
- [Обрыв шлейфа],
- [Короткое замыкание].
- [Потеря связи] (формируется прибором «ЯРС», если от «М2» нет ответа на запрос).

Диаграмма порогов состояний при контроле цепи нагрузки приведена на рисунке 1.81.2 (в скобках указаны значения АЦП с учётом 15% температурного дрейфа источника тока в промышленном диапазоне  $-40 \div +70^{\circ}\text{C}$ ).

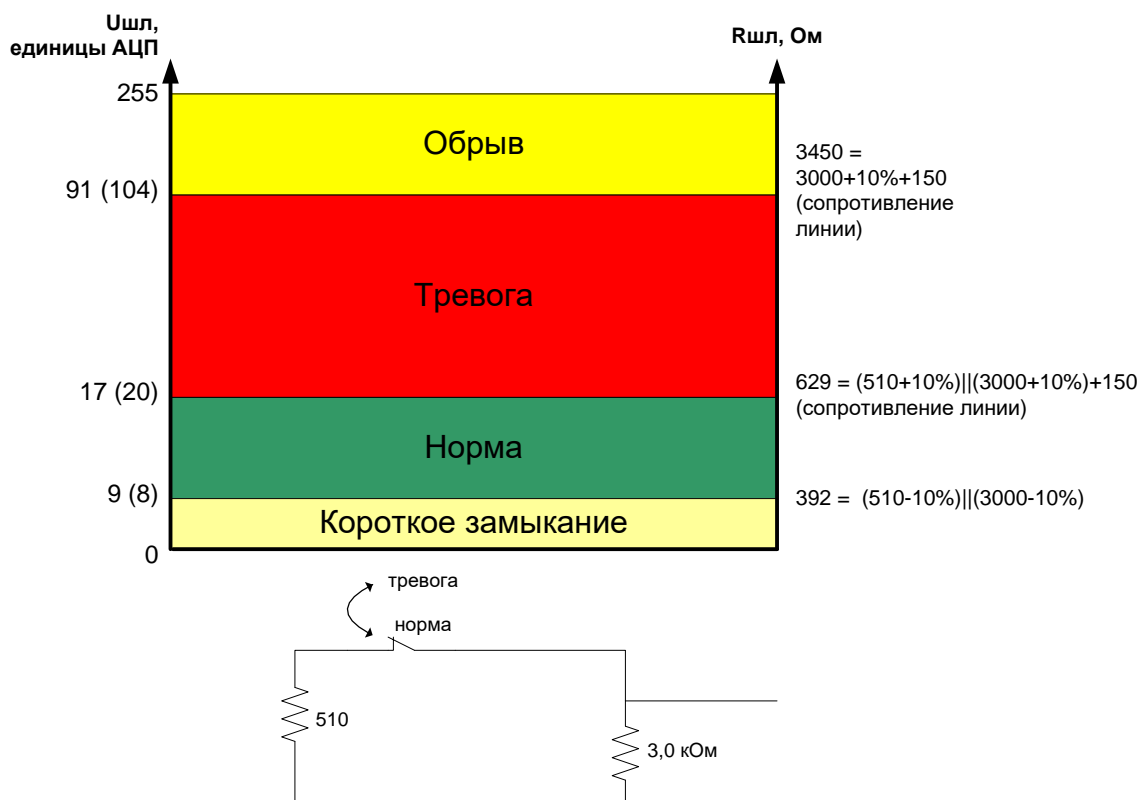


Рисунок 1.8 — Диаграмма порогов состояний при контроле цепи нагрузки

Предусмотрена работа в режиме «сухого контакта» (без контроля неисправности). При этом в качестве порогов состояний «замкнуто» ([Норма]) и «разомкнуто» ([Тревога]) используются границы состояний [Короткое замыкание] + [Норма] и [Тревога] + [Обрыв] соответственно. Диаграмма приведена на рисунке 1.9.

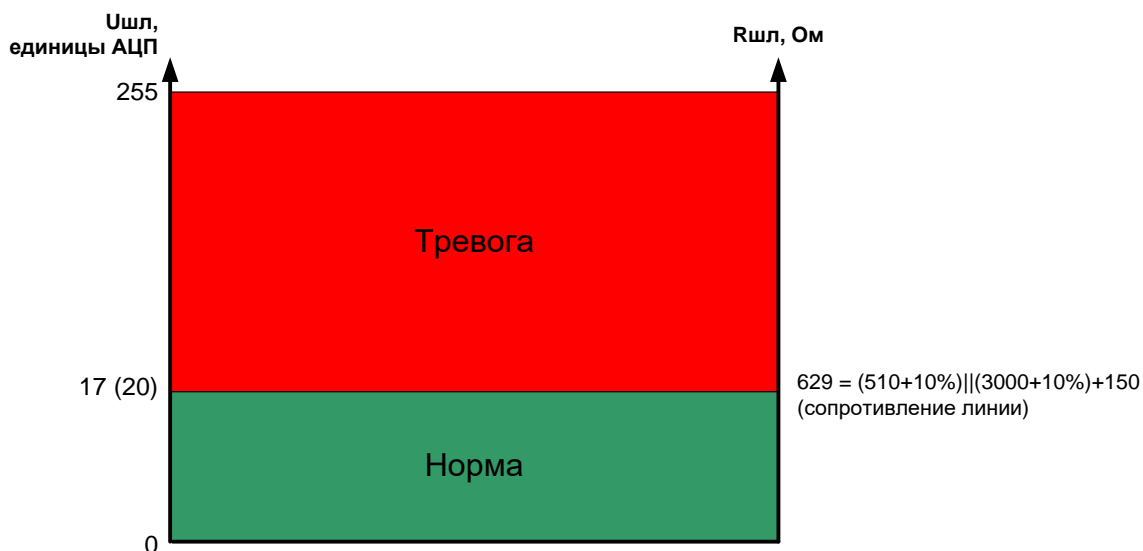


Рисунок 1.9 — Диаграмма порогов состояний без контроля цепи нагрузки

### 1.2.3.2.1 Дополнительные входы

Дискретный вход «Неисправность ИП» (PF, GND) предназначен для приёма сигнала о неисправности внешнего источника питания. Данный вход используется в случае, когда питание устройства осуществляется от бесперебойного источника питания, который самостоятельно выполняет функции контроля исправности первичного источника питания и формирования дискретного сигнала о возникшей неисправности в виде замыкания контактов механического или оптореле.

### 1.2.3.2.2 Выходы управления

На плате модуля предусмотрено 2 релейных выхода для управления замковыми устройствами (тип «электромеханическое реле») и 8 программируемых оптореле для использования в системах управления доступом, пожарной сигнализации и автоматики.

### 1.2.3.2.3 Питание изделия

На плате модуля «M2» предусмотрен один вход для подключения источника питания постоянного тока 12 – 24 В  $\pm 10\%$ .

Напряжение питания постоянного тока	10,8 ÷ 28 В
Максимальный потребляемый ток	200 мА (при напряжении 12 В)

В качестве источника питания рекомендуется применять блок резервного питания БРП-24-01Л (БКЛА.426431.002ТУ). Допускается питание нескольких модулей от одного БРП.

Электропитание считывателей может осуществляться от соответствующего выхода модуля «M2» или отдельными, не подключёнными к Модулю, линиями электропитания.

Переключатель **reader power** предназначен для выбора источника питания считывателей: осуществляет переключение между встроенным источником 9 В постоянного тока и входным питанием модуля «M2».

### 1.2.3.2.4 Конструкция изделия

Модуль «M2» представляет собой конструктивно законченное изделие, состоящее из платы электроники и корпуса из металла или пластика.

Пластиковый корпус имеет степень защиты IP65. Он состоит из основания и крышки. Крышка фиксируется в закрытом состоянии при помощи винтов. Основание корпуса оснащено отверстиями для крепления к стене. Внутри корпуса закреплена металлическая пластина, на которую при помощи стоек устанавливается плата электроники. Для подвода проводов предусмотрены гермовводы (6 штук).

Металлический корпус имеет степень защиты IP21. Он также состоит из основания и крышки, закрепляемой винтами. В основании расположено отверстие, предназначенное для ввода проводов при подключении прибора.

Габаритные и установочные размеры платы и корпусов приведены в разделе [Габаритные и установочные размеры изделия](#).

На плате модуля «M2» расположены кнопка **service pin**, датчик вскрытия корпуса (тампер), переключатель выбора источника питания для считывателей, а также переключатель выбора топологии сети LonWorks.

Кнопка **service pin** предназначена для отправки в сеть LonWorks широковещательного сообщения с уникальным идентификатором модуля. В качестве датчика вскрытия корпуса (тампера) используется кольцевой выключатель с подпружиненным плунжером. Переключатель **reader power** предназначен для выбора типа питания считывателей: переключатель **9V** обеспечивает питание встроенным источником постоянного тока 9 В, переключатель **input** — входным питанием модуля «M2». Переключатель **bus** предназначена для включения оконечного согласующего элемента (согласующей нагрузки) в сети LonWorks при использовании «шинной» топологии, переключатель **free** предназначена для включения согласующей нагрузки в сети LonWorks при использовании произвольной топологии (дополнительную информацию см. в разделе [Топология сети LonWorks](#)).

Описание разъёмов представлено в разделе [Разъёмы платы электроники](#). Схема расположения разъёмов, индикаторов и переключателей представлена на рисунке 1.10.



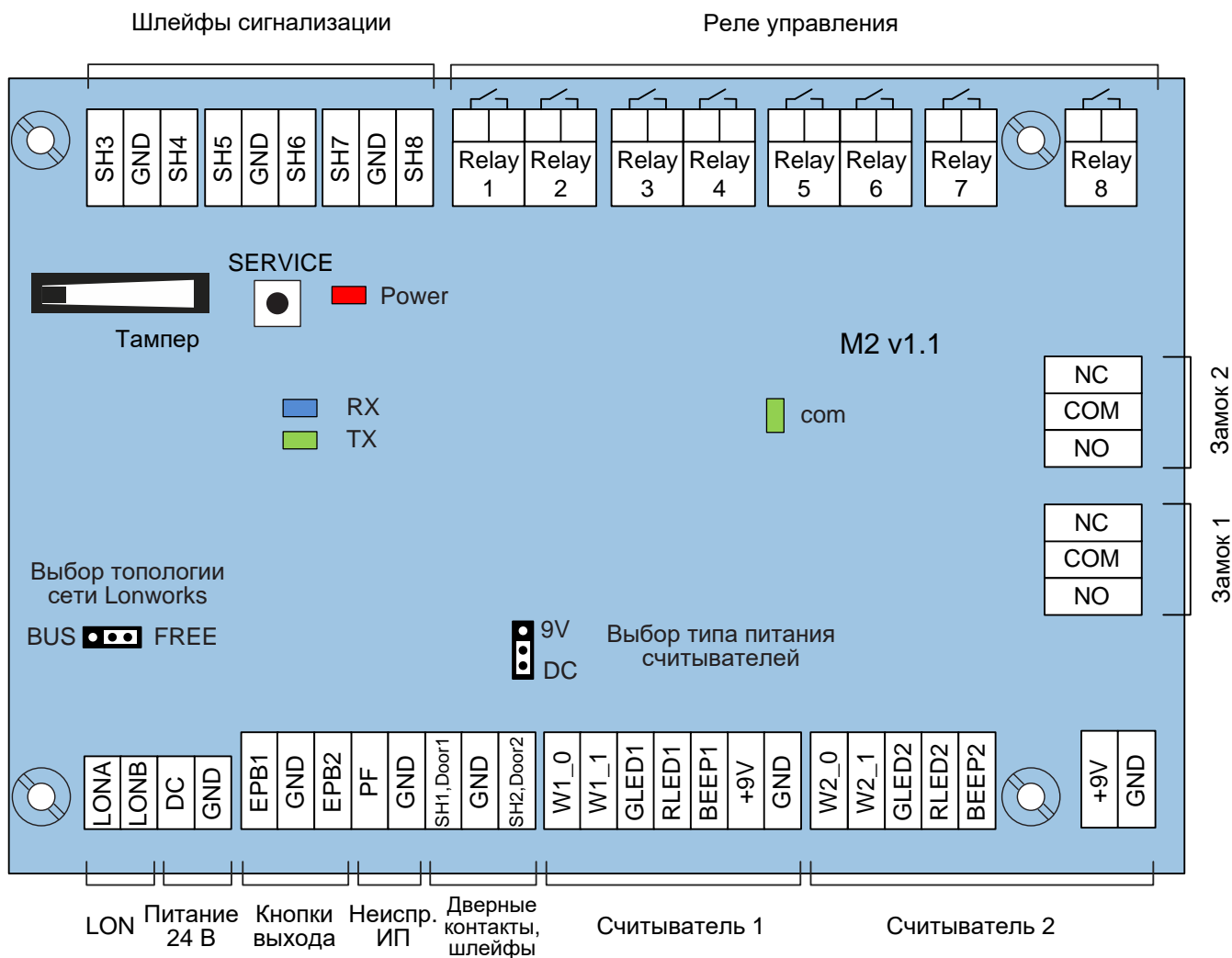


Рисунок 1.10 — Плата электроники модуля «М2»

## 1.2.4 Описание и работа модуля «МДС»

### 1.2.4.1 Общие сведения о модуле «МДС»

Модуль доступа и сигнализации «МДС» предназначен для использования в качестве дверного контроллера в системах управления доступом малых, средних и крупных объектов, а также в качестве прибора приёмно-контрольного в системах охранно-тревожной сигнализации малых, средних и крупных объектов. Модуль подключается к прибору «ЯРС» посредством двухпроводной линии LonWorks. «МДС» расширяет количество точек доступа, шлейфов сигнализации и реле, управляемых прибором «ЯРС». Модуль обеспечивает работу одной односторонней точки доступа и двух шлейфов сигнализации. Два модуля «МДС» могут использоваться для создания двусторонней точки доступа. К одному «ЯРС» может быть подключено до 63 модулей «МДС».

Настройка модуля осуществляется посредством веб-интерфейса, предоставляемого прибором «ЯРС»; средства конфигурирования LonWorks-сетей не требуются.

В штатном режиме требуется наличие постоянной связи с «ЯРС», на котором хранится полная база данных. Поведение модуля в случае аварийного разрыва связи с

«ЯРС», настраивается. Модуль «МДС» может работать в режиме запрета доступа, либо использовать локальный энергонезависимый буфер, в котором хранятся данные последних 1500 предъявленных валидных карт. До восстановления связи с головным контроллером, доступ по всем картам из буфера будет разрешён.

Модуль рассчитан на круглосуточную работу. Питание модуля осуществляется от внешних источников постоянного тока (блоков резервного питания).

## 1.2.4.2 Описание модуля «МДС»

### 1.2.4.2.1 Технические характеристики изделия

#### Сетевые интерфейсы

Назначение интерфейса	Тип интерфейса	Тип канала передачи	Количество интерфейсов
Для связи с «ЯРС»	ANSI / EIA – 709.1 (LonWorks)	Витая пара (TP/FT-10)	1

#### Шлейфы сигнализации

Количество проводников в ШС	3
Тип ШС	Многopоговый двухрезистивный адресный
Номинальное значение сопротивлений резисторов ШС	3±5% кОм и 510±5% кОм, 0,125 Вт
Определяемые прибором состояния с двумя установленными оконечными резисторами	«Норма», «Тревога», «Обрыв», «Короткое замыкание»

#### Управляемые выходы (реле)

Тип контактной группы реле	переключение
Максимальное напряжение коммутации для одного реле (AC/DC)	120 В / 30 В
Максимальный ток коммутации для одного реле (AC/DC)	2 А / 2 А

#### Устройства идентификации

Тип устройства идентификации	Тип интерфейса	Количество интерфейсов
Считыватель	Wiegand (до 64 бит)	1

Режимы индикации считывателей «ЯРС» и «МДС» сходны и приведены в разделе [Режимы индикации считывателей](#).

#### Питание

Напряжение питания, В	Ток потребления (не более), А	Количество входов питания
8 – 16 постоянный ток	0,15 при напряжении 12 В	1

## Параметры корпуса

Код исполнения корпуса	Степень защиты корпуса	Габаритные размеры (ДхШхВ), мм	Масса прибора в корпусе (не более), кг
115	IP22	132x82x35	0,3

### 1.2.4.2.2 Шлейфы сигнализации

К модулю «МДС» возможно подключение до 3 двухпроводных шлейфов; тип «многопороговый резистивный».

Физические состояния контролируемой цепи:

- [Норма],
- [Тревога],
- [Обрыв шлейфа],
- [Короткое замыкание].
- [Потеря связи] (формируется прибором «ЯРС», если нет от «М2» ответа на запрос).

Модуль «МДС» сам формирует логическое состояние его шлейфов. Диаграмма порогов состояний приведена на рисунке 1.11.

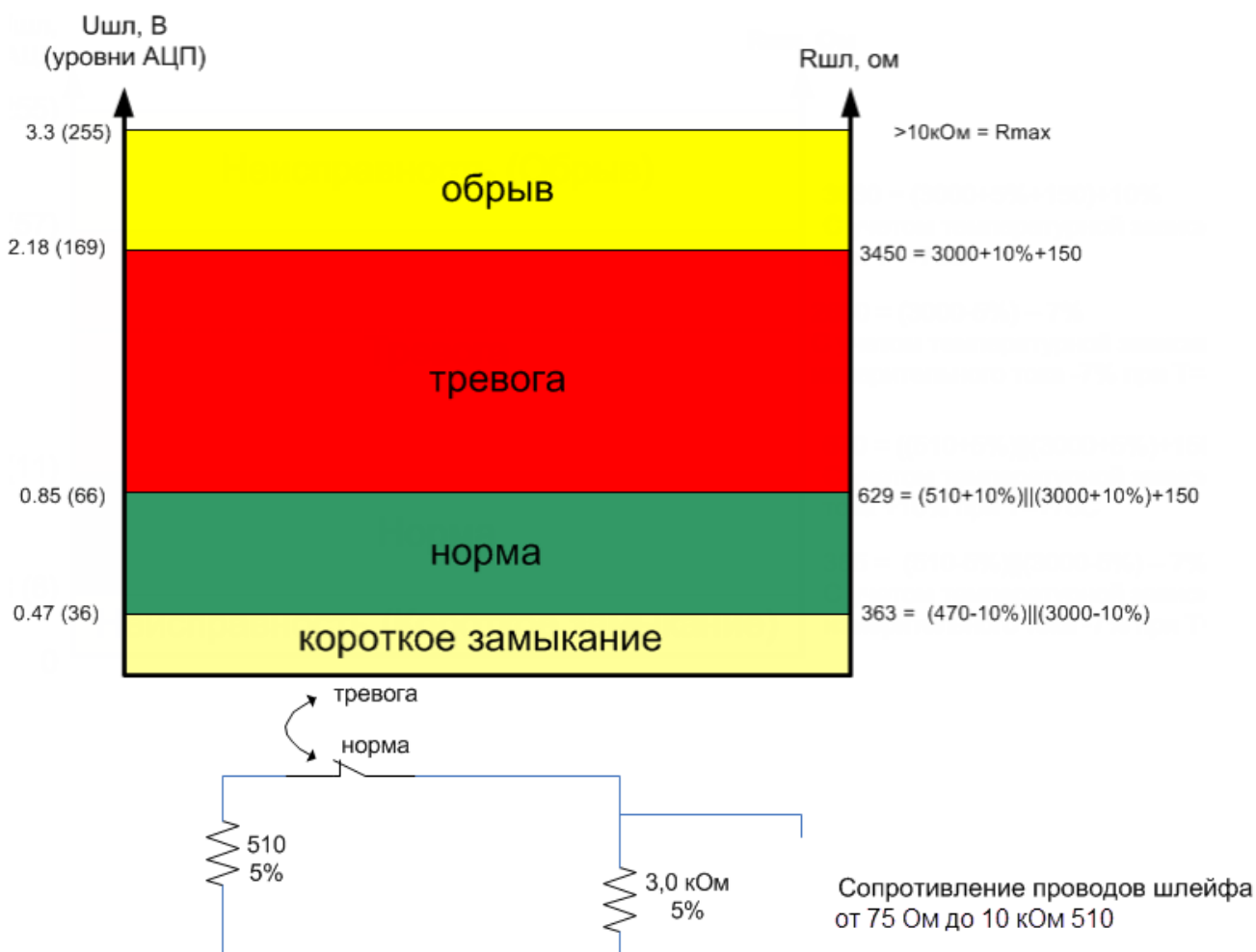


Рисунок 1.11 — Диаграмма порогов состояний шлейфа

### 1.2.4.2.3 Питание изделия

Питание «МДС» осуществляется только от источника постоянного тока 12 В ± 10%, для этого на плате модуля предусмотрен ввод питания.

Напряжение питания постоянного тока	8 – 16 В
Максимальный потребляемый ток	150 мА (при напряжении 12 В)

### 1.2.4.2.4 Конструкция изделия

Модуль представляет собой конструктивно законченное изделие. Основным элементом является плата электроники, размещённая внутри пластикового корпуса.

Корпус состоит из основания и крышки. На основании установлены 4 стойки, к которым крепится плата электроники при помощи 4 саморезов. Крышка крепится к основанию 4 винтами.

В основании корпуса и в боковых стенках крышки корпуса имеются специальные зоны для вскрытия при вводе проводов.

На плате модуля «МДС» расположены винтовые зажимы для подключения считывателей, замка, шлейфов сигнализации. В качестве датчика вскрытия корпуса (тампера) используется тактовая кнопка с пружинкой.

Описание разъёмов представлено в разделе [Разъёмы платы электроники](#). Схема расположения разъёмов представлена на рисунке 1.12.

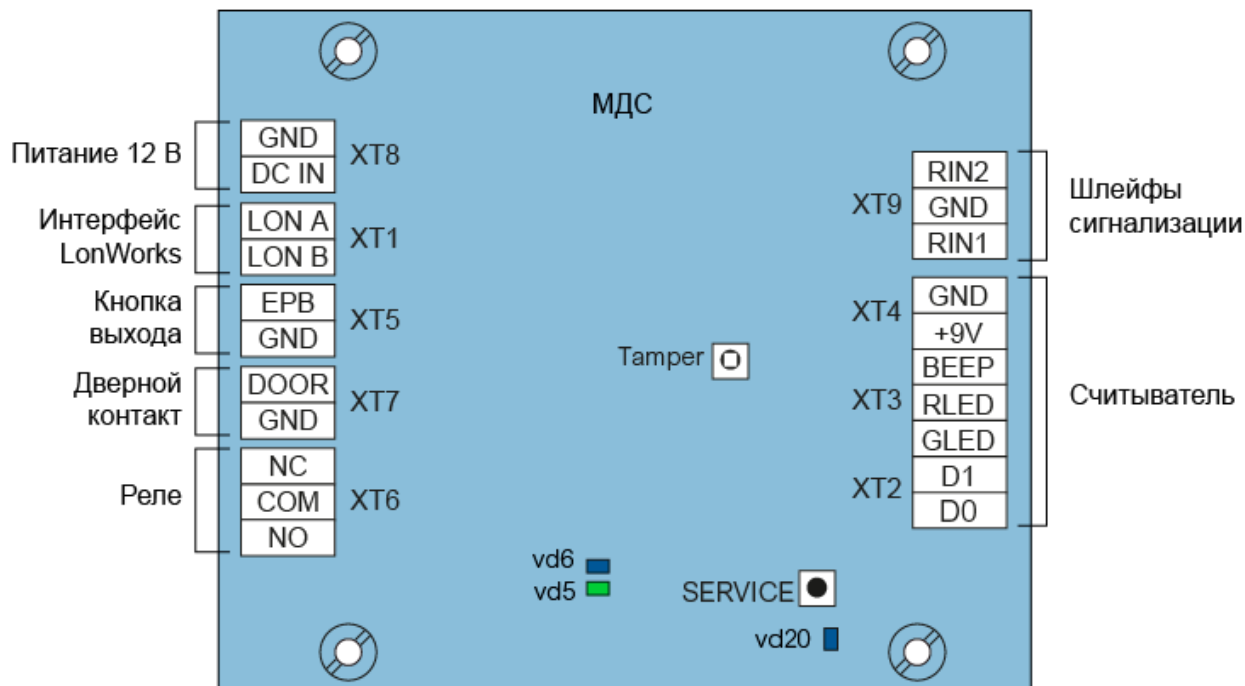


Рисунок 1.12 — Плата электроники «МДС»

## **2 ИСПОЛЬЗОВАНИЕ ПО НАЗНАЧЕНИЮ**

### **2.1 Эксплуатационные ограничения**

По устойчивости к климатическим воздействиям прибор относится к группе исполнения ДЗ ГОСТ Р 52931-2008. При этом рабочий диапазон температуры окружающего воздуха  $-50^{\circ}\text{C} \div +50^{\circ}\text{C}$ , а верхнее значение относительной влажности равно 95% при  $+35^{\circ}\text{C}$  и более низких температурах, без конденсации влаги. При заказе исполнения для помещения В4 ГОСТ 12997-84, рабочий диапазон температуры окружающего воздуха равен  $+5^{\circ}\text{C} \div +55^{\circ}\text{C}$ , а верхнее значение относительной влажности равно 93% при  $+40^{\circ}\text{C}$  и более низких температурах, без конденсации влаги.

По устойчивости к механическим воздействиям прибор относится к группе исполнения L2 ГОСТ Р 52931-2008.

Прибор является пожаробезопасным при правильной установке, монтаже и техническом обслуживании.

#### **2.1.1 Меры безопасности при подготовке изделия**

Прибор не является источником опасности для людей и для защищаемых материальных ценностей (в том числе и в случае аварийных ситуаций).

Конструкция и схемотехнические решения прибора обеспечивают его пожарную безопасность эксплуатации (в том числе и в аварийных режимах работы).

Прибор по способу защиты человека от поражения электрическим током удовлетворяет требованиям III класса безопасности по ГОСТ 12.2.007.0.

В приборе отсутствуют опасные для жизни человека напряжения, но при ремонте, монтаже и эксплуатации необходимо выполнять меры безопасности в соответствии с «Правилами технической эксплуатации электроустановок потребителей».

Перед поставкой изделия проводится выходной контроль.

#### **2.1.2 Осмотр изделия**

Осмотр изделия проводите в следующей последовательности:

1. Проверьте состояние упаковки и распакуйте изделие.
2. Проверьте соответствие комплектности и серийного номера изделия паспортным данным.
3. Произведите внешний осмотр компонентов изделия и убедитесь в отсутствии видимых механических повреждений и загрязнений.
4. Убедитесь в отсутствии посторонних предметов внутри корпуса изделия.
5. Проверьте крепление клеммных колодок.

**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!

## 2.2 Подготовка изделия к использованию

### 2.2.1 Подготовка к работе одного (первого) устройства

Выполните последовательно следующие действия:

1. Закрепите контроллер «ЯРС» в месте установки. Информация по размерности приведена в приложении [Габаритные и установочные размеры изделия](#).
2. Соберите схему в соответствии с рисунком [2.1](#):
  - 1) Установите карту памяти с программным обеспечением устройства в разъем для карт **SD micro**.
  - 2) Подключите устройство к источнику питания. К входам **AF** и **PF** подключите шлейфы технологических входов «Неисправность ИП» и/или «Неисправность аккумулятора» в соответствии со схемой подключения на рисунке [9.8](#). Если технологические входы не используются, то их впоследствии необходимо будет отключить посредством веб-интерфейса (см. п. [6.](#)).
  - 3) Подключите к контроллеру шлейфы сигнализации (дополнительную информацию см. в разделе [Подключение шлейфов охранной сигнализации](#)).
  - 4) Подключите считыватели к соответствующим разъёмам (дополнительную информацию см. в разделе [Подключение считывателей](#)).
  - 5) К релейным выходам подключите замковые устройства (дополнительную информацию см. в разделе [Подключение замковых устройств](#)).
  - 6) Подключите кнопки выхода и дверные контакты к разъёмам входов подключения шлейфов сигнализации **SH1 — SH4** (дополнительную информацию см. в разделе [Подключение дверных контактов](#)).
  - 7) При использовании модуля подключения TP/FT-10 (NeuronModule) и модулей «M2»/«МДС» (рисунок [2.2](#)):
    - 7.1) Подключите контроллер «ЯРС» и модули «M2»/«МДС» к сети LonWorks (дополнительную информацию см. в разделе [Подключение к сети Lonworks](#));
    - 7.2) К разъёмам «M2»/«МДС» подключите шлейфы сигнализации (дополнительную информацию см. в разделе [Подключение шлейфов охранной сигнализации](#));
    - 7.3) К разъёмам «M2»/«МДС» подключите считыватели с интерфейсом Wiegand (дополнительную информацию см. в разделе [Подключение считывателей](#));
    - 7.4) К разъёмам «M2»/«МДС» подключите замковые устройства (дополнительную информацию см. в разделе [Подключение замковых устройств](#));

- 7.5) К разъёмам «M2»/«МДС» подключите кнопки выхода и дверные контакты (дополнительную информацию см. в разделе [Подключение дверных контактов](#));
- 7.6) Подключите модули «M2»/«МДС» к источнику питания 12 В.
- 8) При использовании модулей подключения RS-232 (RS232Module) и RS-485 (RS485Module), подключите внешнее оборудование. Информация по подключению интерфейсов RS-232/RS-485 на примере прибора Handkey-II приведена в разделе [Подключение Handkey-II](#)).
- 9) Подключите прибор к компьютеру посредством разъёма **Ethernet 1**. Настройте сетевое подключение компьютера на работу в диапазоне IP-адресов **10.200.X.YYY** и подсети **255.255.255.0**.

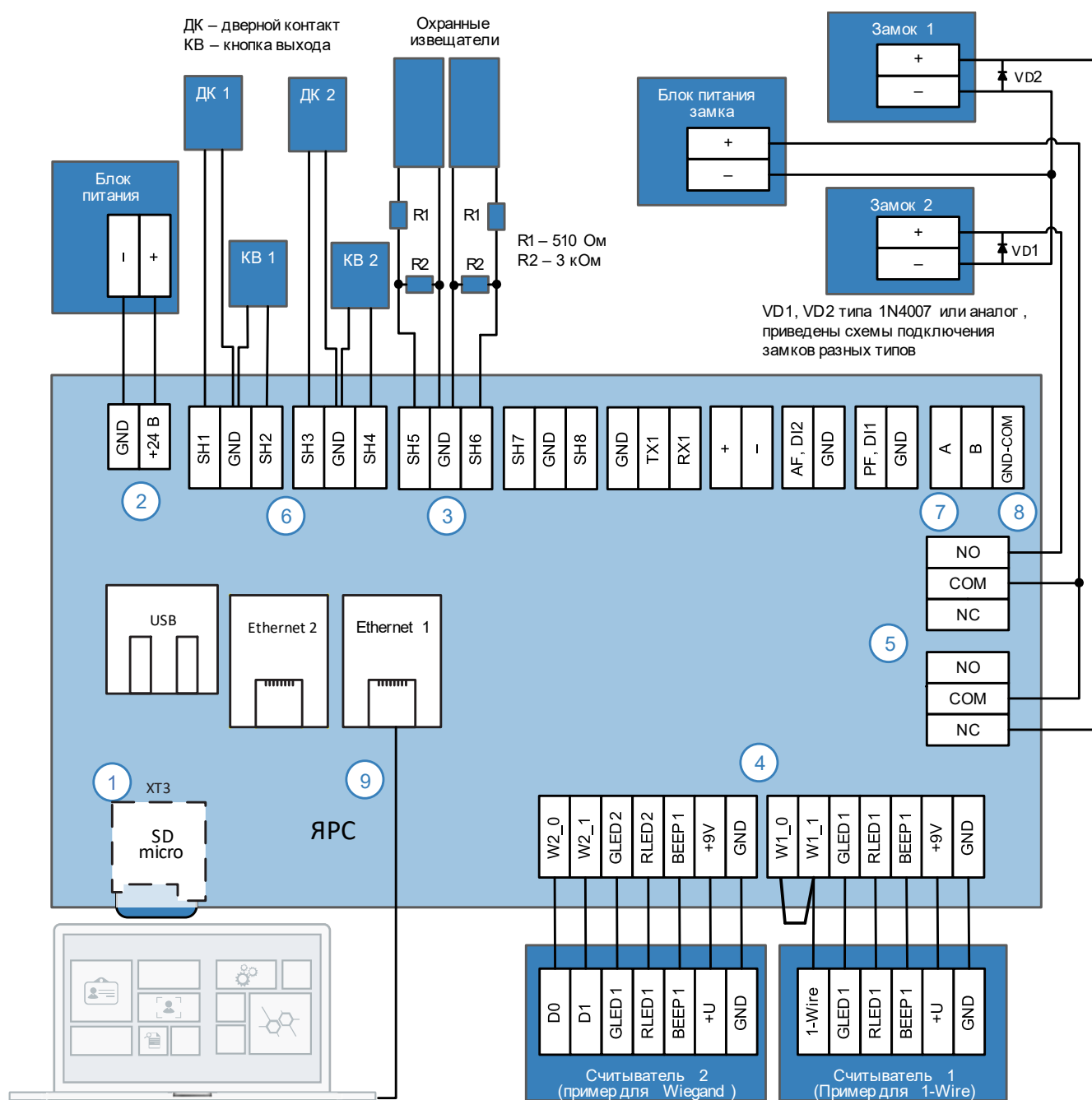


Рисунок 2.1 — Схема подключения «ЯРС»



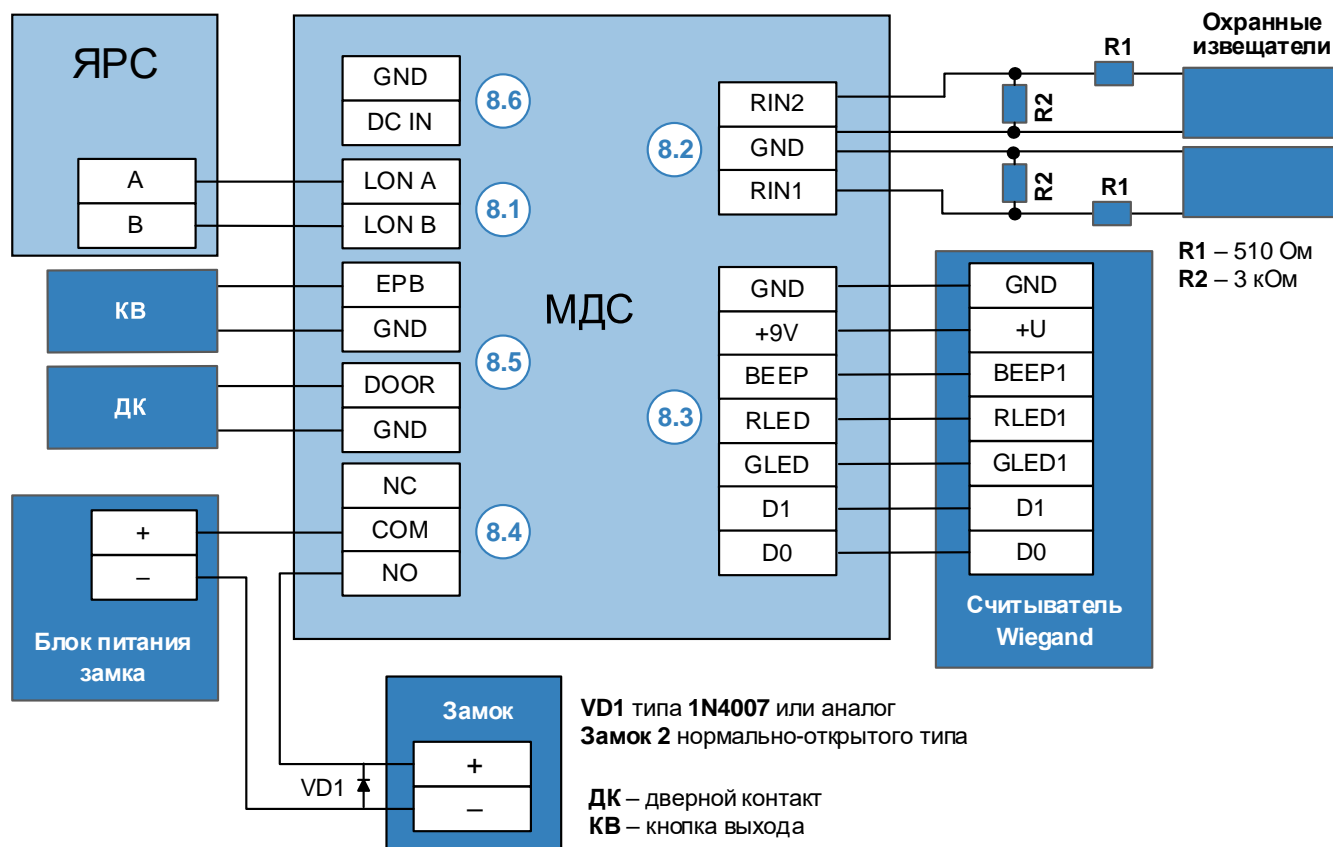


Рисунок 2.2 — Схема подключения модуля «МДС»

3. Включите питание прибора и модулей «МДС». Не более чем через 1 секунду после подачи питания должно наблюдаться непрерывное свечение красного индикатора **PW**, расположенного на плате электроники (рисунок 1.5). Не более чем через 45 секунд после подачи питания проверьте состояние зелёного индикатора **ACT** на плате электроники, который должен мигать с периодом 0,5 Гц, что свидетельствует об успешной загрузке встроенного программного обеспечения прибора и готовности прибора к работе.
4. 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 ip-адрес, указанный на корпусе прибора. С помощью мастера первого запуска задайте общие параметры прибора или восстановите данные из резервной копии (см. раздел [Мастер первого запуска](#)).
5. Перейдите к интерфейсу прибора по заданному IP-адресу и из указанной на предыдущем этапе подсети (см. раздел [Вход в веб-интерфейс](#)). Введите имя пользователя **root** и указанный на предыдущем этапе мастер-пароль (по умолчанию, **root**).
6. Перейдите в раздел **Конфигурация узлов** (см. [Конфигурация узлов](#)) и настройте параметры прибора:
  - Задайте новый мастер-пароль устройства, если пароль не был изменён ранее (см. раздел [Смена мастер-пароля](#));

- В разделе [Сетевые параметры](#), при необходимости, можно задать сменить ip-адрес, задать шлюз, сетевые маршруты и сменить домен 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 изменён мастер-пароль, авторизацию следует проходить под новым паролем.

Домены НЕЙРОСС предназначены для обеспечения взаимодействия нескольких устройств, образующих сеть НЕЙРОСС («ЯРС», «Борей», «КБУ-1», «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(ам).

- 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).
  - Настройте параметры технологических входов **AF** и **PF** (см. раздел [Технологические входы](#)).
  - Настройте параметры шлейфов сигнализации (см. раздел [Зоны сигнализации](#)).
  - Настройте параметры точки (точек) доступа (см. раздел [Точки доступа](#)).
  - В разделе [Модули расширения](#) выполните добавление подключённых LON-модулей и выполните их настройку (см. раздел [Модули расширения](#)). Для настройки двусторонней точки доступа задайте связь со второй точкой доступа.
7. Настройка разделов сигнализации, их группировка для постановки на охрану с помощью считывателя, настройка режимов работы реле по событиям разделов, настройка зон доступа для обеспечения контроля повторного прохода осуществляется в соответствующих приложениях интерфейса, переход к которым осуществляется по ссылкам на рабочем столе (см. раздел [Рабочий стол](#)).
- Настройте разделы сигнализации (см. [Разделы сигнализации](#)).
  - Настройте реле управления (см. раздел [Реле управления](#)).
  - При необходимости блокировки/разблокировки точки доступа при тревоге в разделе охранной сигнализации, перейдите на страницу настройки точки доступа и задайте параметры **Блокировать при тревоге** и **Разблокировать при тревоге** (см. раздел [Точки доступа](#)).
  - При необходимости выполнения контроля повторного прохода, настройте **Зоны доступа** (см. раздел [Зоны доступа](#)), затем вернитесь к настройке точек доступа и задайте параметры **Зона ВХОД** и **Зона ВЫХОД** (см. раздел [Точки доступа](#)).
  - Если точка/точки доступа прибора будут использоваться в качестве терминала для управления охранными разделами, создайте «привязку» разделов к данной точке доступа (см. раздел [Терминалы](#)).

8. Перейдите в раздел **Бюро пропусков** веб-интерфейса прибора (см. приложение [Бюро пропусков](#)).
9. Создайте требуемое количество пропусков (см. раздел [Создание пропуска](#)), для каждого пропуска задайте **Уровень доступа** и, при необходимости, **Уровень управления** (см. разделы [Настройка уровней доступа](#), [Настройка уровней управления](#)).
10. Если в дальнейшем планируется добавить в сеть НЕЙРОСС новое устройство (см. раздел [Сеть НЕЙРОСС](#)
11. ), для выполнения групповых операций обновления, перезагрузки, создания резервных копий и др., создайте так называемую «облачную» учётную запись.
12. При необходимости обеспечения взаимодействия прибора с ПО ИСБ ITRIUM®, на компьютере сервера базы данных настройте «Службу НЕЙРОСС» (см. раздел [Настройка «Службы НЕЙРОСС»](#)). При этом данные контроллера «ЯРС» будут синхронизированы с ITRIUM®, станет возможным мониторинг и управление средствами ITRIUM®.
13. По завершению настройки создайте резервную копию данных (см. раздел [Резервные копии](#)).

Прибор готов к использованию!

### 2.2.2 Добавление устройства к сети НЕЙРОСС

Если в сети организации уже есть хотя бы одно устройство НЕЙРОСС (см. раздел [Понятие сети НЕЙРОСС](#)), то при добавлении нового узла сети необходимо обеспечить синхронизацию даты/времени на устройствах и синхронизировать данные. В добавляемое устройство будут загружены «облачные» учётные данные и общие ресурсы (такие как разделы сигнализации, зоны доступа и пр.). Впоследствии, при изменении данных, внесённые изменения автоматически будут загружены во все устройства сети.

Для добавления в существующую сеть НЕЙРОСС (см. раздел [Понятие сети НЕЙРОСС](#)) нового устройства «ЯРС» выполните следующую последовательность шагов:

1. Выполните пп. 1 – 6 из раздела [Подготовка к работе одного \(первого\) устройства](#).

**Примечание 1** — На этапе 6 обратите внимание, что настройки параметров даты/времени на устройстве должны обеспечивать отсутствие расхождения времени на всех устройствах сети (наилучшим выбором будет задать в настройках всех устройств автоматическую синхронизацию по одному NTP-серверу).

**Примечание 2** — Также на этапе 6 проверьте настройки имени домена. Взаимодействие устройств обеспечивается в пределах домена. Одно устройство может принадлежать разным доменам.

2. Перейдите в раздел **Сеть** (см. приложение [Сеть](#)). Выберите устройство, которое будет выступать в качестве источника данных и синхронизируйте данные (см. раздел [Синхронизация данных между узлами НЕЙРОСС](#)). Процедура синхронизации

данных является точкой начала отслеживания изменений между узлами. В дальнейшем синхронизация будет проводиться автоматически.

3. Создайте новые разделы сигнализации или добавьте зоны нового устройства к существующим разделам (см. [Разделы сигнализации](#)).
4. Задайте режимы управления реле нового устройства (см. раздел [Реле управления](#)).
5. При необходимости блокировки/разблокировки точки доступа при тревоге в разделе охранной сигнализации, перейдите на страницу настройки точки доступа и задайте параметры **Блокировать при тревоге** и **Разблокировать при тревоге** (см. раздел [Точки доступа](#)). В списке разделов будут доступны все разделы сети НЕЙРОСС.
6. При необходимости выполнения контроля повторного прохода, настройте **Зоны доступа** (см. раздел [Зоны доступа](#)), затем вернитесь к настройке точек доступа и задайте параметры **Зона ВХОД** и **Зона ВЫХОД** (см. раздел [Точки доступа](#)).
7. Если точка/точки доступа прибора будут использоваться в качестве терминала для управления охранными разделами, создайте «привязку» разделов к данной точке доступа (см. раздел [Терминалы](#)). При этом можно настроить любую точку доступа на управление любыми охранными зонами сети НЕЙРОСС.
8. Перейдите в раздел **Бюро пропусков** веб-интерфейса прибора (см. приложение [Бюро пропусков](#)). Отредактируйте **Уровень доступа** и, при необходимости, **Уровень управления** с учётом нового устройства (см. разделы [Настройка уровней доступа](#), [Настройка уровней управления](#)).
9. По завершению настройки создайте резервную копию данных (см. раздел [Резервные копии узлов НЕЙРОСС](#)).
10. При авторизации в интерфейсе под «облачной учётной записью», вам станет доступна настройка всех узлов и выполнение групповых операций обновления, синхронизации данных, перезагрузки и создания резервных копий.

**Примечание.** Для перехода к настройкам других приборов сети, в левом сплывающем меню (см. [Конфигурация узлов](#)) выберите требуемую группу устройств и нужное устройство по его ip-адресу. Доступ к групповым операциям осуществляется из раздела **Сеть**.

Прибор готов к использованию!

### 2.2.3 Обновление программных средств

С целью дополнения предоставляемого устройствами НЕЙРОСС функционала, компания-разработчик выпускает обновления программных средств («прошивки») устройств.

**Примечание.** Перед выполнением обновления проверьте наличие резервной копии, а при отсутствии – создайте её. Инструкцию по созданию резервной копии см. в разделе [Резервные копии](#).

Для обновления выполните следующую последовательность шагов:

1. Приготовьте файл архива программных средств (предоставляется в формате **TAR.GZ**).
2. Выполните обновление. Инструкцию см. в разделе [Обновление программных средств \(прошивки\) прибора](#).
3. После обновления выполните очистку кеша браузера, которым вы пользуетесь для подключения к веб-интерфейсу (дополнительную информацию см. в разделе [Вход в веб-интерфейс](#)).
4. Если до обновления устройств домен НЕЙРОСС не был сконфигурирован (использовались настройки по умолчанию), то после обновления каждому устройству на основе его идентификатора будет присвоен уникальный домен вида **NEYROSS-a2581d2d-86af-447a-8e4c-64e8e9a3cc54**. В этом случае устройства потеряют связь друг с другом и с ПО ITRIUM, так как каждое устройство будет находиться в отдельном домене. В этом случае необходимо:
  - Последовательно подключиться к веб-интерфейсу каждого устройства.
  - Перейти в раздел [Конфигурация узлов](#) — [Сетевые параметры](#). Переключится на вкладку **Дополнительно** и в поле **Домен НЕЙРОСС** ввести новое значение (например, **NEYROSS**).
  - Нажать на кнопку **Сохранить**.

**Примечание.** Если домен НЕЙРОСС был изначально сконфигурирован, после обновления его значение не изменится. Рекомендации по настройке доменов см. в разделе [Сеть НЕЙРОСС](#).

5. Обязательно создайте резервную копию данных каждого обновлённого узла (см. раздел [Резервные копии](#)).
6. Убедитесь в корректности настроек и выполненных обновлений:
  - в разделе [Конфигурация узлов](#) — [Настройки узла](#)
  - Основные настройки, на вкладке **Информация** убедитесь, что:
    - в поле **Версия** указана устанавливаемая версия программных средств.
    - в поле **Версия ядра** указана требуемая версия ядра.
  - в разделе [Конфигурация узлов](#) — [Сетевые параметры](#) проверьте настройки IP-адреса, подсети, домена НЕЙРОСС;
  - в разделе [Конфигурация узлов](#) — [Дата и время](#) проверьте настройки NTP-сервера.
7. При необходимости выполните синхронизацию данных (см. раздел [Синхронизация данных между узлами НЕЙРОСС](#)).

#### 2.2.4 Подготовка к работе с турникетом

При необходимости работы с турникетом, выполните следующие шаги:

1. Подключите турникет согласно схеме на рисунке [9.26](#).
2. Перейдите к веб-интерфейсу прибора. В подразделе **Конфигурация узлов — Доступ** задайте следующие настройки (дополнительную информацию см. в разделе Точки доступа):
  - Выберите режим работы **Две односторонние**.
  - В полях **Ждать закрытия двери**, **Ждать открытия двери** задайте значение **Нет**.
  - В поле **Закрывать замок** выберите из раскрывающегося списка значение **По истечению времени**.
  - В поле **Время открытия замка** задайте значение **1 сек**.
  - Сохраните изменения.
  - Повторите настройки для второй точки доступа.
3. Остальные настройки задайте согласно необходимости.

#### 2.2.5 Подготовка к работе с Handkey-II

Ввод биометрических данных осуществляется с помощью компьютера с установленным ПО ИСБ ITRIUM, к которому подключён сканер геометрии руки Handkey-II. Для настройки ввода биопараметров в базу данных пропусков, выполните следующие шаги:

1. В программе «Администратор системы», входящей в комплект поставки ПО ИСБ ITRIUM, к элементу **Компьютер**, символизирующему компьютер, к которому подключён сканер Handkey-II, добавьте и настройте элемент **Драйвер Handkey**. Руководство пользователя к «Драйверу Handkey» можно открыть из окна автозапуска установочного диска, либо скачать по адресу [http://www.itrium.ru/pdf/itrium/Driver\\_HandKey.pdf](http://www.itrium.ru/pdf/itrium/Driver_HandKey.pdf).
2. Для ввода биопараметров руки с базу данных владельцев пропусков, необходимо на соответствующую форму Бюро пропусков добавить поле ввода параметров геометрии руки и связать его со свойством **Владелец пропуска** → **Информация о руке**, а также указать считыватель биометрических данных (устройство Handkey). Краткая инструкция приведена в руководстве пользователя к «Драйверу Handkey».
3. В программе «Администратор системы» добавьте и настройте элемент **Служба НЕЙРОСС** (см. раздел [Настройка «Службы НЕЙРОСС»](#)).
4. Для обеспечения доступа настройте уровни доступа, уровни охраны (если требуется), режимы доступа, для обеспечения загрузки пропусков (в том числе биопараметров) в НЕЙРОСС, настройте «Службу бюро пропусков» и «Службу НЕЙРОСС». Подробная инструкция по настройке всех перечисленных элементов приведена в разделе [Настройка доступа в ПО ИСБ ITRIUM](#).

5. С помощью «Программы оформления пропусков» осуществите ввод данных владельцев пропусков и оформите пропуски. Руководство пользователя к «Программе оформления пропусков» можно открыть из окна автозапуска установочного диска, либо скачать по адресу [http://www.itrium.ru/pdf/itrium/Programma\\_oformleniya\\_propuskov.pdf](http://www.itrium.ru/pdf/itrium/Programma_oformleniya_propuskov.pdf). Все пропуска будут загружены в сеть НЕЙРОСС (в том числе, – контроллеры «ЯРС»).

Для обеспечения двухфакторной идентификации по карте и биометрии, выполните следующие шаги:

1. Подключите считыватель Handkey-II к прибору «ЯРС» (см. раздел [Подключение Handkey-II](#)).
2. Посредством веб-интерфейса прибора «ЯРС» задайте параметры точек доступа. Базовые параметры настраиваются в разделе [Конфигурация узлов — Доступ](#) (см. раздел [Точки доступа](#)). «Привязка» биометрического считывателя к точке доступа осуществляется на странице редактирования параметров расширений (см. раздел [Интеграция с Handkey-II](#)).

## 2.3 Использование изделия

### 2.3.1 Предоставление доступа

Точка доступа контроллера может работать в одном из трёх режимов: «Дежурный», «Заблокировано» и «Разблокировано».

Переключение между режимами работы точки доступа осуществляется по командам оператора **Заблокировать**, **Разблокировать**, **Восстановить режим**, для однократного разрешения доступа без предъявления идентификатора предназначена команда **Инициировать проход**.

Точка доступа может блокироваться автоматически при постановке зоны на охрану или при тревоге в заданной зоне, также возможна автоматическая разблокировка точки доступа при возникновении тревоги в зоне.

#### 2.3.1.1 Дежурный режим

В дежурном режиме для получения доступа необходимо предъявить на соответствующем считывателе валидный идентификатор и/или пин-код. Если в базе данных контроллера содержатся данные о пропуске и удовлетворены условия режима доступа (временной интервал, точка доступа), то происходит предоставление доступа:

- Включается зелёный индикатор считывателя;
- Дверь разблокируется на заданное время;
- Формируется сообщение «Доступ разрешён».

Если в базе данных контроллера нет данных о пропуске или не выполнены условия режима доступа, то происходит отклонение доступа:

- Звуковой индикатор считывателя издаёт продолжительный звуковой сигнал (см. раздел [Режимы индикации считывателей](#));
- Включается красный индикатор считывателя;
- Дверь не разблокируется;
- Формируется сообщение «Доступ запрещён».

При нажатии на кнопку выхода происходит предоставление доступа, формируется сообщение «Доступ разрешён. Кнопка выхода».

После предоставления доступа факт прохода фиксируется в зависимости от настроек точки доступа (см. таблицу [9.11](#) раздела [Точки доступа](#)), формируются сообщения «Проход совершён», «Проход не совершён», «Дверь удержана открытой».

По факту прохода или по истечении времени **Время ожидания открытия двери** дверь блокируется, красный индикатор считывателя начинает мигать с частотой 1 Гц, точка доступа переходит в состояние по умолчанию (см. раздел [Состояния точек доступа](#)).

Доступ может осуществляться по правилу N лиц, с глобальным контролем повторного прохода (antipassbak'ом), с подтверждением доступа:

- При условии доступа по правилу N-лиц, предоставление доступа осуществляется при предъявлении заданного количества валидных идентификаторов в течение заданного промежутка времени.
- При условии контроля повторного прохода, запрещается повторное предъявление идентификатора на считывателе. Доступ разрешается, если данные о текущей зоне в пропуске совпадают с настройками точки доступа. По факту прохода происходит изменение текущей зоны в пропуске. Возможен мягкий и жёсткий режим контроля: в жёстком режиме при нарушении зоны доступа происходит отказ доступа; в мягком режиме доступ разрешается, но формируется тревожное сообщение.
- При условии подтверждения доступа, доступ разрешается только после подтверждения оператором. Подтверждение может осуществляться с помощью приложения «Фотоидентификация» веб-интерфейса прибора, а также из программы «Фотоидентификация» семейства программ ITRIUM®.

### 2.3.1.2 Режим «Разблокировано»

В режиме «Разблокировано» контроль доступа не осуществляется, разрешён проход без предъявления идентификаторов.

В случае разблокировки точки доступа:

- Кнопка выхода не работает,
- Дверной контакт не работает,



- Входные сообщения от считывателя игнорируются.

### 2.3.1.3 Режим «Заблокировано»

В режиме «Заблокировано» доступ не предоставляется, при открытии двери формируется сообщение «Взлом двери».

В случае блокировки точки доступа:

- Кнопка выхода не работает,
- Дверной контакт работает (м.б. сформировано состояние [Взлом двери]).
- Входные сообщения от считывателя игнорируются,
- Текущая транзакция прохода обрывается.

## 2.3.2 Управление зонами и разделами охранной сигнализации

Управление осуществляется с помощью команд сброса тревог, постановки на охрану и снятия с охраны охранных зон шлейфов сигнализации или разделов в целом. Доступ к командам управления возможен из веб-интерфейса или программ семейства ITRIUM® (см. раздел [Команды управления разделами и зонами](#)).

### 2.3.2.1 Управление разделами с помощью считывателя

Точка доступа может использоваться в качестве терминала для постановки на охрану и снятия с охраны разделов сигнализации. Осуществляется групповое управление разделами. Список разделов ограничивается «привязкой» к точке доступа и уровнем охраны пропуска (дополнительная информация представлена в разделе [Настройка уровня](#)).

#### Порядок управления разделами:

1. Предъявите валидный идентификатор и/или пин-код.
  - Если точка доступа предназначена только для управления разделами и не используется для предоставления доступа (в настройках точки доступа в поле **Исключена** (использовать только для постановки/снятия) указано **Да**, см. раздел [Точки доступа](#)), перейдите к п. 3.
  - Если точка доступа заблокирована, перейдите к п. 3.
2. До истечения периода времени **Время ожидания открытия двери** (см. раздел [Точки доступа](#)), откройте дверь и повторно предъявите валидный идентификатор и/или пин-код.
3. По индикации на считывателе определите текущий статус списка разделов охранной сигнализации, разрешённых для управления в данной точке доступа по данному пропуску (определяется пересечением множества «привязанных» к точке доступа

разделов с множеством разделов, заданных уровнем охраны пропуска, более подробную информацию см. в разделе [Настройка уровней](#) ).

4. Повторно предъявите идентификатор и/или пин-код. Будет предпринята попытка постановки на охрану всех «привязанных» разделов сигнализации. Если разделы частично на охране, предварительно они будут сняты с охраны.
5. При успешной постановке точка доступа будет заблокирована.

### 3 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ

#### 3.1 Общие указания и меры безопасности

Для обеспечения долговременной безотказной работы изделия необходимо регулярно, в полном соответствии с установленными нормативами, проводить предусмотренный комплекс технических мероприятий по плановому техническому обслуживанию.

#### 3.2 Порядок технического обслуживания изделия

Плановое техническое обслуживание прибора должно обязательно включать в себя операции, перечисленные в таблице 3.1.

Таблица 3.1 – Порядок технического обслуживания

Наименование работы	Периодичность не реже	Расходные материалы	Количество на 1 устройство
Внешний осмотр, контроль разъёмных и кабельных соединений	1 раз в год	бязь спирт экстра ГОСТ 5962-67	0,25 м <sup>2</sup> 0,06 дм <sup>3</sup>
Очистка корпуса от загрязнения	1 раз в два месяца	бязь спирт экстра ГОСТ 5962-67	0,02 м <sup>2</sup> 0,01 дм <sup>3</sup>
Контроль питающих напряжений	1 раз в два месяца		

Очистка корпуса проводится следующим образом:

- Влажной, смоченной в растворе стирального порошка в воде, отжатой бязевой салфеткой протереть очищаемую поверхность корпуса до удаления видимых глазом следов грязи;
- Влажной, смоченной в чистой воде, отжатой бязевой салфеткой промыть очищаемую поверхность корпуса до удаления видимых глазом следов грязи и стирального порошка;
- Протереть очищаемую поверхность корпуса до удаления видимых глазом следов влаги;
- Влажной, смоченной спиртом, чистой бязевой салфеткой протереть очищаемую поверхность плат;

- Протереть очищаемую поверхность плат до удаления видимых глазом следов влаги.

Контроль питающих напряжений включает в себя проверку блока бесперебойного питания (БРП). Напряжение питания рекомендуется измерять на клеммах прибора.

### 3.3 Проверка работоспособности изделия

**Внимание.** Перед проведением проверки необходимо отключить цепи управления дверными контактами, если их включение недопустимо.

1. Проверка работы органов индикации: проверьте, что световой индикатор **ПИТАНИЕ (pw)** светится непрерывно, индикатор **РАБОТА (act)** периодически мигает, а индикатор наличия коммуникации с сопроцессором **(VD32)** светится прерывисто.
2. Посредством веб-интерфейса проверьте прохождение событий от контроллера «ЯРС», для этого откройте корпус прибора или иницируйте любую тестовую тревогу.
3. Проверьте прохождение событий от «М2»/«МДС» к контроллеру «ЯРС», для этого иницируйте любую неисправность или тестовую тревогу шлейфов сигнализации.
4. Проверьте работу реле контроллера «ЯРС», для этого иницируйте событие доступа, проконтролируйте срабатывание реле с помощью мультиметра.
5. Если прибор подключён к ИСБ ITRIUM®, проверьте отображение событий и состояний элементов прибора в программе «Администратор системы» или «Мониторинг».

**Внимание.** После окончания проверки работоспособности не забудьте включить цепи управления дверными контактами.

## 4 ХРАНЕНИЕ

Хранение прибора в упаковке изготовителя должно производиться в закрытых вентилируемых складах в соответствии с условиями 3 по ГОСТ 15150-69.

Складирование прибора в упаковке изготовителя должно быть в виде штабелей высотой не более 10 упаковок.

Хранение распакованного прибора должно производиться в закрытых чистых коробках с целью защиты от запыления и загрязнения поверхностей модулей.

Воздух в помещениях для хранения прибора не должен содержать паров кислот и щелочей, а также газов, вызывающих коррозию.

Срок хранения прибора в упаковке – не более 2 лет.

## 5 ТРАНСПОРТИРОВАНИЕ

Транспортирование прибора в упаковке предприятия-изготовителя может быть произведено всеми видами закрытого и открытого транспорта при соблюдении следующих условий:

- Перевозка воздушным транспортом должна производиться в герметичных отсеках;

- Перевозка железнодорожным транспортом должна производиться в закрытых чистых вагонах;
- При перевозке открытым транспортом коробки с приборами должны быть накрыты водонепроницаемым материалом;
- При перевозке водным транспортом коробки с приборами должны быть размещены в трюме.

Значения климатических и механических воздействий при транспортировании должны быть:

- Температура от  $-50^{\circ}\text{C}$  до  $+60^{\circ}\text{C}$ ;
- Относительная влажность не более 95% при температуре  $+35^{\circ}\text{C}$ ;
- Транспортная вибрация в соответствии с группой исполнения N2 по ГОСТ Р 52931-2008.

## **6 УТИЛИЗАЦИЯ**

Изделие не представляет опасности для жизни, здоровья людей и окружающей среды. После окончания срока службы его утилизация производится без принятия специальных мер защиты окружающей среды.

## **7 ГАРАНТИИ ИЗГОТОВИТЕЛЯ**

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

Гарантийный срок эксплуатации - 18 месяцев, но не более 24 месяцев со дня отгрузки, при этом срок хранения до ввода прибора в эксплуатацию не должен превышать 6 месяцев.

## **8 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>

## 9 ПРИЛОЖЕНИЯ

[Приложение 1. Габаритные и установочные размеры изделия](#)

[Приложение 2. Линии связи](#)

[Приложение 3. Схемы внешних подключений](#)

[Приложение 4. Сеть НЕЙРОСС](#)

[Приложение 5. Пользовательский интерфейс](#)

[Приложение 6. Настройки узла](#)

[Приложение 7. Настройка общих ресурсов сети](#)

[Приложение 8. Сеть](#)

[Приложение 9. Бюро пропусков](#)

[Приложение 10. Фотоидентификация](#)

[Приложение 11. Журнал событий](#)

[Приложение 12. Журнал аудита](#)

[Приложение 13. ПО ИСБ ITRIUM®](#)

[Приложение 14. Состояния элементов прибора](#)

[Приложение 15. Администрирование узла](#)

## ПРИЛОЖЕНИЕ 1. ГАБАРИТНЫЕ И УСТАНОВОЧНЫЕ РАЗМЕРЫ ИЗДЕЛИЯ

Изделия «ЯРС» и «М2» могут поставляться в металлическом корпусе (исполнение 075, IP22; рисунок 9.1), в пластиковом корпусе (исполнение 041, IP65; рисунки 9.2 и 9.3) или без корпуса (исполнение 000; рисунок 9.4, размеры плат «ЯРС» и «М2» идентичны). Изделие «МДС» поставляется в пластиковом корпусе (исполнение 115; рисунок 9.5). сменные коммуникационные модули поставляются без корпуса.

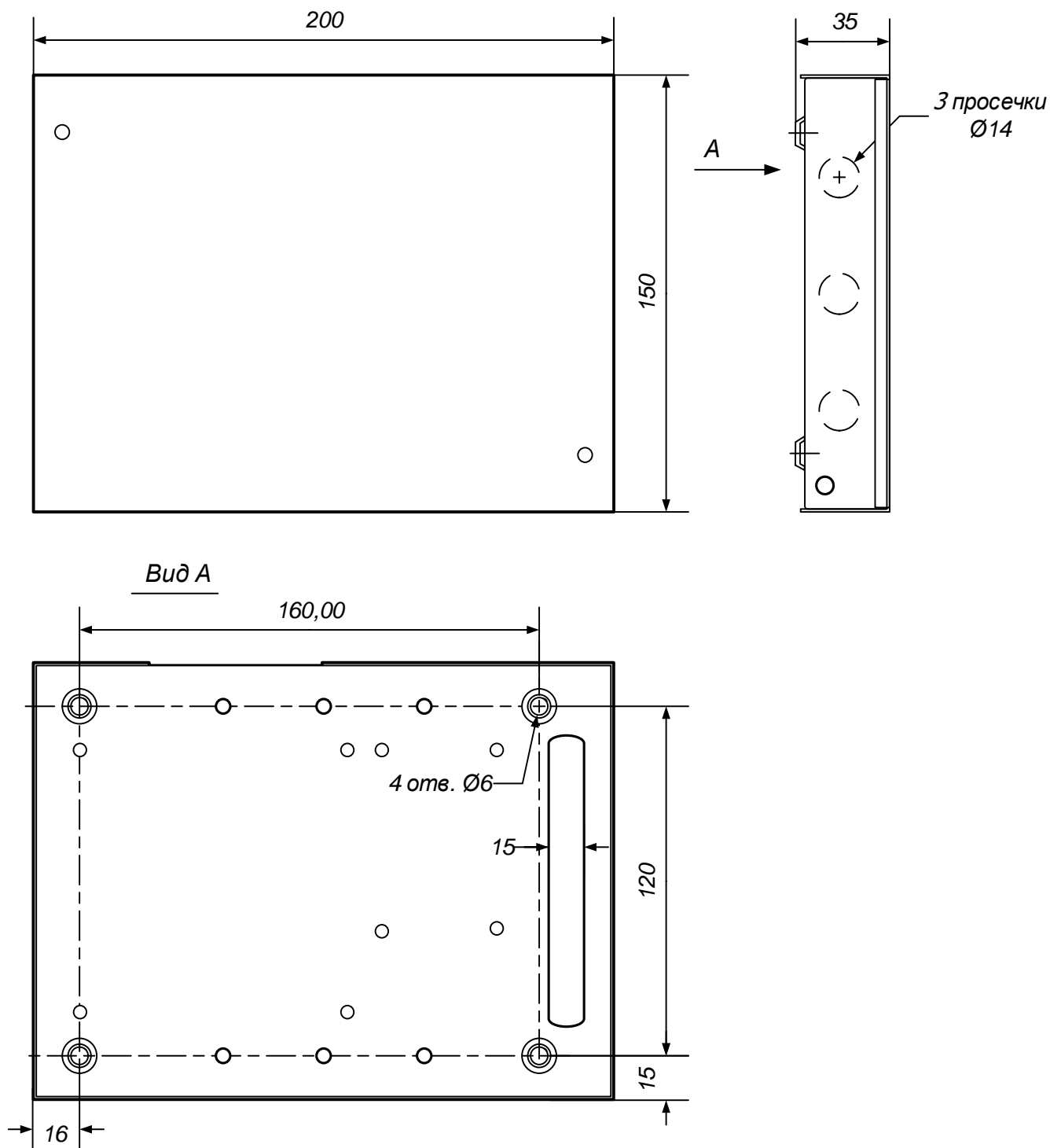


Рисунок 9.1 — Габаритные и установочные размеры изделия в корпусе 075

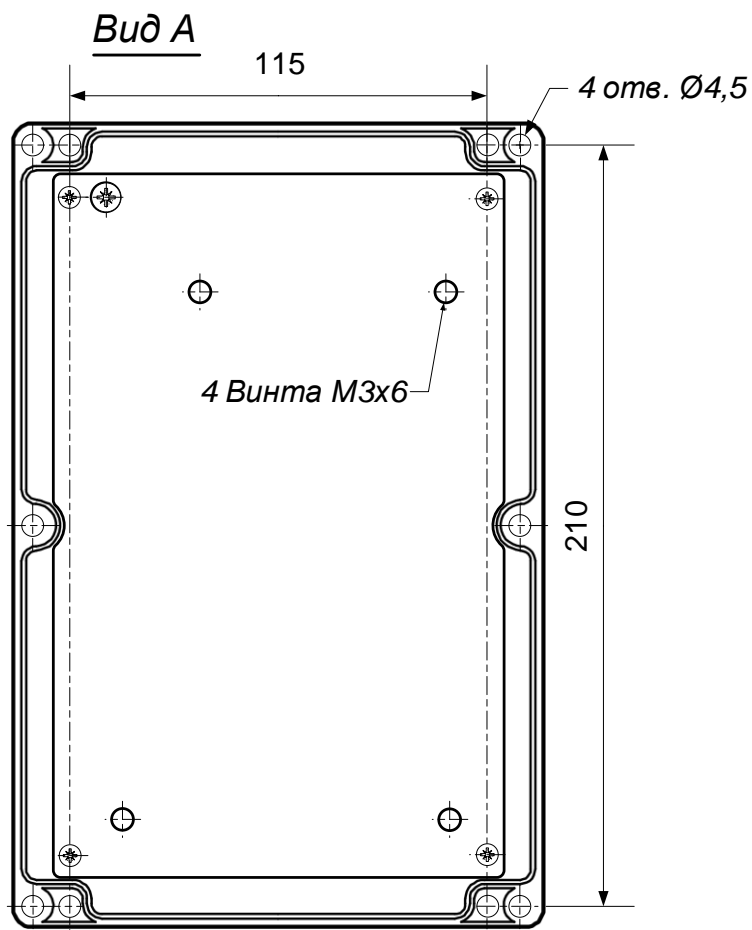
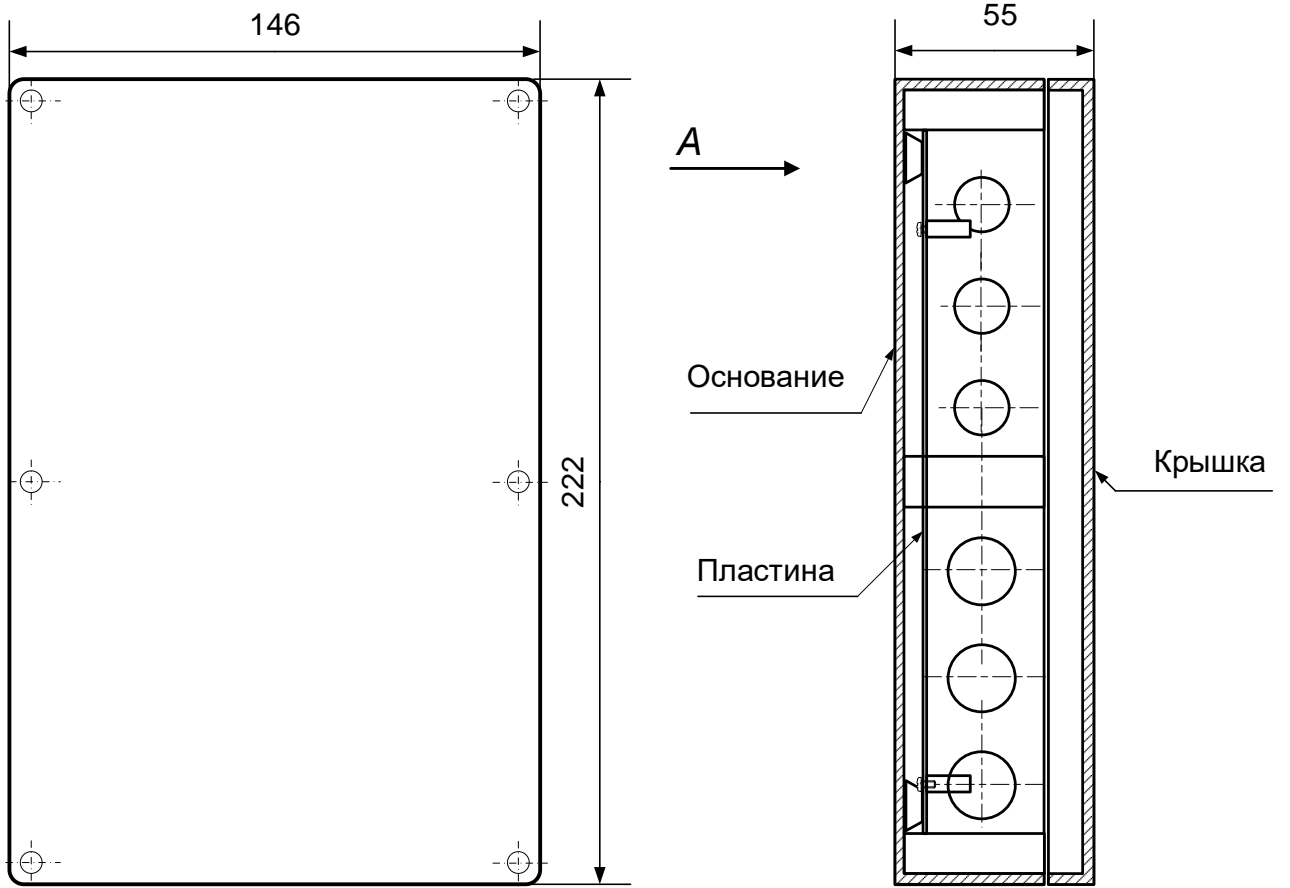


Рисунок 9.2 — Габаритные и установочные размеры изделия в корпусе 041



Рисунок 9.3 — Внешний вид корпуса 041

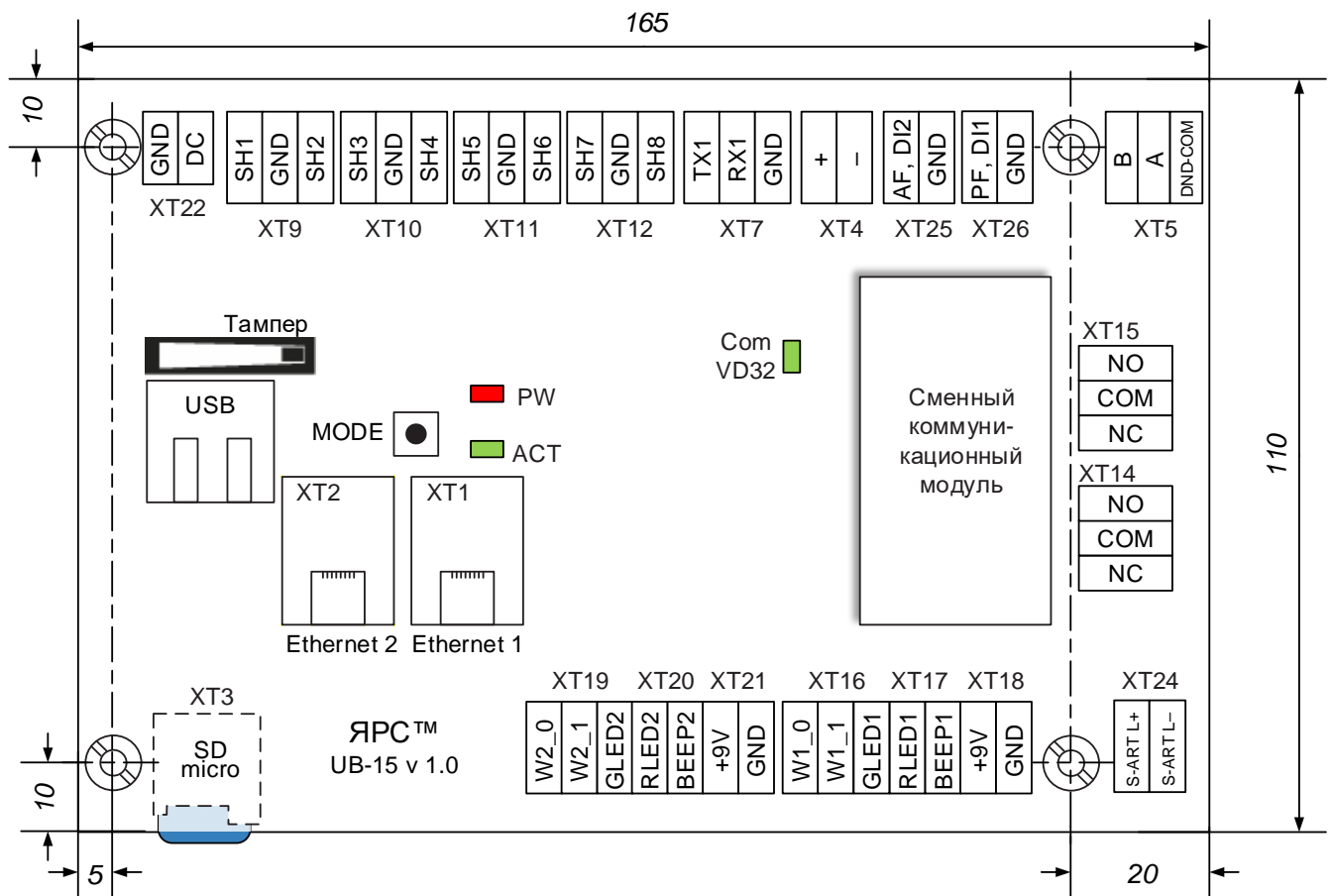


Рисунок 9.4 — Габаритные и установочные размеры платы «ЯРС» и «M2», рисунок приведён на примере платы «ЯРС»



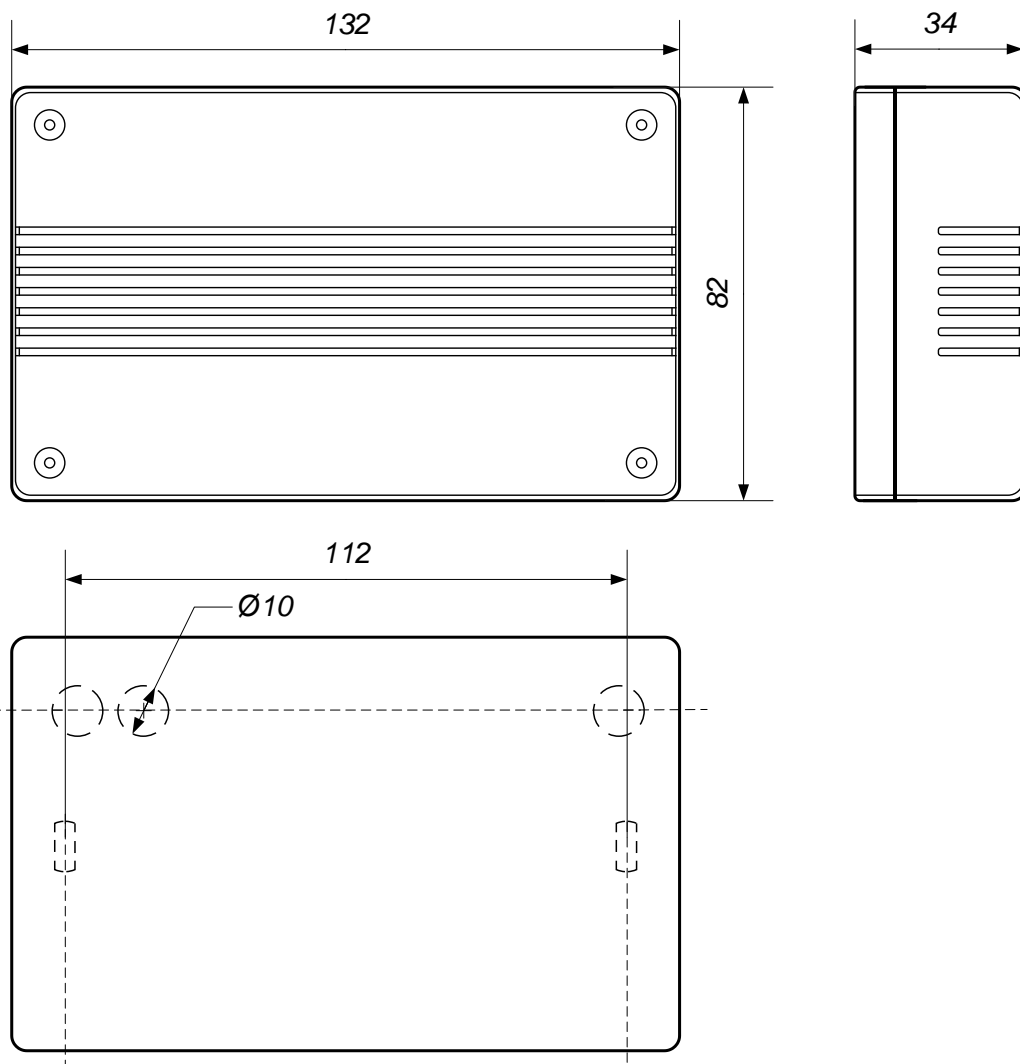


Рисунок 9.5 — Габаритные размеры изделия в корпусе 115

## ПРИЛОЖЕНИЕ 2. ЛИНИИ СВЯЗИ

### Понятие LonWorks

LonWorks® — технология интеллектуального распределённого управления, разработанная компанией Echelon® в США. Это сетевая платформа, которая предлагает мощные средства для построения распределённых систем контроля и управления, принята в качестве стандарта сетей автоматизации зданий во многих странах и регламентируется требованиями международного стандарта ANSI/EIA709.1. Платформа LonWorks

Сеть, использованная в LonWorks, называется LON® (Local Operating Network). В сети LON интеллектуальные устройства, называемые узлами, общаются с помощью протокола LonTalk®.

Взаимодействие обеспечивается с помощью чипа Neuron®, размещённого в каждом узле сети LON. Каждый Neuron имеет уникальный идентификатор Neuron ID.

### Топология сети LonWorks

Тип канала TP/FT-10 позволяет совмещать линию данных и линию электропитания и реализовать различные топологии сети («шина», «звезда», «кольцо», «произвольная»).

Стандартная скорость передачи в сети TP/FT-10 составляет 78 Кбит/с, что соответствует пропускной способности примерно 180 пакетов/с.

Существует два вида топологии сети: шинная (с отводами и без) и произвольная (рисунок 9.6).

Для каждой топологии существуют определённые ограничения на длины кабелей, которые связаны с физической природой среды передачи и распространением в ней электрических сигналов. При использовании стандартного кабеля Cat5 и произвольной топологии ограничение составляет 450 метров, в случае шинной топологии - 900 м. Специальные кабели, например, Belden 8471 или 85102 с диаметром жилы 1,3 мм увеличивают эти расстояния до 500 м и 2700 м для соответствующих топологий. Также возможно использование кабеля JY(St) Y 2x2x0.8. При этом ограничения составят 500 м и 900 м для произвольной и шинной топологии соответственно. Расстояние между двумя узлами при произвольной топологии не должно превышать 320 м. Возможно применение и других кабелей, которые обеспечивают необходимые электрические параметры.

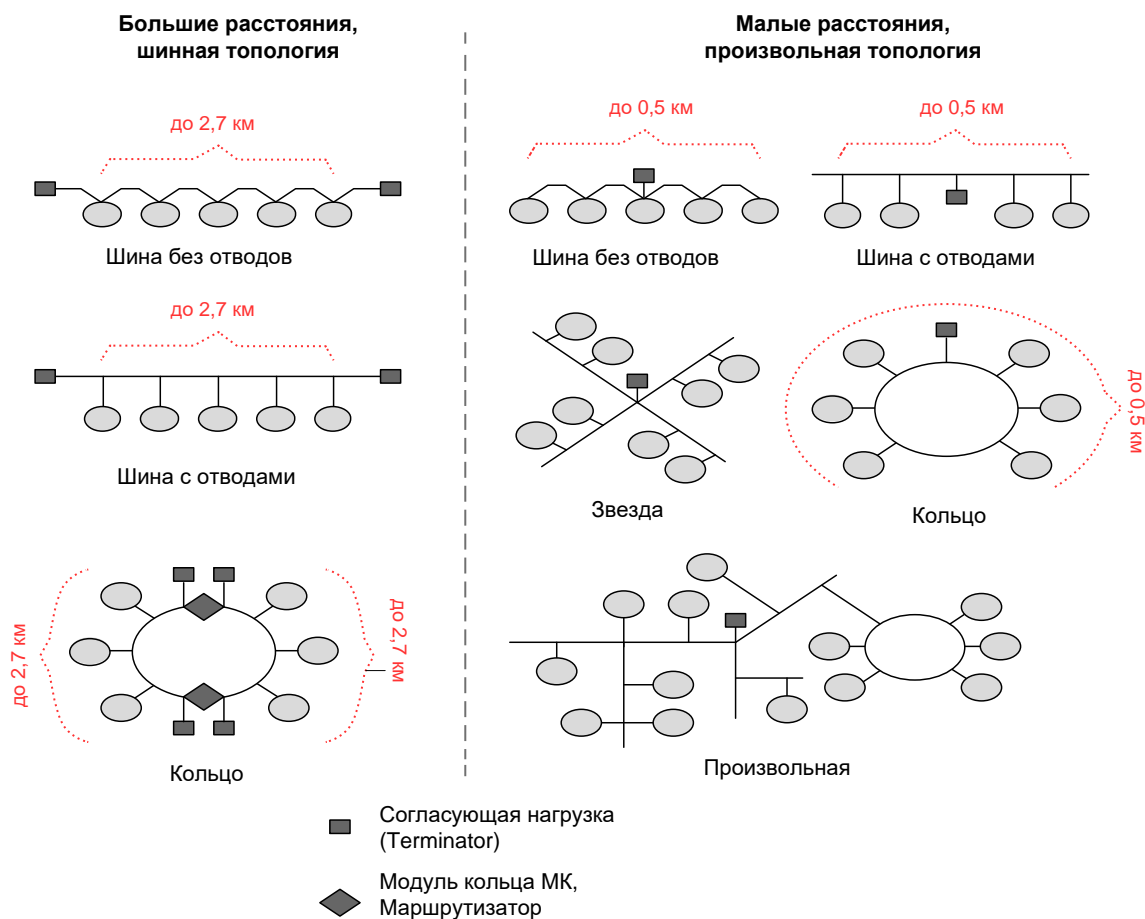


Рисунок 9.6 — Топологии сети LonWorks

Максимальное количество устройств в одном сегменте сети LonWorks — 64.

При использовании топологии типа «шина» устройства соединяются последовательно. Возможно подключение с отводами, при этом длина отвода не должна превышать 3 м.

На концах кабеля необходимо установить согласующие элементы (например, «Согласующая нагрузка (Terminator)»). Произвольная топология сети не имеет никаких ограничений в направлениях соединения устройств, однако, как сказано выше, имеет более жёсткие ограничения на допустимую длину кабеля. Для организации сети произвольной топологии используется один согласующий элемент, который устанавливается в центре сети. Если устройство имеет согласующую нагрузку на плате («ЯРС», M2), достаточно установить переключатель BUS/FREE.

Сеть может состоять из нескольких различных по топологии сегментов, которые следует соединять специальными устройствами – маршрутизаторами (например, «Модуль кольца МК, маршрутизатор»). Маршрутизаторы фильтруют пакеты, что повышает надёжность и жизнеспособность системы, уменьшает трафик и нагрузку на линии связи.

Пример использования маршрутизатора смотрите на рисунке 9.7.

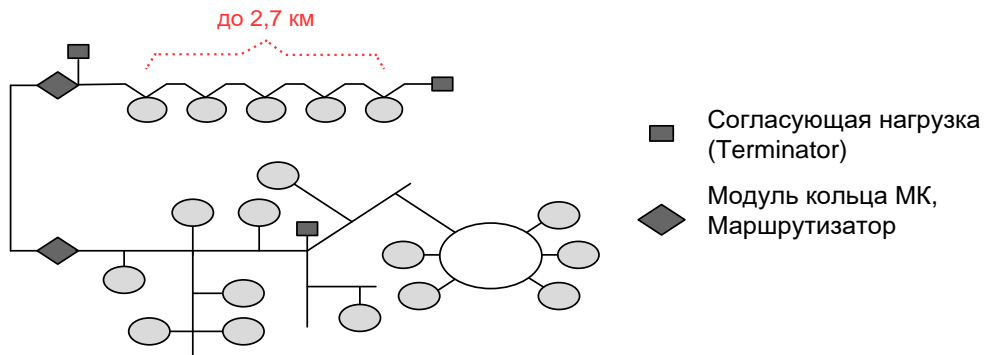


Рисунок 9.7 — Соединение сегментов сети

В случае объединения двух сегментов сети с шинной топологией в кольцо, в два раза увеличивается допустимая длина кабеля, однако на границах сегментов также требуется установка маршрутизаторов, которые предотвращают циклическую передачу пакетов данных (рисунок 9.6).

## ПРИЛОЖЕНИЕ 3. СХЕМЫ ВНЕШНИХ ПОДКЛЮЧЕНИЙ

### 1. Разъёмы платы электроники

Таблица 9.1 — Разъёмы платы электроники «ЯРС»

Описание	Разъём
Разъёмы подключения сигнала неисправности блока питания	PF(DI1), GND
Разъёмы подключения сигнала неисправности аккумулятора	AF(DI2), GND
Разъёмы подключения питания	DC, GND
Выход питания модема (COM), с управлением и защитой от КЗ	+ Питание модема, - Питание модема
Интерфейс RS-232	RX1, TX1, GND
Разъёмы подключения к сети Ethernet	Ethernet 1, Ethernet 2
Входы подключения шлейфов сигнализации (резистивный шлейф)	SH1, GND, SH2, SH3, GND, SH4, SH5, GND, SH6, SH7, GND, SH8
Входы подключения дверных контактов (резистивный шлейф)	ДК1 (SH1, GND), ДК 2 (SH3, GND)
Входы подключения кнопок выхода	KB 1 (SH2, GND), KB 2 (SH4, GND)
Выходы реле	Реле 1 (NC, COM, NO), Реле 2 (NC, COM, NO)
Разъём подключения считывателя 1	W1_0, W1_1, GLED1, RLED1, BEEP1, +9V, GND
Разъём подключения считывателя 2	W2_0, W2_1, GLED2, RLED2, BEEP2, +9V, GND
Разъём для карты памяти	XT3

Таблица 9.2 — Разъёмы платы электроники «M2»

Описание	Разъёмы
Разъём подключения сигнала неисправности блока питания	PF, GND
Разъём подключения питания	Vin, GND
Разъём подключения считывателя 1	W1_0, W1_1, GLED1, RLED1, BEEP1, +9V, GND
Разъём подключения считывателя 2	W2_0, W2_1, GLED2, RLED2, BEEP2, +9V, GND
Интерфейс Lonworks	LON A, LON B
Входы подключения шлейфов сигнализации (резистивный шлейф)	SH1 (DOOR1), GND, SH2 (DOOR2), SH3, GND, SH4, SH5, GND, SH6, SH7, GND, SH8
Входы подключения дверных контактов (резистивный шлейф)	SH1 (DOOR1), GND, SH2 (DOOR2)
Входы подключения кнопок выхода (сухой контакт)	EPB1, GND, EPB2
Выходы управления	RELAY1, RELAY2, RELAY3, RELAY4, RELAY5, RELAY6, RELAY7, RELAY8

<b>Описание</b>	<b>Разъёмы</b>
Выходы управления замком	Замок 1 (COM, NC, NO), Замок 2 (COM, NC, NO)

Таблица 9.3 — Разъёмы платы электроники «МДС»

<b>Описание</b>	<b>Разъёмы</b>
Разъёмы подключения питания	DC IN, GND
Разъем подключения считывателя	D0, D1, GLED, RLED, BEEP, +9V, GND
Интерфейс Lonworks	LON A, LON B
Входы подключения шлейфов сигнализации (резистивный шлейф)	RIN1, GND, RIN2, DOOR, GND
Входы подключения дверного контакта (резистивный шлейф)	DOOR, GND
Вход подключения кнопки выхода (сухой контакт)	EPB, GND
Выход управления замком	NC, COM, NO

## 2. Подключение устройства к источнику питания

Питание контроллера «ЯРС» осуществляется от источника питания постоянного тока 12 – 24 В. Для этого на плате контроллера предусмотрен вход питания.

Дискретный вход «Неисправность ИП» предназначен для приёма сигнала о неисправности внешнего источника питания. Данный вход используется в случае, когда питание устройства осуществляется от источника бесперебойного питания, который самостоятельно выполняет функции контроля исправности первичного источника питания и формирование дискретного сигнала о возникшей неисправности в виде замыкания контактов механического или оптореле.

Дискретный вход «Неисправность аккумулятора» предназначен для приёма сигнала о неисправности аккумулятора источника питания. Данный вход используется в случае, когда питание устройства осуществляется от бесперебойного источника питания, который самостоятельно выполняет функции контроля исправности аккумулятора и формирования дискретного сигнала о возникшей неисправности в виде замыкания контактов механического или оптореле.

Схема подключения источника питания контроллера «ЯРС» приведена на рисунке 9.8.

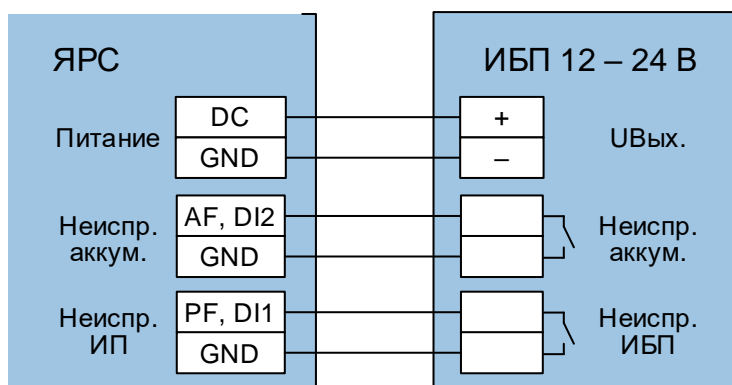


Рисунок 9.8 – Схема подключения источника питания «ЯРС»

Питание модуля «М2» осуществляется от источника постоянного тока (блока резервного питания) 12 – 24 В. Для этого на плате модуля предусмотрен вход питания. Допускается питание нескольких модулей от одного БРП.

Дискретный вход «Неисправность ИП» предназначен для приёма сигнала о неисправности внешнего источника питания. Данный вход используется в случае, когда питание устройства осуществляется от источника бесперебойного питания, который самостоятельно выполняет функции контроля исправности первичного источника питания и формирование дискретного сигнала о возникшей неисправности в виде замыкания контактов механического или оптореле.

Схема подключения источника питания модуля «М2» приведена на рисунке 9.9.

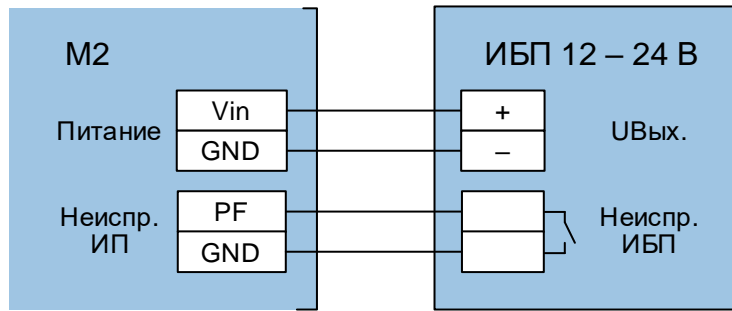


Рисунок 9.9 – Схема подключения источника питания «M2»

Питание модуля «МДС» осуществляется только от источника постоянного тока 12 В. Для этого на плате модуля предусмотрен вход питания. Допускается питание нескольких модулей от одного БРП.

### 3. Подключение к сети Lonworks

Схема подключения «ЯРС», «M2» и «МДС» к сети LonWorks приведена на рисунке 9.10. Дополнительная информация представлена в разделе [Топология сети LonWorks](#).

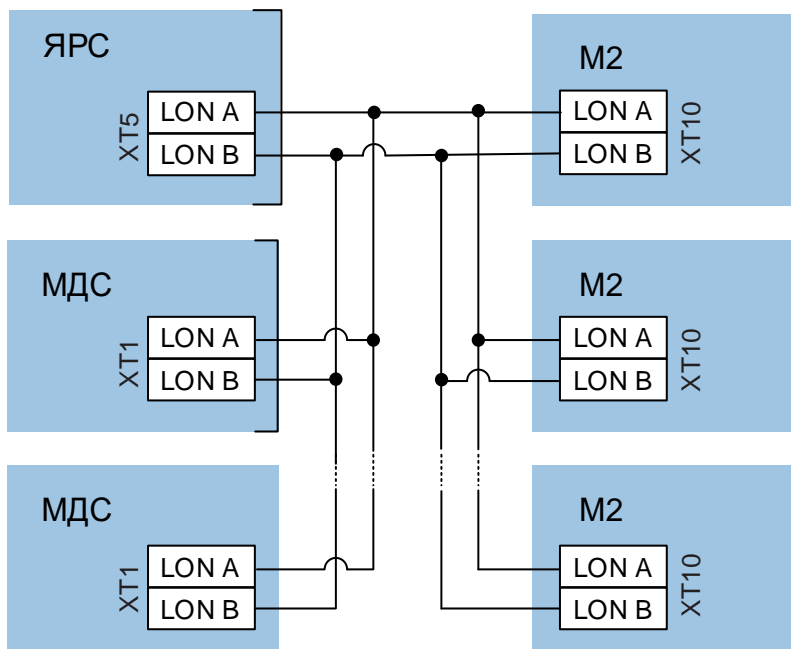


Рисунок 9.10 — Подключение «ЯРС», «M2», «МДС» к сети LonWorks

## 4. Схемы подключения внешнего оборудования

### Подключение GSM-модема

Прибор снабжён двумя интерфейсами RS-232 и двумя интерфейсами USB, предназначенными для подключения дополнительного внешнего оборудования.

Для работы с GSM-модемом предназначен один порт USB и один порт RS-232.



**Примечание.** При выборе модема рекомендуется отдавать предпочтение USB-модему. Для подключения модема используется порт **USB1** (верхний).

При использовании COM-портового модема (например, Fargo Maestro 100) используется разъем **XT7** (см. рисунок 1.5). Кроме того, дополнительно предусмотрен управляемый выход питания (**XT4**) с нагрузочной способностью 22 В при токе 0,4 А и защитой от КЗ с порогом срабатывания защиты 1 А. Схема подключения модема приведена на рисунке 9.11.

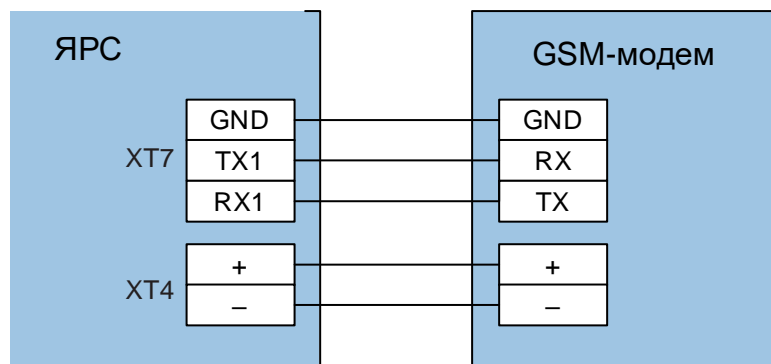


Рисунок 9.11 – Пример подключения GSM-модема по интерфейсу RS-232 с питанием от прибора

### Подключение к сети Ethernet

В каждый контроллер «ЯРС» встроен сетевой коммутатор, обеспечивающий управление трафиком и гальваническую развязку смежных сегментов сети Ethernet.

Подключение нескольких устройств «ЯРС» к сети Ethernet возможно по классической схеме, используя топологию типа «звезда» (рисунок 9.12), либо по схеме «коммутируемой IP-шины» (рисунок 9.13), также возможно замкнуть «шину» в «кольцо». С помощью комбинаций вышеперечисленных схем и согласно правилам сетевых подключений возможно построение произвольной сетевой архитектуры (рисунок 9.14).

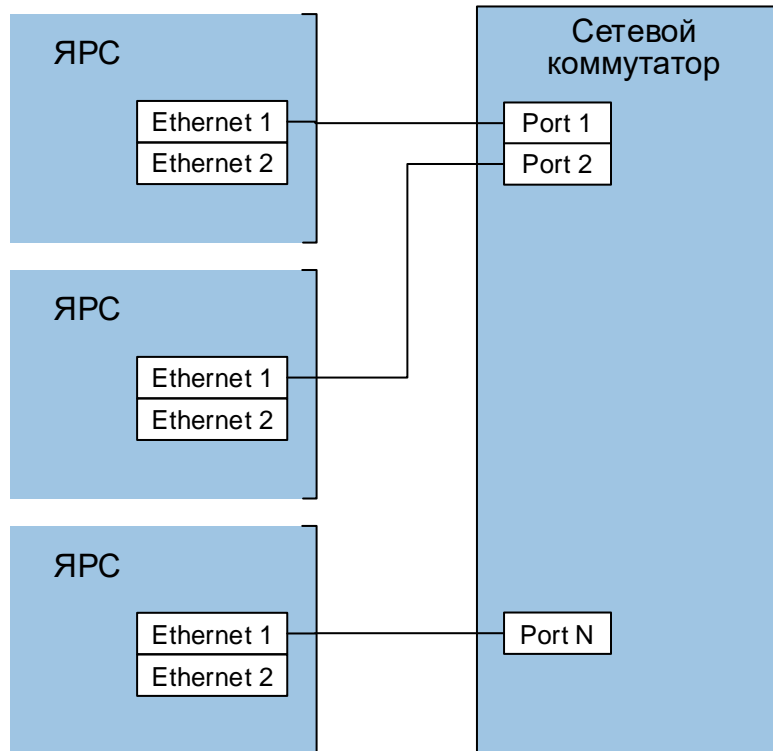


Рисунок 9.12 – Схема подключения приборов к сети Ethernet. Классический вариант

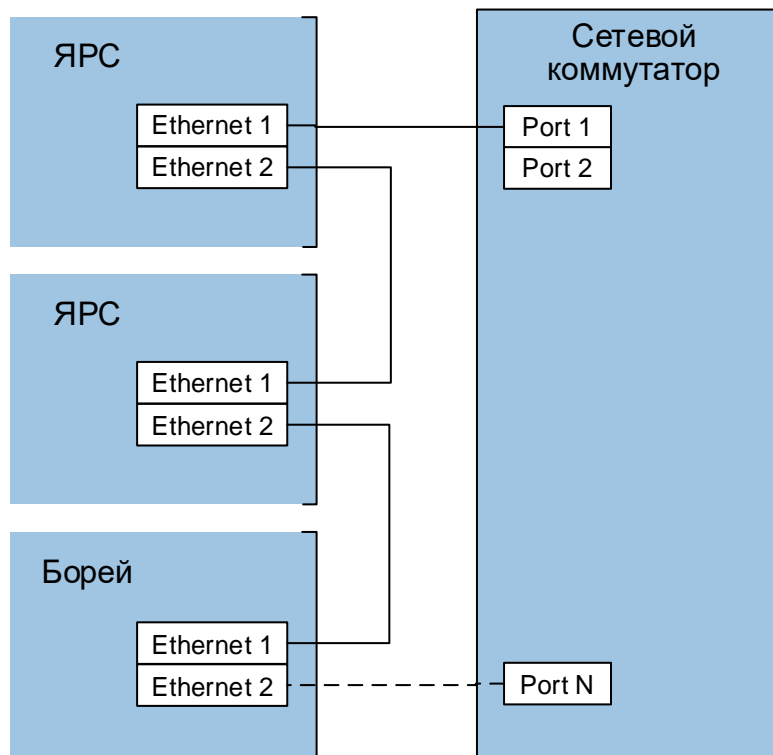


Рисунок 9.13 — Схема подключения приборов к сети Ethernet. «Коммутируемая IP-шина»

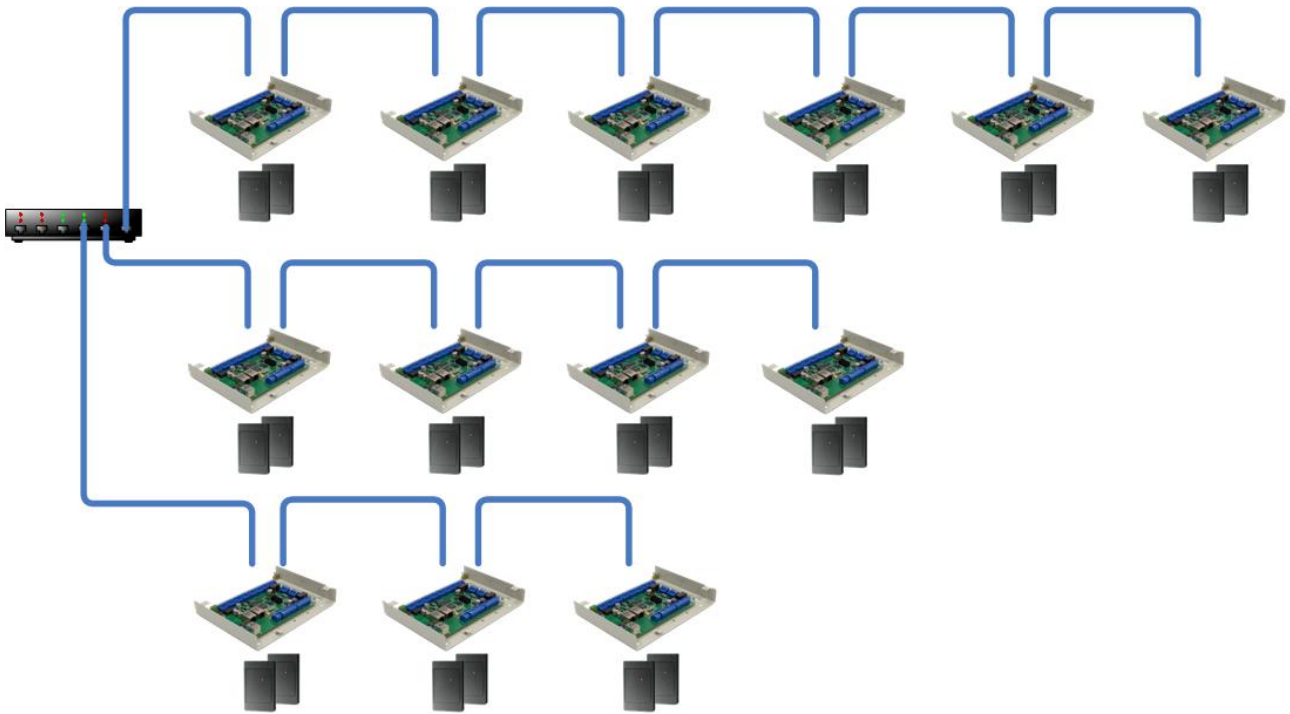


Рисунок 9.14 — Схема подключения приборов к сети Ethernet. Произвольная архитектура

### Подключение шлейфов охранной сигнализации

На плате контроллера «ЯРС» и модуля «М2» предусмотрено по 8 входов для подключения шлейфов охранной сигнализации (ШС). На плате «МДС» предусмотрено три входа для ШС. Маркировка разъемов приведена в разделе [Разъёмы платы электроники](#).

Тип ШС – резистивный многопороговый, для подключения используются резисторы. Пример подключения ШС с извещателями, имеющими выход типа «сухой контакт», к входам устройства приведён на рисунке 9.15. Тип контактов извещателя (нормально замкнут или нормально разомкнут) указывается в веб-интерфейсе.

Типовая схема подключения на примере «ЯРС» приведена на рисунке 9.15.

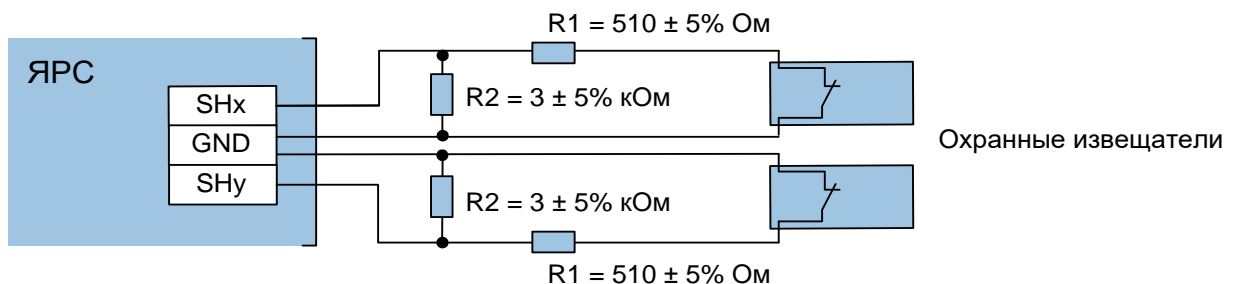


Рисунок 9.15 – Схема подключения ШС с датчиками типа «сухой контакт»

### Подключение считывателей

На плате «ЯРС» предусмотрено 2 входа для подключения считывателей СКУД. Устройство может работать как со считывателями с интерфейсом Wiegand (схема

подключения приведена на рисунке 9.16), так и со считывателями с интерфейсом 1-Wire (схема подключения приведена на рисунке 9.17).

Возможно подключение считывателей с использованием четырехпроводного кабеля. Пример подключения для считывателей multiClass SE (iClass SE) от HID Global (например, RP10) приведён на рисунке 9.18.

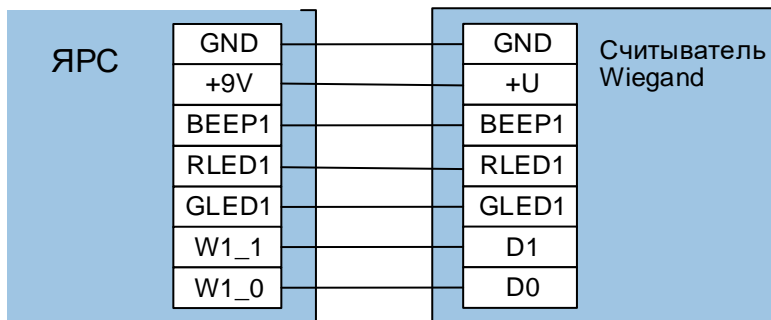


Рисунок 9.16 — Схема подключения считывателя с интерфейсом Wiegand

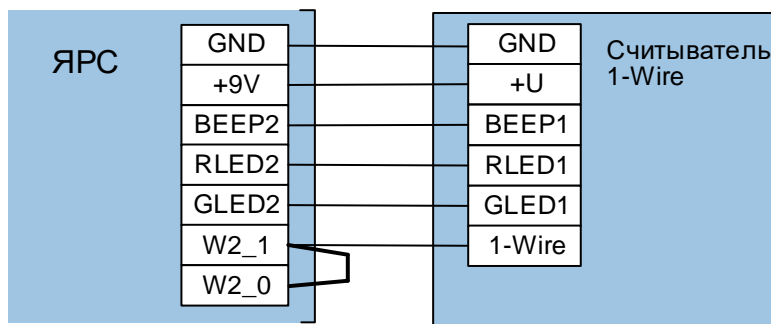


Рисунок 9.17 — Схема подключения считывателя с интерфейсом 1-Wire

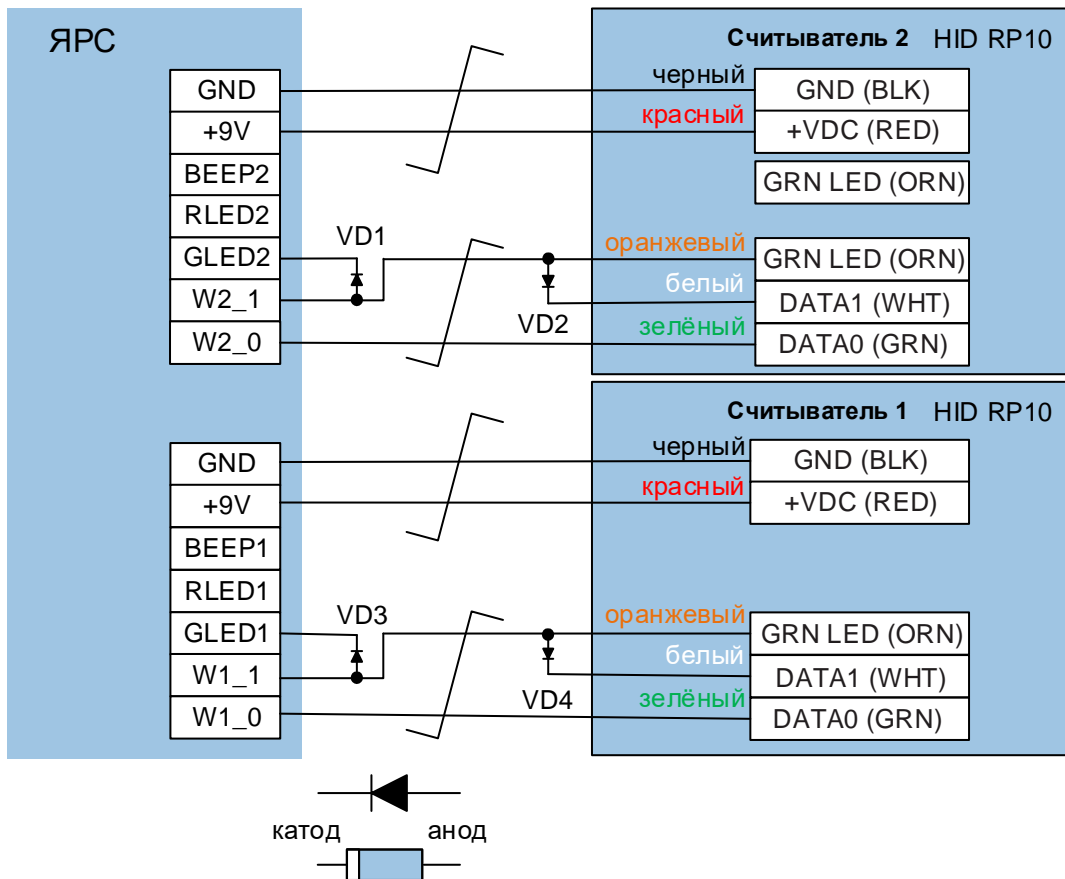


Рисунок 9.18 — Схема подключения считывателя HID RP10 (с использованием четырехпроводного кабеля)

**Примечание.** На схеме 9.18 диоды VD1, VD3 устанавливаются в непосредственной близости от контроллера; диоды VD2, VD4 устанавливаются в непосредственной близости от считывателя; тип диодов 1N4007 или аналог.

На плате модуля «M2» предусмотрено два входа для подключения считывателя с интерфейсом Wiegand (схема подключения приведена на рисунке 9.19).

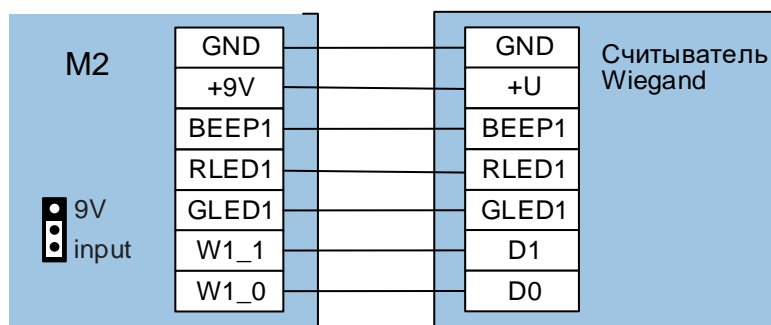


Рисунок 9.19 — Схема подключения считывателя с интерфейсом Wiegand к модулю «M2»

**Внимание.** Для расширения списка поддерживаемых считывателей (за счёт требующих входного напряжения более 9 В) предусмотрен переключатель питания **reader power**. Установив переключку в значение **input**, можно регулировать входное напряжение питания считывателей за счёт регулировки питания модуля в диапазоне 10,8 ÷ 28 В.

На плате модуля «МДС» предусмотрен один вход для подключения считывателя с интерфейсом Wiegand (схема подключения приведена на рисунке 9.20).

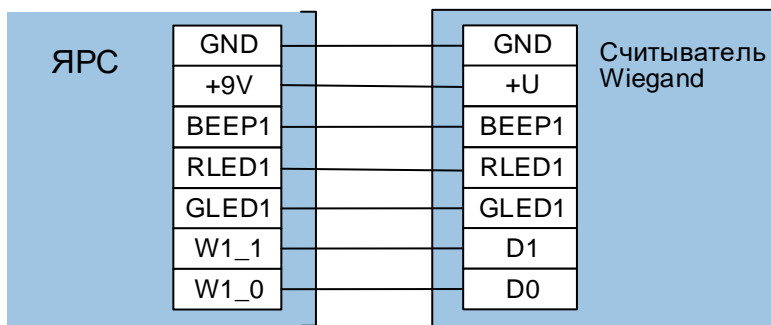


Рисунок 9.20 — Схема подключения считывателя с интерфейсом Wiegand к модулю «МДС»

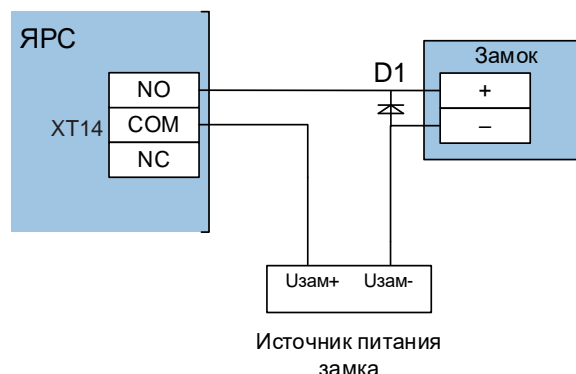
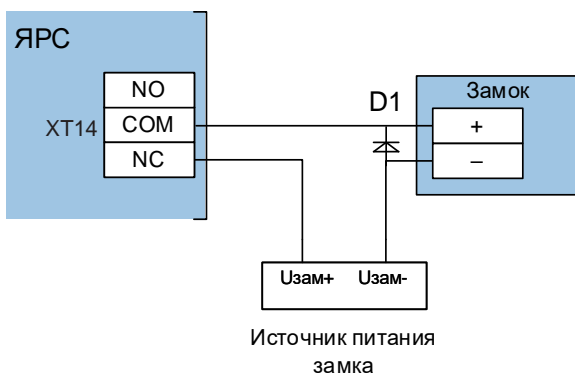
### Подключение замковых устройств

На платах контроллера «ЯРС» и модуля «М2» предусмотрено 2 релейных выходов для подключения замковых устройств в СКУД. Каждый выход содержит группу переключающихся контактов (NC, COM, NO). Типовые схемы подключения замкового устройства приведены на рисунке 9.21.

#### Подключение замка в двусторонней точке доступа

Управление замком выключением питания

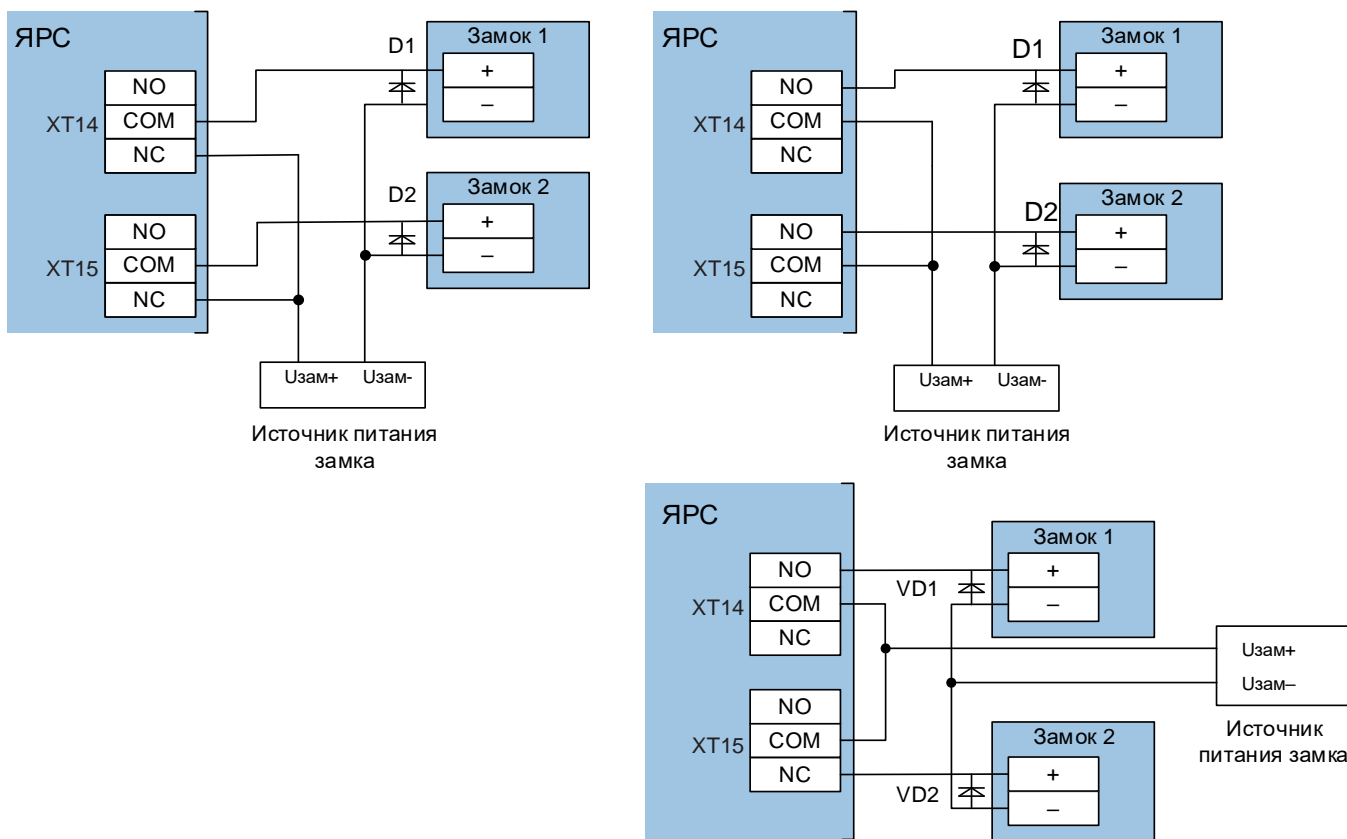
Управление замком включением питания



## Подключение замков в односторонних точках доступа

Управление замками выключением питания

Управление замками включением питания



**Замок 1** нормально-открытого типа,  
**Замок 2** нормально-закрытого типа.

Рисунок 9.21 — Схема подключения замкового устройства

**Примечание.** Для электромеханических замков диоды **VD1**, **VD2** устанавливаются в непосредственной близости от замка; тип диодов **1N4007** или аналог.

На плате «МДС» предусмотрен один релейный выход для подключения замковых устройств в СКУД. Выход содержит группу переключающихся контактов (NC, COM, NO). Типовые схемы подключения замкового устройства приведены на рисунке 9.22. Схема подключения в случае организации двусторонней точки доступа на базе двух модулей «МДС» приведена на рисунках 9.23 и 9.24.

Управление замками выключением питания

Управление замками включением питания

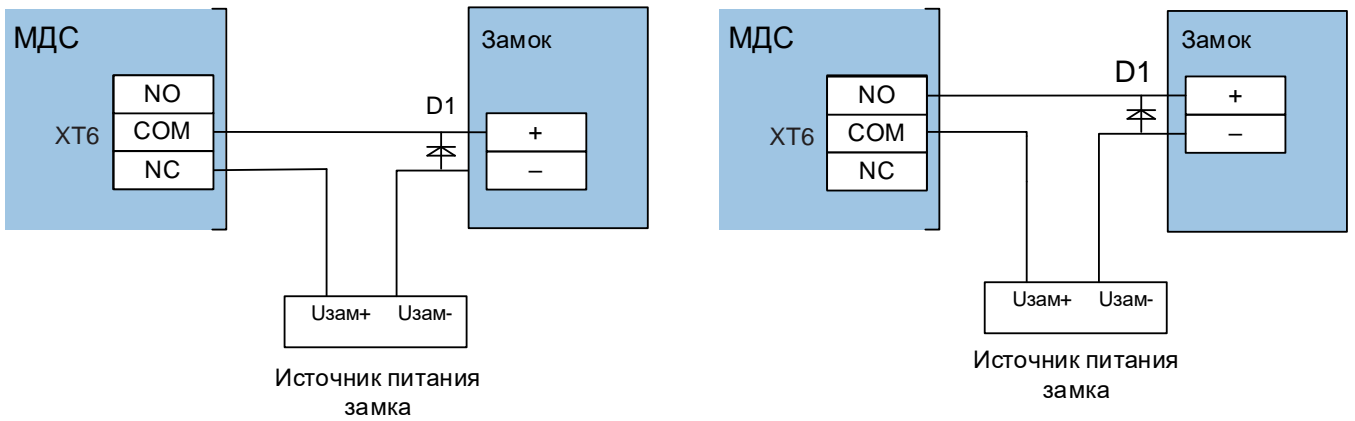


Рисунок 9.22 — Схема подключения замкового устройства к «МДС»

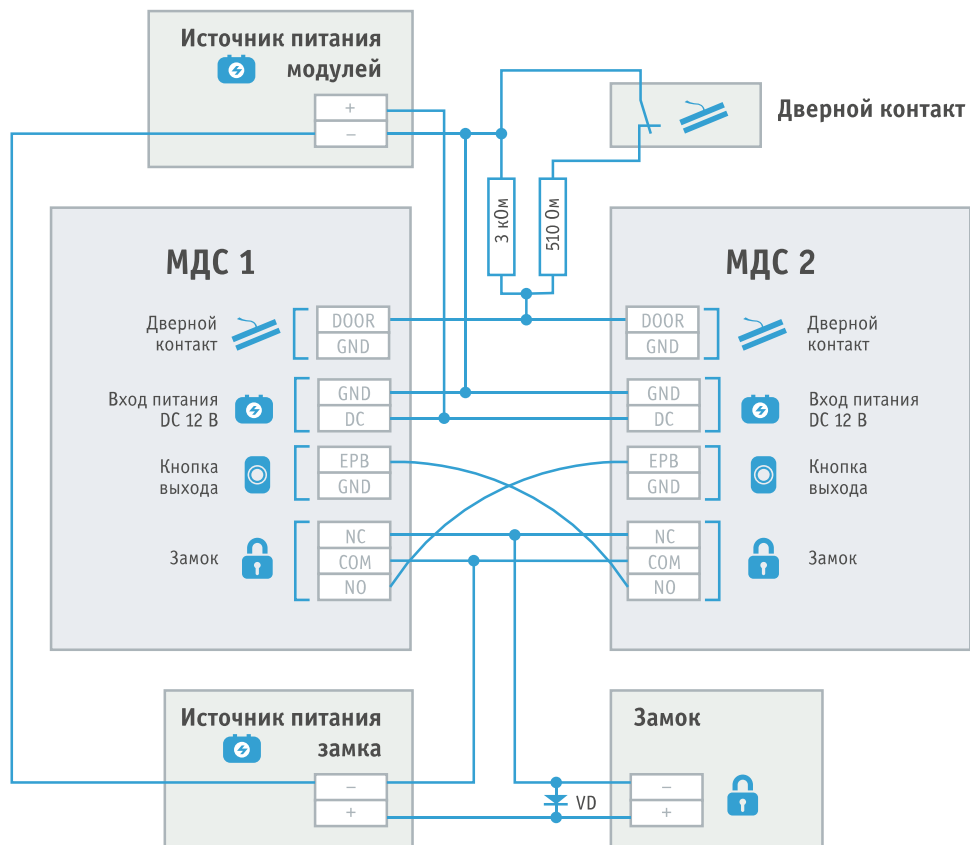


Рисунок 9.23 — Двусторонняя точка доступа. Схема подключений.  
Управление замком выключением питания



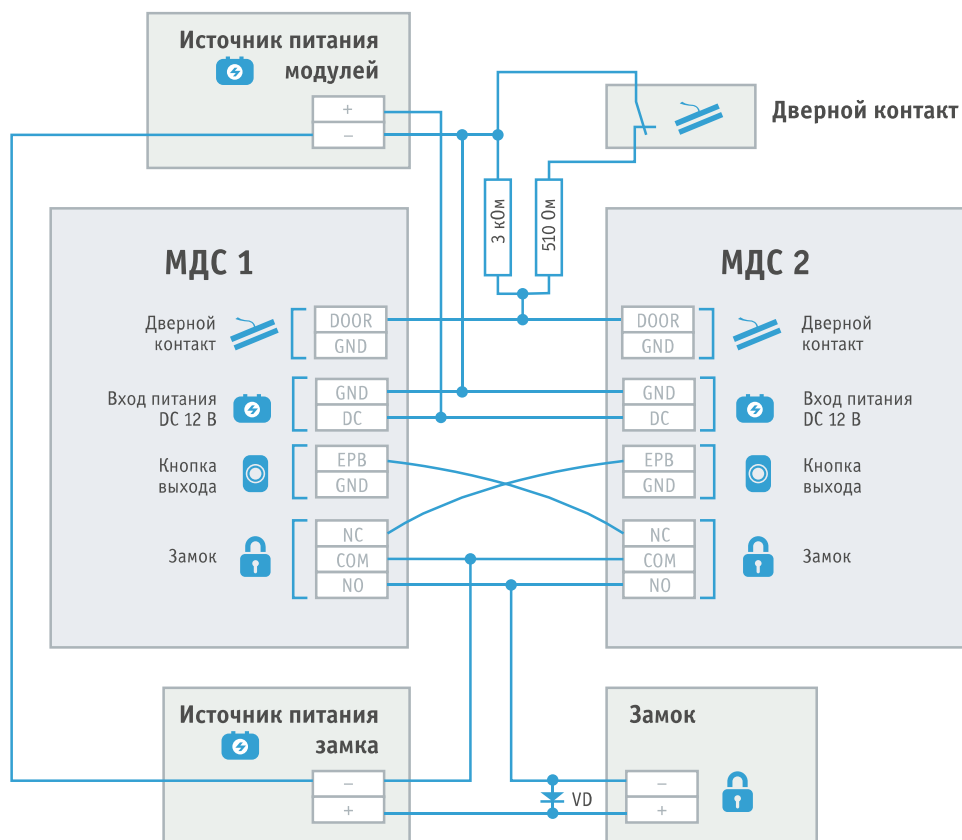


Рисунок 9.24 — Двусторонняя точка доступа. Схема подключений.  
Управление замком включением питания

### Подключение дверных контактов и кнопок выхода

Для подключения к «ЯРС», «М2» и «МДС» дверных контактов используются входы подключения резистивных многопороговых шлейфов сигнализации. Входы могут использоваться одновременно и в СКУД и как охранные шлейфы. Для входов дверных контактов модулей «М2» и «МДС» использование резисторов является обязательным. Для входов дверных контактов «ЯРС» использование резисторов является предпочтительным, так как даёт возможность получать состояния неисправности ([Обрыв], [Короткое замыкание]). В случае отсутствия необходимости контроля неисправности (например, при подключении турникета), резисторы не используются. Кнопки выхода подключаются напрямую. Маркировка разъёмов приведена в разделе [Разъёмы платы электроники](#). Типовая схема подключения на примере ЯРС приведена на рисунке 9.25.

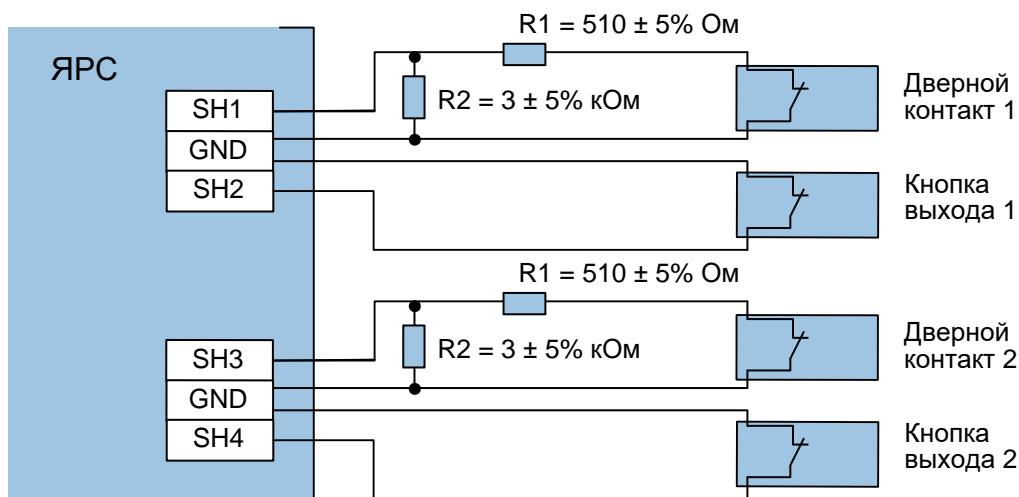


Рисунок 9.25 — Схема подключения дверных контактов и кнопок выхода

При организации двусторонней точки доступа на базе двух «МДС» необходимо замкнуть сигнал открытия замка одного модуля на кнопку выхода другого модуля и соединить шлейфы дверных контактов (см. раздел [Подключение замковых устройств](#)). Также в настройках точек доступа обоих модулей соответственно нужно задать «привязку» к другому модулю и указать для кнопки выхода состояние инициации прохода: «разомнут» для схемы управления замком включением питания; «замнут» — для схемы с управлением выключением питания (см. раздел [Настройка М2/МДС](#)).

### Подключение турникета

Для подключения турникета к «ЯРС» используются входы подключения шлейфов (SH1, GND), (SH3, GND) и оба реле прибора. Для подключения турникета к «М2» используются входы (DOOR1, GND, DOOR2) и оба реле модуля. На входы подключения шлейфов замыкаются контакты выходного сигнала турникета о факте проворота в направлении А или Б, реле подают сигнал разблокировки турникета в направлении А или Б (рисунок 9.26).

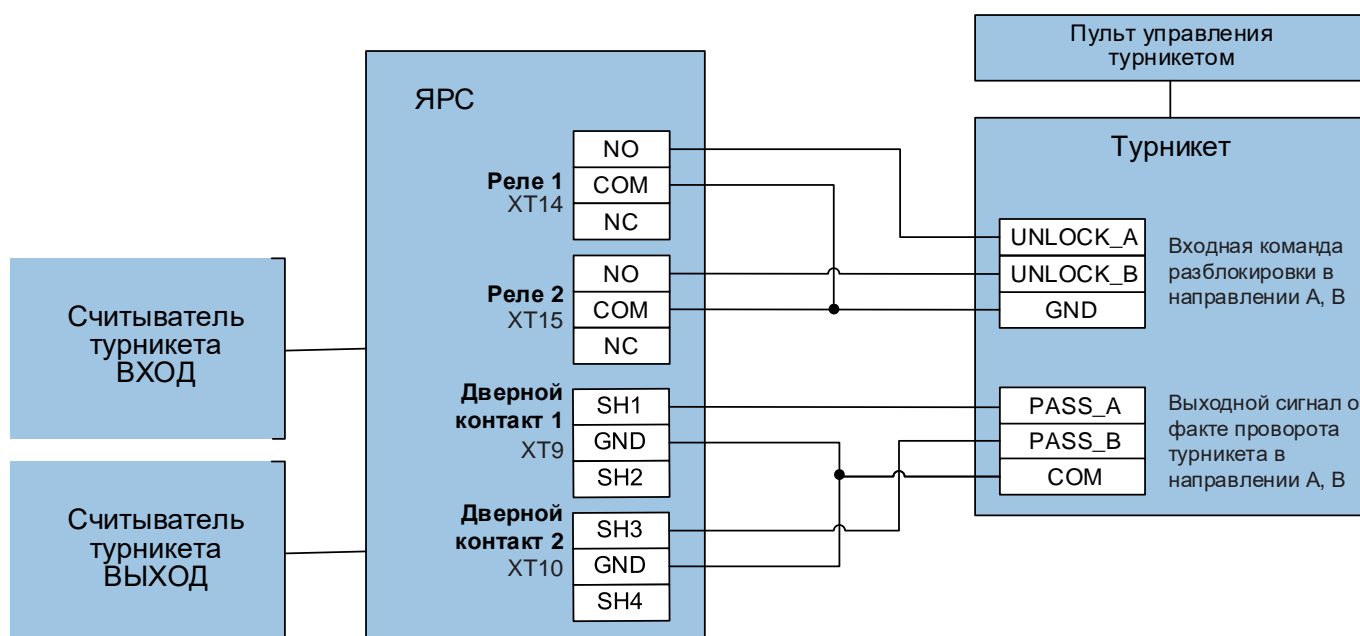


Рисунок 9.26 — Схема подключения турникета

### Подключение картоприёмника

При необходимости использования картоприёмника для изъятия разовых пропусков, необходимо реле прибора «ЯРС» или модуля «М2» замкнуть на входной контакт картоприёмника для передачи команды на изъятие карты, а выходной сигнал замкнуть на кнопку выхода (сигнал об успешном изъятии имитирует нажатие кнопки выхода).

При необходимости использования картоприёмника совместно с системой контроля доступа по многократным пропускам, требуется два прибора «ЯРС» или два модуля «М2». При этом первый прибор предназначен для обеспечения контроля доступа без изъятия пропусков, а второй – для работы с картоприёмником. Пример подключения турникета и картоприёмника см. на рисунке 9.27.

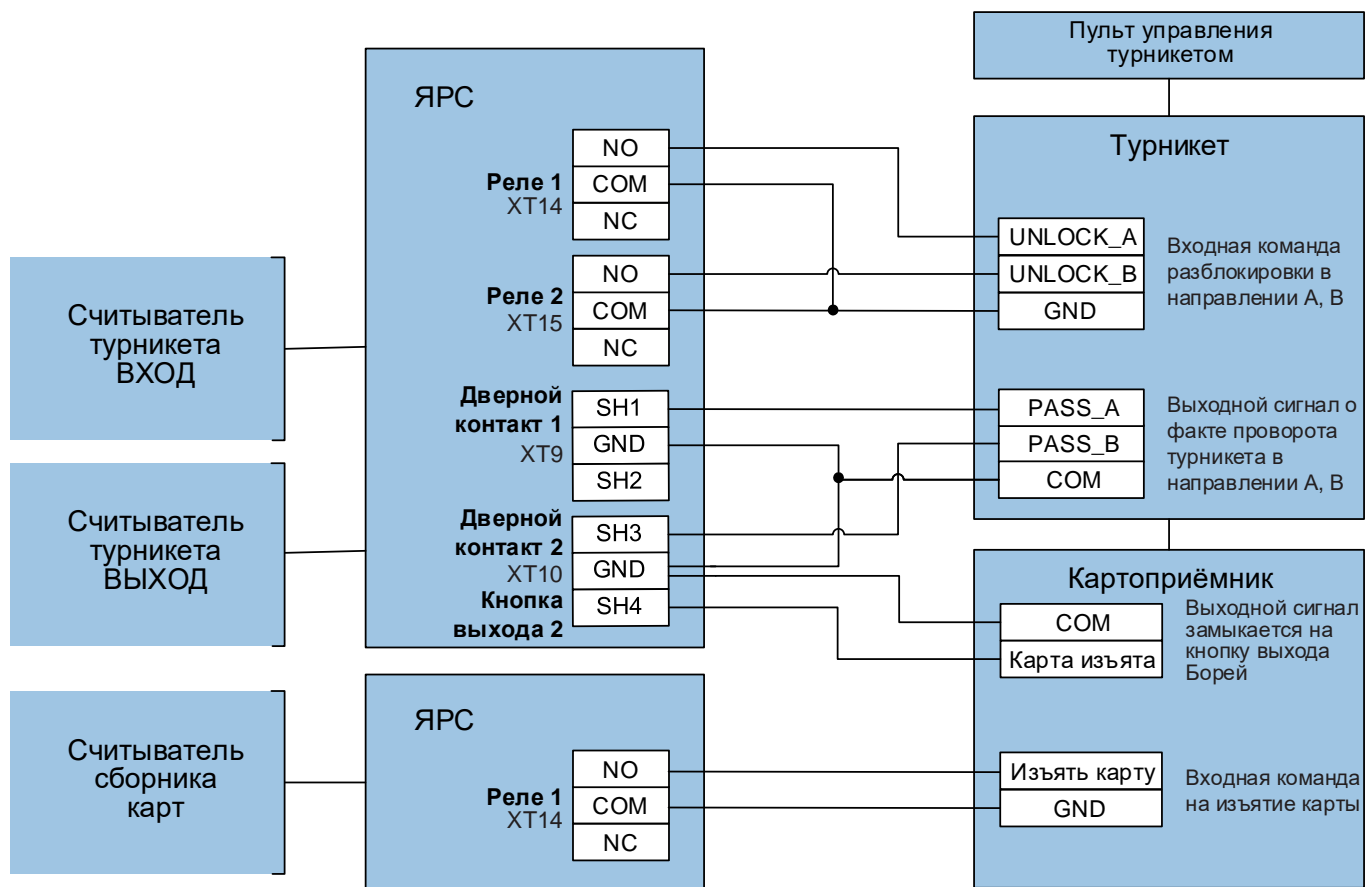


Рисунок 9.27 — Схема подключения картоприёмника

**Примечание.** Планируется выпуск «прошивки» «ЯРС» для работы с турникетами, реализующими возможность изъятия карт. При этом потребуется только один прибор «ЯРС».

При необходимости подключения турникета и картоприёмника к модулям «МДС», используются три модуля «МДС» (пример подключения приведён на рисунке 9.28). При этом «МДС»1 будет обеспечивать доступ в направлении А, «МДС»2 — в направлении Б. Реле модулей подают сигналы разблокировки турникета в направлении А и Б соответственно. На входы дверных контактов замыкаются контакты выходного сигнала турникета о факте проворота турникета в направлении А или Б. Реле «МДС»3 замыкается на входной контакт картоприёмника для передачи команды на изъятие карты, а выходной сигнал картоприёмника замыкается на вход кнопки выхода «МДС»2 (сигнал об успешном изъятии пропуска имитирует нажатие кнопки выхода в направлении Б).

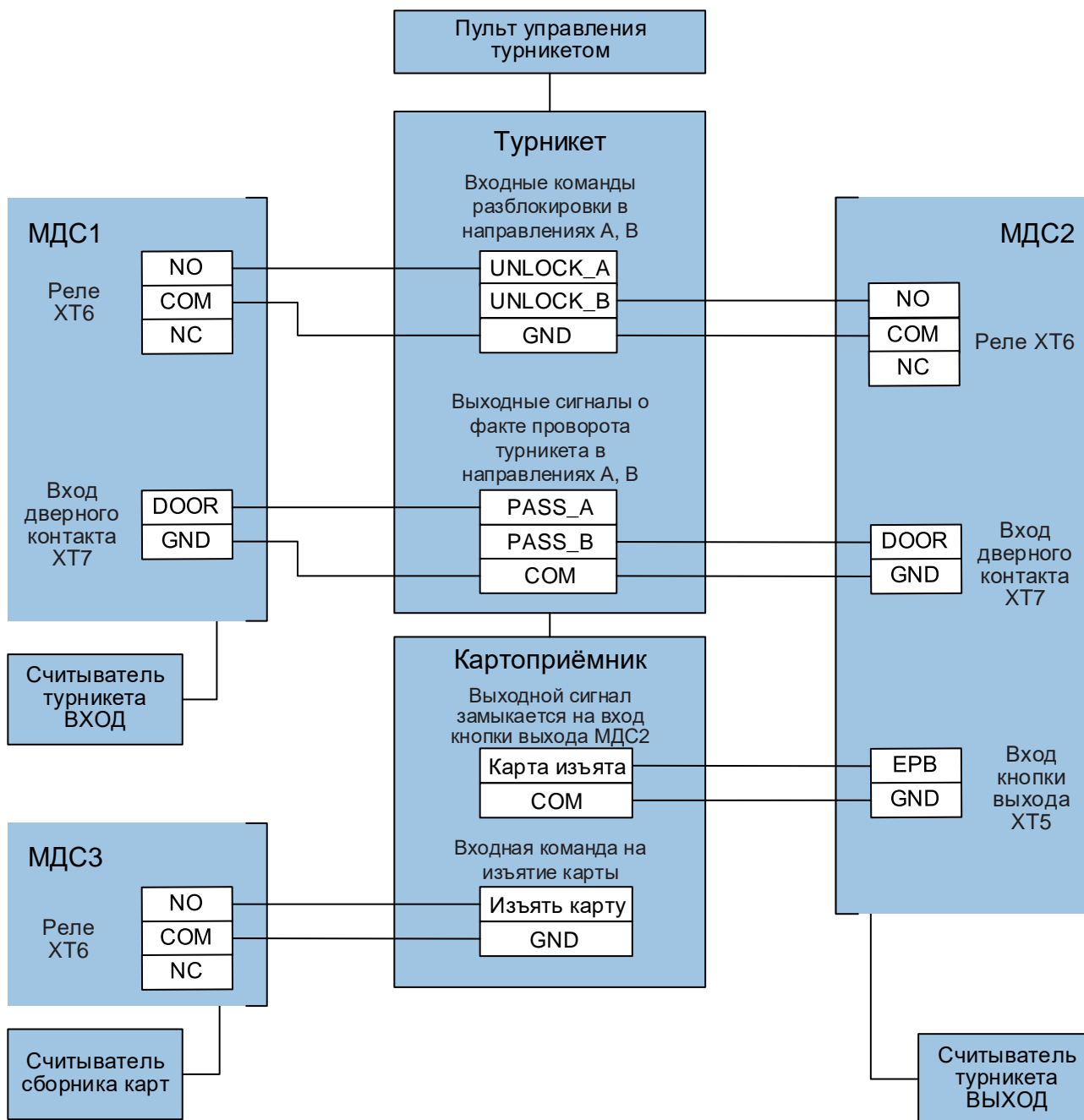


Рисунок 9.28 — Схема подключения турникета и картоприёмника к модулям «МДС»

### Подключение Handkey-II

Обеспечено взаимодействие биометрическим сканером геометрии руки HANDKEY II производства компании Recognition Systems.

Возможно несколько вариантов подключения Handkey-II (рисунки 9.29, 9.30):

- по интерфейсу RS-232 напрямую;
- по интерфейсу Ethernet (при использовании сетевой модели Handkey-II с дополнительным встроенным модулем связи по протоколу TCP/IP). При этом Handkey может

непосредственно подключаться к порту Ethernet прибора «ЯРС», либо по сети с использованием коммутатора;

- по интерфейсу RS-422/RS-485 с использованием преобразователя интерфейсов (например, MOXA NPort 5130);

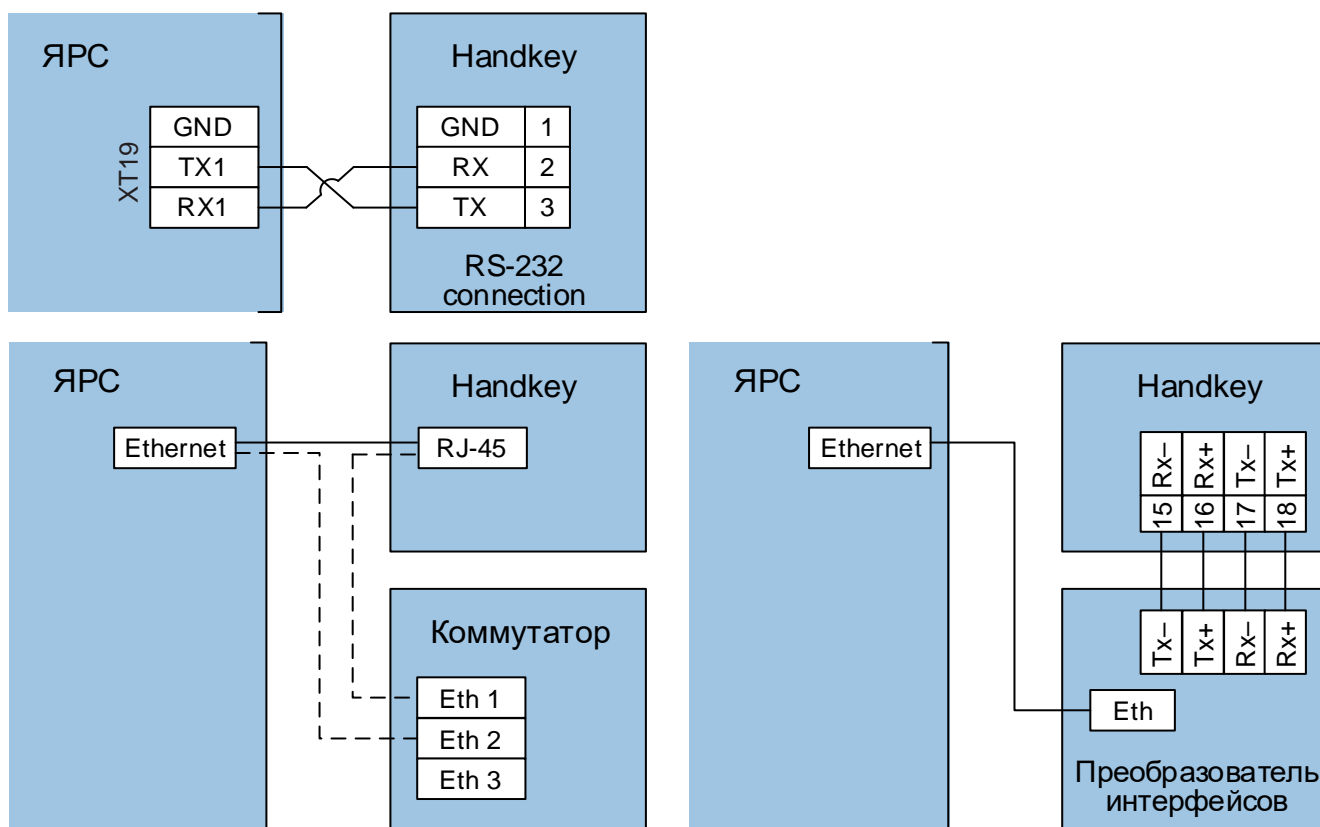


Рисунок 9.29 — Схема подключения Handkey-II посредством интерфейсов RS-232, Ethernet и RS-422

- с использованием модуля подключения RS-232;
- с использованием модуля подключения RS-485.

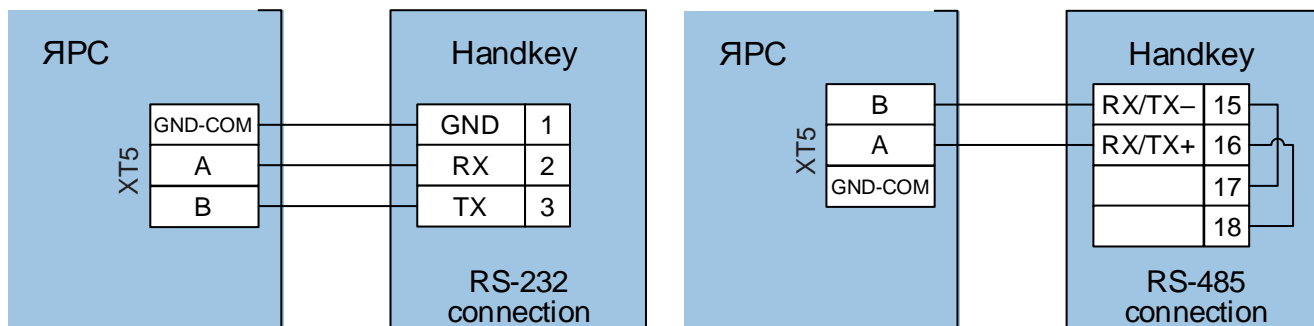


Рисунок 9.30 — Схема подключения Handkey-II посредством модулей подключения RS-232, RS-485

## ПРИЛОЖЕНИЕ 4. СЕТЬ НЕЙРОСС

### Понятие сети НЕЙРОСС

Приборы «Борей», «ЯРС», «ВИК», «МТК», «Игнис», серверы ITRIUM, «НЕЙРОСС Доступ», «НЕЙРОСС Центр», «Контроль операторов», ONVIF IP-камеры образуют сеть НЕЙРОСС и предназначены для построения интегрированной системы безопасности НЕЙРОСС.

Для пользователя ИСБ НЕЙРОСС — это «облако», в котором представлены ресурсы (аппаратные и программные средства сбора и обработки информации), объекты управления, средства интеграции других средств и систем, базы данных, системных параметров и конфигураций, а также средства представления информации. В основу сети НЕЙРОСС заложены такие общие ресурсы, как учётные 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 возможностях и предоставляемых сервисах.

Устройство, входящее в сеть НЕЙРОСС называется **узлом сети НЕЙРОСС** или **узлом НЕЙРОСС**. Каждый узел НЕЙРОСС содержит в себе все необходимые для использования по назначению средства и ресурсы: программное обеспечение охранной сигнализации, управления доступом, мониторинга, локальных и глобальных коммуникаций, интерфейс для работы с ними находятся «на борту» каждого узла.

Пользователь получает доступ к системе с помощью «облачного» веб-интерфейса НЕЙРОСС на основе прав учётной записи пользователя. Для защиты сети от сторонних ONVIF-запросов предусмотрен механизм защиты сетевого взаимодействия.

**Внимание.** «Видимость» узлов друг для друга осуществляется в пределах домена НЕЙРОСС (см. раздел [Понятие домена НЕЙРОСС](#)).

Для обеспечения взаимодействия узлов НЕЙРОСС между собой, они должны быть синхронизированы по времени (см. раздел [Дата и время](#)).

### Понятие домена НЕЙРОСС

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

#### Основные постулаты:

- «Видимость» узлов НЕЙРОСС обеспечивается только в пределах заданного домена.

- Узел может принадлежать нескольким доменам, в этом случае он является связующим узлом между изолированными группами узлов, получает мультикастовые сообщения от «своих» доменов и транслирует их в группы. При этом нагрузка на узел возрастает.
- Имя домена узла может быть в любой момент изменено.
- Внутри домена осуществляется взаимная синхронизация данных, непременным условием которой является отсутствие расхождений текущего времени на всех узлах домена.

Первоначально каждому узлу НЕЙРОСС присвоен уникальный домен вида **NEYROSS-a2581d2d-86af-447a-8e4c-64e8e9a3cc54**. В процессе первоначальной настройки с помощью **Мастера первого запуска** или в любое время впоследствии узлы могут быть сгруппированы по доменам.

### **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.

Узел ITRIUM (при использовании в системе) должен входить во все домены системы.



## ПРИЛОЖЕНИЕ 5. ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС

Каждый узел НЕЙРОСС предоставляет пользовательский веб-интерфейс, предназначенный для обеспечения удалённого конфигурирования всех устройств подсети, способных обмениваться данными в стандарте ONVIF, а также для обеспечения комплексного мониторинга состояний этих устройств и управления. В рамках веб-приложений обеспечиваются функции Бюро пропусков, Фотоидентификации, терминала постановки/снятия и др. Поддерживается работа в нескольких доменах, предназначенных для изолирования/группировки нескольких устройств.

Веб-интерфейс позволяет:

1. Обнаруживать и конфигурировать следующие узлы: «Борей», «ЯРС», «КБУ-1», «ВИК», «Игнис», ITRIUM, «НЕЙРОСС Доступ», «НЕЙРОСС Мониторинг», IP-камеры.
2. Конфигурировать параметры каждого узла, общие сетевые ресурсы (уровни и режимы доступа, разделы охранной сигнализации, терминалы, зоны доступа, пропуска и многое другое).
3. Синхронизировать данные между устройствами сети, в том числе — пропуска ITRIUM.
4. Выполнять управляющие команды (постановку зон и разделов на охрану и снятие с охраны, сброс тревог и многое другое).
5. Подготавливать, создавать и учитывать пропуска в системах пропускного режима.
6. Проводить мониторинг состояния устройств и событий на устройстве.
7. Просматривать «живое» видео с камер видеонаблюдения и события доступа, экспортировать видеофрагменты.
8. Выполнять групповое обновление программного обеспечения («прошивки») приборов, создавать резервные копии настроек и многое другое.

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 узла НЕЙРОСС.

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

Предустановленные сетевые параметры указаны на корпусе прибора:

IP-адрес: **10.200.X.YYY**

Маска подсети: **255.0.0.0**

## 1. Мастер первого запуска

Если узел ранее не конфигурировался или настройки были сброшены, при доступе к интерфейсу для упрощения первичной настройки узла предоставляется мастер первого запуска.

Выполните следующую последовательность шагов:

1. Настройте сетевое подключение вашего компьютера или планшета для работы в диапазоне IP-адресов **10.200.X.YYY** и подсети **255.0.0.0**. (данные указаны на корпусе узла).

**Примечание.** При первом подключении рекомендуется использовать прямое подключение контроллера к компьютеру через сетевой кабель.

Инструкция для Windows 7:

- В окне свойств TCP-соединения в поле **IP-адрес** задайте **10.200.X.YYY**, где **YYY** – любое число в диапазоне от 1 до 254, кроме занятых; в поле **Маска подсети** введите **255.0.0.0** (рисунок 9.31). Нажмите на кнопку **ОК**.

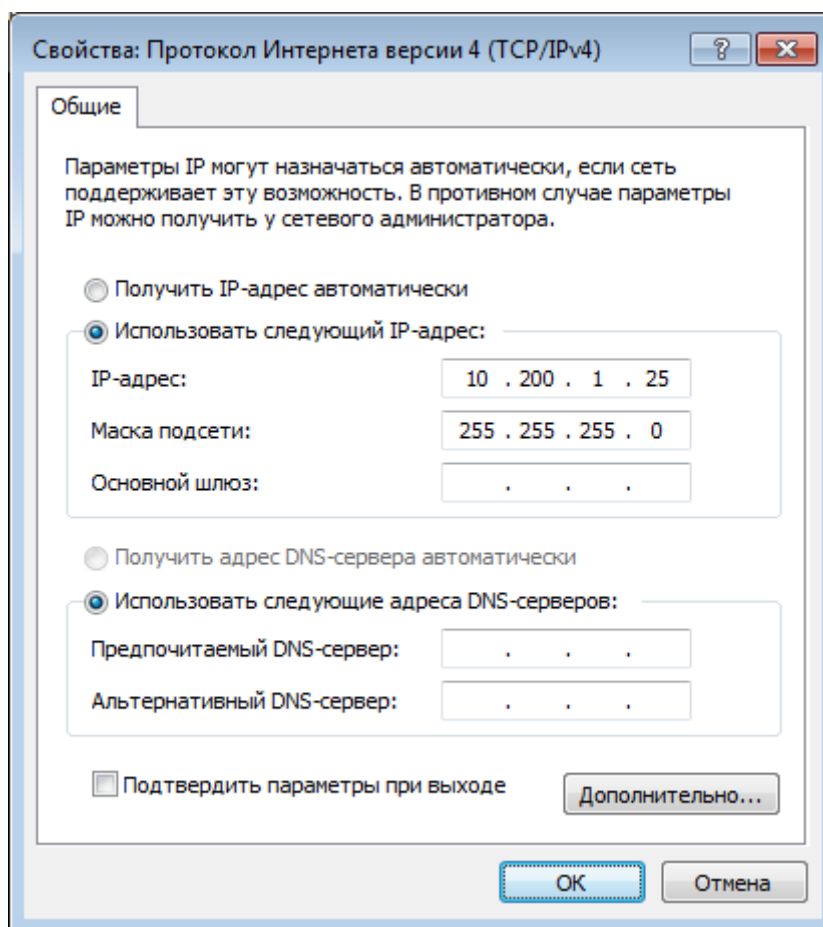


Рисунок 9.31 — Настройка сетевого подключения

**Примечание.** Для проверки наличия соединения или поиска свободного адреса в подсети используйте команду **ping [ip-адрес]**, например, **ping 10.200.1.25**. Для перехода к интерфейсу командной строки, в меню **Пуск** выберите **Программы — Стандартные — Командная строка** или выберите **Выполнить**, введите **cmd** и нажмите **ОК**.

2. Запустите веб-браузер Google Chrome, Mozilla Firefox, Internet Explorer, Safari.

**Внимание.** Если версия браузера устарела, обновите её.

3. Введите в адресной строке браузера ip-адрес, указанный на наклейке на корпусе прибора, например, **10.200.1.125**, нажмите **Ввод** (Enter). Отобразится окно мастера первого запуска (рисунок 9.32).

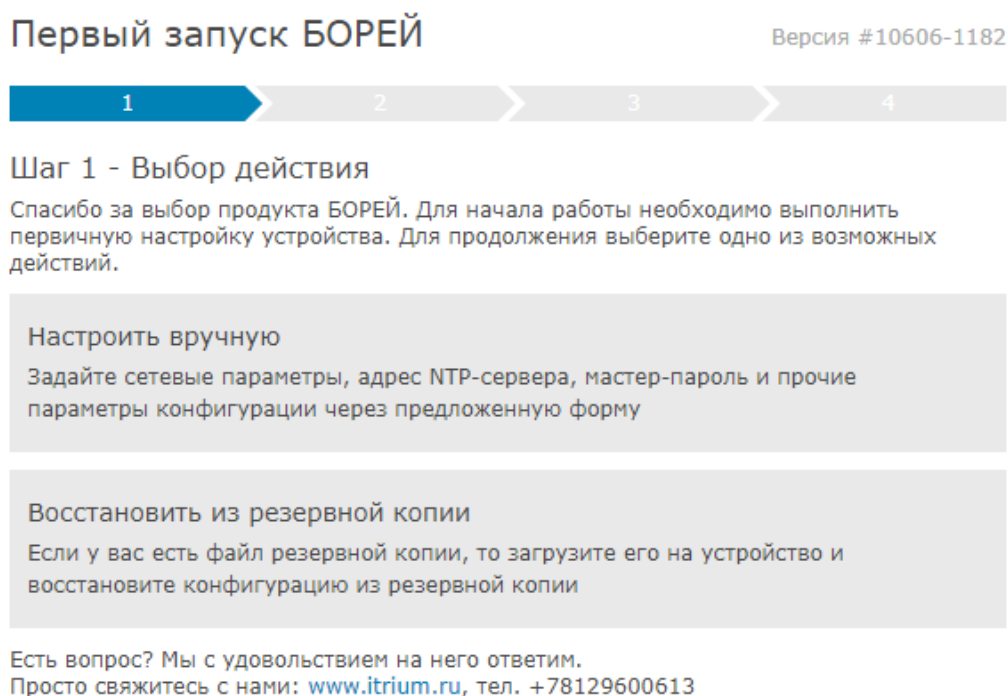


Рисунок 9.32 — Окно мастера первого запуска. Шаг 1

4. Выберите **Настроить вручную**, если файла резервной копии настроек нет.
5. На втором шаге мастера вам потребуется задать наиболее общие параметры прибора (рисунок 9.33, таблица 9.4). Для сохранения изменений, нажмите на кнопку **Применить**. Будут применены заданные настройки, на их основе создана резервная копия данных, затем будет выполнена перезагрузка программных средств узла.

**Внимание.** Если были изменены сетевые параметры узла, после перезагрузки его интерфейс будет доступен по новому IP-адресу и, возможно, и из другой подсети.

В адресной строке браузера введите ip-адрес устройства и нажмите **Ввод** (Enter), перейдите к шагу 7.



Шаг 2 - Настройка параметров

Основной IP-адрес:  .  .  .

Маска основного IP-адреса:  .  .  .

Адрес шлюза:  .  .  .

Мастер-пароль:

Повторите мастер-пароль:

Адрес NTP-сервера:

Домен НЕЙРОСС:

Имя узла в сети НЕЙРОСС:

Строгая фильтрация доменов:  Нет

Multicast выключен:  Нет

Рисунок 9.33 — Окно мастера первого запуска. Шаг 2 — Настройка параметров

Таблица 9.4 — Настройки мастера первичного запуска

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Основной IP-адрес	ip-адрес	Указано на корпусе прибора	Введите IP-адрес, по которому будет выполняться подключение к устройству.
Маска основного IP-адреса	маска подсети	255.0.0.0	Укажите маску подсети, в которой будет находиться устройство.
Адрес шлюза	ip-адрес шлюза		Укажите основной сетевой шлюз устройства, если требуется.
Мастер-пароль	Любое сочетание символов длиной не менее 4	root	Укажите пароль учётной записи root, предназначенной для базового конфигурирования устройства. <b>Настоятельно рекомендуется сменить пароль учётной записи root.</b>

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Адрес NTP-сервера	ip-адрес		Укажите ip-адрес доступного NTP-сервера, например, - компьютера с ITRIUM (если настроена «Служба НЕЙРОСС»).
Домен НЕЙРОСС	Любое сочетание символов и спец. знаков, кроме запятой и пробела; при указании нескольких доменов, их необходимо разделять запятой и пробелом	NEYROSS_{UID}	Домены применяются для сужения группы устройств, среди которых выполняется синхронизация данных (например, пропусков).
Строгая фильтрация доменов	Да/Нет, логическое поле	Нет	При нестрогой фильтрации доменов в сети «видны» устройства, не поддерживающие домены (например, IP-камеры).
Multicast выключен	Да/Нет, логическое поле	Нет	Задаёт, будет ли узел отправлять широковещательные WSD-запросы (подробнее в разделе <a href="#">Понятие сети НЕЙРОСС</a> ) для автоматического поиска НЕЙРОСС-узлов и ONVIF-камер. Если multicast выключен, для обеспечения взаимодействия нескольких устройств, потребуется их добавление вручную.

6. Выберите **Восстановить из резервной копии**, если существует резервная копия с требуемыми настройками.

На втором шаге мастера вам потребуется (рисунок 9.34) выбрать резервную копию из памяти прибора или из файла, если файл резервной копии был предварительно создан и сохранён на каком-либо носителе информации.

Чтобы загрузить файл резервной копии для последующего восстановления, выполните:

- нажмите на кнопку **Выберите файл**,
- укажите путь к файлу,
- нажмите на кнопку **Загрузить**,
- нажмите на кнопку **Восстановить**.

При необходимости восстановления из резервной копии, сохранённой в памяти прибора, выберите из раскрывающегося списка требуемый файл, ознакомьтесь с комментарием ниже и нажмите на кнопку **Восстановить**.

Будет выполнена проверка и восстановление данных из резервной копии.

## Первый запуск БОРЕЙ

Версия #10606-1182



### Шаг 2 - Выбор резервной копии

Выберите резервную копию для восстановления. Вы можете выбрать одну из копий, ранее сохранённых в БОРЕЙ, или загрузить свой файл. Загруженная резервная копия появится в списке доступных.

#### Загрузить резервную копию

Выберите файл для загрузки:  Файл не выбран

#### Выбрать резервную копию

Вы выбрали резервную копию, после восстановления из которой узлу будет назначен сетевой адрес 10.1.31.146, маска подсети 255.248.0.0, идентификатор узла в сети НЕЙРОСС 4be1a1cf-7900-418d-8e4a-ccc23b5ead4d. Резервная копия создана 01.10.2018 13:21.

Для продолжения нажмите кнопку Восстановить внизу окна.

Рисунок 9.34 — Окно мастера первого запуска. Шаг 2 — Выбор резервной копии.

7. Введите данные авторизации: имя пользователя **root** и пароль учётной записи **root** (по умолчанию, **root**). Нажмите **Вход**.

## 2. Вход в веб-интерфейс

**Примечание.** Для доступа к интерфейсу необходимо:

- Настроить сетевое подключение вашего компьютера или планшета для работы в диапазоне IP-адресов узла прибора «ЯРС».
- Установить «свежую» версию браузера. Необходимо использовать одну из последних двух версий следующих браузеров: Google Chrome, Mozilla Firefox, Microsoft Edge, Internet Explorer или Apple Safari. Корректная работа в других браузерах или с устаревшими версиями не гарантируется!

Для подключения к веб-интерфейсу прибора «ЯРС»:

1. Запустите веб-браузер.
2. В адресной строке браузера введите ip-адрес устройства и нажмите **Ввод** (Enter).
3. Введите данные авторизации и нажмите на кнопку **Вход** (рисунок 9.35).

Для базового конфигурирования узла используйте следующие параметры:

- Имя пользователя — root
- Пароль — root

Если пароль не был изменён ранее с помощью [мастера первого запуска](#), в целях безопасности его следует изменить (см раздел [Смена мастер-пароля](#)).

Для управления общими ресурсами и конфигурирования других устройств сети, необходимо воспользоваться «облачной» учётной записью (см. раздел [Пользователи, роли и права](#)).

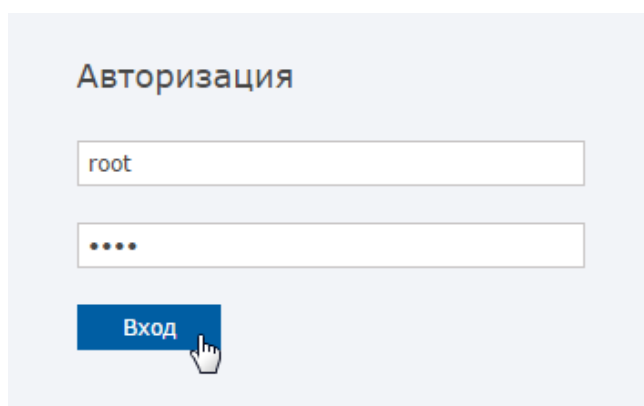


Рисунок 9.35 — Веб-интерфейс. Окно авторизации.

Если данные введены корректно, отобразится рабочий стол (рисунок [9.37](#)). Возможные проблемы и их решение представлены в таблице ниже.

Таблица 9.5

Проблема	Решение
Доступа к веб-интерфейсу нет	<ul style="list-style-type: none"> <li>• Проверьте наличие физического сетевого подключения;</li> <li>• Настройте сетевое подключение компьютера или планшета для работы в диапазоне IP-адресов и подсети узла.</li> <li>• Проверьте отсутствие конфликта IP-адресов устройств, для этого отключите узел от локальной сети, перейдите к интерфейсу командной строки и выполните команду <b>ping [IP-адрес]</b>, например, <b>ping 10.200.1.125</b>.</li> </ul>
Забыли IP-адрес узла, имя и пароль пользователя,	Выполните сброс настроек узла.
Выводится экран предупреждения (рисунок 9.36)	<p>Выполните очистку кэша браузера, так как на данном компьютере или планшете уже проводилась работа с узлом другой версии прошивки, и браузер может использовать устаревшие данные.</p> <div data-bbox="560 748 1445 1574" style="border: 1px solid #ccc; padding: 10px;"> <p style="text-align: center; color: #c00000; font-weight: bold;">Чтобы работать с актуальной версией, сбросьте кэш в настройках браузера и перезагрузите страницу.</p> <p style="font-size: small;">Текущая версия - 10842 <span style="float: right;">Актуальная версия - 10850</span></p> <p><b>Инструкция по сбросу кэша:</b> Нажмите сочетание клавиш - Ctrl+Shift+Del</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>Очистить историю <span style="float: right;">✕</span></p> <p>Удалить указанные ниже элементы <span style="float: right;">за все время ▾</span></p> <p><input type="checkbox"/> История просмотров</p> <p><input type="checkbox"/> История скачиваний</p> <p><input checked="" type="checkbox"/> <u>Файлы cookie, а также другие данные сайтов и плагинов</u></p> <p><input checked="" type="checkbox"/> <u>Изображения и другие файлы, сохраненные в кеше - 186 МБ</u></p> <p><input type="checkbox"/> Пароли</p> <p><input type="checkbox"/> Данные для автозаполнения</p> <p><input type="checkbox"/> Данные размещаемых приложений</p> <p><input type="checkbox"/> Медиалицензии</p> <p style="text-align: right;"><span>Отмена</span> <span style="border: 1px solid red; padding: 2px;">Очистить историю</span></p> </div> </div> <p style="text-align: center;">Рисунок 9.36 — Экран предупреждения</p>

### 3. Рабочий стол

Рабочий стол (рисунок 9.37) предназначен для доступа ко всем функциям веб-приложения, содержит два блока элементов:

1. Блок **Программы** (рисунок 9.38) содержит перечень прикладных программ:

- **Бюро пропусков** – реализует функции Бюро пропусков в системах контроля и управления доступом НЕЙРОСС и ITRIUM, предназначено для просмотра и конфигурирования данных пропусков, их уровней доступа и управления. Блок активен



при наличии в сети НЕЙРОСС контроллера СКУД НЕЙРОСС: «Борей», «ЯРС», терминала «МТК», консоли «ВИК», сервера ITRIUM или «НЕЙРОСС Доступ».

- **Видеонаблюдение** — реализует функции АРМ видеонаблюдения; блок активен, если к сети подключён видеорегистратор «ДеВизор»; по щелчку на элементе происходит переход по ip-адресу видеорегистратора;
- **Фотоидентификация** – реализует функции подтверждения доступа на основе просмотра фото-/видеоданных. Блок активен при наличии в сети НЕЙРОСС контроллера СКУД НЕЙРОСС: «Борей», «ЯРС», «МТК»;
- **Отчёты** — реализует функции построения отчётов по произвольным шаблонам; раздел активен, если к сети подключён сервер «НЕЙРОСС Центр» или «НЕЙРОСС Отчёты», на «борту» которых присутствует соответствующее веб-приложение; по щелчку на элементе происходит переход по ip-адресу сервера;
- **События** – реализует функции журнала событий всей системы в целом с возможностью фильтрации событий по дате и времени, источнику события и др. и последующего экспорта в текстовый файл (см. приложение [События](#)).

2. Блок **Обслуживание** (рисунок 9.39) содержит перечень приложений по настройке и обслуживанию узлов и общих ресурсов системы:

- Приложение **Конфигурация узлов** – предоставляет функционал задания индивидуальных настроек каждого узла системы, с возможностью перехода к настройкам других узлов (см. приложение [Настройки узла](#));
- Приложение **Пользователи, роли и права** – предоставляет функционал настройки пользователей и прав доступа к системе (см. раздел [Пользователи, роли и права](#));
- Приложение **Охранная сигнализация** – предоставляет функционал конфигурирования разделов сигнализации и настройки режимов управления реле по состояниям разделов. Блок активен при наличии в сети НЕЙРОСС контроллера СКУД НЕЙРОСС: «Борей», «ЯРС», «МТК»;
- 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, создания резервных копий данных и др. (см. приложение [Сеть](#)).
- Приложение **Терминалы** – предоставляет функционал конфигурирования терминалов. Блок активен при наличии в сети НЕЙРОСС контроллера СКУД НЕЙРОСС: «Борей», «ЯРС», «МТК»;
- Приложение **Зоны доступа** – предназначено для конфигурирования зон доступа с целью организации контроля повторного прохода. Блок активен при наличии в сети НЕЙРОСС контроллера СКУД НЕЙРОСС: «Борей», «ЯРС», «МТК»;

- Приложение **Настройка видеорегистраторов** – предназначено для задания параметров видеорегистраторов «ДеВизор».

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

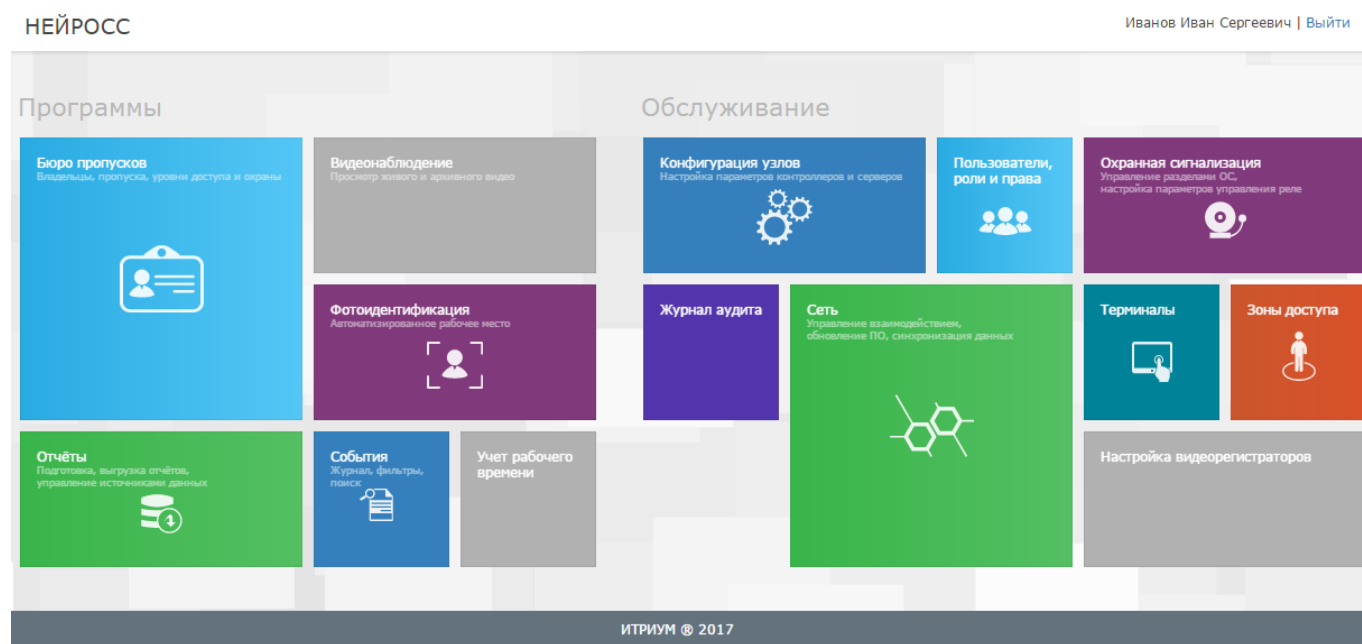


Рисунок 9.37 — Рабочий стол

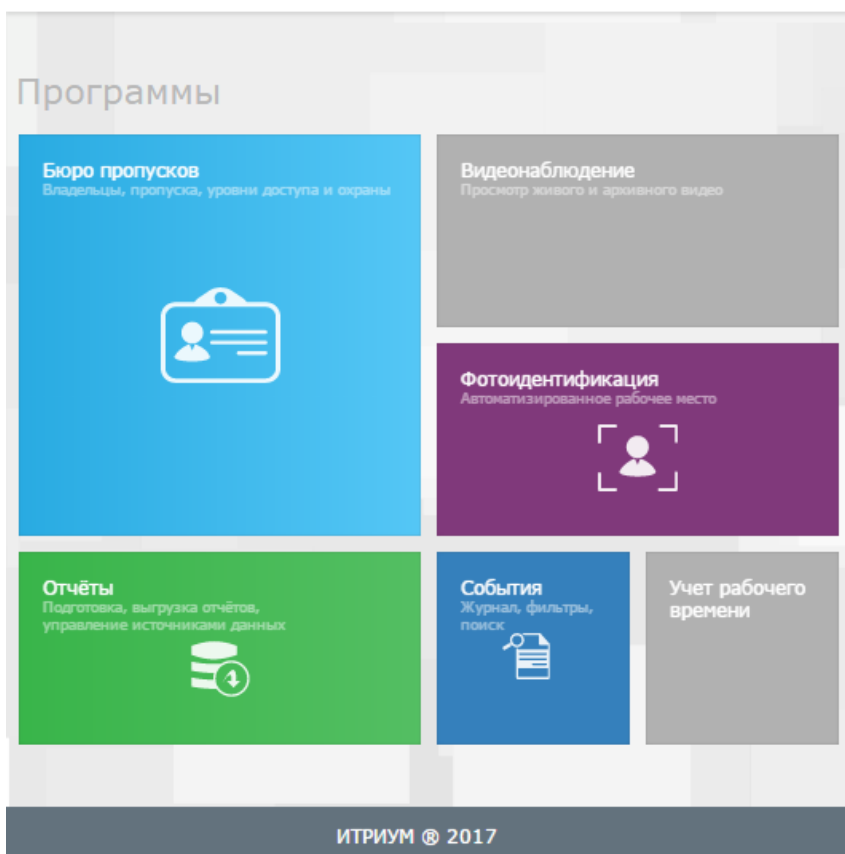


Рисунок 9.38 — Рабочий стол. Блок **Программы**

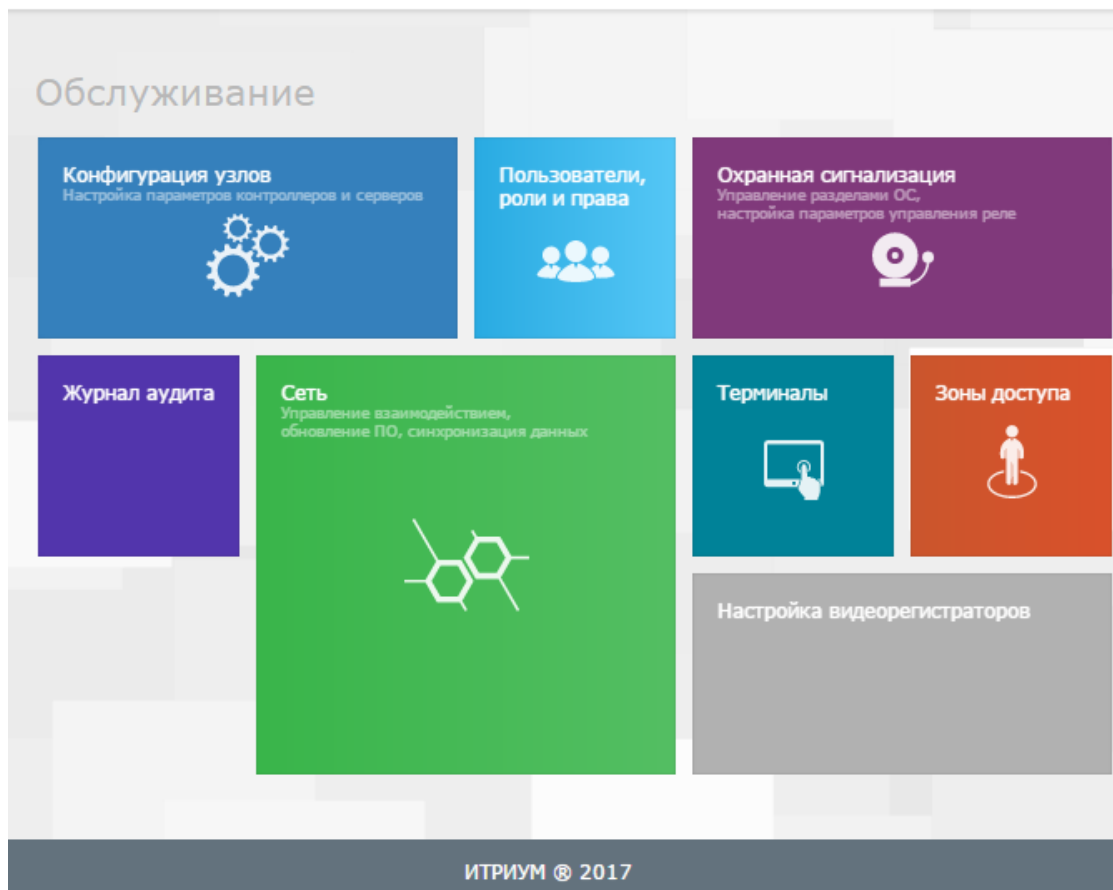


Рисунок 9.39 — Рабочий стол. Блок **Обслуживание**

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 9.40).




Рисунок 9.40 — Пример заголовка окна приложения

## 4. Конфигурация узлов

Работу с интерфейсом следует начинать с раздела **Конфигурация узлов**. Он содержит все частные настройки узла. Другие разделы из блока **Обслуживание** (см. раздел [Рабочий стол](#)) предназначены для настройки общих ресурсов сети.

В левом вертикальном меню раздела содержатся доступные группы настроек узла. Справа отображается список полей выбранной группы: описание приведено в приложении [Настройки узла](#).

Раздел также может использоваться для перехода к частным настройкам других узлов сети.

Для просмотра списка доступных узлов нажмите в области серой панели со стрелкой  в левой части окна (рисунок 9.41). Отобразится скрытое ранее окно со списком доступных узлов (рисунок 9.42).

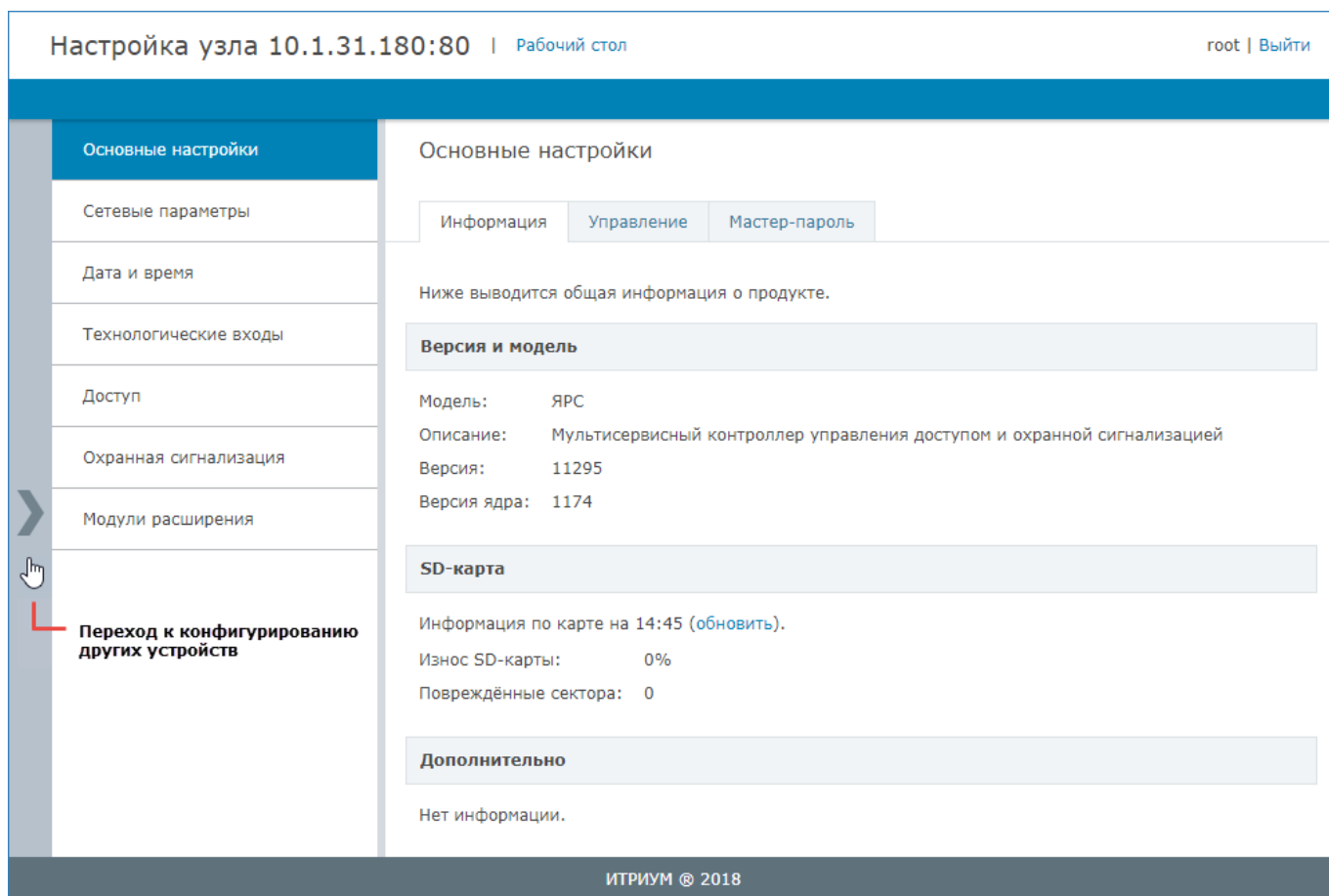


Рисунок 9.41 — Окно конфигурирования

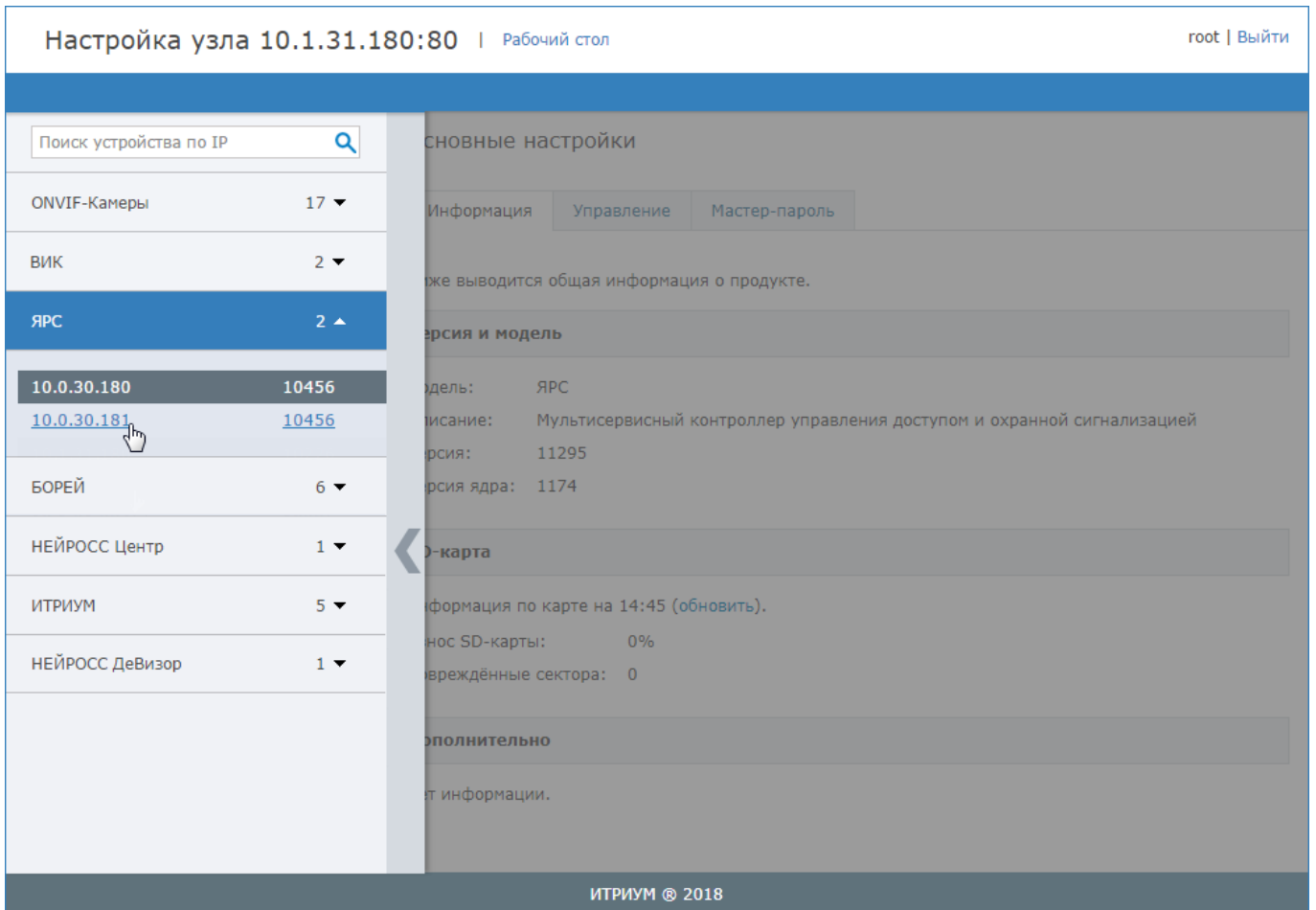


Рисунок 9.42 — Окно конфигурирования со списком узлов

Узлы группируются по модели узла (БОРЕЙ, ЯРС, ИТРИУМ, ВИК, ИГНИС, НЕЙРОСС Центр, НЕЙРОСС ДеВизор, ONVIF-камеры), указывается общее число узлов в группе. Для каждого узла указан его IP-адрес и справочная информация (версия программных средств или прошивки, модель камеры и проч.). Для перехода к конфигурированию других узлов сети, щёлкните левой клавишей мыши по IP-адресу требуемого устройства.

**Внимание.** Учётная запись **root** предназначена для первичной настройки текущего узла. Для работы с «облачными» сервисами и конфигурирования других узлов сети, необходимо авторизоваться под учётной записью из раздела [Пользователи, роли и права](#).

## 5. Выход из веб-интерфейса

Для выхода из веб-интерфейса нажмите на ссылку **Выйти** в правом верхнем углу экрана интерфейса (рисунок 9.43). Выход из программы с помощью закрытия браузера является некорректным, так как другой пользователь может воспользоваться данными авторизации, сохранёнными в cookies-файлах браузера.

Иванов Иван Сергеевич | [Выйти](#)

Рисунок 9.43 — Выход из веб-интерфейса

## ПРИЛОЖЕНИЕ 6. НАСТРОЙКИ УЗЛА

### 1. Основные настройки

Раздел **Основные настройки** предназначен для получения общей информации об узле и выполнения базовых операций. Набор инструментов раздела зависит от модели узла и текущей версии программных средств.

Для доступа к основным настройкам выберите [Конфигурация узлов](#) — **Основные настройки**.

На вкладке **Информация** указана модель и текущая версия прошивки программных средств и ядра: эти данные потребуются при обращении в техподдержку.

Вкладка **Управление** содержит инструментарий программной перезагрузки прибора, обновления прошивки, 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 узла

С точки зрения программных средств, узел «ЯРС» – это полноценный компьютер, работающий под управлением операционной системы семейства Linux. В случае изменения сетевых параметров узла, привязки к доменам НЕЙРОСС и проч., а также если устройство «зависло», необходимо перезагрузить узел. Перезагрузка может быть выполнена аппаратно (см. раздел [Перезапуск узла](#)) или посредством веб-интерфейса.

Для перезапуска программных средств узла выполните:

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 **Заккрыть** (рисунок 9.44).



Рисунок 9.44 — Перезагрузка

### Обновление программных средств

Текущую версию программных средств (прошивки) узла можно уточнить в разделе [Конфигурация узлов](#) — **Основные настройки** на вкладке **Информация**. Обновление программных средств (прошивки) узла осуществляется из файла архива формата **TAR.GZ**. Предварительно подготовьте требуемый файл.

Выполните следующие шаги:

1. В разделе [Конфигурация узлов](#) — **Основные настройки** перейдите к вкладке **Управление**.
2. В блоке **Обновление программных средств** (рисунок 9.45) в поле **Файл обновления** укажите файл архива программных средств, нажмите на кнопку **Обновить**.

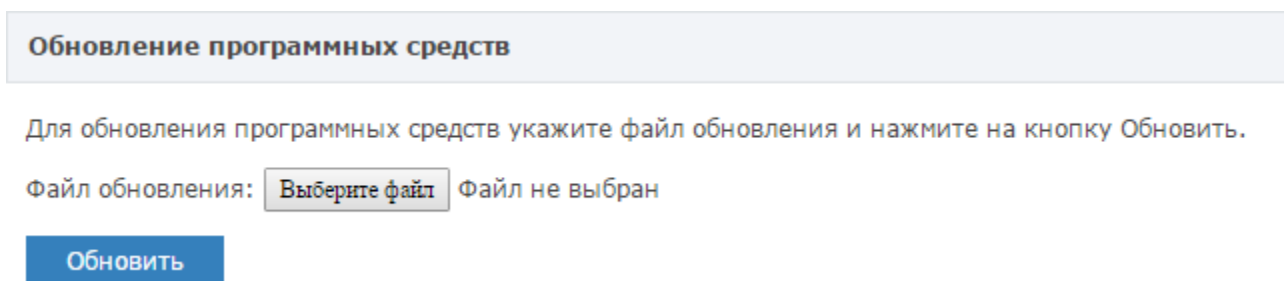


Рисунок 9.45 — Кнопка **Обновление ПО**

3. Будет выполнена процедура обновления с последующей перезагрузкой. По завершении нажмите на кнопку **Заккрыть** (рисунок 9.46).

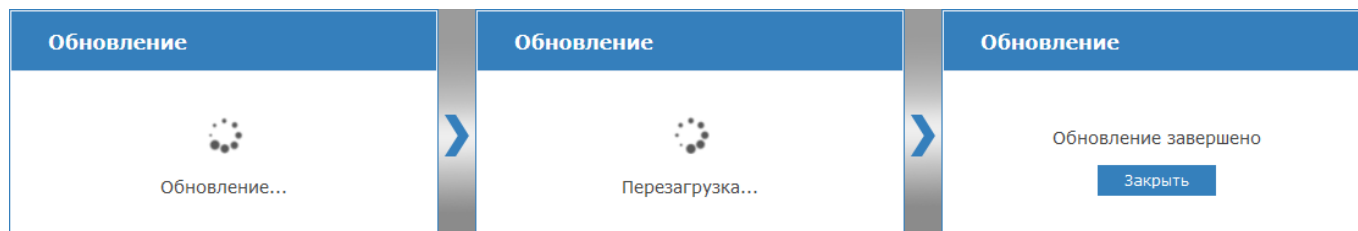


Рисунок 9.46 — Три шага обновления программных средств

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, сохранённые 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 9.47) нажмите на кнопку **Создать**.

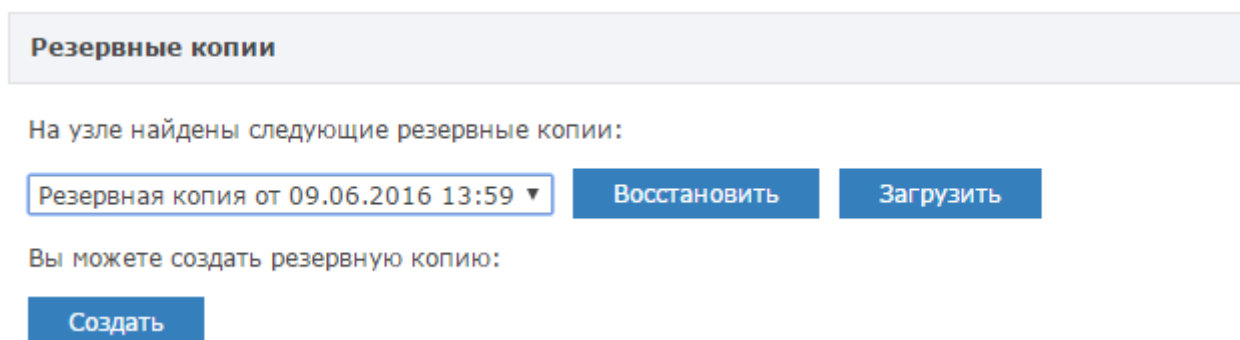


Рисунок 9.47 — Кнопка **Обновление ПО**

3. Будет выполнена процедура создания резервной копии. Ранее созданная резервная копия будет затёрта. В процессе создания копии будет выполнен перезапуск программных средств узла. По завершении нажмите на кнопку **Закреть** (рисунок 9.48).

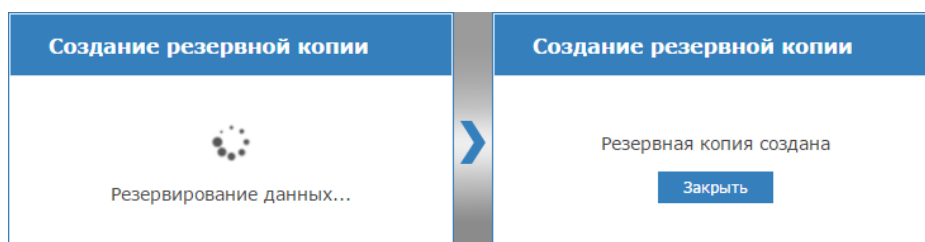


Рисунок 9.48 — Процедура создания резервной копии

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, сохранённой в резервной копии.

По команде **Загрузить** выполняется загрузка файла резервной копии в папку загрузок браузера. Восстановить данные из сохранённого на компьютере файла возможно после сброса настроек (см. раздел [Сброс настроек](#)) при прохождении Мастера первого запуска (см. раздел [Мастер первого запуска](#)).

## Смена мастер-пароля

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

**Внимание.** В целях безопасности рекомендуется изменить пароль учётной записи **root**.

Для смены пароля учётной записи **root**:

Перейдите к вкладке **Мастер-пароль**.

1. В поле **Пароль** введите новый пароль.
2. 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» учётной записью. Дополнительную информацию см. в разделе [Пользователи, роли и права](#).

## 2. Сетевые параметры

Задание сетевых параметров необходимо для обеспечения доступа к узлу по сети Ethernet с целью конфигурирования, мониторинга состояния и управления, при этом необходимо:

- Предотвратить возможный конфликт IP-адресов, так как адрес по умолчанию (указан на корпусе прибора) может быть занят другим устройством, в том числе – устройством «ЯРС»;
- Обеспечить возможность взаимодействия с другими узлами сети, поддерживающими протокол ONVIF («Борей», «ЯРС», «КБУ-1», «ВИК», «Игнис», ITRIUM, «НЕЙРОСС Доступ», «НЕЙРОСС Мониторинг», IP-камеры) путём 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 разделах [Мастер первого запуска](#) и [Вход в веб-интерфейс](#).

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

- На вкладке **Основные** задайте параметры сетевого интерфейса **Ethernet** и параметры сетевого взаимодействия в сети НЕЙРОСС (см. раздел [Основные сетевые параметры](#)).
- При использовании модема, на вкладке **GSM** задайте параметры беспроводной точки доступа по GSM-модему (см. раздел [Параметры GSM](#)).
- При необходимости задания статических маршрутов передачи пакетов извещений в сети, не принадлежащие заданным интерфейсам **Ethernet** и **PPPo**, на вкладке **Маршруты** задайте параметры маршрута (см. раздел [Сетевые маршруты](#)).

**Примечание.** Вкладка **Дополнительно** предназначена для опытных пользователей и содержит дополнительные параметры настройки сетевого взаимодействия узлов НЕЙРОСС (см. раздел [Дополнительные сетевые параметры](#)).

### Основные сетевые параметры

Вкладка **Основные** раздела **Сетевые параметры** предназначена для смены параметров сетевого интерфейса Ethernet и параметров взаимодействия в сети НЕЙРОСС, заданных при первоначальной настройке с помощью мастера первого запуска.

В блоке настроек **Ethernet** задайте параметры **Ethernet** (таблица 9.6), нажмите на кнопку **Сохранить**.

При необходимости, в блоке настроек **Сеть НЕЙРОСС** задайте параметры взаимодействия в сети НЕЙРОСС (таблица 9.7), нажмите на кнопку **Сохранить** и выполните перезагрузку программных средств узла (см. раздел [Перезапуск узла](#)). Дополнительную информацию о сети НЕЙРОСС см. в разделе [Понятие сети НЕЙРОСС](#).

Таблица 9.6 — Настройки сетевых параметров. Вкладка **Основные**, блок **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	255.0.0.0	Укажите маску подсети, в которой будет находиться устройство.

Таблица 9.7 — Настройки сетевых параметров. Вкладка **Основные**, блок **Сеть НЕЙРОСС**

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Имя узла	Любое текстовое описание	«ЯРС»	Предназначено для идентификации узла в списке узлов раздела <a href="#">Сеть</a> .
Домены*	любое сочетание символов и спец. знаков, кроме запятой и пробела; при указании нескольких доменов, их необходимо разделять запятой и пробелом	NEYROSS	Домены применяются для сужения группы устройств, среди которых выполняется синхронизация данных (например, пропусков).
Режим строгой фильтрации доменов	Да/Нет, логическое поле	Нет	При нестрогой фильтрации доменов в сети «видны» устройства, не поддерживающие домены (например, IP-камеры).
Авторизация сетевого взаимодействия**	Да/Нет, логическое поле	Нет	Установите <b>Да</b> при необходимости защиты сетевого трафика. Установите пароль авторизации в поле <b>Пароль</b> .
Пароль	Любое сочетание символов длиной не менее 4		Введите пароль, который будет передаваться в запросе для авторизации узла. Повторите ввод пароля в поле <b>Повторите пароль</b> .
Повторите пароль	Любое сочетание символов длиной не менее 4		Пароли в поле <b>Пароль</b> и <b>Повторите пароль</b> должны совпадать.

\* Взаимодействие узлов НЕЙРОСС осуществляется в пределах домена (дополнительная информация приведена в разделе [Понятие домена НЕЙРОСС](#)). Если какой-либо узел НЕЙРОСС «не виден» в списке узлов (см. приложение [Сеть](#)), он может принадлежать другому домену.

\*\* Режим авторизации сетевого взаимодействия представляет собой механизм защиты узлов НЕЙРОСС от «сторонних» ONVIF-запросов (например, от запроса на перезагрузку узла или синхронизацию ресурсов), которые могут передаваться злоумышленником в незащищённой сети. При включённом режиме запрос будет выполнен только от авторизованного узла (в настройках обоих узлов должен быть включён режим авторизации сетевого взаимодействия и указан одинаковый сетевой пароль).

## Параметры GSM

Вкладка **GSM** раздела **Сетевые параметры** предназначена для задания параметров беспроводной точки доступа по GSM-модему. Параметры интерфейса **PPP0** будут сконфигурированы автоматически при подключении модема.

Описание полей настройки см. в таблице 9.8. Для внесения изменений, 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 9.8 — 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		
<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 удалённого контроля соединения GSM-модема с сетью. Если указанный адрес будет не доступен, устройство определит "зависание" модема и перезагрузит его.

## Сетевые маршруты

Вкладка **Маршруты** раздела **Сетевые параметры** предназначена для задания статических маршрутов 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:


1. Нажмите на кнопку **Добавить** .
2. Задайте параметры маршрута (см. таблицу 9.9).
3. При необходимости, создайте новый маршрут.
4. Нажмите на кнопку **Сохранить**.

Таблица 9.9 — 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.

## Дополнительные сетевые параметры

Вкладка **Дополнительно** раздела **Сетевые параметры** предназначена для опытных пользователей и содержит дополнительные параметры настройки сетевого взаимодействия узлов НЕЙРОСС.

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

### 3. Дата и время

Настройки даты и времени необходимы для фиксации точного времени и хронологии событий в **Журнале событий** (см. приложение [События](#)), а также для обеспечения взаимодействия нескольких узлов НЕЙРОСС и синхронизации данных.

Текущее состояние синхронизации времени можно просмотреть на странице раздела **Сеть** (дополнительную информацию см. в приложении [Сеть](#)).

#### Установка даты и времени вручную

Для указания даты и времени вручную (доступно для узлов «Борей», «ЯРС», «ВИК»):

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**.

#### Синхронизация по NTP-серверу

Для обеспечения взаимодействия узлов НЕЙРОСС между собой, абсолютно 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 сервер ITRIUM, «НЕЙРОСС Центр» или любой другой сервер.

Синхронизация времени на узлах сети НЕЙРОСС (за исключением серверов ITRIUM, «НЕЙРОСС Центр», «Контроль операторов») может быть выполнена двумя способами:

- **Посредством ПО ITRIUM®**: в программе «Администратор системы» в окне частных свойств элемента **Служба НЕЙРОСС** установите флаг в поле **NTP сервер** и сохраните изменения. Не позднее пяти минут на всех узлах домена будет выбран **Автоматический режим**, в качестве NTP-сервера будет указан ip-адрес сервера ITRIUM. Дополнительную информацию см. разделе [Настройка «Службы НЕЙРОСС»](#).
- **Посредством веб-интерфейса**: в разделе **Сеть** выберите устройства, нажмите на кнопку **Синхронизация времени** и введите 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](#).

**Примечание.** Для «НЕЙРОСС Центр», «Контроль операторов» и ITRUIM установка синхронизации времени по NTP-серверу задаётся на самом сервере средствами операционной системы.

#### 4. Технологические входы

В данном разделе выполняется настройка параметров трёх дискретных сигналов контроля технического состояния устройства: сигнала неисправности источника питания (**AF**), неисправности аккумулятора (**PF**) и датчика вскрытия корпуса прибора (**Tamper**).

1. Перейдите к веб-интерфейсу, выберите раздел [Конфигурация узлов](#) — **Технологические входы**. Задайте для каждого из технологических входов параметр активности входа согласно рекомендациям ниже.
2. Если вход используется, в поле **Вход активен** должно быть установлено значение **Да**.
3. В поле **Нормально открыт** установите нормальное состояние входа. Если значение **Да** – вход нормально открыт (то есть в нормальном состоянии вход разомкнут), если значение **Нет** – нормально замкнут (в нормальном состоянии вход замкнут).

**Примечание.** В поле **Название** вы можете задать новое название входа.

4. Нажмите на кнопку **Сохранить**.

##### Вход PF

Дискретный вход **Неисправность ИП** предназначен для приёма сигнала о неисправности внешнего источника питания.

В случае, если источник бесперебойного питания не используется или не выполняет функции контроля первичных источников питания, для предотвращения получения сообщений о неисправности ИП, установите значение поля **Вход активен** в значение **Нет**. Если вход не активен, его состояние не учитывается (всегда в состоянии [Норма]).

##### Вход AF

Дискретный вход **Неисправность аккумулятора** предназначен для приёма сигнала о неисправности аккумулятора источника питания.

В случае, если источник бесперебойного питания не используется или не выполняет функции контроля исправности аккумулятора, для предотвращения получения сообщений о неисправности аккумулятора, установите значение поля **Вход активен** в значение **Нет**. Если вход не активен, его состояние не учитывается (всегда в состоянии [Норма]).



## Тампер

Плата устройства оснащена датчиком вскрытия корпуса устройства (тампером). В случае, если контроль вскрытия корпуса проводить не требуется, установите значение поля **Вход активен** в значение **Нет**. Если вход не активен, его состояние не учитывается (всегда в состоянии [Норма]).

**Примечание. Включено** – флаг, определяющий состояние входа. Если значение **нет**, вход находится в нормальном состоянии, если **да** – вход находится в тревожном состоянии. Нормальное состояние входа определяется свойством **Нормально открыт**.

## 5. Точки доступа

Раздел **Доступ** предназначен для задания параметров точек доступа в случае, если прибор будет использоваться в качестве контроллера доступа.

**Примечание.** Если подключение считывателей, замковых устройств, кнопок выхода и дверных контактов не планируется, в поле **Режим работы** установите значение **Пользовательский**. Соответствующие выходы могут использоваться для подключения шлейфов охранной сигнализации. Тревожные извещения от системы охранной сигнализации и системы контроля доступа передаются параллельно и независимо друг от друга.

Если точку доступа планируется использовать только для постановки на охрану и снятия с охраны разделов сигнализации в поле **Исключена** установите значение **Да**.

1. Перейдите к веб-интерфейсу, выберите раздел [Конфигурация узлов — Доступ](#).
2. В поле **Режим работы** задайте требуемый режим работы точки/точек доступа.
3. Задайте параметры точки доступа (описание см. в таблице 9.10). При выборе режима работы «Две односторонние» задайте параметры последовательно для каждой точки доступа (с помощью переключения вкладок **Точка доступа 1/Точка доступа 2**). При выборе режима «Одна двусторонняя», задайте параметры двусторонней точки доступа.
4. Нажмите на кнопку **Сохранить**.

Таблица 9.10 — Настройки точки/точек доступа

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Режим работы	Пользовательский Две односторонние Одна двусторонняя	Две односторонние	Выберите из раскрывающегося списка режим работы, который указывает на способ организации прохода через данную точку доступа: в одном направлении или в двух. Может осуществляться управление доступом через две односторонние или одну двустороннюю точку прохода.

Параметр	Диапазон значений	Значение по умолчанию	Примечание
<b>Основные параметры</b>			
Название	Любое текстовое описание	Точка доступа 1 Точка доступа 2	Введите название точки доступа. Поле доступно при выборе режима работы «Две односторонние». Данное название будет отображаться в списках точек доступа для выбора терминала постановки/снятия или задания зон доступа.
Режим идентификации	по карте по карте и пинкоду по карте или пинкоду	по карте	Выберите из раскрывающегося списка набор данных, которые необходимо предъявить для разрешения доступа.
Число попыток ввода данных	целое число	5	Число разрешённых попыток ввода пинкода. Указывается при выборе Режим работы «по карте и пинкоду» и предназначено для выявления попыток подбора пинкода. При превышении заданного числа попыток, формируется тревожное сообщение «Попытка подбора идентификатора».
Время ожидания ввода данных	целое число	20	Промежуток времени, в течение которого ожидается ввод пинкода. Указывается при выборе Режим работы «по карте и пинкоду». Если данные введены неправильно, счётчик времени перезапускается, до окончания <b>Числа попыток ввода данных</b> .
<b>Проход под принуждением</b>			
Контроль прохода под принуждением	Да Нет	Нет	Поле доступно, если выбран режим работы <b>по карте и пинкоду</b> . Владелец карты может сигнализировать оператору о том, что совершает проход под угрозой со стороны другого лица. Если указано <b>Да</b> , при вводе кода принуждения формируется тревожное извещение. Разрешение прохода по коду принуждения задаётся в поле <b>Отказ по коду принуждения</b> . Код принуждения задаётся в свойствах пропуска.

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Отказ по коду принуждения	Да Нет	Нет	Поле доступно, если задан <b>Контроль прохода под принуждением</b> . Если задано <b>Нет</b> , после ввода кода принуждения формируется тревожное извещение, но проход разрешается. Если задано <b>Да</b> , после ввода кода принуждения формируется тревожное извещение и проход не разрешается (настоятельно не рекомендуется использовать данную возможность).
<b>Проход с подтверждением</b>			
Ожидать подтверждения на ВХОД	Да Нет	Нет	Если задано <b>Да</b> , для разрешения прохода требуется подтверждение оператора. В настоящий момент не реализовано.
Ожидать подтверждения на ВЫХОД	Да Нет	Нет	Если задано <b>Да</b> , для разрешения прохода требуется подтверждение оператором. В настоящий момент не реализовано.
Время ожидания подтверждения, с	Целое число	5	Укажите период времени в секундах, в течение которого будет ожидаться подтверждение от оператора. Если по истечению указанного периода времени подтверждение не поступит, доступ будет разрешён или запрещён в зависимости от значения поля <b>Разрешать по истечению времени</b> .
Разрешать по истечению времени	Да Нет	Нет	Если задано <b>Да</b> , по истечению периода времени <b>Время ожидания подтверждения</b> , доступ будет разрешён. Если задано <b>Нет</b> , по истечению указанного периода времени, доступ будет запрещён.

Параметр	Диапазон значений	Значение по умолчанию	Примечание
<b>Контроль повторного прохода</b>			
Режим контроля повторного прохода	Без контроля Мягкий Жёсткий	Без контроля	<p>Выберите из раскрывающегося списка требуемый режим контроля повторного прохода (antipassbak).</p> <p>Если задано <b>Без контроля</b>, контроль повторного прохода не осуществляется.</p> <p>Если задано <b>Мягкий</b>, контроль повторного прохода осуществляется в мягком режиме (при нарушении режима доступ разрешается, но формируется тревожное извещение).</p> <p>Если задано <b>Жёсткий</b>, контроль повторного прохода осуществляется в жёстком режиме (при нарушении режима доступ запрещается, формируется тревожное извещение «Нарушение правил контроля повторного прохода»).</p>
Зона ВХОД	нет [№ зоны]. [Наименование зоны]	нет	<p>Выберите из раскрывающегося списка:</p> <ul style="list-style-type: none"> <li>• для односторонней точки доступа – зону расположения считывателя;</li> <li>• для двусторонней точки доступа – зону расположения считывателя на вход (первого считывателя).</li> </ul>
Зона ВЫХОД	нет [№ зоны]. [Наименование зоны]	нет	<p>Выберите из раскрывающегося списка:</p> <ul style="list-style-type: none"> <li>• для односторонней точки доступа – зону расположения кнопки выхода;</li> <li>• для двусторонней точки доступа – зону расположения считывателя на выход (второго считывателя).</li> </ul>
Контроль проходов за интервал времени			Функционал будет реализован в последующих версиях прошивки прибора.
Время контроля повторного прохода, мин			Функционал будет реализован в последующих версиях прошивки прибора.
<b>Доступ по правилу N-лиц</b>			
Ожидание по правилу N-лиц	Да Нет	Нет	Если задано <b>Да</b> , будет осуществляться режим двойной (тройной и т.д.) идентификации.
Количество лиц	целое число	2	Укажите количество лиц, которые должны предъявить валидные идентификаторы для разрешения прохода.
Время ожидания ввода данных, с	целое число	10	Укажите период времени, в течение которого будет ожидаться предъявление идентификатора другого лица.

Параметр	Диапазон значений	Значение по умолчанию	Примечание
<b>Охранная сигнализация</b>			
Исключена (использовать только для постановки/снятия)	Да Нет	Нет	Если задано <b>Да</b> , точка доступа не используется для обеспечения прохода, используется только для постановки /снятия разделов охранной сигнализации. Если задано Нет, точка доступа может использоваться для обеспечения контроля доступа для и постановки /снятия разделов. Привязка разделов к точке доступа осуществляется в разделе <b>Терминалы</b> .
Таймаут постановки/снятия	целое число	60	Задержка постановки на охрану - временной интервал в секундах, по истечении которого все привязанные к точке доступа разделы встанут на охрану, либо задержка перехода в тревогу – временной интервал в секундах, в течение которого необходимо выполнить снятие с охраны, прежде чем раздел(ы) перейдет в состояние тревоги.
Блокировать при взятии всех разделов	Да Нет	Да	Если задано <b>Да</b> , в ситуации, когда все разделы, «привязанные к точке доступа» находятся в состоянии [На охране], точка доступа блокируется до снятия хотя бы одного раздела с охраны.
Разблокировать при тревоге	нет [список охранных зон]	нет	Выберите из раскрывающегося списка зону, при переходе которой в состояние [Тревога] точка доступа должна быть разблокирована (обеспечен свободный проход).
Блокировать при тревоге	нет [список охранных зон]	нет	Выберите из раскрывающегося списка зону, при переходе которой в состояние [Тревога] точка доступа должна быть заблокирована.

Параметр	Диапазон значений	Значение по умолчанию	Примечание
<b>Замок</b>			
Закрывать замок	По закрытию двери По открытию двери По истечении времени	По открытию двери	<p>Выберите из раскрывающегося списка требуемое значение.</p> <ul style="list-style-type: none"> <li>Если выбрано <b>По закрытию двери</b>, то замок закрывается по факту закрытия двери после её открытия. Если дверь не была открыта, замок закрывается через указанный в поле <b>Время ожидания открытия двери</b> период времени.</li> <li>Если выбрано <b>По открытию двери</b>, то замок закрывается по факту открытия двери. Если дверь не была открыта, замок закрывается через указанный в поле <b>Время ожидания открытия двери</b> период времени.</li> <li>Если выбрано <b>По истечении времени</b>, то замок закрывается через указанный в поле <b>Время открытия замка</b> период времени. Указанное значение копируется в поле <b>Время ожидания открытия двери</b>.</li> </ul>
Время открытия замка, с.	1 — 255	10	<p>Укажите период ожидания (таймаут) открытия двери (используется для режима закрытия замка <b>По истечении времени</b>; см. поле выше).</p> <p>Поле недоступно, если в поле <b>Закрывать замок</b> задано <b>По закрытию двери</b> или <b>По открытию двери</b>.</p>
<b>Кнопка выхода</b>			
Использовать кнопку выхода	Да Нет	Да	<p>Если задано <b>Нет</b>, кнопка выхода не контролируется, не используется, не подключается. При этом поле <b>Инициировать проход когда контакт</b> становится недоступным.</p>
Инициировать проход когда контакт	Замкнут Разомкнут	Замкнут	<p>Укажите состояние кнопки выхода, которое иницирует проход (разблокирует дверь).</p> <ul style="list-style-type: none"> <li>Если задано <b>Замкнут</b>, проход иницируется при замыкании кнопки выхода.</li> <li>Если задано <b>Разомкнут</b>, проход иницируется при размыкании кнопки выхода.</li> </ul>

Параметр	Диапазон значений	Значение по умолчанию	Примечание
<b>Считыватель</b>			
Название	текст	Точка доступа 1 Точка доступа 2	Поле доступно, если задан режим работы <b>Одна двусторонняя</b> . Введите наименование каждого считывателя для индикации направления прохода и источника извещений.
Маска номера карты	64 бита в HEX-представлении		Маска номера карты в HEX-представлении. Номер карты в базе содержит 64 бита. Если номер со считывателя длиной 26 бит, то свободные биты в конце заполняются нулями. Если нужно «отбросить» некоторые биты (например, фасилити-код) то в маске они заполняются нулями. Значимые биты в маске помечаются единицами. Итоговая последовательность преобразуется в HEX-представление. Например, структура записи на карте Виеганд-26: PFFFFFFFCCCCCCCCCCCCCCCCCP, где P - биты паритета, C- биты кода карты, F- биты фасилити-кода (не используется). Значение маски: 007FFF8000000000 (рисунок 9.49).

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Формат карты	Автоматически «Сырой»(64 бита) «Сырой» (с переменной длиной)	Автоматически	<p>Задаёт преобразование номера карты.</p> <ul style="list-style-type: none"> <li>Если задано <b>Автоматически</b>, определяет длину (26 или 37 бит), выделяет фасилити-код и номер карты.</li> <li>Если задано <b>«Сырой» (64 бита)</b>, то номер карты в двоичном виде будет дополнен до 64 бит записанными в конец нулями. В десятичном выражении номер карты будет представлять собой большое число. Фасилити пустой.</li> <li>Если задано <b>«Сырой» (с переменной длиной)</b>, то номер карты в ячейке 64 бит будет сдвинут к младшим битам, а старшие биты будут заполнены нулями. Так как нулевые старшие биты отбрасываются, то номер будет представлять собой фактически 26 или 37 бит, и в десятичном формате станет числом, для которого легко провести обратное преобразование. Фасилити пустой.</li> </ul> <p>Маска номера карты накладывается после преобразования.</p>
<b>Дверь</b>			
Дверь без дверного контакта	Да Нет	Нет	Функционал будет реализован в последующих версиях прошивки прибора.
Дверь закрыта когда контакт	Замкнут Разомкнут	Замкнут	Укажите нормальное состояние дверного контакта.
Ждать закрытия двери	Да Нет	Да	<p>Настройка определяет алгоритм предоставления доступа.</p> <ul style="list-style-type: none"> <li>Если задано <b>Да</b>, то проход считается совершенным по факту закрытия двери (после её открытия). До закрытия двери игнорируется повторное предъявление идентификаторов. В поле <b>Ждать открытия двери</b> автоматически устанавливается значение <b>Да</b>.</li> <li>Если задано <b>Нет</b>, то алгоритм доступа определяется в поле <b>Ждать открытия двери</b>.</li> </ul> <p>Описание см. в таблице <a href="#">9.11</a>.</p>
Время ожидания закрытия двери, с.	1 — 255	10	Укажите период ожидания закрытия двери. По истечении указанного периода времени будет зафиксирована ситуация удержания двери.



Параметр	Диапазон значений	Значение по умолчанию	Примечание
Ждать открытия двери	Да Нет	Да	<p>Настройка определяет алгоритм предоставления доступа. Поле доступно для редактирования, если в поле <b>Ждать закрытия двери</b> установлено <b>Нет</b>.</p> <ul style="list-style-type: none"> <li>Если задано <b>Да</b>, то проход считается совершенным по факту открытия двери.</li> <li>Если задано <b>Нет</b>, по проход считается совершенным по факту предъявления карты.</li> </ul> <p>Описание см. в таблице <a href="#">9.11</a>.</p>
Время ожидания открытия двери, с.	1 — 255	10	<p>Укажите период ожидания от момента разрешения доступа до открытия двери. Если дверь не была открыта, по истечении указанного периода времени будет зафиксирована ситуация «проход не совершён», дверь будет автоматически закрыта.</p>

```

| PFFF.FFFF | FCCC.CCCC | CCCC.CCCC | CP00.0000 | 0000.0000 | 0000.0000 | 0000.0000 | 0000.0000 | от считывателя
| 0000.0000 | 0111.1111 | 1111.1111 | 1000.0000 | 0000.0000 | 0000.0000 | 0000.0000 | 0000.0000 | маска Bin
| 0 0 | 7 F | F F | 8 0 | 0 0 | 0 0 | 0 0 | 0 0 | маска Hex
| 0000.0000 | 0CCC.CCCC | CCCC.CCCC | C000.0000 | 0000.0000 | 0000.0000 | 0000.0000 | 0000.0000 | результат
наложения маски

```

Рисунок 9.49 — Пример формирования маски для карт Wiegand-26

Алгоритм доступа и формирование событий «Проход совершён», «Проход не совершён», «Дверь удержана открытой» напрямую зависит от комбинации значений полей **Ждать закрытия двери**, **Ждать открытия двери** (см. таблицу 9.11).

Таблица 9.11 — Зависимость формирования событий доступа от настроек точки доступа

	Ждать открытия двери	
	Да	Нет

Ждать закрытия двери	<b>Да</b>	Проход считается совершенным, если дверь была открыта в период времени, указанный в поле <b>Время ожидания открытия двери</b> . Если дверь не была открыта, формируется сообщение «Проход не совершён». Если дверь была закрыта в период времени, указанный в поле <b>Время ожидания закрытия двери</b> , формируется сообщение «Проход совершён». Если дверь не была закрыта до истечения времени ожидания закрытия двери, то формируется сообщение «Дверь удержана открытой». До закрытия двери игнорируется повторное предъявление идентификатора. При закрытии двери формируются сообщения «Удержание двери (восстановление)» и «Проход совершён».	—
	<b>Нет</b>	Проход считается совершенным по факту открытия двери, формируется сообщение «Проход совершён». Если дверь не была открыта, формируется сообщение «Проход не совершён». Допускается предъявление нескольких карт до закрытия двери. Таймеры ожидания открытия/закрытия двери перезапускаются.	Проход считается совершенным по факту предъявления карты, формируется сообщение «Проход совершён», сразу допускается предъявление идентификатора. Таймер ожидания закрытия двери перезапускается.

### Тестирование правильности настройки точки доступа

Для решения задачи проверки правильности настройки точки доступа введены функции тестовой блокировки, разблокировки, восстановления дежурного режима, имитации нажатия кнопки выхода. Все необходимые команды размещены в правом верхнем углу окна **Доступ** в раскрывающемся списке **Действия** (см. таблицу 9.12).

Таблица 9.12 — Команды управления точкой доступа

Команда	Описание
Инициировать проход	Команда выполняет действие, аналогичное нажатию кнопки выхода. Дверь разблокируется на период времени, указанный в поле <b>Время ожидания открытия двери</b> .
Разблокировать	Команда разблокировки точки доступа. Разрешён проход без предъявления идентификаторов. Дополнительную информацию см. в разделе Режим <a href="#">«Разблокировано»</a> .
Заблокировать	Команда блокировки точки доступа. Проход запрещён. Дополнительную информацию см. в разделе Режим <a href="#">«Заблокировано»</a> .
Восстановить режим	Команда восстановления точки доступа в состояние по умолчанию (см. раздел <a href="#">Смена состояний зон и разделов при постановке на охрану</a> ). Отменяет команды <b>Заблокировать/Разблокировать</b> . Дополнительную информацию см. в разделе Дежурный <a href="#">режим</a> .

В поле **Статус** указывается текущее состояние точки доступа (при наведении указателя мыши, отображается расширенное описание)

## 6. Зоны сигнализации

Раздел «Охранная сигнализация» предназначен для задания параметров охранных шлейфов.

Так как факт подключения шлейфов к входам «ЯРС» не контролируется, для каждого устройства автоматически формируется 38 охранных зон. По умолчанию для всех зон установлен режим контроля **Исключена**. Это значит, что шлейф не подключается, состояние зоны не контролируется. При изменении режима контроля, зона становится «активной», её состояние контролируется.

**Примечание.** «Активная» зона является распределённым ресурсом, информация о ней загружается в другие узлы сети при синхронизации данных (см. раздел [Синхронизация данных между узлами НЕЙРОСС](#)).

Выполните следующую последовательность шагов:

1. Перейдите к веб-интерфейсу, выберите раздел [Конфигурация узлов](#) — **Охранная сигнализация**.
2. Последовательно для каждой охранной зоны задайте параметры зоны (описание см. в таблице 9.13), каждый раз нажимая на кнопку **Сохранить** для сохранения настроек текущей зоны.

**Примечание.** Для облегчения процедуры конфигурирования предусмотрена функция групповой настройки. При необходимости задания одинаковых параметров для нескольких зон, отметьте флажками требуемые зоны и нажмите на кнопку **Настроить** в правой части окна интерфейса (в скобках справа от кнопки указано число выбранных зон).

Таблица 9.13 — Параметры охранной зоны

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Название	Любое текстовое описание	Зона 0.RIN.(1-8)	Введите название охранной зоны. В списке зон «Борея» также присутствуют зоны адресной линии S-ART: Зона 0.SART.(0-29)
Нормально открыт	Да Нет	Нет	Нормальное состояние тревожных извещателей шлейфа. <ul style="list-style-type: none"><li>• Если задано <b>Да</b>, извещатели нормально открытые (то есть в нормальном состоянии их выходные цепи разомкнуты).</li><li>• Если задано <b>Нет</b>, извещатели нормально замкнутые (в нормальном состоянии их выходные цепи замкнуты).</li></ul>

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Режим контроля	По-умолчанию Исключена Охрана 24 часа	По умолчанию	<p>Определяет режим контроля шлейфа.</p> <ul style="list-style-type: none"> <li>Если задано <b>По умолчанию</b>, возможен сброс тревоги зоны, постановка на охрану и снятие с охраны. Формируются извещения об изменениях состояния зоны.</li> <li>Если задано <b>Исключена</b>, то сообщения об изменениях состояния зоны не формируются, команды не доступны.</li> <li>Если задано <b>Охрана 24 часа</b>, после постановки на охрану снять зону с охраны невозможно, возможен только сброс тревоги. Формируются извещения об изменениях состояния зоны. Предназначено для конфигурирования кнопок тревожно-вызывной сигнализации.</li> </ul>
Длительная охрана	Да Нет	Нет	Если задано <b>Да</b> , после постановки на охрану попытка снятия с охраны приводит к формированию тревожного извещения, формируются извещения об изменениях состояния зоны.
Защёлка тревоги	Да Нет	Да	Тревожное состояние шлейфа «защёлкивается» до снятия с охраны или сброса тревоги (не отменяется при восстановлении шлейфа).
Тип сигнализации	Охранная сигнализация Контроль состояния охраны	Охранная сигнализация	Выберите вариант установки.
Тип шлейфа	С контролем неисправности Без контроля неисправности	С контролем неисправности	Поле доступно только для зон, образуемых восьмью радиальными шлейфами «ЯРС» (название по умолчанию <b>Зона 0.RIN.1–Зона 0.RIN.8</b> ). Укажите, требуется ли проводить контроль цепи нагрузки (дополнительную информацию см. в разделе <a href="#">Шлейфы сигнализации</a> ).
Задержка перехода в тревогу (в секундах)	Целое число	0	<p>Укажите промежуток времени до перехода зоны в тревожное состояние.</p> <ul style="list-style-type: none"> <li>Если задано <b>0</b>, зона переходит в состояние [Тревога] сразу после нарушения шлейфа.</li> <li>Если установлено ненулевое значение, при нарушении шлейфа состояние изменяется с [Норма] на [Отложенная тревога]. По истечении заданного периода времени, если снятие с охраны или восстановление шлейфа не произошло, состояние меняется на [Тревога]; в противном случае состояние сбрасывается.</li> </ul>

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Задержка постановки на охрану (в секундах)	Целое число	0	Задайте временной интервал в секундах, по истечении которого будет предпринята попытка постановки зоны на охрану. Если шлейф находится не в нормальном состоянии, зона перейдет в состояние [Невзятие], при восстановлении шлейфа зона будет взята на охрану.
Тревога в снятой с охраны зоне	Да Нет	Нет	Если значение <b>Да</b> , при возникновении тревоги в состоянии [Снята с охраны], формируется тревожное извещение.

### Тестирование правильности настройки зон

Для решения задачи проверки правильности настройки зоны сигнализации введены функции тестовой постановки на охрану, снятия с охраны, а также сброса тревоги.

Для этого отметьте флажками зону/зоны и выберите требуемую команду в правой части окна интерфейса: **Снять с охраны**, **Поставить на охрану**, **Сбросить тревогу**.

**Примечание.** Команда удаления введена на случай появления в интерфейсе «фантомных» зон. Тогда рекомендуется удалить в интерфейсе все зоны и перезагрузить прибор. После перезагрузки все зоны будут заново вычитаны из устройства (см. раздел [Перезапуск узла](#)).

## 7. Модули расширения

Раздел **Модули расширения** предназначен для поиска, конфигурирования, мониторинга состояний и управления модулями «М2» и «МДС», подключаемыми по линии Lon-Works.

В левой части раздела отображается список доступных LON-модулей (М2 и МДС), в правой части отображаются параметры и состояния выбранного в левой части модуля (рисунок 9.50).

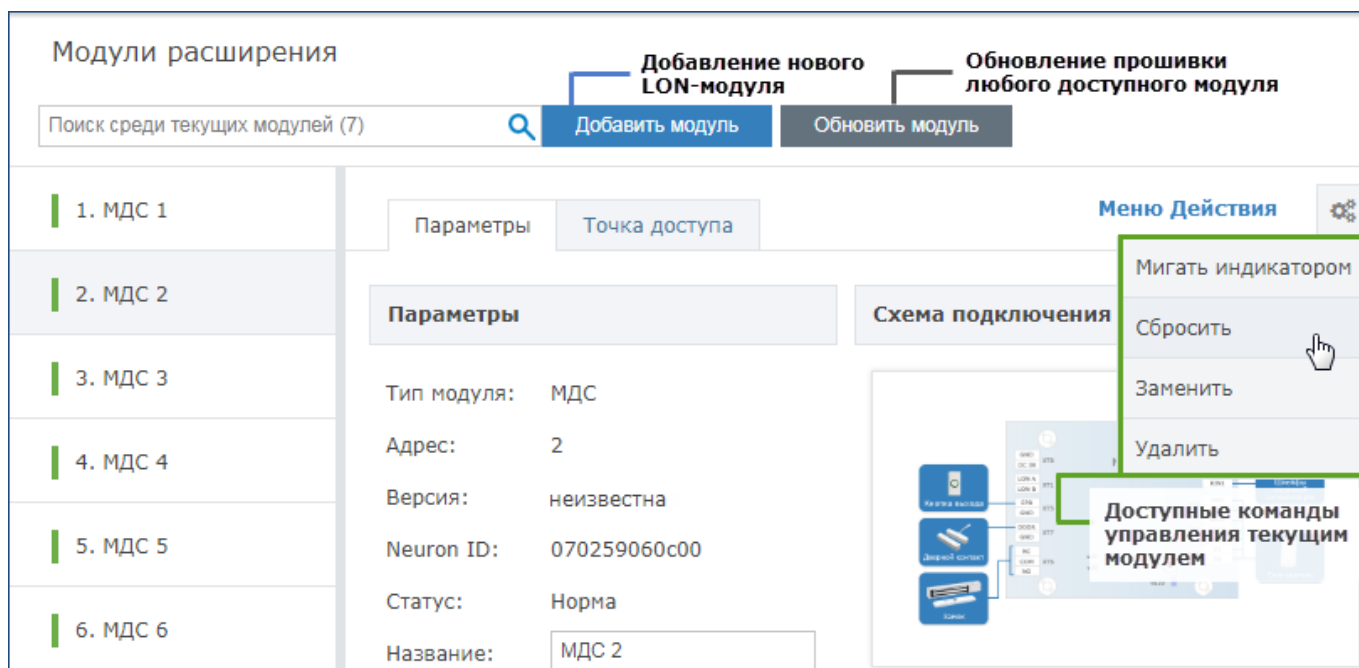


Рисунок 9.50 — Окно раздела **Модули расширения**

### Добавление М2/МДС

Добавление модуля в систему включает:

- Поиск модуля по его уникальному 48-разрядному коду NeuronID, позволяющему однозначно идентифицировать устройство;
- Назначение модулю логического (аппликационного) адреса в диапазоне от 1 до 127 (заводской адрес – 0). Адрес записывается по команде ЯРС в энергонезависимую память чипа Neuron M2 или МДС;
- Автоматическую (скрытую от пользователя) настройку параметров LON-соединения.

Чтобы установить М2 или МДС:

1. Подключите к сети LonWorks и включите питание всех М2 или МДС согласно имеющемуся проекту (если это не было сделано ранее).
2. Перейдите к веб-интерфейсу. Выберите раздел [Конфигурация узлов](#) — [Модули расширения](#). Нажмите на кнопку **Добавить модуль**, расположенную в верхней части раздела (рисунок [9.50](#)).
3. В отобразившемся окне (рисунок [9.51](#)) запрашивается уникальный идентификатор NeuronID модуля. Введите код вручную или нажмите на кнопку **Service pin**, расположенную на плате модуля, для отправки в сеть LonWorks широкополосного сообщения с Neuron ID модуля (схему расположения кнопки **Service pin** на плате модуля М2 см. на рисунке [1.10](#), на плате МДС см. на рисунке [1.12](#)). После нажатия на кнопку, в окне **Добавление модуля** отобразится Neuron ID модуля (рисунок [9.51](#)). Нажмите на кнопку **Добавить**.

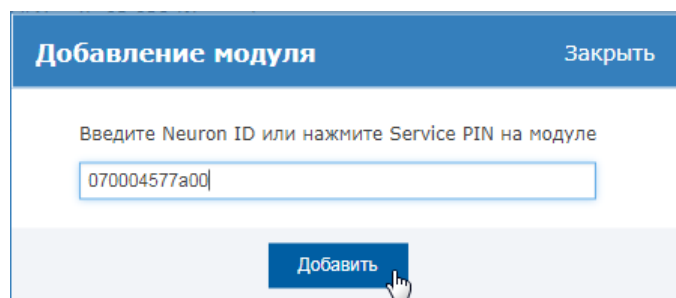


Рисунок 9.51 — Окно добавления LON-модуля

4. Выбранный модуль будет добавлен в систему. Ему будет присвоен аппликационный адрес согласно очередности.
5. Повторите п.п.2 – 4 для каждого последующего LON-модуля.
6. Настройте добавленные M2/МДС (см. раздел [Настройка M2/МДС](#)).

## Настройка M2/МДС

Выполните следующие шаги:

1. Перейдите к веб-интерфейсу, выберите раздел [Конфигурация узлов](#) — [Модули расширения](#).
2. В списке добавленных в систему M2/МДС выберите модуль, параметры которого требуется настроить.
3. На вкладке **Параметры** задайте параметры модуля согласно рекомендациям в таблице 9.14.
4. На вкладке **Точка доступа** задайте параметры точки доступа (описание см. в таблице 9.15).
5. На вкладке **Зоны сигнализации** задайте параметры шлейфов охранной сигнализации (описание см. в таблице ). **В текущей версии не реализовано!**
6. Нажмите на кнопку **Сохранить (CTRL+S)**.

**Примечание 1.** Для ускорения процедуры настройки однотипных точек доступа добавлена функция копирования настроек. Для этого:

- На странице точки-донора нажмите на кнопку **Скопировать настройки**.
- Последовательно перейдите к страницам настройки точек-реципиентов и нажмите на кнопку **Вставить настройки**. При необходимости внесите изменения и нажмите на кнопку **Сохранить (CTRL+S)**.


**Примечание 2.** Команды проверки работоспособности точек доступа M2/МДС аналогичны соответствующим командам «ЯРС» (см. раздел [Тестирование правильности настройки точки доступа](#)). Меню команд раскрывается нажатием кнопки **Действия** на странице настройки точки доступа  **Действия** ▼.

Таблица 9.14 — Настройка общих параметров модулей M2/МДС

Блок	Параметр	Описание
Параметры	Тип модуля	Поддерживаемые типы модулей: M2, МДС

Блок	Параметр	Описание
	Адрес	Аппликационный адрес модуля Адрес присваивается в процессе добавления модуля (см. раздел <a href="#">Добавление M2/МДС</a> ).
	Версия	Номер версии (прошивки) модуля: <ul style="list-style-type: none"> <li>Atmel — версия программного обеспечения процессора Atmel на плате модуля;</li> <li>Neuron — версия программного обеспечения процессора NEURON.</li> </ul> Информация по обновлении версии представлена в разделе <a href="#">Обновление LON-модулей</a> .
	NeuronID	Уникальный идентификатор чипа Neuron® модуля Предназначен для идентификации устройства в сети Lonworks (см. раздел <a href="#">Понятие LonWorks</a> ).
	Статус	Текущее состояние модуля. Определяется суммарным состоянием его зон и точек доступа (см. раздел <a href="#">Состояния элементов прибора</a> ).
	Название	Текстовое описание модуля. Будет указываться в названии после типа устройства и его адреса, например, «МДС 2. Главный вход».
Входы	Тампер	Тампер вскрытия корпуса. По умолчанию включён, осуществляется контроль вскрытия корпуса. Статус входа (используется или не используется) определяет, требуется ли контролировать состояние данного входа.
Статистика	Ошибки...	Тренды увеличения количества ошибок. Могут сигнализировать о некорректной работе модуля.

Таблица 9.15 — Настройки точки доступа «M2»/«МДС»

Параметр	Диапазон значений	Значение по умолчанию	Примечание
<b>Основные параметры</b>			
Название	Любое текстовое описание	Точка доступа	Введите название точки доступа, которое будет отображаться в списках точек доступа для выбора терминала постановки/снятия или задания зон доступа.
Режим работы считывателя	по карте по пинкоду по карте и пинкоду по карте или пинкоду	по карте	Выберите из раскрывающегося списка набор данных, которые необходимо предъявить для разрешения доступа.



Параметр	Диапазон значений	Значение по умолчанию	Примечание
<b>Проход под принуждением</b>			
Контроль прохода под принуждением	Да Нет	Нет	Поле доступно, если выбран режим работы по пинкоду, по карте и пинкоду. Владелец карты сможет сигнализировать оператору о том, что совершает проход под угрозой со стороны другого лица. Если указано <b>Да</b> , при вводе кода принуждения формируется тревожное извещение. Разрешение прохода по коду принуждения задаётся в поле <b>Отказ по коду принуждения</b> . Код принуждения задаётся в свойствах пропуска.
Отказ по коду принуждения	Да Нет	Нет	Поле доступно, если задан <b>Контроль прохода под принуждением</b> . Если задано <b>Нет</b> , после ввода кода принуждения формируется тревожное извещение, но проход разрешается. Если задано <b>Да</b> , после ввода кода принуждения формируется тревожное извещение и проход не разрешается (настоятельно не рекомендуется использовать данную возможность).
<b>Контроль повторного прохода</b>			
Режим контроля повторного прохода	Без контроля Мягкий Жёсткий	Без контроля	Выберите из раскрывающегося списка требуемый режим контроля повторного прохода (antipassbak). Если задано <b>Без контроля</b> , контроль повторного прохода не осуществляется. Если задано <b>Мягкий</b> , контроль повторного прохода осуществляется в «мягком» режиме (при нарушении режима доступ разрешается, но формируется тревожное извещение). Если задано <b>Жёсткий</b> , контроль повторного прохода осуществляется в жёстком режиме (при нарушении режима доступ запрещается, формируется тревожное извещение «Нарушение правил контроля повторного прохода»).
Зона ВХОД	нет [№ зоны]. [Наименование зоны]	нет	Выберите из раскрывающегося списка: для односторонней точки доступа – зону расположения считывателя; для двусторонней точки доступа – зону расположения считывателя на вход (первого считывателя).

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Зона ВЫХОД	нет [№ зоны]. [Наименование зоны]	нет	Выберите из раскрывающегося списка: для односторонней точки доступа – зону расположения кнопки выхода; для двусторонней точки доступа – зону расположения считывателя на выход (второго считывателя).
<b>Замок</b>			
Закрывать замок	По закрытию двери По открытию двери По истечении времени	По открытию двери	Выберите из раскрывающегося списка требуемое значение. Если выбрано <b>По закрытию двери</b> , то замок закрывается по факту закрытия двери после её открытия. Если дверь не была открыта, замок закрывается через указанный в поле <b>Время ожидания открытия двери</b> период времени. Если выбрано <b>По открытию двери</b> , то замок закрывается по факту открытия двери. Если дверь не была открыта, замок закрывается через указанный в поле <b>Время ожидания открытия двери</b> период времени. Если выбрано <b>По истечении времени</b> , то замок закрывается через указанный в поле <b>Время открытия замка</b> период времени. Указанное значение копируется в поле <b>Время ожидания открытия двери</b> .
Время открытия замка, 0,1 с.	1 — 255	10	Укажите период ожидания (таймаут) открытия двери (используется для режима закрытия замка <b>По истечении времени</b> ; см. поле выше). Обратите внимание, что значение указывается в 0,1 сек (5 секунд соответствует 50 в значениях поля). Поле недоступно, если в поле <b>Закрывать замок</b> задано <b>По закрытию двери</b> или <b>По открытию двери</b> .
Задержка закрытия замка, сек	1 — 255	0	Поле предусмотрено во избежание повреждения ригельных замков при закрытии замка колеблющейся двери. Задаёт задержку от получения команды на закрытие двери до фактического закрытия двери. Взлом двери контролируется.
<b>Организация двусторонней точки доступа</b>			

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Связанная точка доступа	Список точек доступа	Не выбрана	<p>Выберите из раскрывающегося списка точку доступа, совместно с которой будет осуществляться контроль двустороннего прохода.</p> <p><b>Внимание!</b> В настройках текущей и выбранной точки должна быть симметрично задана связь друг с другом, а также должны совпадать тайминги ожидания открытия/закрытия двери и режим работы кнопки выхода: <b>Разомкнут</b> для схемы с управлением замком включением питания и <b>Замкнут</b> для схемы с управлением отключением питания.</p>
<b>Кнопка выхода</b>			
Инициировать проход когда контакт	Замкнут Разомкнут	Замкнут	<p>Укажите состояние кнопки выхода, которое иницирует проход (разблокирует дверь).</p> <ul style="list-style-type: none"> <li>Если задано <b>Замкнут</b>, проход иницируется при замыкании кнопки выхода.</li> </ul> <p>Если задано <b>Разомкнут</b>, проход иницируется при размыкании кнопки выхода.</p>
<b>Считыватель</b>			
Маска номера карты	64 бита в HEX-представлении		<p>Маска номера карты в HEX-представлении.</p> <p>Номер карты в базе содержит 64 бита. Если номер со считывателя длиной 26 бит, то свободные биты в конце заполняются нулями. Если нужно «отбросить» некоторые биты (например, фасилити-код) то в маске они заполняются нулями. Значимые биты в маске помечаются единицами. Итоговая последовательность преобразуется в HEX-представление.</p> <p>Например, структура записи на карте Виеганд-26:  PFFFFFFFFCCCCCCCCCCCCCCCCCCP,  где P - биты паритета, C- биты кода карты, F- биты фасилити-кода (не используется).</p> <p>Значение маски: 007FFF8000000000 (рисунок 9.49).</p>

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Формат карты	Автоматически «Сырой»(64 бита) «Сырой» (с переменной длиной)	Автоматически	<p>Задаёт преобразование номера карты. Если задано <b>Автоматически</b>, определяет длину (Wiegand-26 или Wiegand-37), выделяет фасилити-код и номер карты.</p> <ul style="list-style-type: none"> <li>Если задано <b>«Сырой» (64 бита)</b>, то номер карты в двоичном виде будет дополнен до 64 бит записанными в конец нулями. В десятичном выражении номер карты будет представлять собой большое число. Фасилити пустой.</li> <li>Если задано <b>«Сырой» (с переменной длиной)</b>, то номер карты в ячейке 64 бит будет сдвинут к младшим битам, а старшие биты будут заполнены нулями. Так как нулевые старшие биты отбрасываются, то номер будет представлять собой фактически 26 или 37 бит, и в десятичном формате станет числом, для которого легко провести обратное преобразование. Фасилити пустой.</li> </ul> <p>Маска номера карты накладывается после преобразования.</p>
<b>Дверь</b>			
Ждать закрытия двери	Да Нет	Да	<p>Настройка определяет алгоритм предоставления доступа.</p> <p>Если задано <b>Да</b>, то проход считается совершенным по факту закрытия двери (после её открытия). До закрытия двери игнорируется повторное предъявление идентификаторов. В поле <b>Ждать открытия двери</b> автоматически устанавливается значение <b>Да</b>.</p> <p>Если задано <b>Нет</b>, то алгоритм доступа определяется в поле <b>Ждать открытия двери</b>.</p> <p>Описание см. в таблице <a href="#">9.11</a>.</p>
Время ожидания закрытия двери, с.	1 — 255	10	<p>Укажите период ожидания закрытия двери. По истечении указанного периода времени будет зафиксирована ситуация удержания двери.</p>

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Ждать открытия двери	Да Нет	Да	<p>Настройка определяет алгоритм предоставления доступа. Поле доступно для редактирования, если в поле <b>Ждать закрытия двери</b> установлено <b>Нет</b>.</p> <ul style="list-style-type: none"> <li>• Если задано <b>Да</b>, то проход считается совершенным по факту открытия двери.</li> <li>• Если задано <b>Нет</b>, по проход считается совершенным по факту предъявления карты.</li> </ul> <p>Описание см. в таблице <a href="#">9.11</a>.</p>
Время ожидания открытия двери, с.	1 — 255	10	<p>Укажите период ожидания от момента разрешения доступа до открытия двери. Если дверь не была открыта, по истечении указанного периода времени будет зафиксирована ситуация «проход не совершён», дверь будет автоматически закрыта.</p>
<b>Прочее</b>			

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Поведение в отсутствие ответа от модуля базы данных	Запретить доступ Использовать локальный буфер	Запретить доступ	<p>Определяет работу точки доступа при нарушении LON-соединения с контроллером «ЯРС», на котором хранится база данных пропусков и который принимает решение о разрешении и запрете доступа.</p> <ul style="list-style-type: none"> <li>• Если задано <b>Запретить доступ</b>, формируется отказ доступа для любых идентификаторов;</li> <li>• Если задано <b>Использовать локальный буфер</b>, разрешается доступ с идентификаторами, по которым уже когда-то было принято положительное решение (все предъявленные валидные идентификаторы сохраняются в локальной энергонезависимой памяти модуля ёмкостью до 1200 для «М2» и до 1500 для «МДС» пропусков соответственно). При превышении ёмкости памяти, удаляются наиболее «старые» данные по идентификаторам. Также удаление осуществляется, если при наличии связи с «ЯРС» предъявлен более не валидный идентификатор.</li> </ul> <p><b>Внимание!</b> Если более не валидный идентификатор предъявлен при отсутствии связи с «ЯРС» и его данные есть в буфере, доступ будет разрешён.</p>
Максимальное время ожидания ответа от модуля базы данных, с	1 — 255	3	<p>Период времени в секундах, по истечении которого при отсутствии ответа от «ЯРС» модуль переходит в режим запрета доступа или использования локального буфера.</p> <p><b>Внимание!</b> Заданное по умолчанию значение следует изменять только при использовании не стандартных алгоритмов доступа (например, при обеспечении работы шлюза).</p>

Таблица 9.16 — Параметры зон сигнализации «М2»/«МДС»

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Название	Любое текстовое описание		Введите название охранной зоны

Параметр	Диапазон значений	Значение по умолчанию	Примечание
Нормально открыт	Да Нет	Нет	Нормальное состояние тревожных извещателей шлейфа. <ul style="list-style-type: none"> <li>Если задано <b>Да</b>, извещатели нормально открытые (то есть в нормальном состоянии их выходные цепи разомкнуты).</li> <li>Если задано <b>Нет</b>, извещатели нормально замкнутые (в нормальном состоянии их выходные цепи замкнуты).</li> </ul>
Режим контроля	По-умолчанию Исключена Охрана 24 часа	По умолчанию	Определяет режим контроля шлейфа. <ul style="list-style-type: none"> <li>Если задано <b>По умолчанию</b>, возможен сброс тревожной зоны, постановка на охрану и снятие с охраны. Формируются извещения об изменениях состояния зоны.</li> <li>Если задано <b>Исключена</b>, то сообщения об изменениях состояния зоны не формируются, команды не доступны.</li> <li>Если задано <b>Охрана 24 часа</b>, после постановки на охрану снять зону с охраны невозможно, возможен только сброс тревог. Формируются извещения об изменениях состояния зоны. Предназначено для конфигурирования кнопок тревожно-вызывной сигнализации.</li> </ul>
Задержка постановки на охрану (в секундах)	Целое число	0	Задайте временной интервал в секундах, по истечении которого будет предпринята попытка постановки зоны на охрану. Если шлейф находится не в нормальном состоянии, зона перейдёт в состояние [Невзятие], при восстановлении шлейфа зона будет взята на охрану.
Задержка перехода в тревогу (в секундах)	Целое число	0	Укажите промежуток времени до перехода зоны в тревожное состояние. <ul style="list-style-type: none"> <li>Если задано <b>0</b>, зона переходит в состояние [Тревога] сразу после нарушения шлейфа.</li> <li>Если установлено ненулевое значение, при нарушении шлейфа состояние изменяется с [Норма] на [Отложенная тревога]. По истечении заданного периода времени, если снятие с охраны или восстановление шлейфа не произошло, состояние меняется на [Тревога]; в противном случае состояние сбрасывается.</li> </ul>
Тревога в снятой с охраны зоне	Да Нет	Нет	Если значение <b>Да</b> , при возникновении тревоги в состоянии [Снята с охраны], формируется тревожное извещение.
Защёлкивать тревогу в зоне	Да Нет	Да	Тревожное состояние шлейфа «защёлкивается» до снятия с охраны или сброса тревоги (не отменяется самостоятельно при восстановлении шлейфа).

**Примечание.** Так как факт подключения шлейфа к входам модулей не контролируется, для каждого устройства автоматически формируется набор охранных зон. Если шлейф не подключается, в поле **Режим контроля**, установите **Исключена**.

## Замена M2/МДС

«ЯРС» обеспечивает возможность замены неисправного модуля M2/МДС с автоматической перезаписью всех данных (конфигурации модуля). Таким образом, вам не потребуется дополнительно ничего настраивать. Новому модулю будет присвоен тот же аппликационный адрес, параметры входов/выходов, точек доступа и зон сигнализации не изменятся. Для произведения замены:

1. Физически отключите старый модуль и подключите новый. Переподключите всю периферию.
2. Перейдите к веб-интерфейсу. Выберите раздел [Конфигурация узлов](#) — [Модули расширения](#). В списке установленных в системе M2/МДС выберите устройство, которое требуется заменить.
3. В меню **Действия** (рисунок [9.50](#)) выберите команду **Заменить**.
4. В отобразившемся окне (рисунок 9.52) введите вручную Neuron ID или нажмите на кнопку **Service pin** на плате (аналогично процедуре добавления модуля, раздел [Добавление M2/МДС](#)). Нажмите на кнопку **Заменить**.

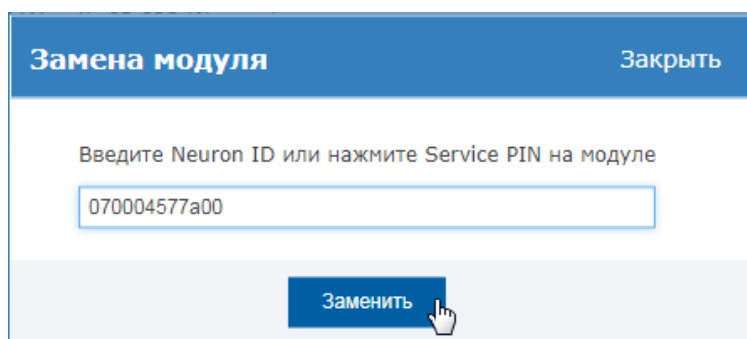


Рисунок 9.52 — Окно замены LON-модуля

5. Будет произведена запись конфигурации в новый модуль. Информация о новом Neuron ID модуля будет сохранена в «ЯРС».

## Удаление M2/МДС

Если какой-либо из модулей M2/МДС выведен из эксплуатации, его необходимо удалить из конфигурации системы. Для этого:

1. Перейдите к веб-интерфейсу. Выберите раздел [Конфигурация узлов](#) — [Модули расширения](#). В списке установленных в системе M2/МДС выберите устройство, которое требуется удалить.
2. В меню **Действия** (рисунок [9.50](#)) выберите команду **Удалить модуль**.

**Примечание.** Так как все настройки M2/МДС хранятся в памяти самого модуля, то после удаления исправного модуля и последующего повторного добавления в систему, все настройки самого модуля будут вычитаны и работоспособность будет восстановлена.



## Восстановление конфигурации М2/МДС

**Примечание.** В текущей версии не реализовано.

Так как информация о конфигурации М2/МДС хранится и в «ЯРС», и в самом модуле, для предотвращения коллизии данных, которая может возникнуть при смене конфигурации в условиях отсутствия связи с модулем, предусмотрена возможность перезаписи конфигурации модуля по данным «ЯРС». Для этого:

1. Перейдите к веб-интерфейсу. Выберите раздел [Конфигурация узлов](#) — [Модули расширения](#). В списке установленных в системе модулей выберите устройство, конфигурацию которого требуется перезаписать.
2. В меню **Действия** (рисунок 9.50) выберите команду **Восстановить конфигурацию**.

## 8. Интеграция с Handkey-II

Веб-интерфейс позволяет обеспечить работоспособность связки прибора «ЯРС» с Handkey: «привязать» биометрический считыватель к точке доступа и задать дополнительные параметры.

Выполните следующую последовательность шагов:

1. Перейдите к веб-интерфейсу по адресу [http://\[IP-адрес прибора\]/plugin/manager/](http://[IP-адрес прибора]/plugin/manager/).
2. В отобразившемся окне Управление расширениями в списке расширений наведите указатель мыши в строке расширения **Интеграция с Handkey II** и нажмите на кнопку

**Настроить...** 

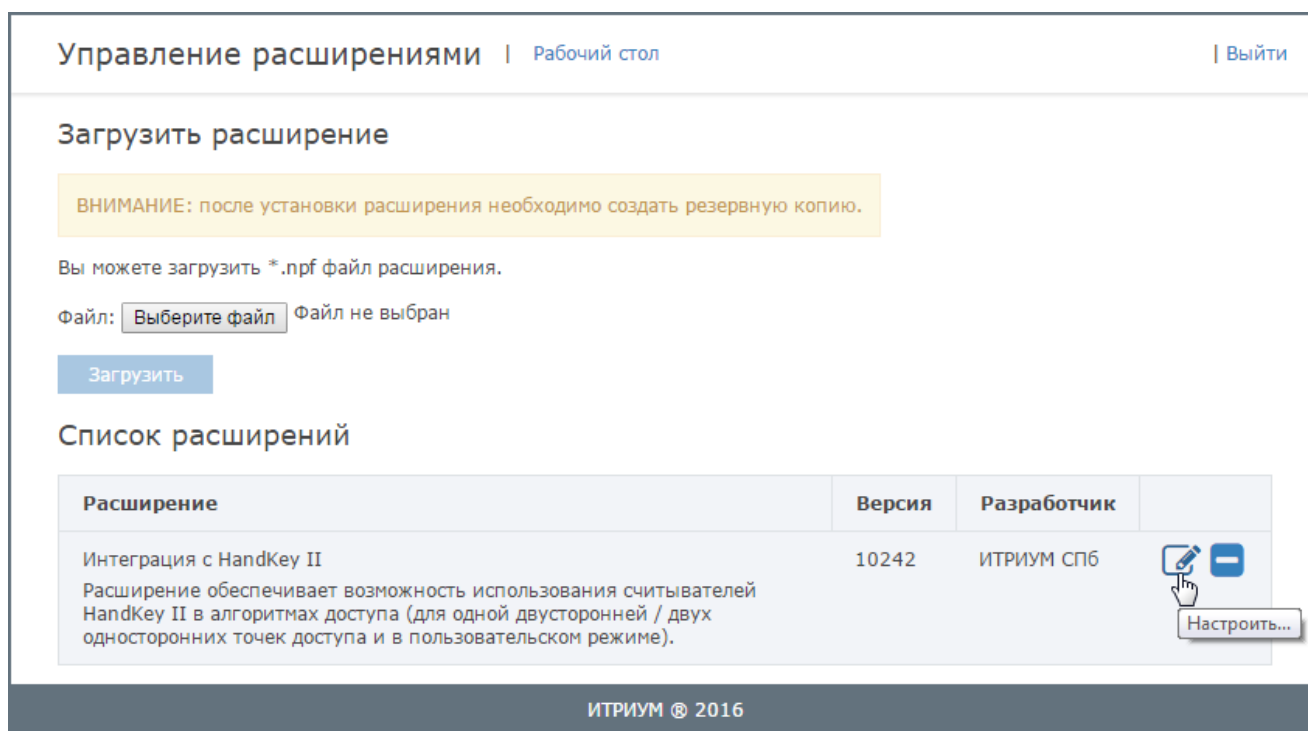


Рисунок 9.53 — Окно управления расширениями

3. Задайте параметры интеграции (описание см. в таблице 9.17). Первоначально рекомендуется зарегистрировать устройство Handkey: указать адрес, тип и параметры подключения (см. блок **Добавить устройство** таблицы 9.17) и нажать на кнопку **Добавить**. Устройство станет доступным для выбора в поле **Устройство**. По окончании настройки нажмите на кнопку **Изменить**. Пример настройки приведён на рисунке 9.54.

Таблица 9.17 — Параметры интеграции с Handkey-II

Параметр	Диапазон значений	Значение по умолчанию	Примечание
<b>Точка доступа 1   Вход, Точка доступа 2   Выход</b>			
Проверять биометрию руки	Да, Нет	Нет	Задайте <b>Да</b> , если требуется идентификация по биометрическим параметрам.
Использовать пин-код	Да, Нет	Нет	Задайте <b>Да</b> , если требуется запрашивать ввод пин-кода на считывателе биометрии.
Порог отказа	целое число	100	Уровень чувствительности 100 – лучшее значение для большинства случаев. Повышение порогового уровня снижает чувствительность Handkey к различиям в положении руки пользователя на рабочей плоскости. Снижение уровня может привести к большему количеству отказов, но в тоже время способствует повышению уровня безопасности системы.
Устройство	Значение из списка	–	Выберите из списка устройств Handkey. Для добавления устройства в список требуется его подключить к «ЯРС» и настроить параметры в блоке <b>Добавить устройство</b> .
<b>Добавить устройство</b>			
Логический адрес	Целое число в диапазоне от 0 до 254	–	Введите адрес устройства. Адрес задаётся на устройстве с помощью команды <b>Set Address</b> . Дополнительную информацию см. в руководстве пользователя на устройство Handkey-II.
Транспорт	TCP/RS232	TCP	Выберите из раскрывающегося списка используемый тип подключения: TCP (Ethernet) или RS-232.
Сетевой адрес	IP-адрес, либо [IP-адрес]:[порт]	–	При использовании Ethernet для подключения Handkey, укажите его IP-адрес и порт. Настройки задаются в параметрах Ethernet-адаптера Handkey или в параметрах преобразователя интерфейсов, в зависимости от используемого типа подключения.
Сетевой порт	Номер порта	–	

## Параметры интеграции

Точка доступа 1 | Вход

Проверять биометрию руки:  Да  Нет

Использовать пинкод:  Нет  Да

Порог отказа:

Устройство:

Точка доступа 2 | Выход

Проверять биометрию руки:  Нет  Да

Использовать пинкод:  Нет  Да

Порог отказа:

Устройство:

[Изменить](#)

## Добавить устройство

Логический адрес:

Транспорт:

Сетевой адрес:

Сетевой порт:

[Добавить](#)

## Список зарегистрированных устройств


Идентификатор	Транспорт	Сетевой адрес	Локальный адрес	
f70fe387-501a-4619-afca-c9acb20d4d49	TCP	192.168.1.105:8181	7	

Рисунок 9.54 — Окно задания параметров интеграции с Handkey

## ПРИЛОЖЕНИЕ 7. НАСТРОЙКА ОБЩИХ РЕСУРСОВ СЕТИ

### 1. Пользователи, роли и права

Учётные записи пользователей предназначены для разграничения полномочий пользователя по работе с веб-интерфейсом. Каждая учётная запись имеет роль, которая определяет права пользователя. Учётная запись **root** является «заводской» и предназначена для первичного конфигурирования узла. Смена пароля учётной записи **root** (по умолчанию – **root**), осуществляется в разделе [Конфигурация узлов](#) — [Настройки узла](#)

Основные настройки.

Чтобы иметь возможность редактировать параметры других узлов, управлять ими и выполнять операции из раздела [Сеть](#), а также необходимо:

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

**Примечание 1.** Если в сети присутствует только один узел, «облачную» учётную запись создавать не обязательно, так как она нужна для конфигурирования нескольких узлов сети и выполнения функций раздела **Сеть** интерфейса (см. приложение).

**Примечание 2.** При добавлении нового узла в 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](#)).

**Примечание 3.** Для создания учётных записей операторов «НЕЙРОСС Центр» используйте роль без прав.

Чтобы создать новую учётную запись, выполните следующую последовательность шагов:


1. Перейдите в раздел **Пользователи, роли и права**.
2. На вкладке **Роли** создайте роль пользователя. Для этого:
  - Нажмите кнопку **Добавить** ;
  - В отобразившемся окне (рисунок 9.55) задайте права новой роли (если вы хотите создать полнофункциональную роль, выберите **Все**) и нажмите на кнопку **Создать**.

Рисунок 9.55 — Окно добавления роли пользователя

- Новая роль добавится в список ролей (рисунок 9.56). Роль можно удалить или отредактировать с помощью кнопок, расположенных в строке роли.

Пользователи		Роли	
Название	Права	Действия	
<input type="text"/>	<input type="text"/>	+	Добавить новую роль
administrator	Общее / Обслуживание	[-] [Pencil]	Удалить роль Редактировать роль

Рисунок 9.56 — Список ролей

3. Перейдите к вкладке **Пользователи** и создайте учётную запись с данной ролью. Для этого:


- Нажмите на кнопку **Добавить** ;
- В отобразившемся окне (рисунок 9.57) введите данные нового пользователя, в поле **Роль** выберите из списка созданную на предыдущем этапе роль, нажмите на кнопку **Создать**.

Рисунок 9.57 — Окно добавление новой учётной записи пользователя

- Новая учётная запись пользователя добавится в список **Пользователи** (рисунок 9.58). 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 9.58 — Список пользователей интерфейса НЕЙРОСС

Чтобы **удалить** учётную запись, нажмите на кнопку в строке данной учётной записи.

Чтобы **отредактировать** параметры учётной записи, нажмите на кнопку в строке учётной записи и измените требуемые данные (рисунок 9.59).

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

Рисунок 9.59 — Окно редактирования параметров учётной записи пользователя

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

## 2. Охранная сигнализация

### Разделы сигнализации

Для конфигурирования разделов охранной сигнализации, перейдите к разделу [Охранная сигнализация](#), к вкладке **Разделы** (отображается по умолчанию; рисунок 9.60).

Окно разделено на две вертикальные области: слева указан номер и наименование раздела, справа отображаются охранные зоны раздела. Если разделы ранее не конфигурировались, отобразится пустое окно.

Доступны следующие действия с разделами:

- [Создание раздела](#);
- [Перенос раздела](#);
- [Удаление раздела](#).

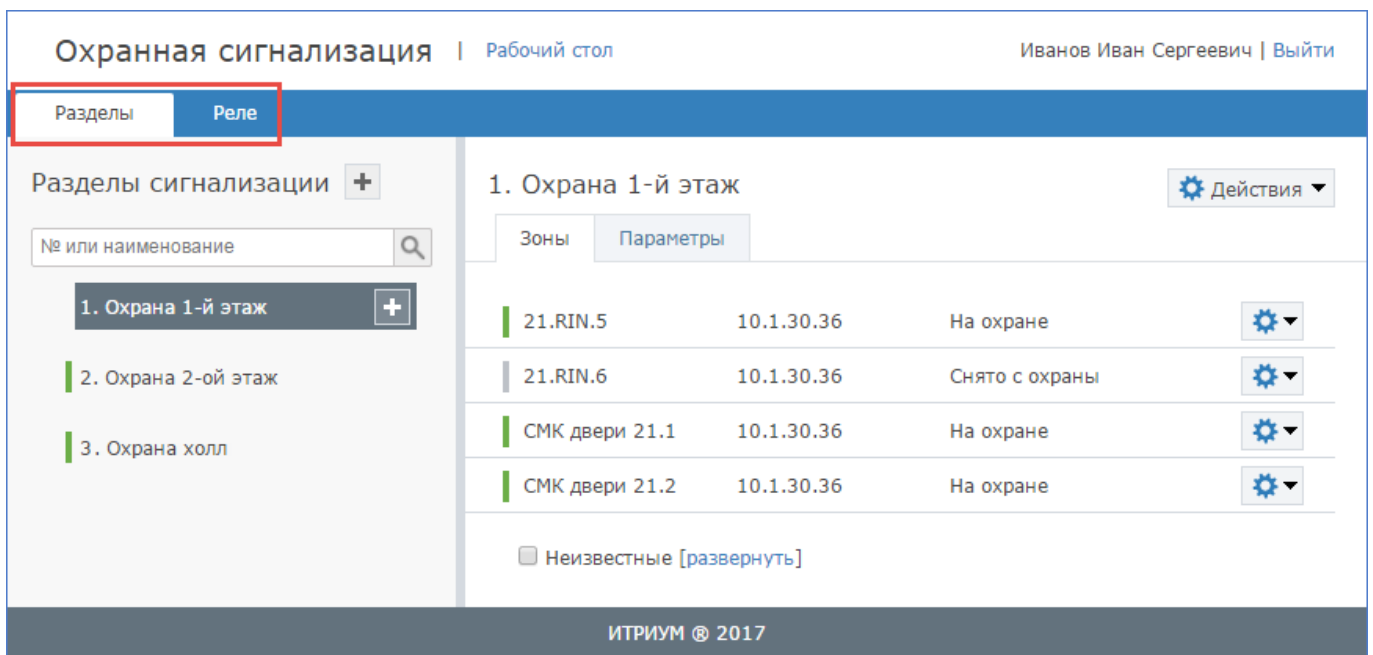




Рисунок 9.60 — Окно конфигурирования разделов

### Создание раздела

1. Создайте пустой раздел, для этого:

- В столбце **Разделы сигнализации** нажмите на кнопку .
- Укажите номер раздела и его название (рисунок 9.61). Нажмите на кнопку .

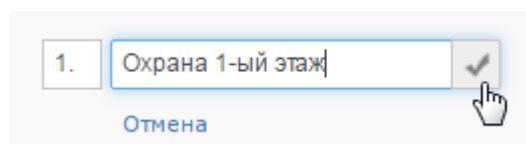




Рисунок 9.61 — Добавление раздела

**Примечание.** При необходимости создания дочернего раздела, нажмите на кнопку  в строке родительского 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 9.62).

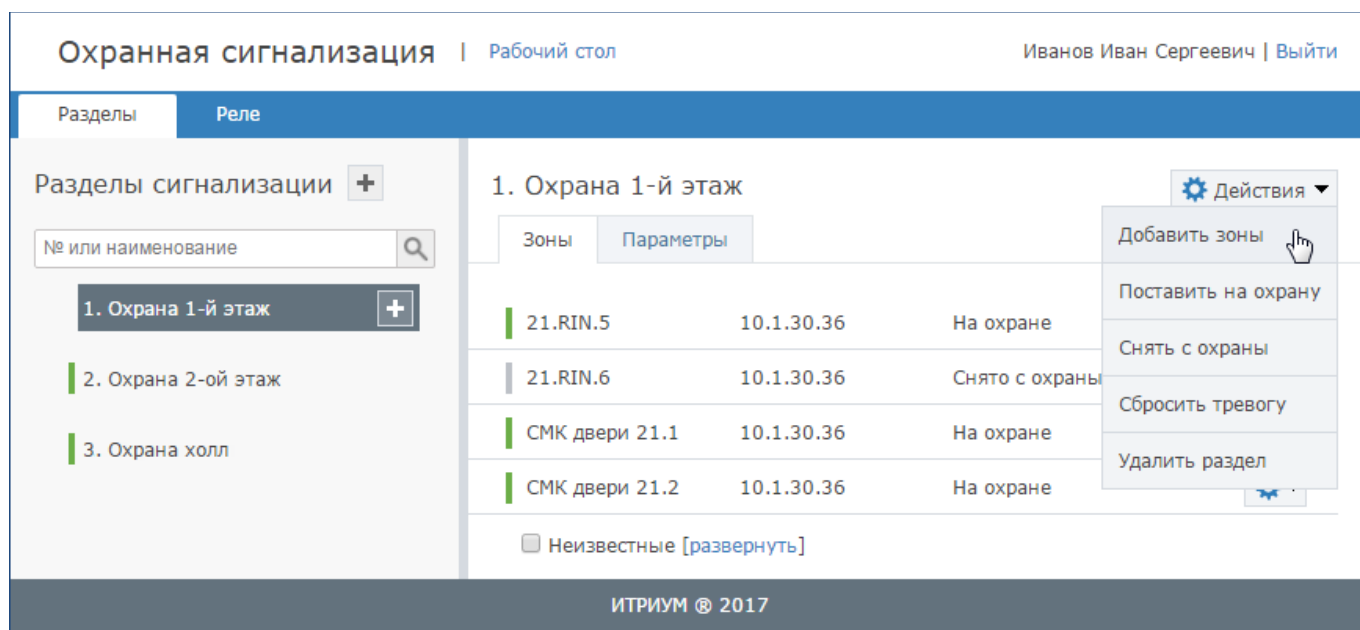



Рисунок 9.62 — Добавление охранных зон в раздел

- В отобразившемся окне в поле **Устройство** введите IP-адрес устройства (или часть IP-адреса), 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  в блоке **Список выбранных зон** (рисунок 9.63). В один раздел могут входить зоны разных устройств.

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



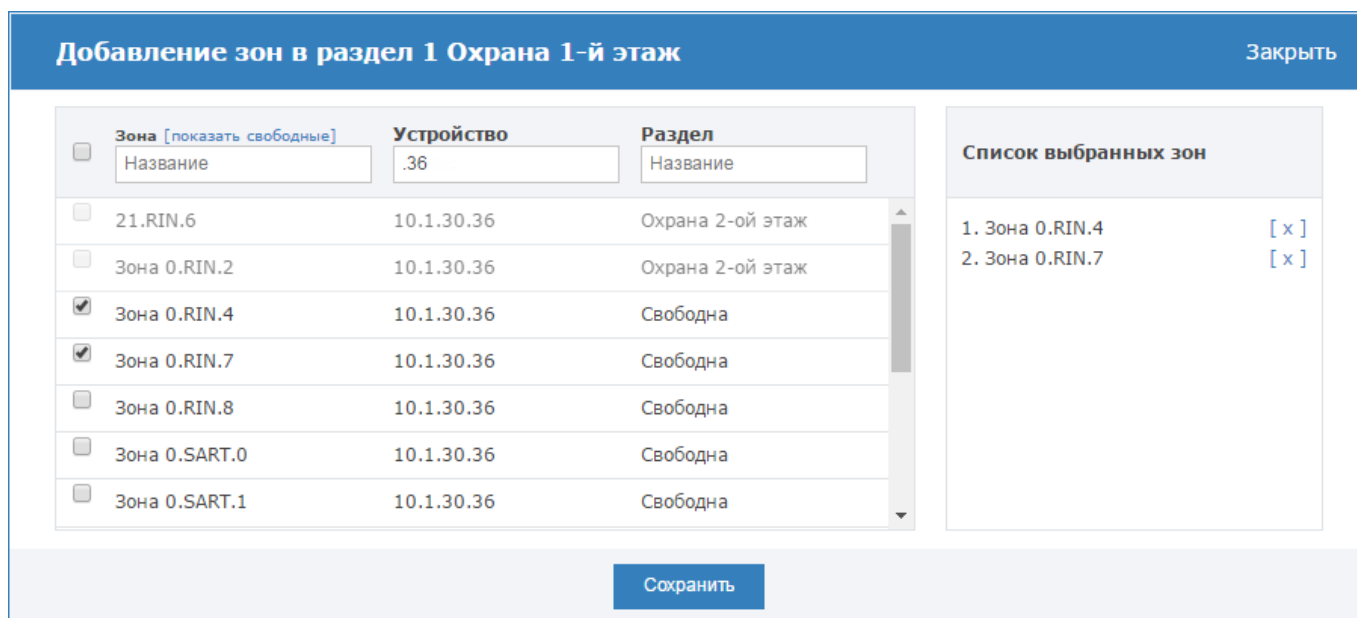


Рисунок 9.63 — Добавление охранных зон в раздел

- По завершении нажмите на кнопку **Сохранить**.

**Примечание.** Блок **Неизвестные** в списке зон раздела предназначен для удаления неактуальных разделов сигнализации (зоны которого принадлежат более не существующим узлам сети; рисунок 9.64).

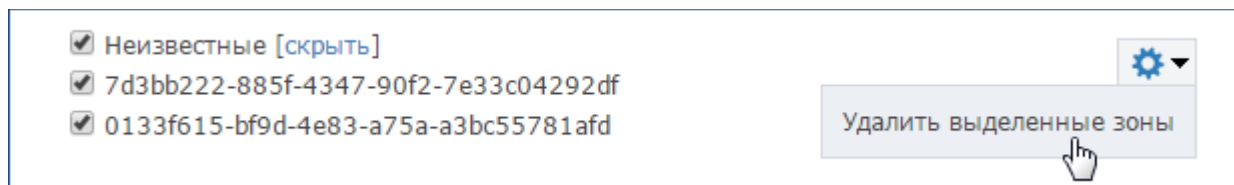


Рисунок 9.64 — Удаление «старых» разделов

### 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 9.65).
3. Отпустите клавишу мыши. Дерево разделов обновится с учётом перенесённого раздела.

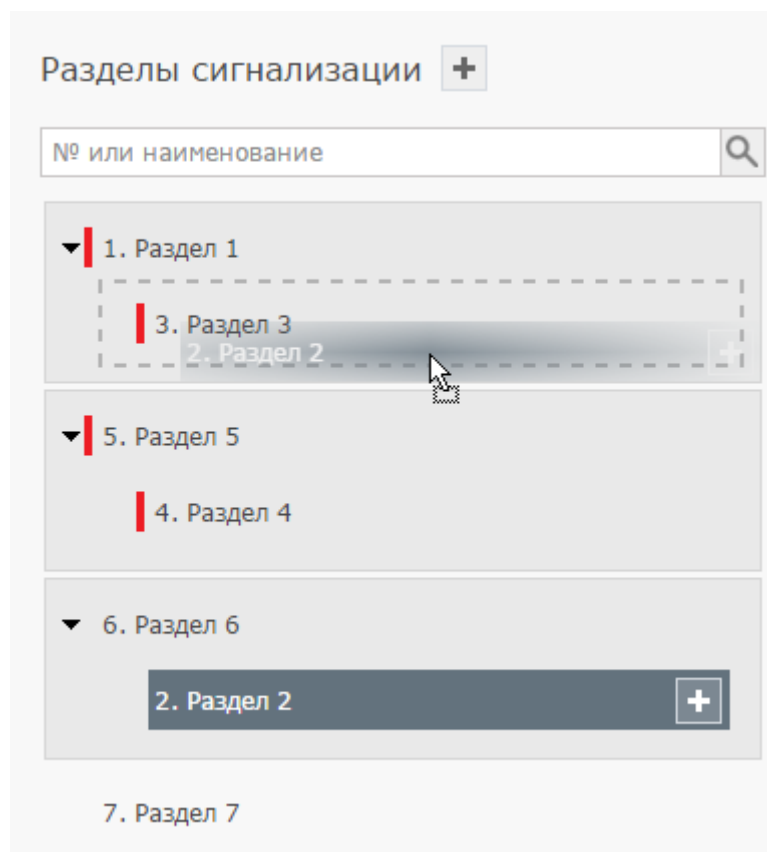



Рисунок 9.65 — Процедура переноса раздела


### Удаление раздела

1. В столбце **Разделы сигнализации** выберите раздел, который требуется удалить.
2. В окне справа 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 зоны/раздела, удаление зоны/раздела, добавление зон в раздел. Описание команд управления см. в таблице [9.18](#).

#### Веб-интерфейс. Доступ к командам управления разделом:

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 **Конфигурация узлов — Охранная сигнализация**.
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, откройте контекстное меню элемента и выберите требуемую команду.
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 9.18 — 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	<p>Команда постановки раздела на охрану. Будет предпринята попытка постановки всех зон раздела на охрану.</p> <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> <p>Если некоторые зоны раздела находятся в тревожном состоянии, раздел перейдёт в состояние [Частично на охране]. Если некоторые зоны раздела находятся в неисправном состоянии, состояние зон и раздела не изменится ([Неисправно]) *.</p>
	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 приведёт 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](#).

### Реле управления

Для настройки режимов управления реле, перейдите к разделу [Охранная сигнализация](#), к вкладке **Реле** (рисунок 9.66).

Окно разделено на две вертикальные области: слева отображаются доступные узлы НЕЙРОСС, справа отображается список реле узла.

Так как факт подключения исполнительных устройств к выходным реле «Борей», «ЯРС» не контролируется, для каждого устройства автоматически формируется максимальное количество элементов **Реле**. Например, для узла «Борей» формируется 32 реле (2 собственных реле и 30 реле модулей расширения, подключаемых по SART). К каждому реле можно «привязать» любое количество разделов сигнализации и задать режим управления реле.

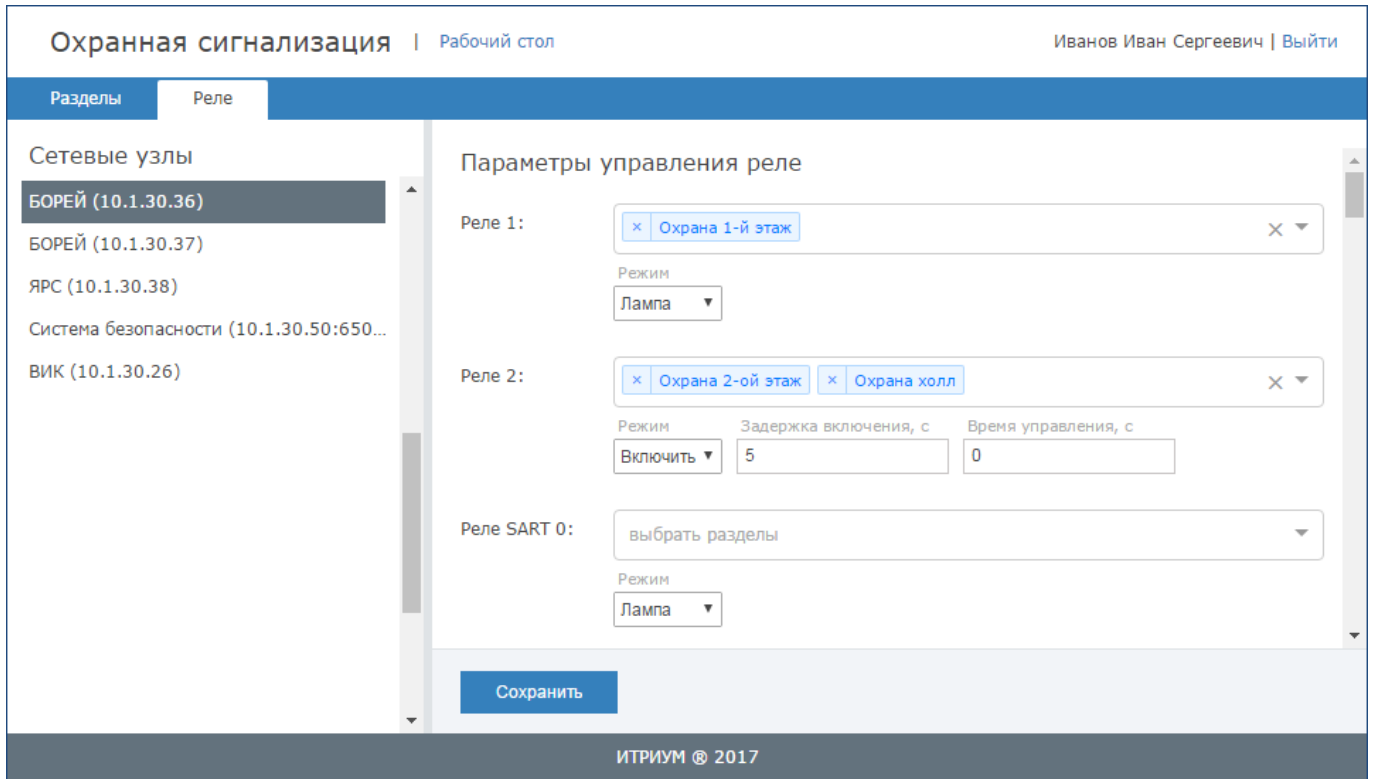


Рисунок 9.66 — Настройка режимов управления реле

Выполните следующие шаги:

1. В списке сетевых узлов выберите устройство «Борей» или «ЯРС».
2. В списке реле найдите реле, которое требуется настроить.
3. В поле **выбрать разделы** выберите из раскрывающегося списка разделы сигнализации, по состоянию которых требуется управление данным реле.

**Примечание.** По состоянию любого раздела сигнализации возможно управление любым количеством реле в разных режимах, поэтому в раскрывающемся списке выводятся все разделы НЕЙРОСС.

4. В поле **Режим** выберите из раскрывающегося списка требуемый режим управления реле и, при необходимости, настройте дополнительные параметры (описание режимов управления реле приведено в таблице 9.19, описание режимов работы реле приведено в таблице 9.20). Описание возможных состояний разделов сигнализации приведено в разделе [Состояния разделов охранной сигнализации](#). Также смотрите [Смена состояний зон и разделов при постановке на охрану](#).

5. Нажмите на кнопку **Сохранить**.

Таблица 9.19 — Режимы управления реле

Режим	Описание	Параметры режима
Лампа	Режим предназначен для управления выносным индикатором. В состоянии [На охране] реле включено, в состоянии [Тревога] — мигает.	нет
Включить Мигать	Режимы предназначены для индикации тревожного состояния раздела. При переходе раздела в тревожное состояние, по окончании периода <b>Задержка включения</b> включается (режим <b>Включить</b> ) или начинает мигать (в режиме <b>Мигать</b> ) до окончания периода <b>Время управления</b> или раньше, при отмене/сбросе тревоги.	<b>Задержка включения</b> — период времени в секундах, по истечению которого реле включается/начинает мигать; если задано 0 — реле начинает работать без задержки. <b>Время управления</b> — период времени работы реле; если задано 0 — реле работает до отмены/сброса тревоги.

Таблица 9.20 — Режимы работы реле

	Лампа	Включить	Мигать
<b>Снято с охраны</b>	Выключено	Выключено	Выключено
<b>На охране</b>	Включено	Выключено	Выключено
<b>Частично на охране</b>	Выключено	Выключено	Выключено
<b>Тревога</b>	Мигает	Включено	Мигает
<b>Неисправность</b>	Выключено	Выключено	Выключено

### 3. Терминалы

Терминал в комплексных системах безопасности — это узел системы, который обеспечивает связь системы с пользователем. Каждому терминалу назначается права по управлению системой.

В качестве терминала НЕЙРОСС могут использоваться считыватели «БОРЕЙ» и «ЯРС», консоли «ВИК». Терминалам НЕЙРОСС доступны функции постановки на охрану и снятия с охраны разделов сигнализации, а также блокировка/разблокировка и прочие функции по управлению точками доступа системы.

Раздел «Терминалы» предназначен для задания списка разделов охранной сигнализации, доступных для управления с конкретного терминала. Предварительно необходимо сконфигурировать разделы сигнализации (см. раздел [Разделы сигнализации](#)).

Список доступных функций по управлению разделом/точкой доступа определяется уровнем управления пропуска (дополнительную информацию см. в разделе [Настройка уровней управления](#)).

Для настройки терминалов, перейдите к веб-интерфейсу прибора (см. раздел [Рабочий стол](#)) и выберите пункт **Терминалы**. Страница раздела разделена на две области.

Слева отображается список точек доступа системы или устройств «ВИК», справа — список сконфигурированных разделов сигнализации (рисунок 9.67).

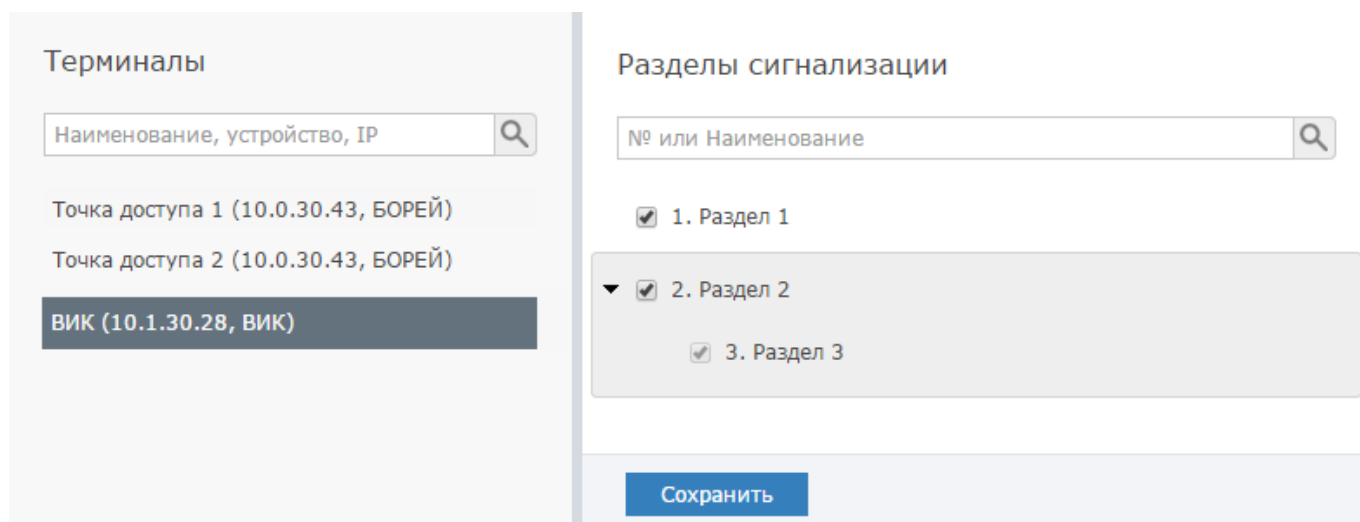


Рисунок 9.67 — Страница раздела «Разделы сигнализации»

### Настройка терминала

Выполните следующую последовательность шагов:

1. В окне **Терминалы** выделите требуемый терминал (точку доступа или консоль «ВИК»).
2. В окне **Разделы сигнализации** определите набор разделов, которыми разрешено управлять посредством данного терминала. Для этого установите флаги для требуемых разделов.
3. Нажмите на кнопку **Сохранить**.
4. Проверьте, что уровень охраны пропуска, по которому будет осуществляться постановка на охрану и снятие с охраны, обладает правами управления данными разделами (см. раздел [Настройка уровней](#).)

## 4. Зоны доступа

Зоны доступа предназначены для обеспечения контроля повторного прохода (APB, antipassbak). По факту прохода номер зоны привязывается к пропуску, и, при попытке предъявления на считывателе другой зоны, формируется тревожное сообщение и доступ может быть запрещён (при жёстком режиме контрольного прохода).

Для начала работы с зонами, перейдите к веб-интерфейсу прибора (см. раздел [Рабочий стол](#)) и выберите пункт **Зоны доступа**.

Окно раздела **Зоны доступа** (рисунок 9.68) содержит список зон доступа. Если разделы ранее не конфигурировались, отобразится пустое окно.

Зоны доступа +

Номер	Название	
1	Первая	
1	Зона доступа 1	
2	Зона доступа 2	
12	Зона ВХОД	
14	Зона ВЫХОД	
666	Туда	
999	Обратно	
1000	Зона доступа 1000	-

Рисунок 9.68 — Окно конфигурирования зон доступа

### Создание зон доступа

Чтобы создать новую зону доступа, выполните следующую последовательность шагов:

1. Нажмите на кнопку +.
2. В новой строке введите номер и название зоны доступа (рисунок 9.69).
3. Нажмите на кнопку **Сохранить**.

Рисунок 9.69 — Окно добавления зоны доступа

4. Повторите шаги выше для создания второй зоны.
5. Для осуществления АРВ, перейдите к настройкам точки доступа (см. раздел Точки доступ) и задайте данные зоны **в** полях **Зона ВХОД**, **Зона ВЫХОД**. Выбор зоны осуществляется из списка предварительно созданных зон.

Чтобы **отредактировать зону доступа**, щёлкните в строке данной зоны, внесите требуемые изменения и нажмите на кнопку **Сохранить**.

Чтобы **удалить зону доступа**, щёлкните в строке зоны и нажмите на кнопку -.



## ПРИЛОЖЕНИЕ 8. СЕТЬ

Приложение «Сеть» предназначено для проверки состояния связи с узлом и наличия расхождений по времени и данным между узлами, а также для выполнения операций синхронизации времени и данных, обновления, перезагрузки и резервного копирования. Окно приложения содержит список узлов сети, принадлежащих домену (доменам) текущего устройства (устройств, с IP-адреса которого выполнен вход в интерфейс) (рисунок 9.70).

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

**Примечание.** Если кнопка инструмента не активна, значит в списке выбранных узлов есть узел, 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

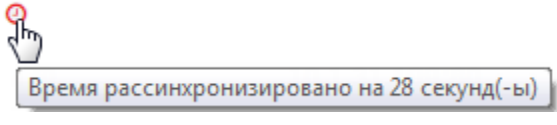


Рисунок 9.70 — Окно раздела Сеть

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 с помощью мастера первого запуска (см. раздел [Мастер первого запуска](#)) или в разделе [Конфигурация узлов – Сетевые параметры](#) (см. раздел [Сетевые параметры](#)).

В столбце **Состояние** указано состояние связи с устройством (таблица 9.21).

Таблица 9.21 — Список состояний узлов

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

Состояние	Обозначение	Описание
Рассинхронизация времени		Узел ответил на все запросы, интервал расхождения более 5 сек. Точную 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

**Примечание.** Обновление программных средств сервера ITRIUM, «НЕЙРОСС Центр» или терминала «МТК» выполняется локально на сервере/терминале и удалённо недоступно.

Выполните следующие шаги:

1. Перейдите к веб-интерфейсу узла, выберите раздел **Сеть**.
2. В списке узлов сети выберите требуемый узел или несколько узлов одной модели, нажмите на кнопку **Обновление ПО** (рисунок 9.71).

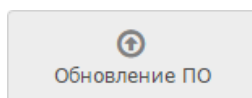


Рисунок 9.71 — Кнопка **Обновление ПО**

3. В отобразившемся окне нажмите на кнопку **Выберите файл** для указания пути к файлу обновления, предоставленному производителем; затем нажмите на кнопку **Обновить** (рисунок 9.72). Будет выполнено обновление программных средств узлов с последующей перезагрузкой.

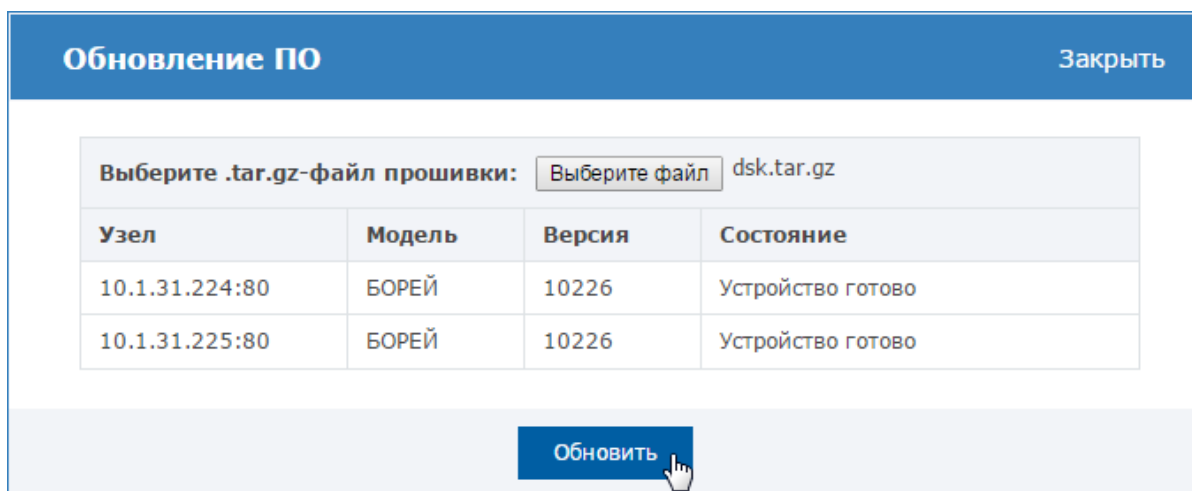


Рисунок 9.72 — Окно обновления прошивки нескольких узлов

4. Выполните очистку кеша браузера. Это необходимая процедура, так как веб-интерфейс узла, возможно, претерпел изменения.

**Инструкция для Google Chrome:** В меню **Настройки** выберите **История**, нажмите **Очистить историю...**, выберите **Файлы Cookie...** и **Изображения и другие файлы, сохранённые 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 узла — перезагрузка приложения:

1. Перейдите к веб-интерфейсу узла, выберите раздел **Сеть**.
2. В списке устройств сети выберите требуемое устройство(а), нажмите на кнопку **Перезагрузка** (рисунок 9.73).

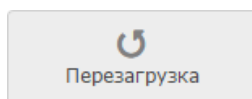


Рисунок 9.73 — Кнопка **Перезагрузка**

3. В окне подтверждения повторно нажмите на кнопку **Перезагрузить**.
4. По окончании процесса перезагрузки отобразится информационное окно (рисунок 9.74). Нажмите на кнопку **Закреть**.

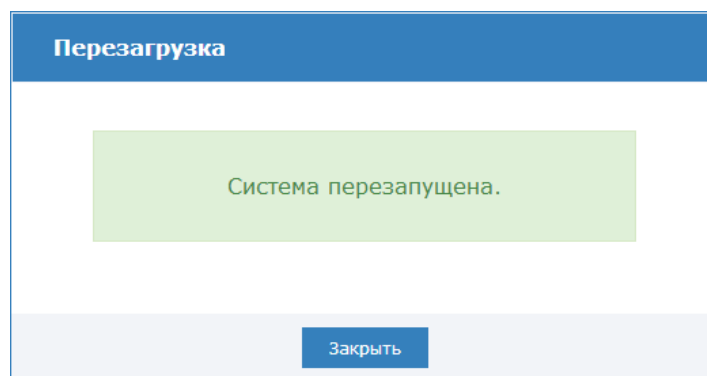


Рисунок 9.74 — Окно подтверждения завершения перезагрузки

### Резервные копии узлов НЕЙРОСС

**Примечание.** Для сервера ITRIUM и «НЕЙРОСС Центр» создание резервной копии выполняется локально на сервере и удалённо недоступно. Средств создания резервной копии «МТК» не предусмотрено.

Посредством веб-интерфейса можно создать резервную копию программного обеспечения (прошивки) узла и его настроек и выполнить восстановление из резервной копии.

1. Перейдите к веб-интерфейсу прибора, выберите раздел **Сеть**.
2. В списке устройств сети выберите требуемый узел, нажмите на кнопку **Резервные копии** (рисунок 9.75).

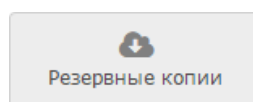


Рисунок 9.75 — Кнопка **Резервные копии**

3. Выберите требуемую команду (рисунок 9.76).

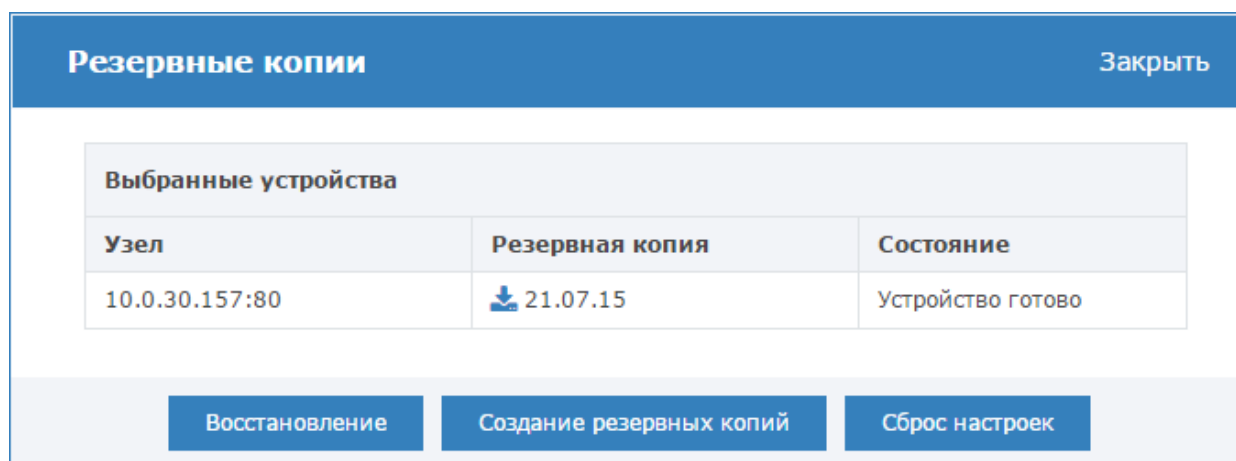



Рисунок 9.76 — Работа с резервными копиями

По команде **Создание резервных копий** выполняется создание резервных копий выбранных узлов. Ранее созданная резервная копия будет затёрта.

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 **Восстановление** выполняется восстановление данных из ранее созданной резервной копии (будет выбрана последняя версия копии).

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

При нажатии кнопки **Загрузить**  выполняется загрузка файла резервной копии в папку загрузок браузера. Восстановить данные из сохранённого на компьютере файла возможно после сброса настроек (см. раздел [Сброс настроек](#)) при прохождении Мастера первого запуска (см. раздел [Мастер первого запуска](#)).

### Синхронизация времени на узлах НЕЙРОСС

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

Отсутствие расхождений по времени на таких узлах НЕЙРОСС, как «Борей», «ЯРС», «ВИК», можно обеспечить настройками каждого узла (дополнительную информацию см. в разделе [Дата и время](#)) или средствами «Службы НЕЙРОСС» сервера ITRIUM (см. раздел [Настройка «Службы НЕЙРОСС»](#)).

**Примечание.** Параметры даты и времени на сервере ITRIUM и «НЕЙРОСС Центр» следует устанавливать средствами операционной системы Windows/Linux. Параметры даты и времени «МТК» следует настраивать средствами операционной системы Android. При этом рекомендуется настроить все узлы на синхронизацию по единому серверу времени (NTP-серверу).

В разделе **Сеть** может быть выполнена разовая процедура синхронизации времени на устройствах «Борей», «ЯРС», «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 9.77).

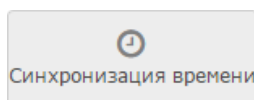


Рисунок 9.77 — Кнопка **Синхронизация времени**

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

В процессе выполнения будет отображаться текущий статус (рисунок 9.78).

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..

Рисунок 9.78 — Окно синхронизации времени

### Синхронизация данных между узлами НЕЙРОСС

Обязательным условием успешного взаимодействия узлов сети (таких как «Борей», «ЯРС», серверов ITRIUM, «НЕЙРОСС Центр» и др.) является синхронизация данных.

Под данными понимается набор элементов конфигурации системы ОПС и СКУД: пропусков, владельцев пропусков, уровней доступа, уровней управления, зон доступа (для контроля повторного прохода), 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 9.79).

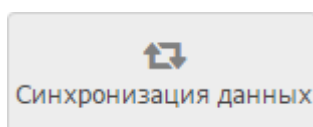


Рисунок 9.79 — Кнопка **Синхронизация данных**

3. Выберите требуемый способ синхронизации (рисунок 9.80).



Рисунок 9.80 — 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 управления**, **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 9.81);.

**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.



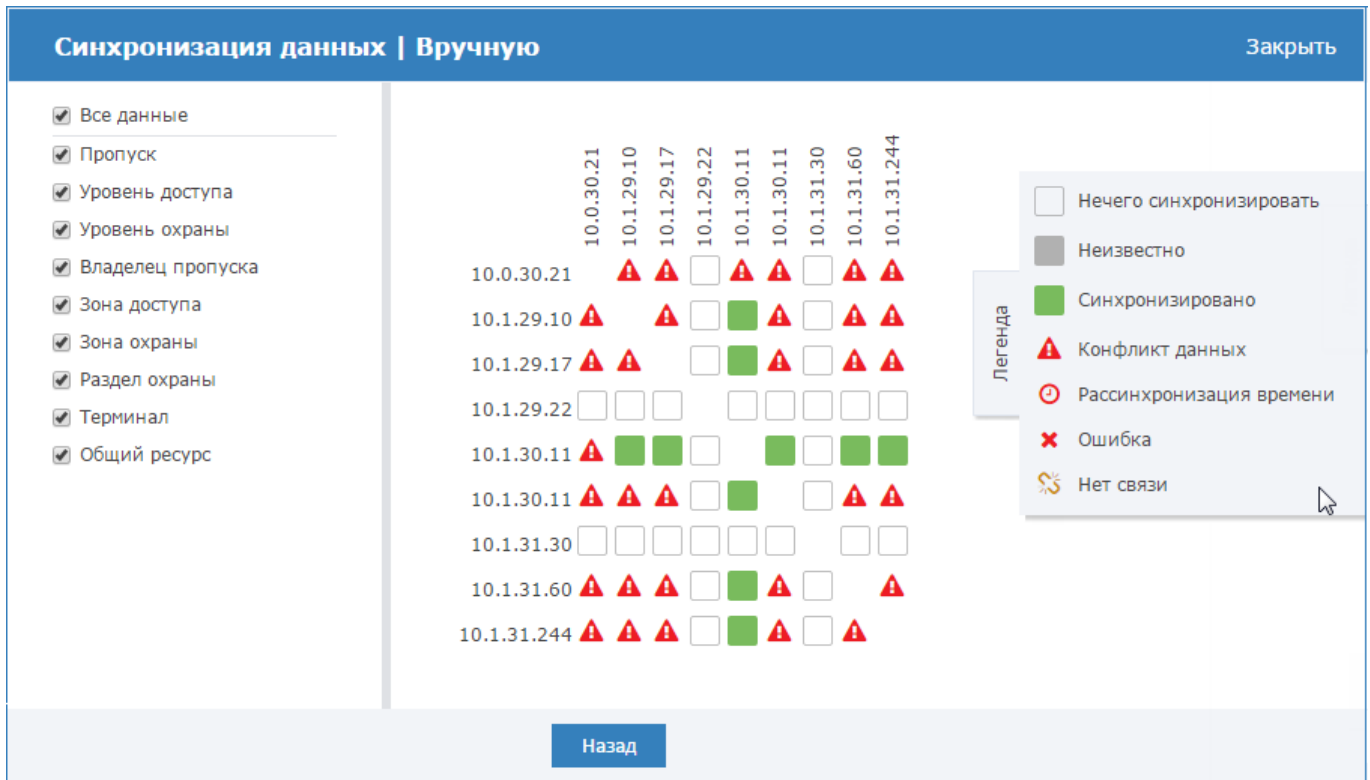


Рисунок 9.81 — Состояние синхронизации данных между узлами

- 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 9.82).

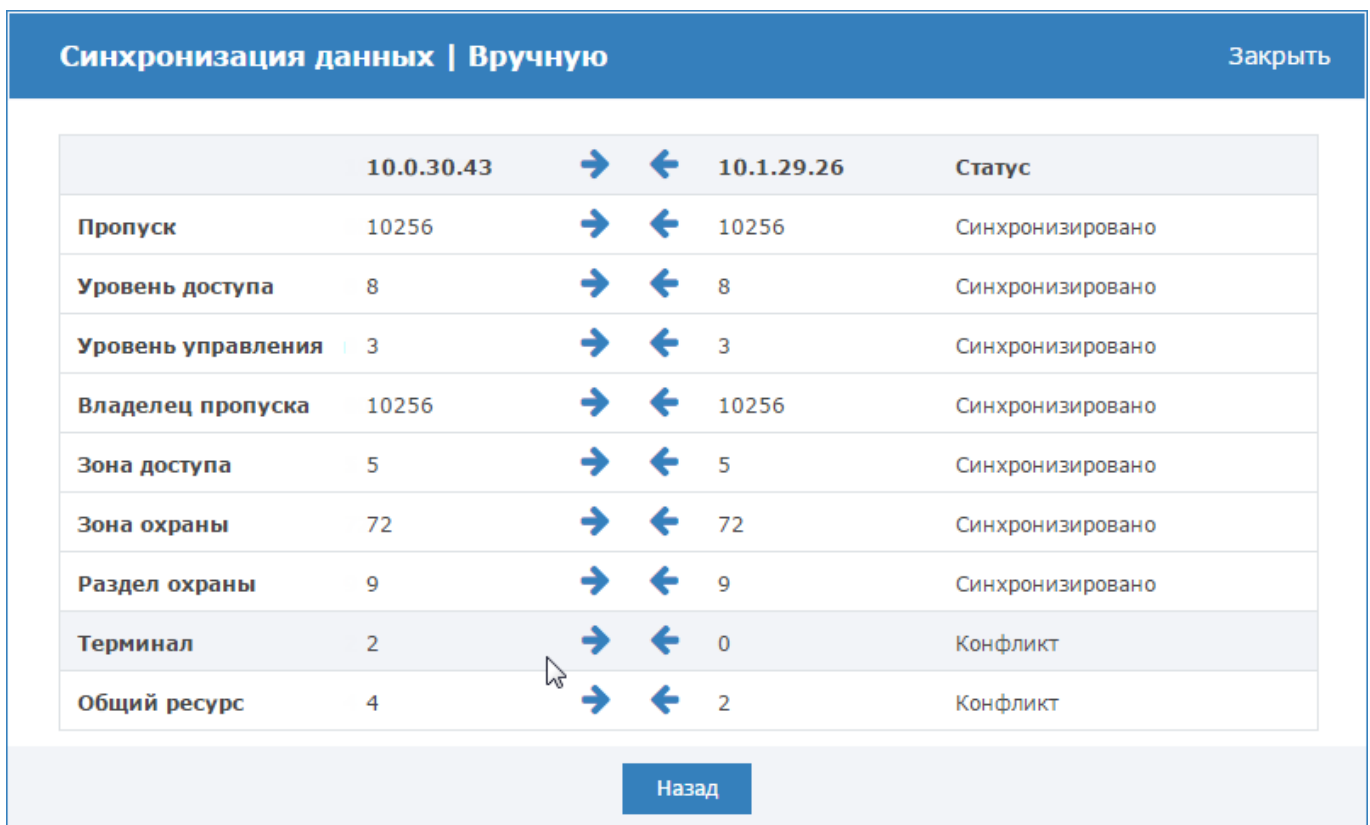


Рисунок 9.82 — Синхронизация данных по типам

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

### Удаление узлов НЕЙРОСС

Если какой-то узел удалён 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 9.77).

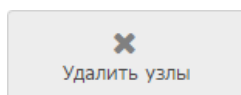


Рисунок 9.83 — Кнопка **Удалить узлы**

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

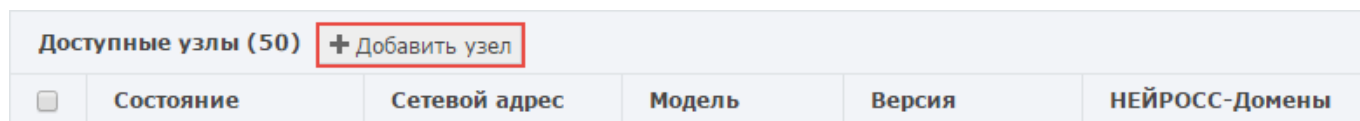
**Примечание 2.** Чтобы удалить недоступный узел из списка всех узлов сети, необходимо повторить процедуру удаления в интерфейсе каждого узла.

### Добавление узлов НЕЙРОСС

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

В некоторых случаях (например, если отключен мультикаст) 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 9.84).



Доступные узлы (50)		<b>+ Добавить узел</b>			
<input type="checkbox"/>	Состояние	Сетевой адрес	Модель	Версия	НЕЙРОСС-Домены

Рисунок 9.84 — Заголовок таблицы списка устройств сети НЕЙРОСС

3. Выберите, хотите ли вы добавить узел НЕЙРОСС (прибор «Борей», «ЯРС», «ДеВизор», «ВИК», «МТК», сервер ITRIUM, сервер «НЕЙРОСС Центр») 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.

## Создание кольцевой топологии узлов НЕЙРОСС

Благодаря наличию на плате прибора «ЯРС» двух портов Ethernet, возможно подключать приборы последовательно один к другому и затем замкнуть кольцо на коммутаторе. Это позволяет упростить монтаж и обслуживание сетевой инфраструктуры.

Однако в целях предотвращения закольцовывания широковещательных пакетов, рассылаемых узлами НЕЙРОСС для обеспечения синхронизации данных, средствами программного обеспечения производится искусственный разрыв кольца путём выключения передачи (forwarding'a) пакетов между портами 1 и 2 прерывателя. В качестве прерывателя может выступать узел НЕЙРОСС, который подключен непосредственно к коммутатору посредством порта Ethernet1 (рисунок 9.85).

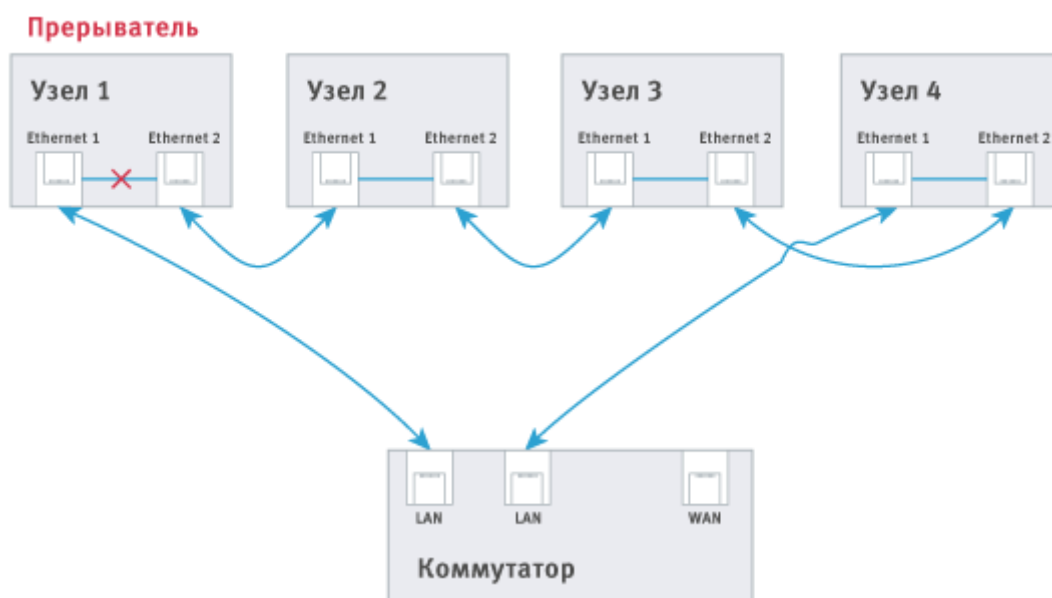


Рисунок 9.85 — Топология типа «кольцо» с прерывателем

В случае разрыва кольца (например, при потере связи с каким-либо узлом), «потерянные» узлы разорванного сегмента формируют широковещательное извещение, прерыватель получает сообщение и включает передачу пакетов между своими портами (рисунок 9.86).

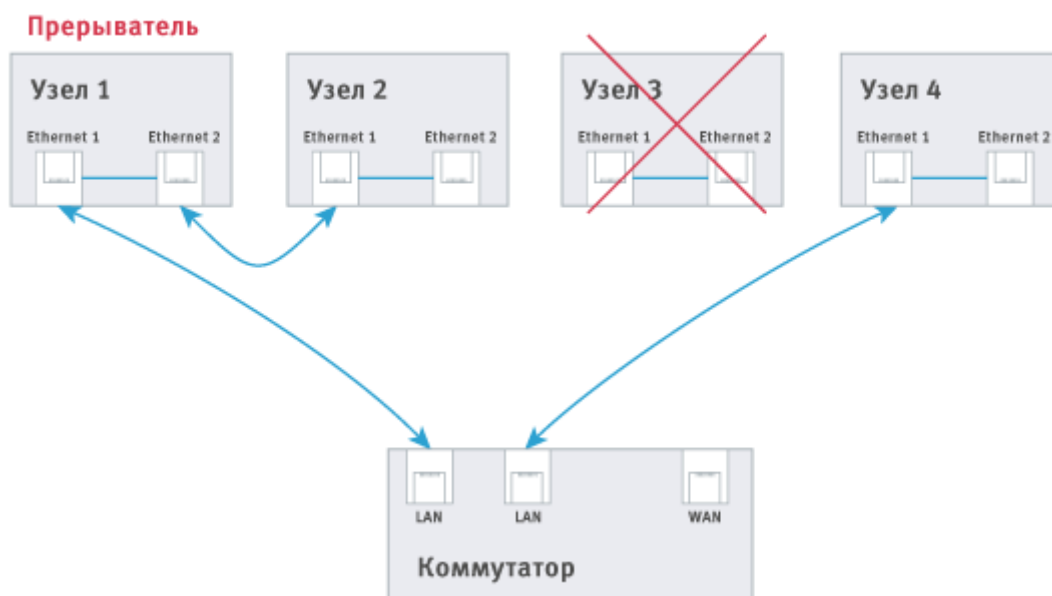



Рисунок 9.86 — Топология типа «кольцо» с прерывателем. Потеря связи с узлом 3.

При восстановлении связи, прерыватель получает соответствующее извещение и отключает передачу пакетов между своими портами. Весь механизм обеспечения работоспособности кольца скрыт от пользователя и выполняется автоматически, пользователю необходимо обозначить группу приборов, замкнутых в кольцо и назначить главный узел (прерыватель), который должен быть один!

Чтобы создать кольцо, выполните следующую последовательность шагов:

1. Перейдите к веб-интерфейсу прибора, выберите раздел **Сеть**.
2. Перейдите к вкладке [Топология](#).
3. В блоке [Кольца](#) нажмите на кнопку , укажите номер кольца и из списка узлов выберите узлы, которые будут подключены с использованием кольцевой топологии. На всех выбранных узлах будет инициирована перезагрузка с применением новых параметров.
4. Назначьте узел, порт Ethernet1 которого непосредственно подключен к коммутатору, главным.

## ПРИЛОЖЕНИЕ 9. БЮРО ПРОПУСКОВ

Веб-приложение «Бюро пропусков» предназначено для просмотра и конфигурирования следующих данных пропусков НЕЙРОСС:

1. Тип пропуска: постоянный, временный, разовый;
2. Данные владельца: фамилия, имя, отчество, подразделение, должность, табельный номер, фотография;
3. Данные пропуска:
  - Номер карты и код предприятия (facility-код), — может быть считан с помощью выбранного считывателя;
  - Пин-код и код принуждения — если используется авторизация по пин-коду;
  - Уровень доступа — если используется в СКУД (список разрешенных точек доступа/ключей и временные интервалы);
  - Уровень управления — если требуется управление ОТС и/или СКУД;

База данных пропусков (пропуска, уровни доступа и уровни управления) является общей для всей системы в целом. При создании пропуска средствами веб-интерфейса НЕЙРОСС, данные автоматически обновляются во всех доступных узлах сети (контроллерах «Борей», «ЯРС», терминалах «МТК», консолях «ВИК»), на серверах ITRIUM® и «НЕЙРОСС Доступ».

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

Окно приложения «Бюро пропусков» (рисунок 9.87) 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 управления** — вкладка предназначена для создания, просмотра и редактирования уровней управления разделами сигнализации и точками доступа.

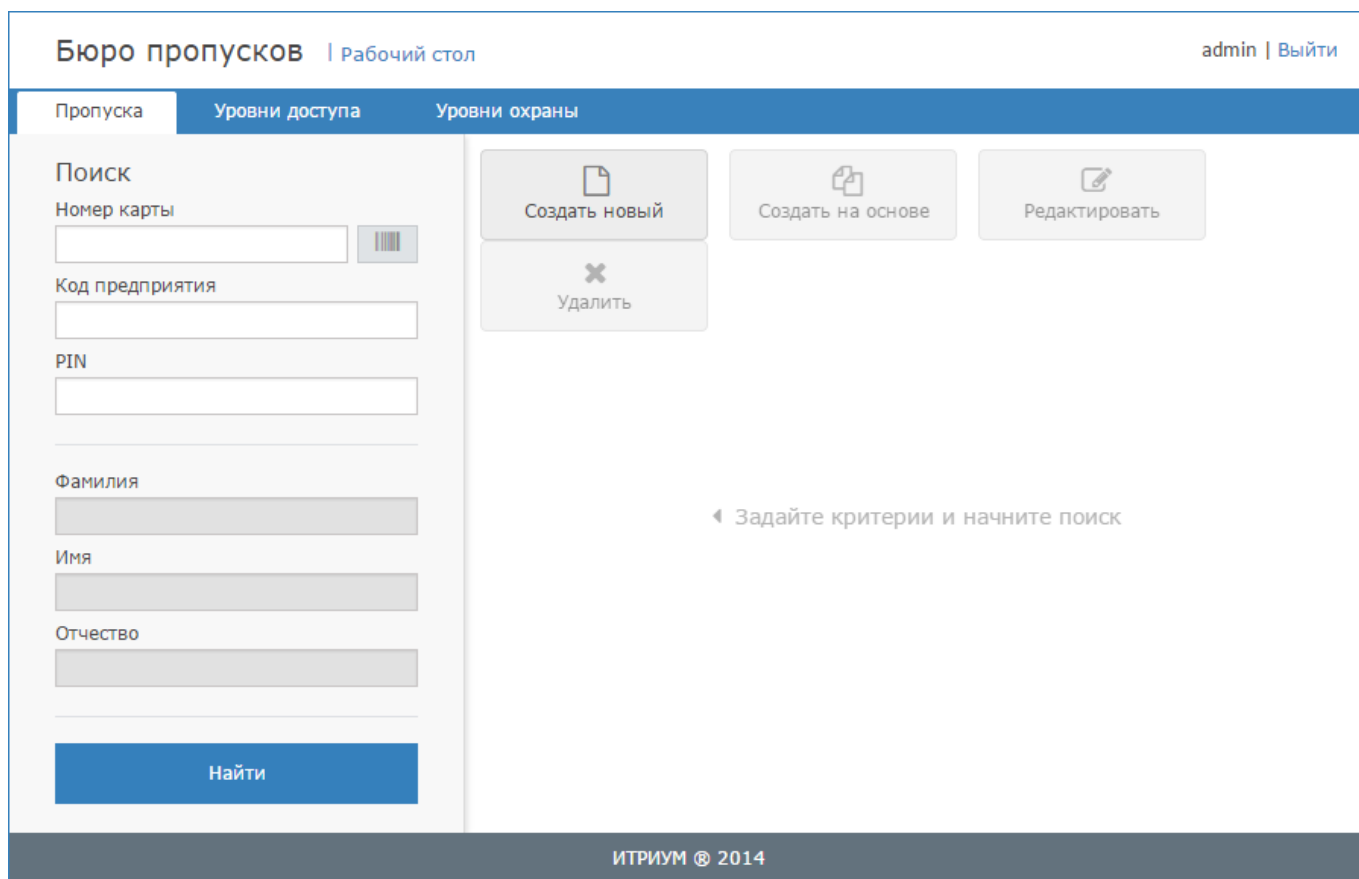


Рисунок 9.87 — Окно Бюро пропусков

### 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 9.89) и введите данные владельца пропуска (рисунок 9.88).

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

Постоянный

Загрузить фото

К карте → Сохранить

Рисунок 9.88 — Окно создания нового пропуска. Вкладка **Владелец**

Новый пропуск: Постоянный

- Постоянный
- Временный
- Разовый**
- Транспортный

Рисунок 9.89 — 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 9.90) поверните и измените, если требуется, границы фотографии, отцентрируйте при помощи перетаскивания видимой области. Нажмите на кнопку **Сохранить**.



Рисунок 9.90 — Окно редактора изображения пропуска


4. Перейдите к вкладке **Карта** или нажмите на кнопку **К карте** (рисунки 9.88 и 9.91).

Рисунок 9.91 — 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](#)).
9. Если данному пропуску требуются права на управление разделами сигнализации и/или точками доступа, в поле **Уровень управления** выберите из раскрывающегося списка созданный ранее уровень управления (порядок настройки уровней управления представлен в разделе [Настройка уровней управления](#)).
10. 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 определённым 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** ).

Чтобы отредактировать данные пропуска, найдите требуемый пропуск. Далее выделите требуемый пропуск и нажмите на кнопку **Редактировать**, или откройте форму пропуска двойным щелчком.

Кнопка  предназначена для очистки всех полей пропуска.

## Сброс зоны APB

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

1. Перейдите к приложению «Бюро пропусков»
2. Выполните поиск пропуска.
3. В таблице пропусков, в поле **Зона APB** требуемого пропуска нажмите на кнопку  **Сбросить зону** (рисунок 9.92).




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

Рисунок 9.92 — Окно списка пропусков

## Настройка уровней доступа

Уровень доступа назначается пропуску или группе пропусков и определяет список разрешенных объектов доступа и время, в течение которого разрешён доступ. В качестве объектов доступа могут выступать точки доступа и/или ключи системы KMS. Конфигурируются следующие параметры:

- список точек доступа;
- список ключей системы KMS;
- временные интервалы — периоды времени, в течение которого разрешается доступ к заданным объектам.

Один пропуск в разные периоды времени может предоставлять разные права доступа, поэтому один уровень доступа может содержать несколько правил — связок типа «группа объектов доступа — список временных интервалов». Настройка уровней доступа осуществляется в приложении «Бюро пропусков» на вкладке **Уровни доступа**.

Окно конфигурирования уровней доступа (рисунок 9.93) разделено на три вертикальные области: слева задаётся номер и имя уровня доступа, по центру указываются временные интервалы, может быть создано несколько правил. Справа выбираются объекты доступа: точки доступа любого узла сети, ключи системы KMS.

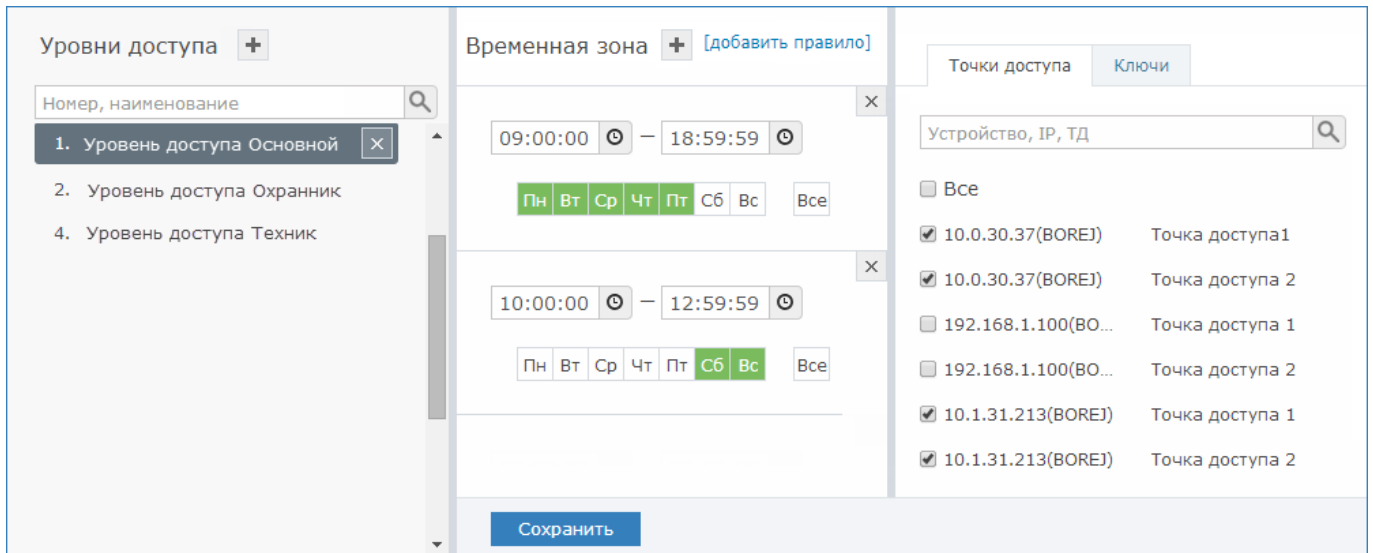


Рисунок 9.93 — Окно конфигурирования уровней доступа

Если уровни доступа ранее не конфигурировались, отобразится пустое окно (рисунок 9.94).

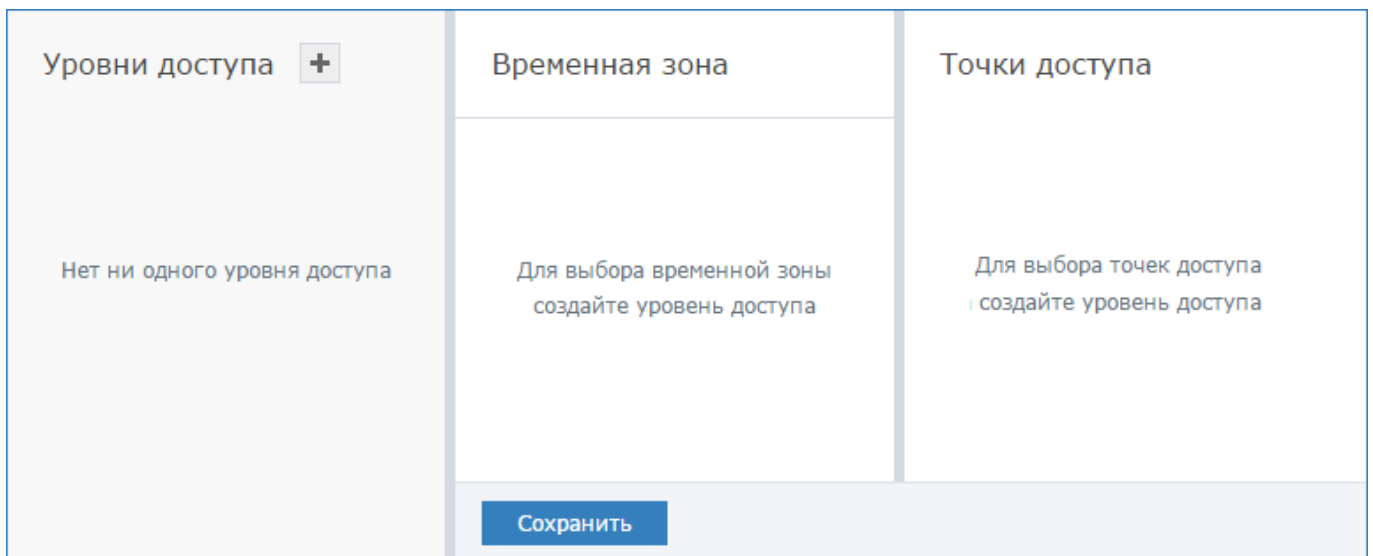




Рисунок 9.94 — Окно конфигурирования уровней доступа. Не создано ни одного уровня

### Добавление уровня доступа:

1. В столбце **Уровень доступа** нажмите на кнопку  **Добавить уровень доступа**.
2. Укажите номер и наименование уровня доступа (рисунок 9.95). Нажмите на кнопку .

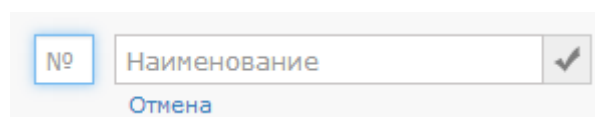


Рисунок 9.95 — Добавление уровня доступа

3. В столбце **Временная зона** (рисунок 9.96) укажите период времени и дни недели, в течение которых разрешён 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 клавиши мыши. При необходимости выбора всех дней недели, нажмите на кнопку **Все**.



Рисунок 9.96 — 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 правом столбце на вкладке **Точки доступа** выберите точки доступа, проход по которым разрешён для данного уровня доступа. Можно осуществлять поиск точки доступа по IP-адресу контроллера, его названию или названию точки доступа. На вкладке **Ключи** выберите номера ячеек, ключи из которых будут доступны данному уровню доступа (список ключей не пустой, если текущий узел настроен на совместную работу с системой KMS).
6. Если список объектов доступа (точек и ключей) должен варьироваться в зависимости от времени/дня недели, нажмите на ссылку [добавить правило] и повторите пп. 3-5.
7. Нажмите на кнопку **Сохранить**.

#### **Изменение уровня доступа:**

В окне конфигурирования уровней доступа слева выберите требуемый уровень (или воспользуйтесь поиском по номеру или наименованию), выберите текущее правило (если создано несколько правил) измените временные интервалы или объекты доступа, нажмите на кнопку **Сохранить**.

### **Настройка уровней управления**

Уровень управления назначается пропуску и определяет список объектов охраны, разрешенные команды управления и время, в течение которого разрешено управление заданными объектами. Конфигурируются следующие параметры:

- список разделов сигнализации и разрешённые действия по управлению разделом (постановка, снятие, сброс тревог) - по каждому разделу индивидуально;
- список точек доступа и разрешённые действия по управлению точкой доступа (блокировка, разблокировка, восстановление в дежурный режим, разрешение разового прохода) - индивидуально по каждой точке доступа;

- временные интервалы — периоды времени, в течение которого разрешается управление разделами и точками доступа.

**Примечание.** Один пропуск может обладать правами управления разделами с нескольких терминалов. Список разделов сигнализации, с которыми может работать конкретный терминал, задаётся в разделе [Терминалы](#). Права пропуска по управлению разделами на конкретном терминале определяются пересечением множества «привязанных» к терминалу разделов с множеством разделов, заданных уровнем управления пропуском (рисунок 9.97).



Рисунок 9.97 — Уровень управления пропуском на терминале

**Примечание.** Один пропуск может обладать правами управления точками доступа с нескольких терминалов. Список точек доступа, доступных к управлению с терминала «ВИК» определяется составом его индикаторов. Разрешённые действия определяются уровнем управления пропуском.

Настройка уровней управления осуществляется в приложении «Бюро пропусков». Для перехода в «Бюро пропусков», перейдите на **Рабочий стол** (см. раздел [Рабочий стол](#)) и выберите пункт **Бюро пропусков**, далее перейдите к вкладке **Уровни управления**.

Окно конфигурирования уровней управления (рисунок 9.98) разделено на три вертикальные области: слева задаётся номер и имя уровня управления, по центру указываются временные интервалы, в течение которых разрешено управление разделами и точками доступа, справа на вкладке **Разделы сигнализации** выбираются разделы сигнализации и разрешённые действия по управлению разделами, на вкладке **Точки доступа** выбираются точки доступа и разрешённые действия по управлению ими.

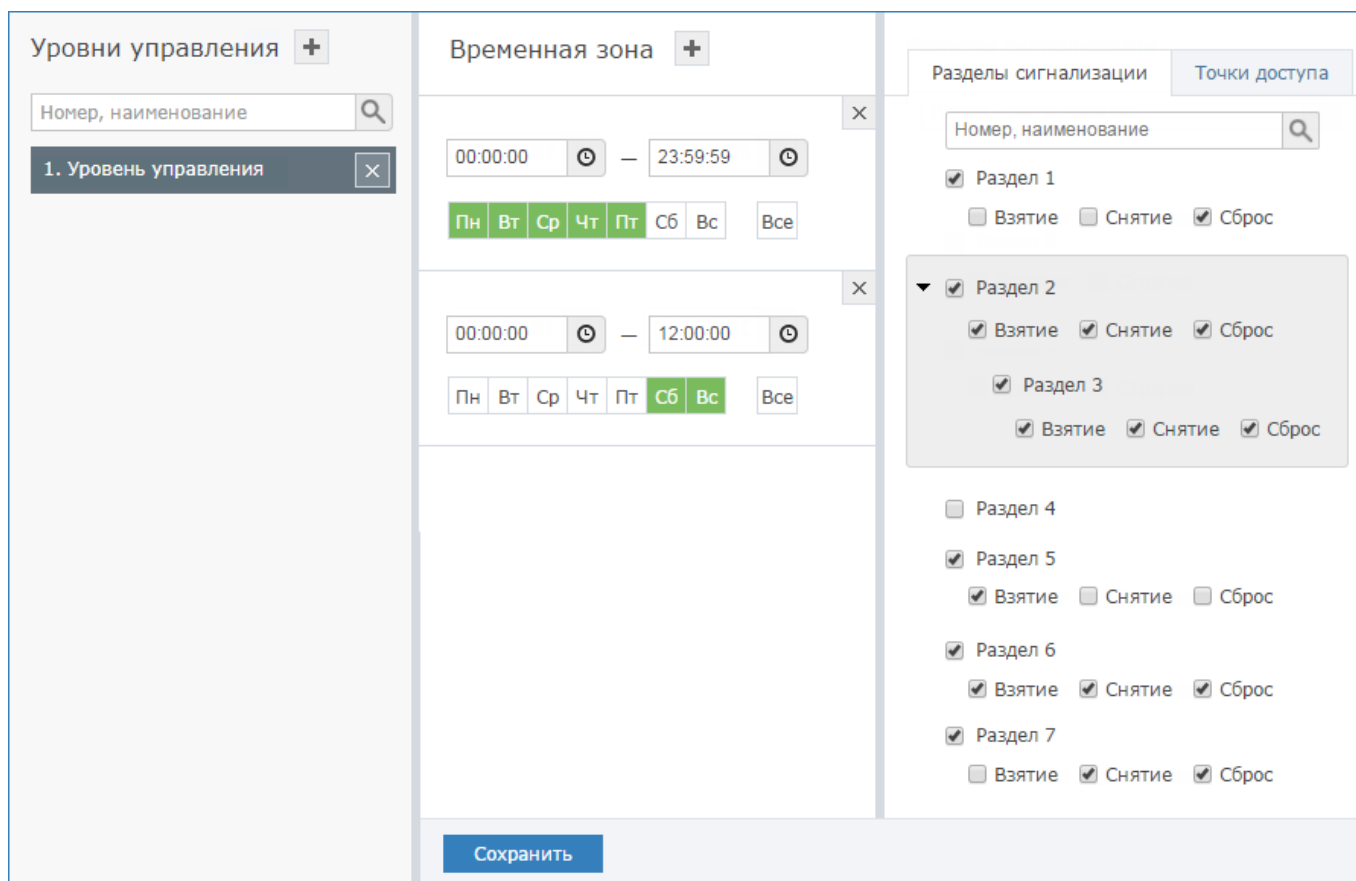


Рисунок 9.98 — Окно конфигурирования уровней управления

Если уровни управления ранее не конфигурировались, отобразится пустое окно (рисунок 9.99).

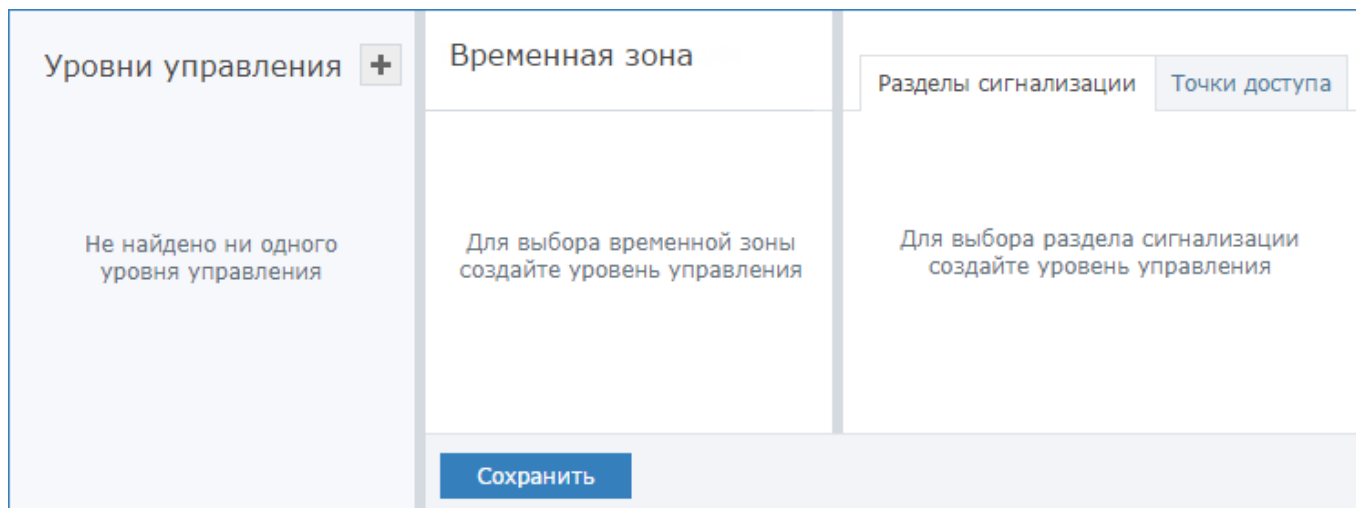



Рисунок 9.99 — Окно конфигурирования уровней управления. Не создано ни одного уровня

### Добавление уровня управления

1. В столбце **Уровни управления** нажмите на кнопку  **Добавить уровень управления**.

2. Укажите номер и наименование уровня управления (рисунок 9.100). Нажмите на кнопку .

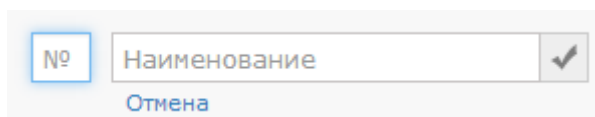



Рисунок 9.100 — Добавление уровня управления

3. В столбце **Временная зона** (рисунок 9.101) укажите временной интервал и дни недели, в течение которых разрешено управление разделами сигнализации и точками доступа. 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**.

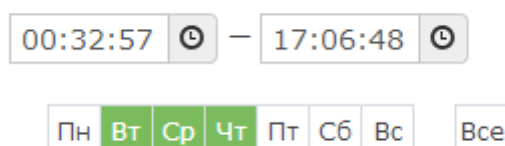



Рисунок 9.101 — Добавление временного интервала

4. При необходимости добавления к этому уровню управления нового временного интервала, нажмите на кнопку  **Добавить временную зону** и задайте параметры новой зоны.
5. В столбце справа на вкладке **Разделы сигнализации** выберите разделы сигнализации и разрешённые действия по управлению разделами, затем перейдите в вкладке **Точки доступа** и выберите точки доступа и разрешённые действия по управлению ими (рисунок 9.102).

**Примечание.** Список разрешённых действий отображается после выбора раздела/точки доступа.

Можно осуществлять поиск раздела по его номеру или наименованию, а также поиск точки доступа по наименованию, виду устройства или ip-адресу.

Разделы сигнализации
Точки доступа

- Точка доступа 1 (10.1.30.36, БОРЕЙ)
  - Восстановление
  - Разблокировка
  - Блокировка
  - Инициация прохода
- Точка доступа 2 (10.1.30.36, БОРЕЙ)
  - Восстановление
  - Разблокировка
  - Блокировка
  - Инициация прохода
- Точка доступа (ВХОД) (10.1.30.11, БОРЕЙ)
  - Восстановление
  - Разблокировка
  - Блокировка
  - Инициация прохода
- Точка доступа (ВЫХОД) (10.1.30.11, БОРЕЙ)
  - Восстановление
  - Разблокировка
  - Блокировка
  - Инициация прохода

Рисунок 9.102 — Команды управления точкой доступа

6. Нажмите на кнопку **Сохранить**.
7. При необходимости создания нового уровня управления, повторите действия пп.1. 1. - 6.
8. Впоследствии параметры уровней управления могут быть изменены, для этого перейдите в окно конфигурирования уровней управления, слева выберите требуемый уровень (или воспользуйтесь поиском по номеру или наименованию), измените список разделов/точек доступа, разрешённые действия или временные интервалы, нажмите на кнопку **Сохранить**.



## ПРИЛОЖЕНИЕ 10. ФОТОИДЕНТИФИКАЦИЯ

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

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

Окно приложения разделено на две области:

- Слева расположена область ленты событий системы доступа (рисунок 9.103);
- Основное окно поделено на области, в каждой из которых отображаются события по выбранной точке доступа (рисунок 9.104). При наличии «привязанной» камеры, в случае запроса доступа отображается «живое видео».

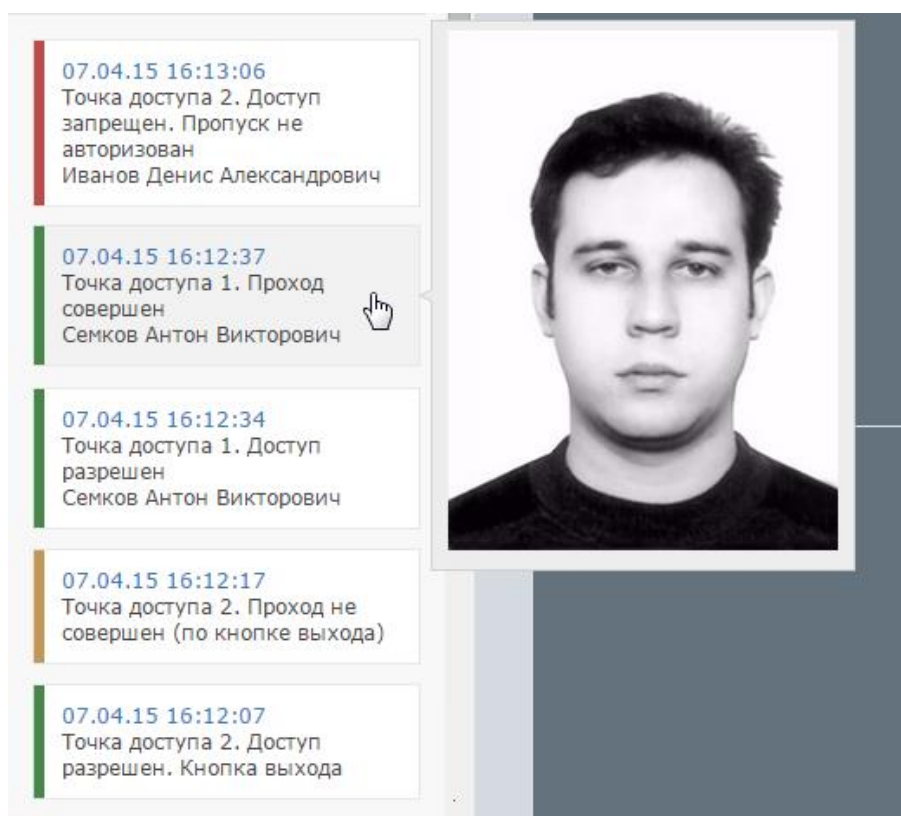


Рисунок 9.103 — Лента событий приложения «Фотоидентификация»

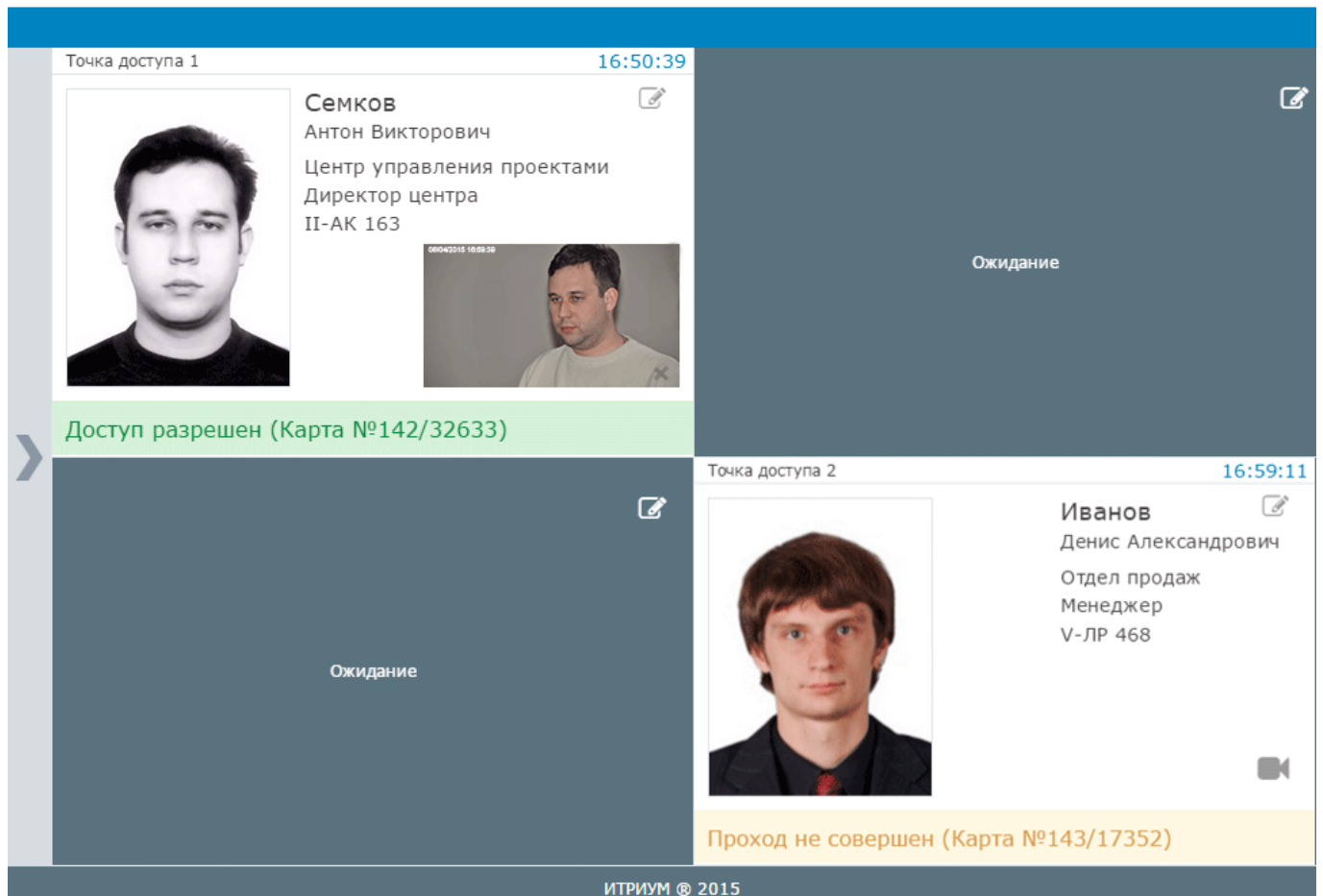


Рисунок 9.104 — Основное окно приложения «Фотоидентификация»



## ПРИЛОЖЕНИЕ 11. СОБЫТИЯ

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 9.105).

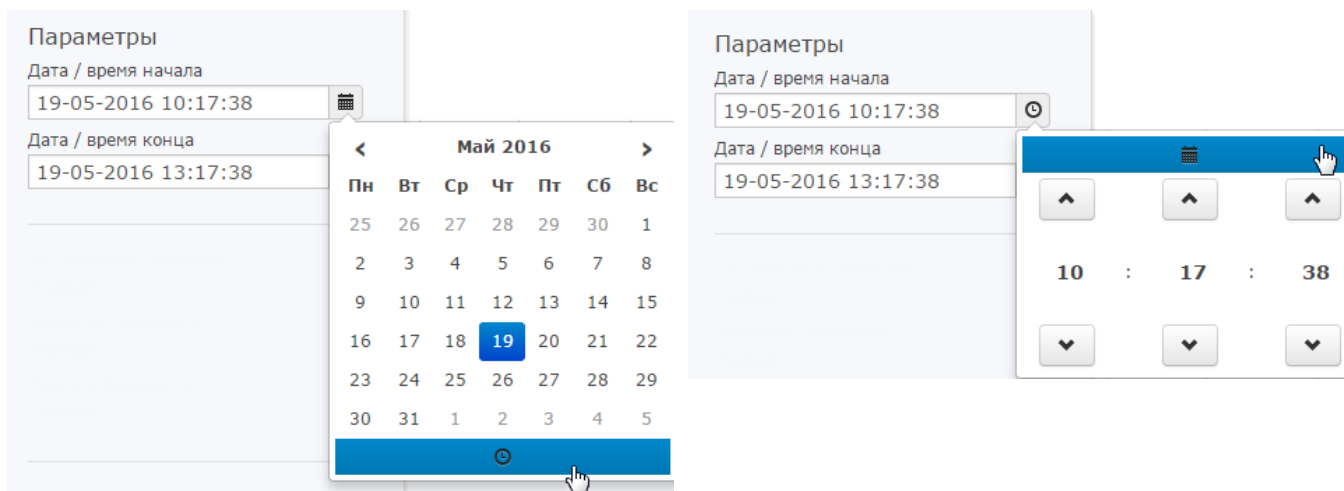




Рисунок 9.105 — Добавление временного интервала

По завершению поиска, список событий можно экспортировать в формат **CSV** для редактирования в MS Excel и др. программах. Для экспорта нажмите на кнопку  (рисунок 9.106).

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 9.106 — Список событий за заданный период времени

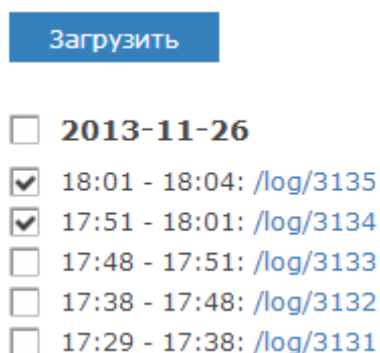
## ПРИЛОЖЕНИЕ 12. ЖУРНАЛ АУДИТА

**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 9.107). Скачивание начнется незамедлительно. Выбранные файлы будут сформированы в архив формата **.tar.gz**.



The image shows a user interface for downloading log files. At the top is a blue button labeled 'Загрузить'. Below it is a list of log files, each with a checkbox and a timestamp followed by a file path. The first item is a date '2013-11-26' with an unchecked checkbox. The following five items are time intervals with file paths, each with a checked checkbox: '18:01 - 18:04: /log/3135', '17:51 - 18:01: /log/3134', '17:48 - 17:51: /log/3133', '17:38 - 17:48: /log/3132', and '17:29 - 17:38: /log/3131'.

File Name	Selected
2013-11-26	<input type="checkbox"/>
18:01 - 18:04: /log/3135	<input checked="" type="checkbox"/>
17:51 - 18:01: /log/3134	<input checked="" type="checkbox"/>
17:48 - 17:51: /log/3133	<input type="checkbox"/>
17:38 - 17:48: /log/3132	<input type="checkbox"/>
17:29 - 17:38: /log/3131	<input type="checkbox"/>

Рисунок 9.107 — Список лог-файлов

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

## ПРИЛОЖЕНИЕ 13. ПО ИСБ ITRIUM®

Программное обеспечение ITRIUM® — это интеграционная платформа для создания интегрированных систем безопасности.

ITRIUM® обеспечивает:

- Поддержку стандартных и нестандартных протоколов для интеграции систем безопасности и технических средств различных производителей;
- Тесную взаимосвязь между подсистемами охранной сигнализации, пожарной сигнализации, системой контроля и управления доступом (СКУД), аналогового и IP-видеонаблюдения, диспетчеризации и другими;
- Автоматизацию процессов управления безопасностью объекта: комплексный мониторинг безопасности, управление пропускным режимом, видеонаблюдение;

Для выполнения функций мониторинга и управления предназначены программы «Администратор системы» и «Мониторинг». Для создания планов и размещения объектов на планах предназначена программа «Администратор мониторинга». Для ввода данных пропусков предназначена «Программа оформления пропусков», для формирования отчетов — программа «Отчёты». Все вышеперечисленные программы входят в базовый пакет поставки ITRIUM®, за исключением «Программы оформления пропусков», лицензия на использование которой приобретается отдельно.

### 1. Настройка «Службы НЕЙРОСС»

«Служба НЕЙРОСС» входит в базовый пакет ITRIUM® и предназначена для осуществления взаимодействия (интеграции) системы безопасности, построенной на платформе ITRIUM® и интегрированной системой безопасности НЕЙРОСС.

**В результате интеграции появляется возможность:**

- Осуществления единого пропускного режима на базе приборов «Борей». «ЯРС», терминалов «МТК» и любых других контроллеров доступа, интегрированных в ITRIUM®;
- Объединения систем доступа, построенных на базе независимых экземпляров ПО ITRIUM®, в общую систему;
- Графического мониторинга состояний и управление точками доступа, разделами и зонами охранной сигнализации всей системы в целом на базе единого интерфейса;
- Автоматического управления элементами сторонних систем по событиям от элементов системы НЕЙРОСС и наоборот — управления точками доступа и охранными разделами по событиям от систем сторонних производителей (с использованием лицензируемой «Службы автоматического управления»);

- Просмотра видеопотока (в том числе архивного) и управления элементами нескольких экземпляров ITRIUM® посредством веб-интерфейса (с использованием «НЕЙРОСС Центр»);
- Использования унифицированных рабочих мест, таких как «Бюро пропусков», «Фотоидентификация» в системе НЕЙРОСС;
- Использования мощного административного ресурса: архивирование базы данных, построение отчётов и многое другое.

### **Режимы работы службы:**

Служба может работать в одном из двух режимов:

- Обычный режим работы — обеспечение взаимодействия с сетью НЕЙРОСС;
- Режим распределённого доступа.

### **Обычный режим**

В обычном режиме «Служба НЕЙРОСС» обеспечивает работу ITRIUM®, как полноправного узла сети ONVIF-устройств НЕЙРОСС: обеспечивает взаимную синхронизацию данных с другими узлами НЕЙРОСС, мониторинг состояний и управление элементами систем.

Синхронизация инициируется устройством (контроллером или компьютером в лице «Службы НЕЙРОСС»), на котором произошли изменения: устройство формирует сетевые запросы ко всем смежным узлам сети с информацией о времени и характере изменения. Другие узлы сети получают данный запрос и обновляют собственные данные. Если в момент обновления связь с каким-либо узлом была прервана, при восстановлении связи, «потерянный» узел сам инициирует запросы на получение информации об изменениях.

### **Функции службы в обычном режиме:**

- Поиск узлов сети НЕЙРОСС, вычитывание конфигурации и данных;
- Синхронизация данных ITRIUM® с данными всех узлов НЕЙРОСС (устройств «Борей», «ЯРС», «МТК», «ДеВизор», серверов ITRIUM®, «НЕЙРОСС Доступ» и «НЕЙРОСС Центр»).
- Мониторинг состояний элементов всех узлов НЕЙРОСС их охранных зон, разделов и точек доступа.
- Взаимная передача команд управления из ITRIUM® в НЕЙРОСС и обратно.

**Примечание.** Данные являются общими для всех устройств системы безопасности НЕЙРОСС. При обновлении информации на одном устройстве (например, создан новый уровень доступа или раздел охранной сигнализации), данные автоматически подгружаются во все устройства сети. Компьютер с ПО ITRIUM® является равноправным узлом

сети НЕЙРОСС. Загрузка пропусков из ITRIUM® осуществляется совместно со «Службой бюро пропусков».

- Синхронизация времени на всех устройствах и компьютерах, необходимая для успешной синхронизации данных;

**Примечание.** Необходимым условием успешного взаимодействия всех узлов сети НЕЙРОСС является их синхронизация по времени. Для этого в пакет установки ITRIUM® входит NTP-сервер. При расхождении текущего времени на устройствах более 5 секунд, формируется сообщение «Рассинхронизация времени».

### Режим распределённого доступа

Режим распределённого доступа предназначен для объединения нескольких локальных СКУД ITRIUM® (узлов системы распределённого доступа) в единую систему доступа вне зависимости от производителя интегрированного в каждом узле оборудования.

В результате такого объединения появляется возможность создания единого Бюро пропусков с возможностью задания для пропуска индивидуальных параметров доступа к каждому узлу распределённой системы. Созданный пропуск будет автоматически передан каждому экземпляру ITRIUM®, а затем локально в каждой системе разгружен в контроллеры доступа.

Настройка службы в режим распределённого доступа выходит за рамки данного руководства, ниже приведём порядок настройки службы для обеспечения взаимодействия с сетью НЕЙРОСС.

Выполните следующую последовательность шагов:

1. На компьютер с операционной системой семейства Windows установите серверную часть программного обеспечения ITRIUM®.

**Примечание.** Системные требования к серверу можно посмотреть по ссылке <http://www.itrium.ru/products/itrium/requirements.php>. Установочный диск можно получить у изготовителя, либо скачать ISO-образ диска, заполнив форму по адресу <http://www.itrium.ru/support/download/itrium.php>. Дополнительно требуется приобрести ключ HASP с лицензиями на использование. Инструкцию по установке и другие руководства можно открыть из окна автозапуска установочного диска, либо скачать по адресу <http://www.itrium.ru/support/documentation/itrium.php>.

Обеспечьте сетевое соединение между компьютером и прибором «ЯРС» (инструкцию см. в разделе [Мастер первого запуска](#)).

2. Запустите программу «Администратор системы», в окне авторизации введите: Имя пользователя – sysdba, пароль – Masterkey96000613.
3. Примечание. Руководство [пользователя к программе](#) «Администратор системы» можно открыть из окна автозапуска установочного диска, либо скачать по адресу <http://www.itrium.ru/support/documentation/itrium.php>



4. В дереве элементов к элементу Компьютер добавьте дочерний элемент Служба НЕЙРОСС, для этого:
5. Выделите элемент Компьютер, нажмите на правую кнопку мыши и выберите команду **Создать новый элемент** (рисунок 9.108).

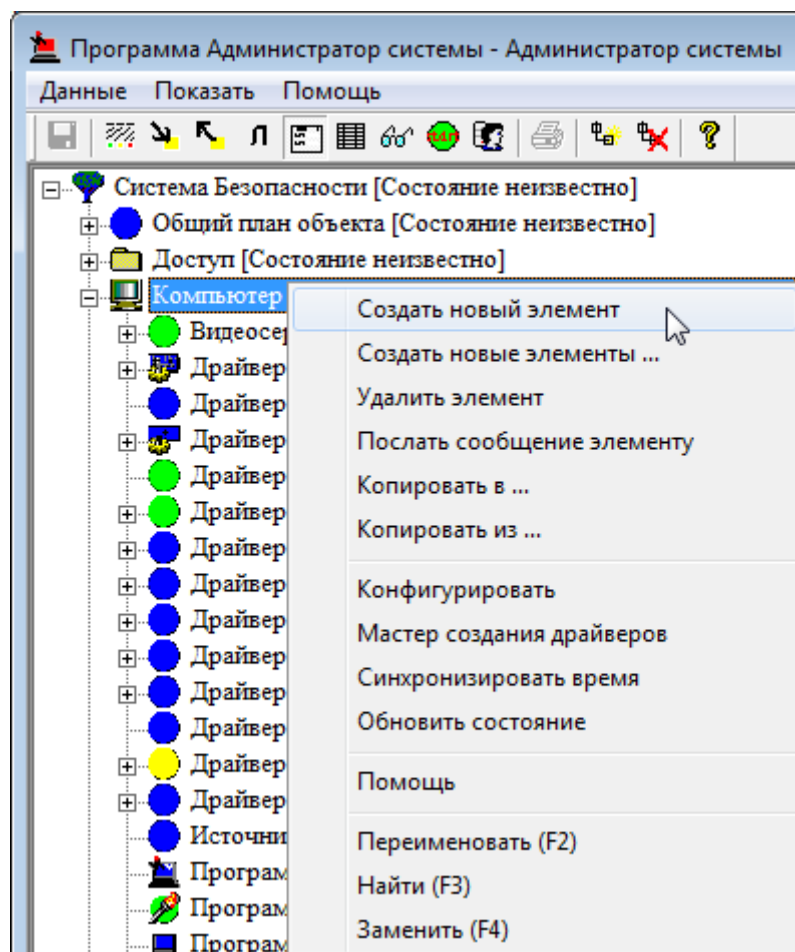




Рисунок 9.108 — Окно [программы «Администратор системы»](#)

[В новом окне выберите Служба НЕЙРОСС и нажмите на кнопку Добавить, в отображенном окне нажмите на кнопку Принять.](#)

6. Проверьте настройки частных свойств Службы **НЕЙРОСС** (см. таблицу 9.22). Окно свойств изображено на рисунке 9.109. Для доступа к окну свойств выделите элемент **Служба НЕЙРОСС** и нажмите на кнопку  **Частные свойства** Панели инструментов. Перейдите к вкладке **Свойства**. Описание полей вкладки представлено в таблице 9.22. Если были внесены какие-либо изменения, нажмите на кнопку  **Сохранить** Панели управления.

Сеть IP-устройств:

Порт TCP:

NTP сервер:

Папка пропусков:

Домен НЕЙРОСС\*:   
\*Если значение не указано, то используется: "NEYROSS"

Строгий режим фильтрации доменов:

Группа операторов:

---

Авторизация сетевого взаимодействия:

Пароль:

---

Папка пропусков -"Доступ":

Объединение 'Систем безопасности':  Для объединения нескольких 'Систем безопасности' в общую систему доступа создайте дочерний элемент - 'Узел системы распределенного доступа'. Лицензионный ключ - обязателен!

- Рисунок 9.109 — Окно частных свойств элемента Служба НЕЙРОСС
- Таблица 9.22 – Свойства «Службы НЕЙРОСС»

Название поля	Назначение поля
Сеть IP-устройств	<p>Определяет элемент <b>Сеть IP-устройств</b>, являющийся родительским по отношению к добавляемым элементам (<b>ONVIF-устройство</b>, <b>Контроллер БОРЕЙ/ ЯРС</b>, <b>Видеоинформационная консоль</b>, <b>Мобильный терминал контроля</b>, <b>ONVIF-устройство</b> и др.). Элемент <b>Сеть IP-устройств</b> добавляется автоматически при первичном запуске «Службы НЕЙРОСС», идентификатор элемента присваивается данному полю. Оставьте поле пустым.</p> <p><b>Примечание.</b> Элемент <b>Сеть IP-устройств</b> является корневым элементом системы безопасности. При необходимости настройки нескольких служб НЕЙРОСС, элемент может быть создан вручную и впоследствии выбран из раскрывающегося списка в поле <b>Сеть IP-устройств</b>.</p>
Порт TCP	<p>Номер порта для связи с другими устройствами сети. Значение по умолчанию <b>6501</b>. Если порт занят, укажите другой свободный порт.</p>

Название поля	Назначение поля
NTP-сервер*	<p>Определяет, требуется ли синхронизировать время на всех узлах «БОРЕЙ», «ЯРС» по NTP-серверу данного компьютера. По умолчанию флаг не установлен.</p> <p>Если флаг установлен, в настройках даты и времени узлов «Борей», «ЯРС» устанавливается <b>Автоматический</b> режим, в поле <b>Адрес NTP-сервера</b> прописывается IP-адрес компьютера. Синхронизация осуществляется средствами <b>Службы времени Windows (Windows Time)</b>.</p> <p><b>Внимание.</b> Если в системе есть несколько серверов ITRIUM® или «НЕЙРОСС Центр», во избежание конфликтов флаг должен быть установлен только на одном компьютере. Остальные компьютеры должны быть синхронизированы по первому средствами Windows (в настройках даты и времени задать синхронизацию по ip-адресу первого компьютера).</p>
Папка пропусков	<p>Название папки для хранения пропусков раздела <b>Доступ</b> дерева элементов системы безопасности ITRIUM®, в которую будут вычитываться пропуска из узлов сети НЕЙРОСС. По умолчанию пропуска загружаются в папку <b>Пропуска НЕЙРОСС/Сеть IP-устройств</b>. Можно выбрать другую существующую папку или создать новый элемент типа <b>Пропуска</b> и затем выбрать данный элемент из раскрывающегося списка поля <b>Папка пропусков</b>.</p> <p>При необходимости использования корневой папки <b>Доступ</b> для хранения пропусков, установите флаг в поле <b>Папка пропусков - "Доступ"</b>. При этом настройки поля <b>Папка пропусков</b> будут игнорироваться.</p>
Домен НЕЙРОСС	<p>Домен НЕЙРОСС — это символьное обозначение закрытой для внешнего доступа группы узлов НЕЙРОСС. Взаимное сетевое обнаружение осуществляется только внутри «своего» домена. В данном поле устанавливается, какому домену будет принадлежать данный узел ITRIUM. Как и любой узел НЕЙРОСС, ITRIUM может принадлежать нескольким доменам, тогда взаимное сетевое обнаружение осуществляется в пределах группы доменов. Значение поля по умолчанию — <b>NEYROSS</b>. При необходимости указания нескольких доменов, введите имена доменов через запятую. Система не ограничивает количество доменов, таким образом достигается оптимизация информационного обмена узлов друг с другом.</p> <p>В сети с несколькими доменами, узел ITRIUM должен принадлежать всем доменам сети. Для этого необходимо через запятую указать имена всех используемых в системе доменов.</p>
Строгий режим фильтрации доменов	<p>Поле задаёт, принимать ли извещения от устройств, не имеющих домены (например, от ONVIF-камер). Если флаг не установлен, такие устройства «видны» в системе безопасности. Если принимать извещения от таких устройств не требуется, установите флаг в данном поле.</p>
Группа операторов	<p>Поле задаёт, права какой группы операторов требуется использовать при предоставлении доступа системе НЕЙРОСС (в частности, — приложению «НЕЙРОСС Центр») к элементам системы безопасности ITRIUM и командам управления ими.</p>
Папка пропусков - «Доступ»	<p>Если флаг установлен, пропуска будут вычитываться в корневую папку <b>Доступ</b> и настройки поля <b>Папка пропусков</b> будут игнорироваться.</p>

7. Запустите **Службу НЕЙРОСС**. Для этого в окне свойств службы перейдите к вкладке **Драйвер**, в группе **Параметры запуска** выберите **В выделенном приложении**, нажмите на кнопку **Принять**. Реакция системы на ваши действия будет следующей:

- К элементу **Система безопасности** будет автоматически добавлен элемент **Сеть IP-устройств**.

- К элементу **Сеть IP-устройств** автоматически будут добавлен элемент **Контроль доступа НЕЙРОСС** с дочерним элементом **Папка уровней доступа НЕЙРОСС**, а также элемент **Охрана и управление НЕЙРОСС** с дочерними элементами **Уровни управления НЕЙРОСС**, **Разделы охранной сигнализации НЕЙРОСС** и **Папка терминалов НЕЙРОСС** (рисунок 9.110).

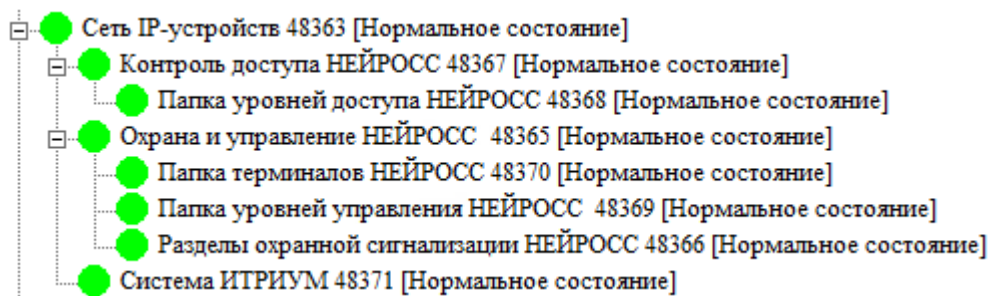


Рисунок 9.110 — Сеть IP-устройств. Дерево элементов

- Также будет произведён поиск всех устройств НЕЙРОСС («Борей», «ЯРС» и проч.), принадлежащих заданным в поле **Домен НЕЙРОСС** доменам. Для найденных устройств будут сконфигурированы соответствующие элементы **Контроллер БОРЕЙ**, **Контроллер ЯРС**, **Система ИТРИУМ** и проч., и их дочерние элементы: **Точка доступа НЕЙРОСС**, **Зона охранной сигнализации НЕЙРОСС**, **Реле устройства НЕЙРОСС** и проч. (рисунок 9.111).

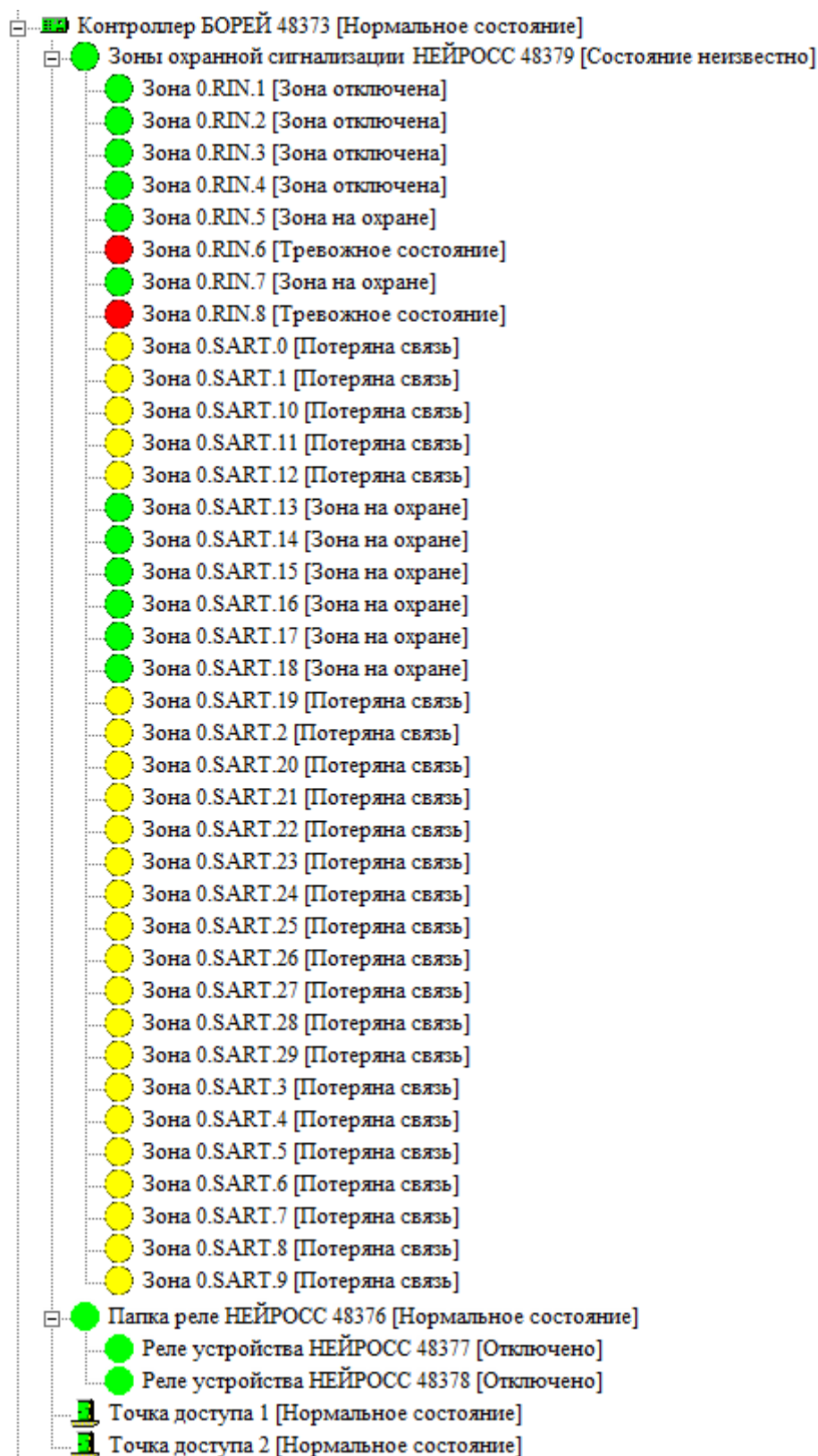


Рисунок 9.111 — Элемент **Контроллер БОРЕЙ**. Дочерние элементы

- Уровни доступа, уровни управления и охранные разделы являются общими ресурсами сети НЕЙРОСС. При наличии сконфигурированных на каком-либо устройстве сети уровней доступа, уровней управления и охранных разделов, к элементу **Сеть IP-устройств** будут добавлены соответствующие элементы: в **Папку**

уровней доступа НЕЙРОСС будут добавлены элементы **Уровень доступа НЕЙРОСС**, в Папку уровней управления НЕЙРОСС — элементы **Уровень управления НЕЙРОСС**, в папку **Разделы охранной сигнализации НЕЙРОСС** — элементы **Раздел охранной сигнализации НЕЙРОСС** и проч. (рисунок 9.112).

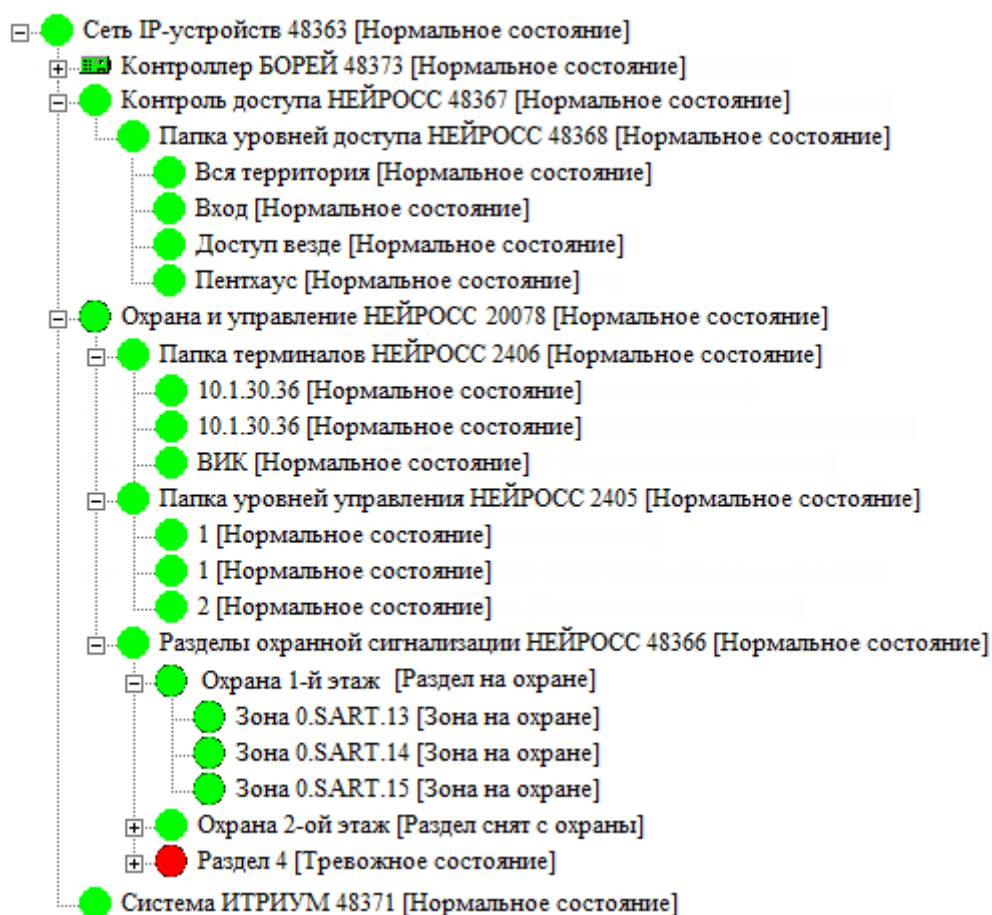


Рисунок 9.112 — Элемент **Сеть IP-устройств**. Дерево элементов

- По умолчанию задан не строгий режим фильтрации доменов. Это означает, что принимаются извещения от устройств, не имеющих домены (например, ONVIF-камер) и устройства «видны» в системе безопасности (рисунок 9.113). Если принимать извещения от таких устройств не требуется, необходимо в окне частных свойств элемента **Служба НЕЙРОСС** установить флаг в поле **Строгий режим фильтрации доменов**, сохранить параметры и перезапустить службу.

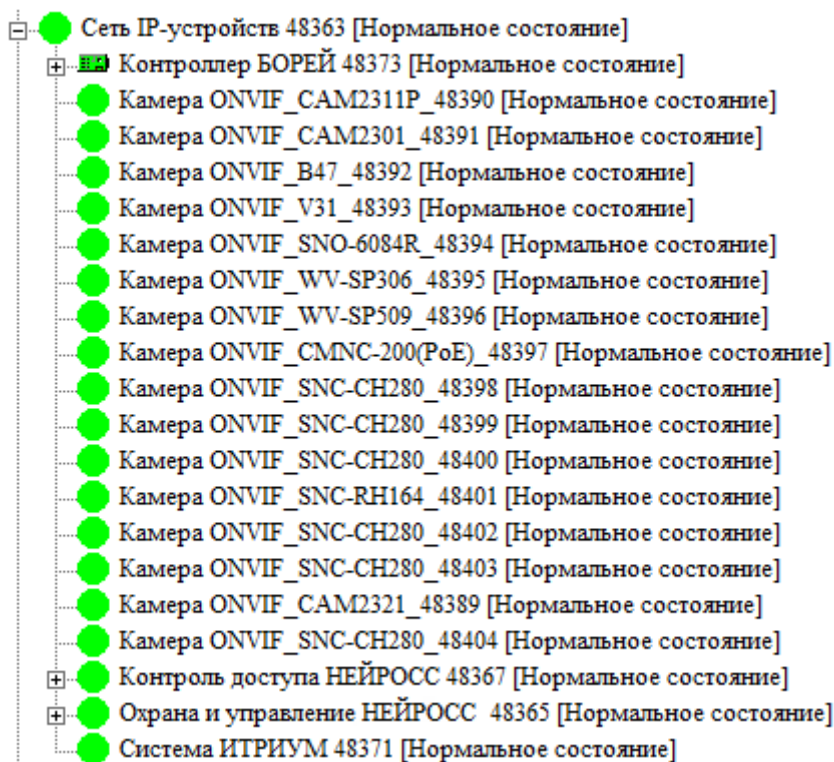


Рисунок 9.113 — Сеть IP-устройств. Дерево элементов с ONVIF-устройствами

**Примечание 1.** Чтобы проверить, выполнена ли синхронизация времени на всех устройствах в системе, запустите веб-браузер, в адресной строке введите [http://ip-адрес компьютера:\[номер порта\]](http://ip-адрес компьютера:[номер порта]), например <http://10.200.1.243:6501/> (номер порта указан в поле **Порт TCP**). Нажмите на клавишу **Enter**. В окне веб-интерфейса перейдите к разделу **Сеть** (дополнительную информацию см. приложение Сеть).

**Примечание 2.** Если в системе безопасности ITRIUM® для ввода данных владельцев пропусков или пропусков используются данные биометрического сканера или весовой платформы, для обеспечения загрузки этих данных в контроллеры СКУД и ОТС «Борей»/«ЯРС» необходимо вручную добавить соответствующие свойства для элемента **Служба НЕЙРОСС**. Аналогично, если требуется загрузка дополнительных данных о пропуске или владельце пропуска для отображения на терминале «МТК» необходимо добавить соответствующие свойства для элемента **Служба НЕЙРОСС**. Описание процедуры настройки см. в разделе [Загрузка данных в НЕЙРОСС](#).

## 2. Команды управления

После запуска «Службы НЕЙРОСС» (см. раздел [Настройка «Службы НЕЙРОСС»](#)), к элементу **Сеть IP-устройств** добавляются элементы, соответствующие узлам НЕЙРОСС, их точкам доступа, реле и зонам сигнализации, а также элементы, **Папка уровней доступа**, **Разделы охранной сигнализации** и другие элементы, соответствующие общим ресурсам сети (уровням доступа, уровням управления, разделам охранной сигнализации и др.). Состояния элементов в дереве элементов соответствует их текущему состоянию.

С помощью команд контекстного меню можно управлять точками доступа, реле, разделами и зонами охранной сигнализации. Список доступных команд зависит от типа

элемента и варьируется в зависимости от текущего состояния элемента. Описание возможных состояний см. в разделе [Состояния элементов прибора](#).

Список команд управления представлен в таблице 9.23. Для вызова команды, нажмите на правую кнопку мыши на элементе, которому требуется отправить команду, и в отобразившемся меню выберите требуемую команду.

Таблица 9.23 – Команды управления

Тип элемента	Команда	Описание
Точка доступа НЕЙРОСС	Инициировать проход	Команда выполняет действие, аналогичное нажатию кнопки выхода. Дверь разблокируется на период времени, указанный в поле <b>Время ожидания открытия двери</b> .
	Разблокировать	Команда разблокировки точки доступа. Разрешён проход без предъявления идентификаторов.
	Заблокировать	Команда блокировки точки доступа. Проход запрещён.
	Восстановить режим	Команда восстановления точки доступа в состояние по умолчанию (см. раздел <a href="#">Смена состояний зон и разделов при постановке на охрану</a> ). Отменяет команды <b>Заблокировать/Разблокировать</b> .
Зона охранной сигнализации НЕЙРОСС	Сброс тревоги	Команда сброса тревоги зоны <sup>1)</sup> .
	Снять с охраны	Команда снятия зоны с охраны <sup>1)</sup> .
	Поставить на охрану	Команда постановки зоны на охрану <sup>1)</sup> .
Раздел охранной сигнализации НЕЙРОСС	Сброс тревоги	Команда сброса тревоги раздела <sup>1)</sup> .
	Снять с охраны	Команда снятия раздела с охраны <sup>1)</sup> .
	Поставить на охрану	Команда постановки раздела на охрану <sup>1)</sup> .
Реле устройства НЕЙРОСС	Выключить реле	Команда выключения реле
	Включить реле	Команда включения реле

<sup>1)</sup> Дополнительную информацию см. в разделе [Команды управления разделами и зонами](#).

### 3. Настройка доступа в ПО ИСБ ITRIUM

Настройка доступа через веб-интерфейс включает следующие шаги:

1. Настройка **Уровней доступа**. Уровень доступа определяет, через какие точки доступа и в какое время владельцу пропуска разрешён доступ. Для каждого уровня доступа может быть настроено несколько временных интервалов. Инструкция приведена в разделе [Настройка уровней доступа](#).
2. Настройка **Уровней управления**. Уровни управления также настраиваются для всей системы в целом и содержат информацию о правах управления точками доступа и разделами сигнализации. Инструкция по настройке уровней охраны приведена в разделе [Настройка уровней управления](#).



3. **Создание пропусков.** Пропуска настраиваются для всей системы в целом и содержат информацию о владельце, номере пропуска, а также его уровне доступа и, при необходимости, его уровне управления. Инструкция приведена в разделе [Создание пропуска](#).


Если «Служба НЕЙРОСС» запущена, база пропусков ITRIUM® и узлов СКУД НЕЙРОСС автоматически синхронизируется.

Однако пропуска также могут быть сконфигурированы посредством ПО ИСБ ITRIUM. При этом потребуется выполнение следующих шагов.

1. Настройка **Уровней доступа** в ITRIUM® (см. раздел [Уровни доступа](#)).
2. Настройка **Уровней управления** в ITRIUM® (см. раздел [Уровни управления](#)).
3. Настройка **Режимов доступа**. Режим доступа назначается пропуску и содержит ссылки на уровни доступа. Режим доступа также может включать уровни доступа контроллеров СКУД других производителей. Инструкция по настройке режимов доступа приведена в разделе [Настройка режимов доступа](#).
4. Загрузка пропусков в оборудование осуществляется «Службой НЕЙРОСС» совместно со «Службой бюро пропусков». Для загрузки пропусков в узлы НЕЙРОСС никаких дополнительных настроек службы не требуется («Служба бюро пропусков» должна быть запущена). Руководство пользователя к «Службе бюро пропусков» можно открыть из окна автозапуска установочного диска, либо скачать по адресу <http://www.itrium.ru/support/documentation/itrium.php>.
5. База данных пропусков располагается в папке **Доступ** дерева элементов. Оформление пропусков в ITRIUM® осуществляется с помощью «Программы оформления пропусков». Руководство пользователя к «Программе оформления пропусков» можно открыть из окна автозапуска установочного диска, либо скачать по адресу <http://www.itrium.ru/support/documentation/itrium.php>.
6. При необходимости загрузки в контроллеры «Борей», «ЯРС» биометрических параметров и данных весовой платформы, а в терминалы «МТК» — дополнительных полей данных о пропуске или владельце пропуска, необходимо задать соответствующие свойства вручную в настройках «Службы НЕЙРОСС» (см. раздел [Загрузка данных в НЕЙРОСС](#)).

### Уровни доступа

Для настройки уровня доступа выполните следующую последовательность шагов:

1. В программе «Администратор системы» в дереве элементов выделите элемент **Папка уровней доступа НЕЙРОСС** (последовательно разверните список дочерних элементов элемента **Сеть IP-устройств** и **Контроль доступа НЕЙРОСС**).
2. Перейдите к окну частных свойств выделенного элемента, для этого нажмите на кнопку  **Частные свойства** панели инструментов.

3. В окне частных свойств нажмите на кнопку **Настроить уровни доступа...** Будет запущен браузер, заданный по умолчанию, и выполнен переход к HTML-странице настройки уровней доступа по адресу [http://\[ip-адрес компьютера\]:\[порт\]/neyross/accesslevels/](http://[ip-адрес компьютера]:[порт]/neyross/accesslevels/), например <http://10.200.1.243:6501/neyross/accesslevels/> (номер порта задаётся в поле **Порт ТСР** окна частных свойств «Службы НЕЙРОСС», IP-адрес компьютера указан в окне частных свойств элемента **Компьютер**). Процедура настройки уровней доступа описана в подразделе [Настройка уровней доступа](#).

**Примечание.** При переходе к конфигурированию уровней доступа по нажатию кнопки из программы «Администратор системы», уровни доступа настраиваются на компьютере, откуда произошёл переход. Загрузка сконфигурированных уровней доступа в контроллеры осуществляется «Службой НЕЙРОСС». Чтобы проверить, корректно ли произошла загрузка данных на контроллеры, перейдите на страницу настройки уровней доступа контроллера по адресу [http://\[ip-адрес контроллера «Борей»\]/neyross/accesslevels/](http://[ip-адрес контроллера «Борей»]/neyross/accesslevels/) (обратите внимание, что порт не указывается).

Настройка уровней доступа может производиться напрямую через веб-интерфейс контроллера по указанной выше ссылке. Новые данные будут синхронизированы с данными других контроллеров и ITRIUM®.

### Уровни управления

Уровни управления в ITRIUM® настраиваются аналогично уровням доступа. Для настройки уровня управления выполните следующую последовательность шагов:

1. В программе «Администратор системы» в дереве элементов выделите элемент **Папка уровней управления НЕЙРОСС** (последовательно разверните список дочерних элементов элемента **Сеть IP-устройств** и **Охрана и управление НЕЙРОСС**).
2. В окне частных свойств выделенного элемента нажмите на кнопку **Настроить уровни управления...** Будет запущен браузер, заданный по умолчанию, и выполнен переход к HTML-странице настройки уровней управления по адресу [http://\[ip-адрес компьютера\]:\[порт\]/neyross/alarmlevels/](http://[ip-адрес компьютера]:[порт]/neyross/alarmlevels/), например <http://10.200.1.243:6501/neyross/alarmlevels/> (номер порта задаётся в поле **Порт ТСР** окна частных свойств «Службы НЕЙРОСС», IP-адрес компьютера указан в окне частных свойств элемента **Компьютер**). Процедура настройки уровней доступа описана в подразделе [Настройка уровней доступа](#).

**Примечание.** При переходе к конфигурированию уровней управления по нажатию кнопки из программы «Администратор системы», уровни управления настраиваются на компьютере, откуда произошёл переход. Загрузка сконфигурированных уровней управления в контроллеры осуществляется «Службой НЕЙРОСС». Чтобы проверить, корректно ли произошла загрузка данных на контроллеры, перейдите на страницу настройки уровней управления контроллера по адресу [http://\[ip-адрес контроллера\]/neyross/alarmlevels/](http://[ip-адрес контроллера]/neyross/alarmlevels/) (обратите внимание, что порт не указывается).


Настройка уровней управления может производиться напрямую через веб-интерфейс контроллера по указанной выше ссылке. Новые данные будут синхронизированы с данными других контроллеров и ITRIUM®.

## Настройка режимов доступа

Режимы доступа настраиваются в программе «Администратор системы». Режим доступа назначается пропуску. Каждому пропуску может быть назначен свой режим доступа. Режим доступа содержит ссылки на уровни доступа. Так как в системе охранной сигнализации и управления доступом НЕЙРОСС пропуск содержит информацию об уровне доступа и уровне управления владельца, то режим доступа в ITRIUM® содержит ссылки на соответствующие элементы **Уровень доступа НЕЙРОСС** и **УРОВЕНЬ управления НЕЙРОСС**.

**Внимание.** Подробное руководство по настройке доступа в ITRIUM® приведено в документе «Конфигурирование доступа», которое можно открыть из окна автозапуска установочного диска, либо скачать по адресу <http://www.itrium.ru/support/documentation/itrium.php>. Ниже представлена краткая инструкция по созданию режима доступа с помощью **Мастера доступа**.

Выполните следующую последовательность шагов:

1. Запустите программу «Администратор системы». В дереве конфигурации выберите элемент **Доступ**. Перейдите к окну частных свойств, для этого нажмите на кнопку  панели инструментов. Перейдите к вкладке **Мастер доступа**.
2. На вкладке **Мастер доступа** нажмите на кнопку **Добавить**.
3. В окне мастера доступа (рисунок 9.114) нажмите на кнопку **Да**.

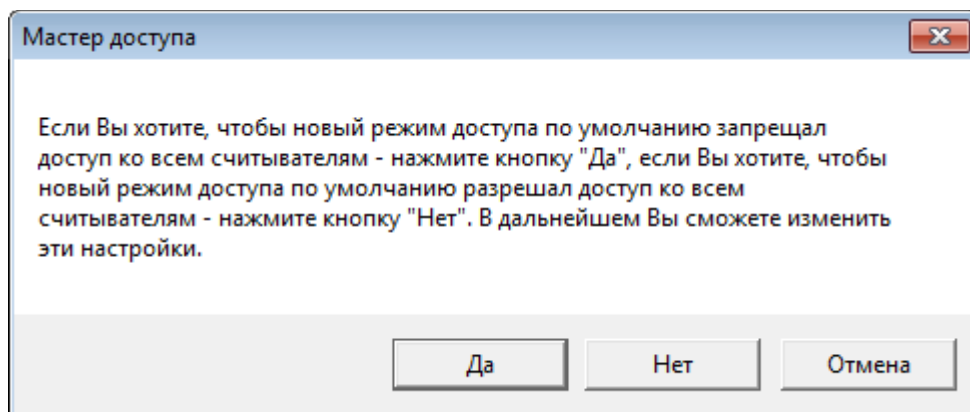


Рисунок 9.114 — Окно **Мастера доступа**

4. Если имеется несколько папок для хранения режимов доступа, **Мастер доступа** предложит выбрать папку, в которую необходимо добавить режим доступа (рисунок 9.115). Если режимы доступа должны быть разделены для каждой категории пропусков, следует предварительно добавить к папке **Доступ** необходимые категории. Затем к соответствующим категориям добавить элементы **Режимы доступа**. Выберите папку для хранения режима доступа и нажмите на кнопку **ОК**. В отобразившемся окне свойств в поле **Имя** введите название **Режима доступа** и нажмите на кнопку **Принять**.

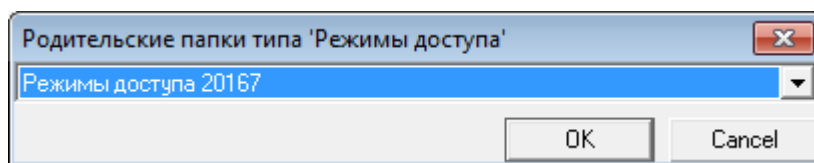


Рисунок 9.115 — Выбор папки для хранения режима доступа

**Примечание.** Если при интеграции в ITRIUM®, в системе НЕЙРОСС уже были созданы пропуска, то при вычитывании конфигурации в папке **Доступ** будет создана папка **Пропуска НЕЙРОСС/Сеть IP-устройств**, а в ней созданы элементы, соответствующие пропускам, папка **Режимы доступа** и др. (рисунок 9.116). В этом случае имеет смысл создавать новые режимы доступа в данной папке.

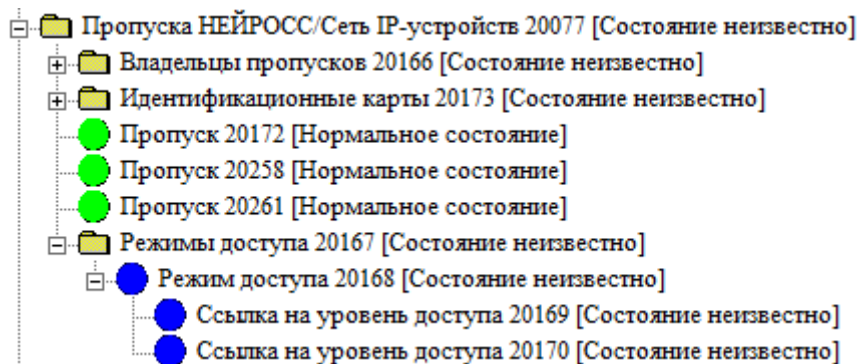



Рисунок 9.116 — Дерево элемента Пропуска НЕЙРОСС/Сеть IP-устройств

5. На вкладке **Мастер доступа** (рисунок 9.117) добавленного режима доступа, в строке **Контроль доступа НЕЙРОСС** в поле **Уровень доступа** выберите из раскрывающегося списка созданный ранее уровень доступа, в строке **Охранная сигнализация НЕЙРОСС** в поле **Уровень доступа** выберите из раскрывающегося списка созданный ранее уровень управления. Нажмите на кнопку  **Сохранить** панели инструментов.

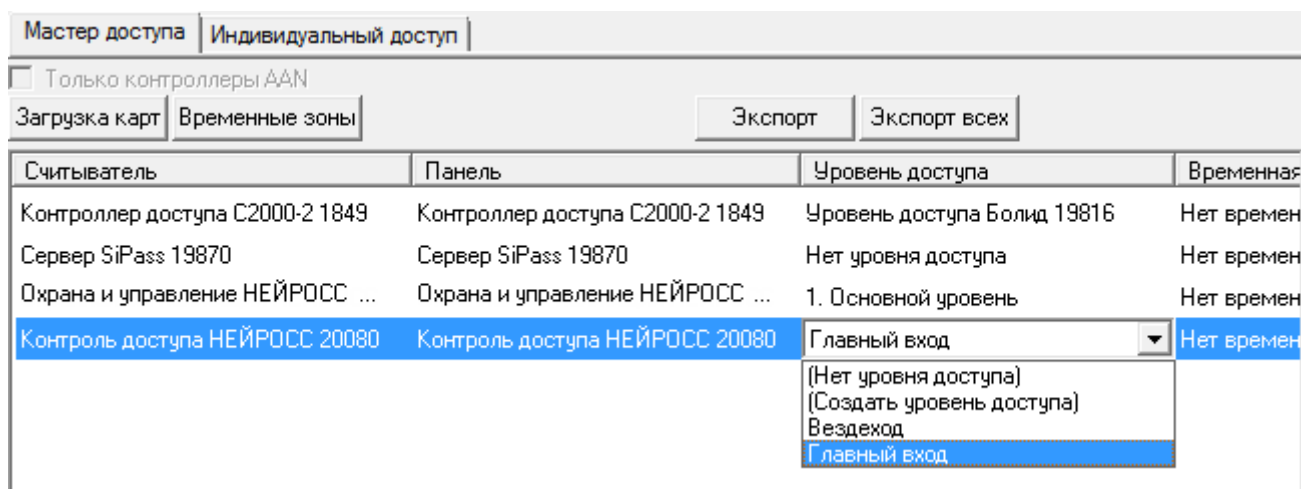


Рисунок 9.117 — Выбор уровня доступа для режима доступа

## Команды управления точками доступа

По командам оператора возможно переключение режимов работы точки доступа: «Дежурный», «Заблокировано», «Разблокировано». Дополнительную информацию см. в разделе [Команды управления](#).

### 4. Загрузка данных в НЕЙРОСС

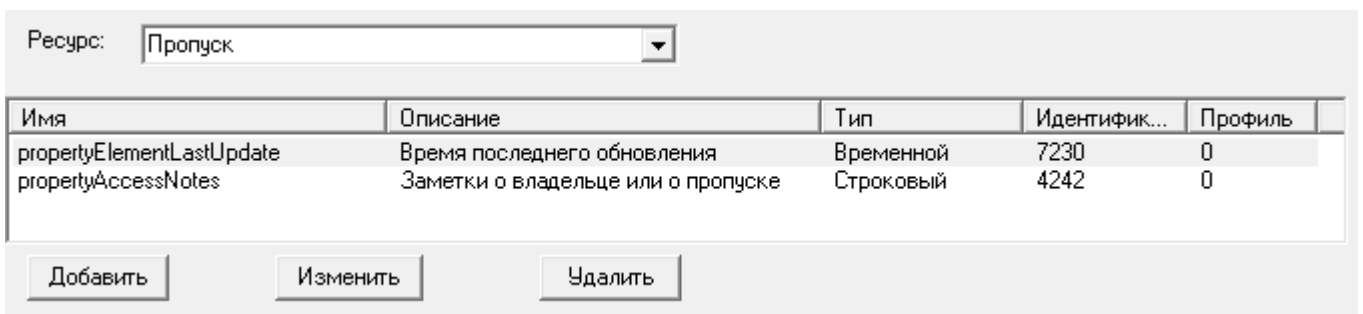
«Служба НЕЙРОСС» предназначена для осуществления взаимодействия (интеграции) системы безопасности, построенной на платформе ITRIUM® с системой контроля и управления доступом и охранно-пожарной сигнализации «НЕЙРОСС», построенной на контроллерах «Борей», «ЯРС», «Игнис», консолях «ВИК» и терминалах «МТК». Совместно со «Службой бюро пропусков», «Служба НЕЙРОСС» осуществляет загрузку данных пропусков в контроллеры «Борей», «ЯРС», терминалы «МТК» и другие узлы НЕЙРОСС, которые осуществляют пропускной режим, постановку/снятие с охраны и проч.

Если в системе безопасности ITRIUM® для ввода данных владельцев пропусков используется биометрический сканер геометрии руки Handkey-II производства компании Recognition Systems, для осуществления двухфакторной авторизации по карте и биометрии Handkey с помощью контроллера ОТС и СКУД «Борей»/«ЯРС», необходимо загрузить биометрические данные в контроллер. Аналогично, для использования данных веса, информация от весовой платформы также должна быть загружена в контроллер «Борей»/«ЯРС». Также для вывода дополнительных сведений о пропуске или его владельце в интерфейсе мобильного терминала «МТК», необходимо загрузить эти данные в «МТК».

Для этого «Служба НЕЙРОСС» должна быть сконфигурирована и запущена. При этом для загрузки в сеть НЕЙРОСС дополнительных данных (биометрических данных, данных веса, нестандартных данных пропуска/владельца пропуска), необходимо указать идентификаторы свойств и профиль, в котором содержатся требуемые данные.

Выполните следующую последовательность шагов:

1. В окне частных свойств элемента **Служба НЕЙРОСС** перейдите к вкладке **Доп. атрибуты ресурсов** (рисунок 9.118).



Имя	Описание	Тип	Идентифик...	Профиль
propertyElementLastUpdate	Время последнего обновления	Временной	7230	0
propertyAccessNotes	Заметки о владельце или о пропуске	Строковый	4242	0

Рисунок 9.118 — Окно частных свойств элемента **Служба НЕЙРОСС**, вкладка **Доп. атрибуты ресурсов**

2. В поле **Ресурс** выберите из раскрывающегося списка **Владелец пропуска**, если данные следует хранить в базе владельцев пропусков: биометрические данные,

данные весовой платформы, дополнительные данные владельца пропуска (должность и проч., текстовый комментарий). Выберите **Пропуск**, если данные следует хранить в базе пропусков: дата обновления пропуск и любая другая имеющаяся информация.

3. Нажмите на кнопку **Добавить**. В отобразившемся окне (рисунок 9.119) выберите из раскрывающегося списка требуемое свойство, в поле **Профиль** укажите номер профиля, в котором содержатся требуемые данные (обычно, «0»). Для быстрого поиска свойства, начните вводить первые буквы его названия. Если вы знаете идентификатор свойства, установите флаг в поле **Сортировать список по идентификатору свойства** и введите в поле требуемый идентификатор.

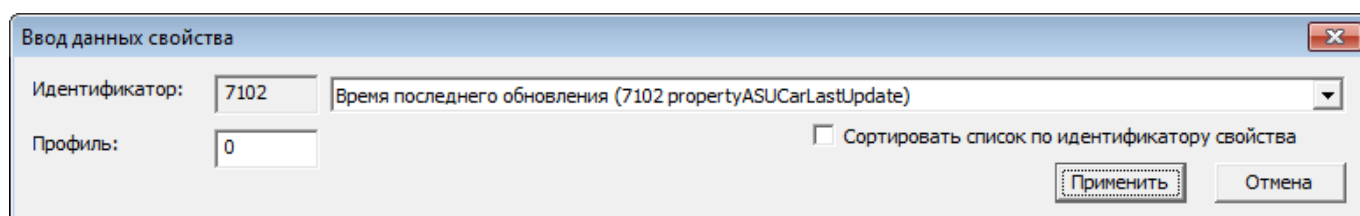



Рисунок 9.119 — Окно добавления свойства

4. Нажмите на кнопку **Применить**.
5. При необходимости добавления других свойств, повторите пп. 2-4 для каждого свойства.
6. Перезапустите «Службу НЕЙРОСС». Подождите несколько минут (обычно около десяти) для загрузки данных в НЕЙРОСС.

**Примечание.** Возможность добавления нестандартных свойств при помощи вкладки **Доп. атрибуты ресурсов** реализована в версии ITRIUM, начиная с 6.1.1362. В более ранних версиях имеется возможность вручную добавить и настроить свойство **7644**.

Выполните следующую последовательность шагов:

1. В программе «Администратор системы» выберите элемент **Компьютер**, на котором добавлена и сконфигурирована «Служба НЕЙРОСС». и перейдите к элементу **Служба НЕЙРОСС**.
2. С помощью кнопки **Показать свойства**  на панели управления перейдите к окну свойств.
3. На вкладке **Свойства** нажмите на правую кнопку мыши в пустой области и в отобразившемся контекстном меню выберите команду **Добавить...**
4. В отобразившемся окне (рисунок 9.120):

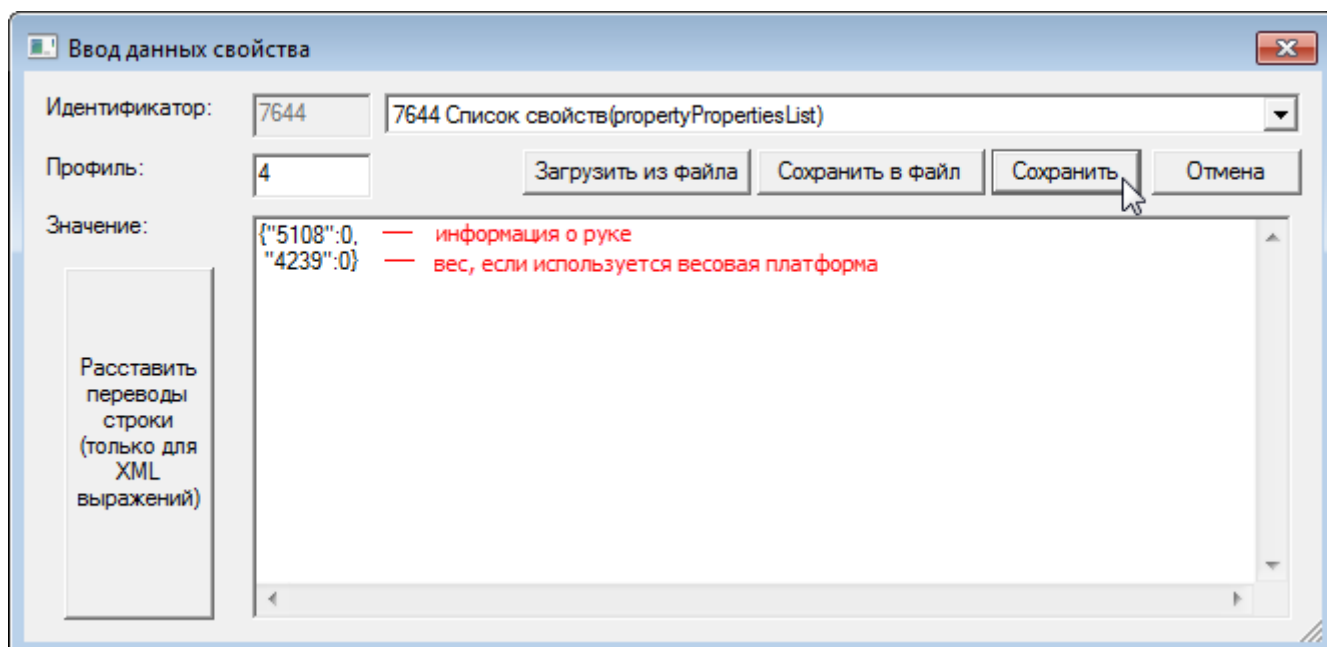


Рисунок 9.120 — Окно добавления свойства ITRIUM

- В поле **Идентификатор** выберите из раскрывающегося списка свойство **7644 «Список свойств (propertyPropertiesList)**;
- В поле **Профиль** укажите значение **4**, если данные следует хранить в базе владельцев пропусков: биометрические данные, данные весовой платформы, дополнительные данные владельца пропуска (должность и проч., текстовый комментарий). Укажите профиль **1**, если данные следует хранить в базе пропусков: срок действия пропуска, дата обновления данных пропуска и любая другая имеющаяся информация;
- В поле **Значение** введите JSON

```
{"5108":0,
"4239":0,}
```

Для других полей используйте соответствующие идентификаторы. К службе может быть добавлено несколько свойств 7644 с разными профилями.

- Нажмите на кнопку **Сохранить**.

5. Перезапустите «Службу НЕЙРОСС».

## ПРИЛОЖЕНИЕ 14. СОСТОЯНИЯ ЭЛЕМЕНТОВ ПРИБОРА

### 1. Состояния технологических входов

#### Неисправность питания

- Неисправность источника питания (вход **PF**),
- Неисправность аккумулятора (вход **AF**)

Таблица 24

Состояние	Описание
Норма	Состояние по умолчанию.
Тревога	Неисправность источника питания, неисправность аккумулятора.

#### Тампер вскрытия корпуса устройства — Tamper

Таблица 25

Состояние	Описание	Дополнительно
Норма	Состояние по умолчанию.	
Вскрытие	Сработал тампер вскрытия корпуса.	Открыт корпус устройства

### 2. Состояния охранных зон

Таблица 9.26

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].



Состояние	Описание
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, 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 (см. раздел [Шлейфы сигнализации](#)).

### 3. Состояния разделов охранной сигнализации

Таблица 9.27

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

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

Таблица 9.28

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.
<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>Обрыв шлейфа,</li> <li>Короткое замыкание;</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>Неисправность;</li> <li>Потеря связи;</li> </ul> <p>Для зон прибора, связь с которым потеряна</p> <ul style="list-style-type: none"> <li>Неизвестно</li> </ul>	<ul style="list-style-type: none"> <li>Неисправность</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](#).

Описание настроек зоны дано в разделе [Зоны сигнализации](#).

## 5. Состояния точек доступа

Таблица 9.29

Тип состояния	Состояние	Описание
Нормальное состояние	Ожидание идентификации	Состояние по умолчанию.
	Проход разрешён, ожидание прохода	Предъявлен валидный идентификатор и/или пин-код. В зависимости от факта прохода формируются сообщения «Проход совершён», «Проход не совершён». По окончании точка переходит в состояние по умолчанию.
	Заблокирована	Дверь заблокирована автоматически (при переходе связанной зоны в состояние [Тревога]) или по команде управления точкой доступа. Проход запрещён.
	Разблокирована	Дверь разблокирована автоматически или по команде управления точкой доступа. Проход разрешён.
Тревожное состояние	Взлом двери	Произведён взлом двери (проход запрещён, изменено состояние дверного контакта). При восстановлении состояния контакта формируется сообщение «Снята тревога взлома двери».
	Удержание двери	Предъявлен валидный идентификатор. После открытия двери, в течение интервала времени <b>Время ожидания закрытия двери</b> дверь не была закрыта. Формируется сообщение «Дверь удержана открытой». При закрытии двери состояние точки переходит в состояние по умолчанию, формируется событие «Незакрытая дверь закрыта».
	Заблокирована. Взлом двери	Дверь заблокирована автоматически. Проход запрещён. Взлом двери.

## ПРИЛОЖЕНИЕ 15. АДМИНИСТРИРОВАНИЕ УЗЛА

### 1. Сброс настроек

Если получить доступ к веб-интерфейсу не удаётся (например, забыли IP-адрес или учётные данные), может потребоваться сброс настроек. Сброс настроек прибора осуществляется с помощью кнопки **MODE**, расположенной на плате контроллера «ЯРС» (см. рисунок [1.5](#)).

При необходимости сброса только сетевых настроек прибора без полной очистки конфигурации, нажмите и удерживайте кнопку **MODE** в течение 3–10 секунд.

Для сброса всех настроек прибора, необходимо нажать и удерживать кнопку **MODE** более 10 секунд. Будет инициирована перезагрузка прибора с заводскими установками.

**Внимание.** По выполнении команды сброса настроек, доступ к прибору будет возможен только по IP-адресу, указанному на корпусе прибора, и из подсети **255.0.0.0**. Будет запущен мастер первого запуска (см. раздел [Мастер первого запуска](#)).

### 2. Перезапуск узла

#### 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 программных средств

При наличии доступа к веб-интерфейсу возможна дистанционная перезагрузка программных средств узла:

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

### 3. Обновление программных средств (прошивки) прибора

#### Обновление узла

Средства пользовательского интерфейса 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 **Сеть** (см. раздел [Обновление ПО узлов НЕЙРОСС](#)).

### Обновление LON-модулей

Прибор «ЯРС» обеспечивает возможность произвести обновление программных средств («прошивок») модулей М2 и МДС без использования специальных средств обслуживания сети Lonworks. Причём имеется возможность проведения обновления/восстановления конфигурации модулей, чья неработоспособность привела к невозможности добавления такого модуля в систему.

Для выполнения обновления:

1. Перейдите к веб-интерфейсу. Выберите раздел [Конфигурация узлов](#) — [Модули расширения](#). Нажмите на кнопку **Обновить модуль**, расположенную в верхней части раздела (рисунок [9.50](#)).
2. В отобразившемся окне (рисунок 9.121):
  - Выберите из раскрывающегося списка модуль, прошивку которого требуется обновить или нажмите на кнопку **Service Pin** на плате модуля (рисунок [1.10](#) для модуля М2, рисунок [1.12](#) для модуля МДС);

**Примечание.** Если модуль выбран из списка, его NeuronID-идентификатор будет вычитан из памяти прибора и вписан в поле ниже.

- Нажмите **Выберите файл** и укажите путь к файлу прошивки в формате **HEX**.
- Нажмите на кнопку **Обновить**.

Рисунок 9.121 — Окно обновления прошивки LON-модуля

3. Будет выполнена процедура обновления. В процессе обновления сеть Lonworks будет переключена в сервисный режим и связь со всеми LON-модулями временно будет потеряна. По завершении нажмите на кнопку **Заккрыть** (рисунок 9.46).

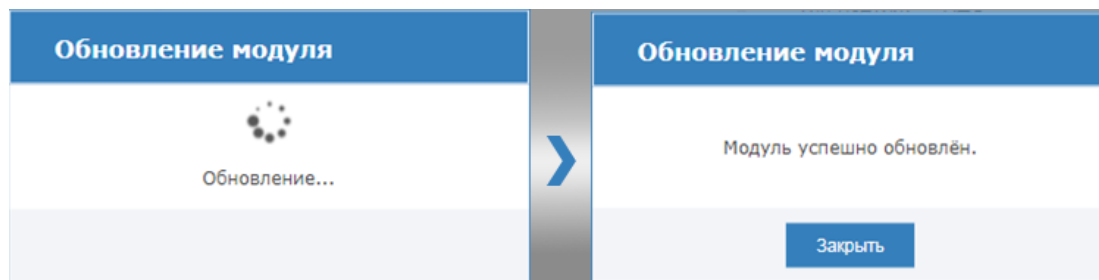


Рисунок 9.122 — Обновление программных средств LON-модулей

#### 4. 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](#)).