



**BOSCH**

# **BVMS**

**ru**

Руководство по конфигурации



# Содержание

<b>1</b>	<b>Использование справки</b>	<b>14</b>
1.1	Поиск информации	14
1.2	Печать Справки	15
<b>2</b>	<b>Введение</b>	<b>16</b>
<b>3</b>	<b>Обзор системы</b>	<b>18</b>
3.1	Требования к аппаратному оборудованию	19
3.2	Требования к программному обеспечению	19
3.3	Лицензионные требования	19
<b>4</b>	<b>Понятия</b>	<b>20</b>
4.1	Основы проектирования BVMS	20
4.1.1	Система с одним сервером управления	20
4.1.2	Enterprise System	21
4.1.3	Server Lookup	22
4.1.4	Неуправляемый объект	23
4.2	Запись	25
4.2.1	Автоматическая компенсация сети (ANR)	25
4.2.2	Двойная / резервная запись	26
4.2.3	Режимы записи VRM	28
4.2.4	Воспроизведение источников записи VRM	30
4.3	Обработка сигналов тревоги	35
4.4	Сопоставление событий ONVIF	37
4.5	Отключение при бездействии	38
4.6	Клиент Operator Client, независимый от версии	39
4.6.1	Работа в режиме совместимости	39
4.7	Режимы просмотра панорамной камеры	40
4.7.1	Панорамная камера 360°, монтируемая на полу или потолке	40
4.7.2	Панорамная камера 180°, монтируемая на полу или потолке	42
4.7.3	Панорамная камера 360°, монтируемая на стене	44
4.7.4	Панорамная камера 180°, монтируемая на стене	45
4.7.5	Кадрированное представление изображения с панорамной камеры	46
4.8	Туннелирование SSH	47
4.9	Многопутевой ввод-вывод	47
<b>5</b>	<b>Поддерживаемое оборудование</b>	<b>49</b>
5.1	Установка аппаратного оборудования	50
5.2	Установка клавиатуры KBD Universal XF	50
5.3	Подключение клавиатуры Bosch IntuiKey к BVMS	51
5.3.1	Сценарии подключения клавиатур Bosch IntuiKey	51
5.3.2	Подключение клавиатуры Bosch IntuiKey к декодеру	53
5.3.3	Обновление программного обеспечения клавиатуры Bosch IntuiKey	54
5.4	Подключение матричного коммутатора Bosch Allegiant к BVMS	55
5.4.1	Общие сведения о подключении Bosch Allegiant	55
5.4.2	Настройка контрольного канала	57
5.4.3	Понятие о сателлитной конфигурации Allegiant компании Bosch	59
5.5	Команды Allegiant CCL, поддерживаемые в системе BVMS	60
<b>6</b>	<b>Начало работы</b>	<b>63</b>
6.1	Установка программных модулей	63
6.2	Использование мастера настройки конфигурации	63
6.3	Запуск Configuration Client	72

6.4	Настройка языка Configuration Client	73
6.5	Настройка языка Operator Client	73
6.6	Поиск устройств	73
6.7	Доступ к системе	74
6.8	Использование просмотра сервера	74
6.9	Настройка удаленного доступа	75
6.9.1	Удаленный доступ	75
6.9.2	Настройка без корпоративной системы	78
6.9.3	Настройка с помощью корпоративной системы	78
6.10	Активация лицензии на программное обеспечение	78
6.10.1	Скачать информационный файл Bundle Information	79
6.10.2	Получение цифровой подписи компьютера	79
6.10.3	Получение ключа активации	80
6.10.4	Активация системы	80
6.11	Обслуживание BVMS	80
6.12	Замена устройства	82
6.12.1	Замена MS / EMS	82
6.12.2	Замена VRM	83
6.12.3	Замена кодера или декодера	84
6.12.4	Замена клиента оператора	87
6.12.5	Заключительные проверки	87
6.12.6	Восстановление Divar IP 3000/7000	87
6.13	Настройка синхронизации времени	87
6.14	Настройка носителей данных кодера	88
7	<b>Создание системы Enterprise</b>	<b>89</b>
7.1	Настройка списка серверов для корпоративной системы	89
7.2	Создание Enterprise User Group	90
7.3	Создание Enterprise Account	91
8	<b>Настройка командных сценариев</b>	<b>93</b>
8.1	Управление командными сценариями	93
8.2	Настройка автоматического запуска командного сценария	94
8.3	Импорт командного сценария	94
8.4	Экспорт командного сценария	95
8.5	Настройка командного сценария, выполняющегося при запуске (страница «Настройки»)	95
9	<b>Управление параметрами конфигурации</b>	<b>96</b>
9.1	Активация текущей конфигурации	96
9.2	Активация конфигурации	97
9.3	Экспорт параметров конфигурации	98
9.4	Импорт параметров конфигурации	98
9.5	Экспорт конфигурационных данных в OPC	99
9.6	Проверка состояния кодеров/декодеров	99
9.7	Настройка мониторинга SNMP	99
9.8	Создание отчета	100
10	<b>примеры конфигурации</b>	<b>101</b>
10.1	Добавление моста Bosch ATM/POS	101
10.2	Добавление входа сигнализации Bosch Allegiant	102
10.3	Добавление и настройка 2 камер Dinion IP для записи VRM	102
11	<b>Главные окна Configuration Client</b>	<b>104</b>

<b>11.1</b>	Окно Конфигурация	<b>104</b>
<b>11.2</b>	Команды меню	<b>105</b>
<b>11.3</b>	Диалоговое окно «Диспетчер активации» (меню «Система»)	<b>107</b>
<b>11.4</b>	Диалоговое окно «Активировать конфигурацию» (меню «Система»)	<b>108</b>
<b>11.5</b>	Диалоговое окно «Первоначальный поиск устройств» (меню «Оборудование»)	<b>109</b>
<b>11.6</b>	Диалоговое окно «Защита устройств с помощью всеобщего пароля по умолчанию» (меню «Оборудование»)	<b>109</b>
<b>11.7</b>	Диалоговое окно «Изменить пароли устройств» (меню «Оборудование»)	<b>110</b>
<b>11.8</b>	Диалоговое окно «Обновить микропрограммное обеспечение устройства» (меню «Оборудование»)	<b>111</b>
<b>11.9</b>	Диалоговое окно «Изменить IP-адрес и сетевые параметры устройства» (меню «Оборудование»)	<b>112</b>
<b>11.10</b>	Диалоговое окно «Монитор устройств» (меню «Оборудование»)	<b>114</b>
<b>11.11</b>	Диалоговое окно «Исследователь лицензий» (меню «Инструменты»)	<b>114</b>
<b>11.12</b>	Диалоговое окно «Диспетчер лицензий» (меню «Инструменты»)	<b>114</b>
<b>11.13</b>	Диалоговые окна «Отчеты» (меню «Отчеты»)	<b>115</b>
<b>11.13.1</b>	Диалоговое окно "Расписания записей"	<b>115</b>
<b>11.13.2</b>	Диалоговое окно Настройки записи по расписанию	<b>115</b>
<b>11.13.3</b>	Диалоговое окно "Расписания задач"	<b>115</b>
<b>11.13.4</b>	Диалоговое окно "Камеры и параметры записи"	<b>115</b>
<b>11.13.5</b>	Диалоговое окно "Параметры качества потока"	<b>116</b>
<b>11.13.6</b>	Диалоговое окно "Настройки событий"	<b>116</b>
<b>11.13.7</b>	Диалоговое окно "Настройки составных событий"	<b>116</b>
<b>11.13.8</b>	Диалоговое окно "Настройки тревог"	<b>116</b>
<b>11.13.9</b>	Диалоговое окно "Настроенные пользователи"	<b>116</b>
<b>11.13.10</b>	Диалоговое окно "Группы пользователей и учетные записи"	<b>116</b>
<b>11.13.11</b>	Диалоговое окно "Разрешения для устройств"	<b>116</b>
<b>11.13.12</b>	Диалоговое окно "Рабочие разрешения"	<b>116</b>
<b>11.13.13</b>	Диалоговое окно «Разрешения конфигурации»	<b>117</b>
<b>11.13.14</b>	Диалоговое окно «Разрешения групп пользователей»	<b>117</b>
<b>11.13.15</b>	Диалоговое окно «Параметры безопасности»	<b>117</b>
<b>11.13.16</b>	Диалоговое окно «Обход устройств»	<b>117</b>
<b>11.14</b>	Диалоговое окно «Настройки тревог» (меню «Настройки»)	<b>117</b>
<b>11.15</b>	Диалоговое окно «Настройки SNMP» (меню «Настройки»)	<b>117</b>
<b>11.16</b>	Диалоговое окно «Параметры» (меню «Настройки»)	<b>118</b>
<b>11.17</b>	Диалоговое окно «Параметры удаленного доступа» (меню «Настройки»)	<b>120</b>
<b>11.17.1</b>	Диалоговое окно "Таблица распределения портов"	<b>121</b>
<b>12</b>	<b>Страница Устройства</b>	<b>122</b>
<b>12.1</b>	Обновление состояний и возможностей устройств	<b>122</b>
<b>12.2</b>	Изменение пароля для IP-устройств	<b>123</b>
<b>12.3</b>	Добавление устройства	<b>124</b>
<b>12.4</b>	Страница «Список серверов/Адресная книга»	<b>127</b>
<b>12.4.1</b>	Диалоговое окно Добавить сервер	<b>128</b>
<b>12.4.2</b>	Настройка Server Lookup	<b>128</b>
<b>12.4.3</b>	Настройка списка серверов	<b>128</b>
<b>12.4.4</b>	Экспорт списка серверов	<b>129</b>
<b>12.4.5</b>	Импорт списка серверов	<b>129</b>
<b>12.5</b>	Страница про сетевые видеорегистраторы NVR, резервные сетевые видеорегистраторы NVR и избыточные сетевые видеорегистраторы NVR	<b>130</b>

<b>12.6</b>	Страница DiBos	<b>130</b>
<b>12.6.1</b>	Добавление системы DiBos путем поиска	<b>130</b>
<b>12.6.2</b>	Страница Настройки	<b>131</b>
<b>12.6.3</b>	Страница Камеры	<b>131</b>
<b>12.6.4</b>	Страница Входы	<b>131</b>
<b>12.6.5</b>	Страница Реле	<b>131</b>
<b>12.6.6</b>	Настройка интеграции системы DiBos	<b>131</b>
<b>12.7</b>	Страница DVR (цифровой видеореги­стратор)	<b>132</b>
<b>12.7.1</b>	Цифровые видеореги­страторы	<b>132</b>
<b>12.7.2</b>	Добавление устройств DVR путем поиска	<b>133</b>
<b>12.7.3</b>	Диалоговое окно "Добавить цифровой видеореги­стратор"	<b>134</b>
<b>12.7.4</b>	Вкладка "Настройки"	<b>134</b>
<b>12.7.5</b>	Вкладка "Камера"	<b>134</b>
<b>12.7.6</b>	Вкладка "Входы"	<b>135</b>
<b>12.7.7</b>	Вкладка "Реле"	<b>135</b>
<b>12.7.8</b>	Настройка интеграции цифрового видеореги­стратора	<b>135</b>
<b>12.8</b>	Страница Матричные коммутаторы	<b>135</b>
<b>12.8.1</b>	Добавление устройства Bosch Allegiant	<b>136</b>
<b>12.8.2</b>	Настройка устройства Bosch Allegiant	<b>136</b>
<b>12.8.3</b>	Страница Выходы	<b>137</b>
<b>12.8.4</b>	Страница Входы	<b>137</b>
<b>12.8.5</b>	Страница Соединение	<b>138</b>
<b>12.8.6</b>	Страница Камеры	<b>138</b>
<b>12.9</b>	Страница Рабочая станция	<b>138</b>
<b>12.9.1</b>	Добавление рабочей станции вручную	<b>139</b>
<b>12.9.2</b>	Настройка клавиатуры Bosch IntuiKey (страница «Настройки») (рабочая станция)	<b>139</b>
<b>12.9.3</b>	Активация поиска на рабочей станции (страница «Настройки»)	<b>140</b>
<b>12.9.4</b>	Настройка командного сценария, выполняющегося при запуске (страница «Настройки»)	<b>140</b>
<b>12.9.5</b>	Страница Настройки	<b>140</b>
<b>12.9.6</b>	Изменение сетевого адреса рабочей станции	<b>142</b>
<b>12.10</b>	Страница Декодеры	<b>142</b>
<b>12.10.1</b>	Добавление кодера и декодера вручную	<b>143</b>
<b>12.10.2</b>	Диалоговое окно «Изменить кодер / Изменить декодер»	<b>144</b>
<b>12.10.3</b>	Изменение пароля кодера и декодера («Изменить пароль»/«Введите пароль»)	<b>145</b>
<b>12.10.4</b>	Профиль декодера	<b>147</b>
<b>12.10.5</b>	Данные на мониторе	<b>147</b>
<b>12.10.6</b>	Настройка клавиатуры Bosch IntuiKey (декодер)	<b>147</b>
<b>12.10.7</b>	Настройка декодера для использования с клавиатурой Bosch IntuiKey	<b>148</b>
<b>12.10.8</b>	Удалить логотип декодера	<b>148</b>
<b>12.11</b>	Страница «Группы мониторов»	<b>148</b>
<b>12.11.1</b>	Добавление группы мониторов вручную	<b>149</b>
<b>12.11.2</b>	Настройка группы мониторов	<b>149</b>
<b>12.12</b>	Страница Настенная панель мониторов	<b>150</b>
<b>12.12.1</b>	Добавление видеостены вручную	<b>151</b>
<b>12.13</b>	Страница Устройства связи	<b>152</b>
<b>12.13.1</b>	Добавление сервера электронной почты/SMTP	<b>152</b>
<b>12.13.2</b>	Добавление устройства SMS	<b>152</b>
<b>12.13.3</b>	Страница Сервер SMTP	<b>153</b>

<b>12.13.4</b>	Настройка устройства связи	<b>154</b>
<b>12.13.5</b>	Диалоговое окно Отправить тестовое электронное сообщение	<b>154</b>
<b>12.13.6</b>	Страница Настройки GSM / Настройки SMSC	<b>154</b>
<b>12.14</b>	Страница ATM/POS	<b>155</b>
<b>12.14.1</b>	Добавление моста Bosch ATM/POS вручную	<b>156</b>
<b>12.14.2</b>	Страница Мост ATM/POS Bosch	<b>156</b>
<b>12.14.3</b>	Настройка периферийных устройств	<b>157</b>
<b>12.14.4</b>	Страница "Настройки DTP"	<b>157</b>
<b>12.14.5</b>	Страница Настройки банкомата	<b>157</b>
<b>12.14.6</b>	Страница Входы	<b>158</b>
<b>12.15</b>	Устройства чтения кредитных карточек	<b>158</b>
<b>12.15.1</b>	Диалоговое окно "Добавление устройства чтения кредитных карточек"	<b>159</b>
<b>12.15.2</b>	Страница "Параметры устройства чтения кредитных карточек"	<b>159</b>
<b>12.16</b>	Страница Виртуальные входы	<b>159</b>
<b>12.16.1</b>	Добавление виртуальных входов вручную	<b>160</b>
<b>12.17</b>	Страница SNMP	<b>160</b>
<b>12.17.1</b>	Добавление SNMP вручную	<b>161</b>
<b>12.17.2</b>	Настройка приемника запросов SNMP (страница приемника запросов SNMP)	<b>161</b>
<b>12.17.3</b>	Диалоговое окно Журнал регистрации запросов SNMP	<b>162</b>
<b>12.18</b>	Страница "Назначить клавиатуру"	<b>163</b>
<b>12.19</b>	Страница Модули ввода/вывода	<b>164</b>
<b>12.19.1</b>	Добавление модуля ввода/вывода вручную	<b>164</b>
<b>12.19.2</b>	Настройка модуля ввода/вывода	<b>164</b>
<b>12.19.3</b>	Страница ADAM	<b>165</b>
<b>12.19.4</b>	Страница Входы	<b>165</b>
<b>12.19.5</b>	Страница Реле	<b>166</b>
<b>12.20</b>	Страница Эмуляция Allegiant CCL	<b>166</b>
<b>12.20.1</b>	Добавление эмуляции Allegiant CCL вручную	<b>166</b>
<b>12.20.2</b>	Команды Allegiant CCL	<b>167</b>
<b>12.20.3</b>	Настройка эмуляции Allegiant CCL	<b>167</b>
<b>12.21</b>	Страница Мобильный видеосервис	<b>167</b>
<b>12.21.1</b>	Mobile Video Service	<b>168</b>
<b>12.21.2</b>	Добавление Mobile Video Service вручную	<b>168</b>
<b>12.22</b>	Страница "Охранные панели"	<b>169</b>
<b>12.22.1</b>	Добавление тревожной панели вручную	<b>169</b>
<b>12.22.2</b>	Страница "Настройки"	<b>170</b>
<b>12.23</b>	Страница «Системы контроля и управления доступом»	<b>170</b>
<b>12.23.1</b>	Добавление системы контроля и управления доступом	<b>170</b>
<b>12.23.2</b>	Изменение системы контроля и управления доступом	<b>171</b>
<b>12.23.3</b>	Страница «Настройки»	<b>171</b>
<b>12.24</b>	Страница Video Analytics	<b>171</b>
<b>12.24.1</b>	Страница параметров видеоаналитики	<b>171</b>
<b>12.24.2</b>	Добавление устройства Video Analytics	<b>172</b>
<b>12.24.3</b>	Страница устройств Person Identification	<b>172</b>
<b>12.24.4</b>	Добавление Person Identification Device (PID)	<b>173</b>
<b>12.24.5</b>	Страница PID	<b>174</b>
<b>12.24.6</b>	Восстановление доступа к PID после сбоя центрального сервера BVMS	<b>174</b>
<b>12.24.7</b>	Добавление камер к Person Identification Device (PID)	<b>175</b>
<b>12.24.8</b>	Настройка параметров камеры для тревог Person Identification	<b>175</b>

<b>12.24.9</b>	Настройка групп людей	<b>176</b>
<b>12.24.10</b>	Добавление устройства LPR	<b>177</b>
<b>12.25</b>	Страница Устройства VRM	<b>178</b>
<b>12.25.1</b>	Добавление устройств VRM путем поиска	<b>178</b>
<b>12.25.2</b>	Добавление основного или вторичного VRM вручную	<b>180</b>
<b>12.25.3</b>	Редактирование устройства VRM	<b>181</b>
<b>12.25.4</b>	Страница Настройки VRM	<b>182</b>
<b>12.25.5</b>	Страница SNMP	<b>182</b>
<b>12.25.6</b>	Страница "Учетные записи"	<b>182</b>
<b>12.25.7</b>	Страница Дополнительно	<b>183</b>
<b>12.25.8</b>	Шифрование записи для VRM	<b>183</b>
<b>12.25.9</b>	Изменение пароля устройства VRM	<b>184</b>
<b>12.25.10</b>	Добавления пула VRM	<b>185</b>
<b>12.25.11</b>	Добавление резервного диспетчера VRM вручную	<b>185</b>
<b>12.25.12</b>	Добавление зеркального диспетчера VRM вручную	<b>186</b>
<b>12.25.13</b>	Добавление кодеров путем поиска	<b>187</b>
<b>12.25.14</b>	Добавление устройств VSG путем поиска	<b>188</b>
<b>12.25.15</b>	Синхронизация конфигурации BVMS	<b>188</b>
<b>12.26</b>	Страница "Пул"	<b>188</b>
<b>12.26.1</b>	Настройка автоматического режима записи в пуле	<b>190</b>
<b>12.26.2</b>	Добавление кодера и декодера вручную	<b>190</b>
<b>12.26.3</b>	Добавление устройства iSCSI вручную	<b>191</b>
<b>12.26.4</b>	Добавление Video Streaming Gateway вручную	<b>192</b>
<b>12.26.5</b>	Добавление устройства iSCSI DSA E-Series вручную	<b>193</b>
<b>12.26.6</b>	Добавление кодеров путем поиска	<b>196</b>
<b>12.26.7</b>	Добавление устройств VSG путем поиска	<b>196</b>
<b>12.26.8</b>	Настройка двойного режима записи в Дереве устройств	<b>197</b>
<b>12.27</b>	Страница «Кодер/декодер Bosch»	<b>197</b>
<b>12.28</b>	Страница устройства iSCSI	<b>198</b>
<b>12.28.1</b>	Пул хранения iSCSI	<b>198</b>
<b>12.28.2</b>	Добавление устройства iSCSI вручную	<b>199</b>
<b>12.28.3</b>	Добавление устройства iSCSI DSA E-Series вручную	<b>200</b>
<b>12.28.4</b>	Настройка устройства iSCSI	<b>202</b>
<b>12.28.5</b>	Страница "Базовая конфигурация"	<b>204</b>
<b>12.28.6</b>	Диалоговое окно "Распределение нагрузки"	<b>205</b>
<b>12.28.7</b>	Перемещение системы iSCSI в другой пул («Изменение пула...»)	<b>205</b>
<b>12.28.8</b>	Страница устройств LUN	<b>206</b>
<b>12.28.9</b>	Добавление устройства LUN	<b>206</b>
<b>12.28.10</b>	Форматирование LUN	<b>208</b>
<b>12.28.11</b>	Диалоговое окно iqn-Mapper	<b>208</b>
<b>12.29</b>	Страница устройства Video Streaming Gateway	<b>208</b>
<b>12.29.1</b>	Добавление Video Streaming Gateway вручную	<b>209</b>
<b>12.29.2</b>	Изменение шлюза Video Streaming Gateway	<b>211</b>
<b>12.29.3</b>	Добавление камеры в VSG	<b>211</b>
<b>12.29.4</b>	Диалоговое окно "Добавить кодер Bosch"	<b>212</b>
<b>12.29.5</b>	Диалоговое окно "Добавить кодер ONVIF"	<b>213</b>
<b>12.29.6</b>	Диалоговое окно "Добавить камеру JPEG"	<b>215</b>
<b>12.29.7</b>	Диалоговое окно "Добавить кодер RTSP"	<b>216</b>
<b>12.29.8</b>	Перемещение VSG в другой пул («Изменение пула»)	<b>217</b>



<b>12.29.9</b>	Настройка многоадресной передачи (вкладка «Многоадресная передача»)	<b>217</b>
<b>12.29.10</b>	Настройка ведения журналов (вкладка «Дополнительно»)	<b>218</b>
<b>12.29.11</b>	Запуск ONVIF Camera Event Driver Tool из Configuration Client	<b>219</b>
<b>12.30</b>	Страница Режим реального времени и локальное хранилище	<b>219</b>
<b>12.30.1</b>	Добавление устройств, работающих только в режиме реального времени, путем поиска	<b>219</b>
<b>12.30.2</b>	Добавление кодера и декодера вручную	<b>220</b>
<b>12.30.3</b>	Предоставление пароля пункта назначения декодеру («Проверка подлинности...»)	<b>222</b>
<b>12.31</b>	Страница Локальное хранилище	<b>222</b>
<b>12.32</b>	Страница Unmanaged Site	<b>223</b>
<b>12.32.1</b>	Добавление объекта unmanaged site вручную	<b>223</b>
<b>12.32.2</b>	Импорт неуправляемых объектов	<b>224</b>
<b>12.32.3</b>	Страница «Unmanaged Site»	<b>224</b>
<b>12.32.4</b>	Добавление unmanaged сетевого устройства	<b>224</b>
<b>12.32.5</b>	Настройка часового пояса	<b>225</b>
<b>13</b>	<b>Страница «Кодер/декодер/камера Bosch»</b>	<b>226</b>
<b>13.1</b>	Добавление кодера в пул VRM	<b>228</b>
<b>13.2</b>	Добавление кодера, работающего только в режиме реального времени	<b>228</b>
<b>13.3</b>	Добавление кодера локального хранилища	<b>228</b>
<b>13.4</b>	Редактирование кодера	<b>229</b>
<b>13.4.1</b>	Шифрование видео в режиме реального времени («Изменение кодера»)	<b>229</b>
<b>13.4.2</b>	Обновление возможностей устройства («Изменение кодера»)	<b>230</b>
<b>13.4.3</b>	Диалоговое окно «Изменить кодер / Изменить декодер»	<b>230</b>
<b>13.5</b>	Управление проверкой подлинности	<b>232</b>
<b>13.5.1</b>	Проверка подлинности	<b>232</b>
<b>13.5.2</b>	Настройка проверки подлинности	<b>233</b>
<b>13.5.3</b>	Отправка сертификата	<b>234</b>
<b>13.5.4</b>	Загрузка сертификата	<b>234</b>
<b>13.5.5</b>	Установка сертификатов на рабочей станции	<b>235</b>
<b>13.6</b>	Предоставление пароля пункта назначения декодеру («Проверка подлинности...»)	<b>235</b>
<b>13.7</b>	Изменение пароля кодера и декодера («Изменить пароль»/«Введите пароль»)	<b>236</b>
<b>13.8</b>	Перемещение кодера в другой пул («Изменение пула»)	<b>237</b>
<b>13.9</b>	Восстановление записей с замененного кодера (диалоговое окно «Связать с записями предшествующего устройства»)	<b>237</b>
<b>13.10</b>	Настройка кодеров/декодеров	<b>238</b>
<b>13.10.1</b>	Настройка носителей данных кодера	<b>238</b>
<b>13.10.2</b>	Настройка нескольких кодеров / декодеров	<b>239</b>
<b>13.10.3</b>	Настройка резервного режима записи на кодере	<b>241</b>
<b>13.10.4</b>	Страница "Управление записью"	<b>242</b>
<b>13.10.5</b>	Страница "Параметры записи"	<b>242</b>
<b>13.11</b>	Настройка многоадресной передачи	<b>242</b>
<b>14</b>	<b>Страница "ONVIF"</b>	<b>244</b>
<b>14.1</b>	Добавление устройства ONVIF, работающего только в режиме реального времени, путем сканирования	<b>244</b>
<b>14.2</b>	Страница "Кодер ONVIF"	<b>244</b>
<b>14.3</b>	Страница "События кодера ONVIF"	<b>245</b>
<b>14.3.1</b>	Добавление и удаление профиля ONVIF	<b>247</b>
<b>14.3.2</b>	Экспорт файла таблицы сопоставления ONVIF	<b>248</b>
<b>14.3.3</b>	Импорт файла таблицы сопоставления ONVIF	<b>248</b>

14.3.4	Настройка таблицы сопоставления ONVIF	249
14.4	Страница конфигурации ONVIF	251
14.4.1	Доступ к устройству	252
14.4.2	Дата / время	253
14.4.3	Управление пользователями	253
14.4.4	Страница "Профиль видеокодера"	254
14.4.5	Профиль аудиокодера	257
14.4.6	Обработка изображений, общие данные	257
14.4.7	Компенсация фоновой засветки	258
14.4.8	Экспозиция	258
14.4.9	Фокусировка	260
14.4.10	Широкий динамический диапазон	260
14.4.11	Баланс белого	261
14.4.12	Доступ к сети	262
14.4.13	Области	264
14.4.14	Реле	265
14.5	Страница "Источник событий ONVIF"	266
14.6	Назначение профиля ONVIF	267
15	<b>Вкладка Карты и структура</b>	<b>268</b>
16	<b>Настройка логического дерева</b>	<b>270</b>
16.1	Настройка логического дерева	270
16.2	Добавление устройства в логическое дерево	270
16.3	Удаление элемента дерева	270
16.4	Управление файлами ресурсов	271
16.4.1	Диалоговое окно Диспетчер ресурсов	272
16.4.2	Диалоговое окно Выбрать ресурс	273
16.5	Добавление документа	273
16.5.1	Диалоговое окно Добавить URL-адрес	274
16.6	Диалоговое окно Ссылка на внешнее приложение	274
16.7	Добавление командного сценария	275
16.8	Добавление последовательности камер	275
16.8.1	Диалоговое окно Конструктор последовательностей	276
16.9	Управление предварительно настроенными последовательностями камер	277
16.9.1	Диалоговое окно Добавить последовательность	278
16.9.2	Диалоговое окно Добавить шаг последовательности	278
16.10	Добавление папки	278
16.11	Добавление карты	279
16.12	Добавление ссылки на другую карту	279
16.12.1	Диалоговое окно Выбрать карту для ссылки	280
16.13	Назначение карты папке.	280
16.14	Управление устройствами на карте	280
16.15	Добавление реле сигнализации о неисправностях	281
16.15.1	Диалоговое окно "Реле сигнализации о неисправностях"	282
16.16	Настройка обхода устройств	283
17	<b>Страница Расписания</b>	<b>284</b>
17.1	Страница Расписания записей	284
17.2	Страница Расписания задач	285
18	<b>Настройка расписаний</b>	<b>287</b>
18.1	Настройка расписания записей	287

18.2	Добавление расписания задач	288
18.3	Настройка стандартного расписания задач	288
18.4	Настройка повторяющегося расписания задач	289
18.5	Удаление расписания задач	289
18.6	Добавление выходных дней и дней исключений	289
18.7	Удаление выходных дней и дней исключений	290
18.8	Переименование расписания	291
19	<b>Страница Камеры и запись</b>	<b>292</b>
19.1	Страница Камеры	292
19.2	Страницы параметров записи (только сетевой видеореги­стратор)	296
20	<b>Настройка камер и параметров записи</b>	<b>297</b>
20.1	Копирование и вставка в таблицы	297
20.2	Экспорт таблицы камер	298
20.3	Настройка параметров качества потока	299
20.3.1	Диалоговое окно Параметры качества потока	299
20.4	Настройка свойств камеры	302
20.5	Настройка параметров записи (только VRM и Локальное хранилище)	302
20.6	Настройка параметров записи (только Сетевой видеореги­стратор)	303
20.7	Диалоговое окно Настройки записи по расписанию (только VRM и локальное хранилище)	304
20.8	Настройка параметров портов PTZ	307
20.9	Настройка предустановленных положений и дополнительных команд	307
20.10	Диалоговое окно «Предустановленные положения и дополнительные команды»	309
20.11	Настройка функции ROI	309
20.12	Копирование параметров записи (только Сетевой видеореги­стратор)	310
20.12.1	Диалоговое окно Копировать настройки записи (только сетевой видеореги­стратор)	310
20.13	Настройка функции ANR	311
20.14	Настройка двойного режима записи в Таблице камер	311
20.15	Управление шлюзом Video Streaming Gateway	312
20.15.1	Назначение профиля ONVIF	312
21	<b>Страница События</b>	<b>313</b>
21.1	Вкладка "Настройки задержки"	314
21.2	Вкладка "Настройки" для расширенного отображения карты	314
21.3	Вкладка "Настройки" для конфигурации событий	315
21.4	Диалоговое окно Редактор командных сценариев	316
21.5	Диалоговое окно Создать сложное событие / Редактировать сложное событие	316
21.6	Диалоговое окно Выберите язык сценария	317
21.7	Диалоговое окно Изменение приоритетов типа события	317
21.8	Диалоговое окно Выбор устройств	318
21.9	Диалоговое окно "Запись текстовых данных"	318
22	<b>Страница Тревожные сигналы</b>	<b>319</b>
22.1	Диалоговое окно Настройки тревог	320
22.2	Диалоговое окно Выбрать содержимое Области изображений	321
22.3	Диалоговое окно «Выбрать содержимое области изображений» (MG)	322
22.4	Диалоговое окно Параметры тревог	323
22.5	Диалоговое окно Выбрать ресурс	326
23	<b>Настройка событий и тревог</b>	<b>328</b>
23.1	Копирование и вставка в таблицы	329
23.2	Удаление строки из таблицы	329

23.3	Управление файлами ресурсов	329
23.4	Настройка события	330
23.5	Дублирование события	330
23.6	Регистрация пользовательских событий	330
23.7	Настройка кнопок пользовательских событий	331
23.8	Создание сложного события	332
23.9	Редактирование сложного события	333
23.10	Настройка тревоги	333
23.11	Настройка параметров для всех тревог	334
23.12	Настройка длительности до и после срабатывания тревожного сигнала	334
23.13	Включение записи по тревоге с помощью текстовых данных	335
23.14	Добавление текстовых данных к непрерывной записи	336
23.15	Защита записи по тревоге	336
23.16	Настройка мигающих активных точек	336
23.17	События и тревоги для систем контроля и управления доступом	337
24	<b>Страница Пользовательские группы</b>	<b>339</b>
24.1	Страница Свойства пользовательской группы	341
24.2	Страница Свойства пользователей	342
24.3	Страница Свойства комбинации для входа в систему	343
24.4	Страница Разрешения камеры	344
24.5	Страница Приоритеты управления	346
24.6	Диалоговое окно Копировать разрешения пользовательской группы	346
24.7	Страница Разрешения декодера	347
24.8	Страница События и тревоги	347
24.9	Диалоговое окно Настройки сервера LDAP	348
24.10	Страница Учетные данные	349
24.11	Страница Логическое дерево	350
24.12	Страница Свойства оператора	351
24.13	Страница Приоритеты	354
24.14	Страница Интерфейс пользователя	354
24.15	Страница Доступ к серверу	356
24.16	Страница Разрешения конфигурации	356
24.17	Страница Разрешения групп пользователей	357
24.18	Страница политик учетной записи	358
24.18.1	Operator Client в автономном режиме	360
25	<b>Настройка пользователей, разрешений и корпоративного доступа</b>	<b>364</b>
25.1	Создание группы или учетной записи	365
25.1.1	Создание стандартной группы пользователей	365
25.1.2	Создание Enterprise User Group	366
25.1.3	Создание Enterprise Account	366
25.2	Создание пользователя	367
25.3	Создание группы с двойной авторизацией	368
25.4	Добавление комбинации для входа в систему к группе с двойной авторизацией	369
25.5	Настройка группы администраторов	370
25.6	Настройка параметров LDAP	370
25.7	Связывание группы LDAP	371
25.8	Составление расписания разрешений на вход пользователей в систему	372
25.9	Настройка рабочих привилегий	372
25.10	Настройка разрешений устройств	373

---

<b>25.11</b>	Настройка различных приоритетов	<b>373</b>
<b>25.12</b>	Копирование разрешений пользовательской группы	<b>374</b>
<b>26</b>	<b>Настройка обнаружения пожара с помощью видео</b>	<b>376</b>
<b>26.1</b>	Настройка камеры для обнаружения пожара	<b>376</b>
<b>26.2</b>	Добавление кодера в пул VRM	<b>377</b>
<b>26.3</b>	Добавление кодеров путем поиска	<b>377</b>
<b>26.4</b>	Добавление устройств, работающих только в режиме реального времени, путем поиска	<b>378</b>
<b>26.5</b>	Добавление кодеров локального хранилища путем поиска	<b>378</b>
<b>26.6</b>	Настройка события пожара	<b>379</b>
<b>26.7</b>	Настройка тревожного сигнала пожара	<b>379</b>
<b>27</b>	<b>Настройка MIC IP 7000, подключенного к VIDEOJET 7000 connect</b>	<b>380</b>
<b>28</b>	<b>Устранение неполадок</b>	<b>381</b>
<b>28.1</b>	Настройка языка в Windows	<b>383</b>
<b>28.2</b>	Повторная установка соединения с клавиатурой Bosch IntuiKey	<b>384</b>
<b>28.3</b>	Сокращение количества камер Allegiant	<b>384</b>
<b>28.4</b>	Используемые порты	<b>384</b>
<b>28.5</b>	Включение журнала для событий ONVIF	<b>391</b>
	<b>Глоссарий</b>	<b>393</b>
	<b>Указатель</b>	<b>404</b>

---


# 1 Использование справки

Чтобы получить дополнительные сведения о выполнении определенных действий в системе BVMS, откройте интерактивную справку одним из следующих способов.

**Для использования вкладок «Содержание», «Указатель» и «Поиск» выполните следующие действия.**

- ▶ В меню **Справка** выберите пункт **Показать справку**. Используйте кнопки и ссылки для перехода к соответствующим разделам справки.

**Для вызова справки в окне или диалоговом окне выполните следующие действия.**

- ▶ На панели инструментов щелкните значок  .
- ИЛИ
- ▶ Нажмите клавишу F1 для вызова справки по окну программы или диалоговому окну.

## 1.1 Поиск информации

Информацию в справке можно искать несколькими способами.

Для поиска информации в интерактивной справке:

1. В меню **Справка** выберите пункт **Справка**.
2. Если левая часть скрыта, нажмите кнопку **Показать**.
3. В окне "Справка" выполните следующее:

Элемент	Действие
<b>Содержание</b>	Отобразить содержание интерактивной справки. Нажмите по очереди каждый значок книги, чтобы открыть нужный раздел. Затем нажмите ссылку на страницу для отображения соответствующего раздела справа.
<b>Указатель</b>	Начать поиск определенных слов или выражений либо сделать выбор из списка ключевых слов указателя. Дважды нажмите ключевое слово для отображения соответствующего раздела справа.
<b>Поиск</b>	Найти слова или выражения в содержании данного раздела. Введите слово или выражение в текстовое поле, нажмите клавишу ВВОД и выберите нужный раздел из списка.

Текст интерфейса пользователя выделен **жирным шрифтом**.

- ▶ Щелкните подчеркнутый текст или элемент приложения, на который указывает стрелка..

**Дополнительная информация**

- ▶ Нажмите для отображения раздела, содержащего сведения об используемом вами окне приложения. В данном разделе содержатся сведения об управляющих элементах окна приложения.

*Понятия, Страница 20* предоставляет основные сведения по выбранным вопросам.



### Замечание!

Этот символ указывает на потенциальный риск повреждения собственности или потери данных.

## 1.2 Печать Справки

При использовании интерактивной справки можно распечатать разделы и сведения непосредственно из окна обозревателя.

**Чтобы распечатать раздел Справки:**

1. Щелкните правой кнопкой мыши в области справа и выберите пункт **Печать**.  
Откроется диалоговое окно **Печать**.
  2. Нажмите кнопку **Печать**.
- ✓ Раздел будет распечатан на указанном принтере.

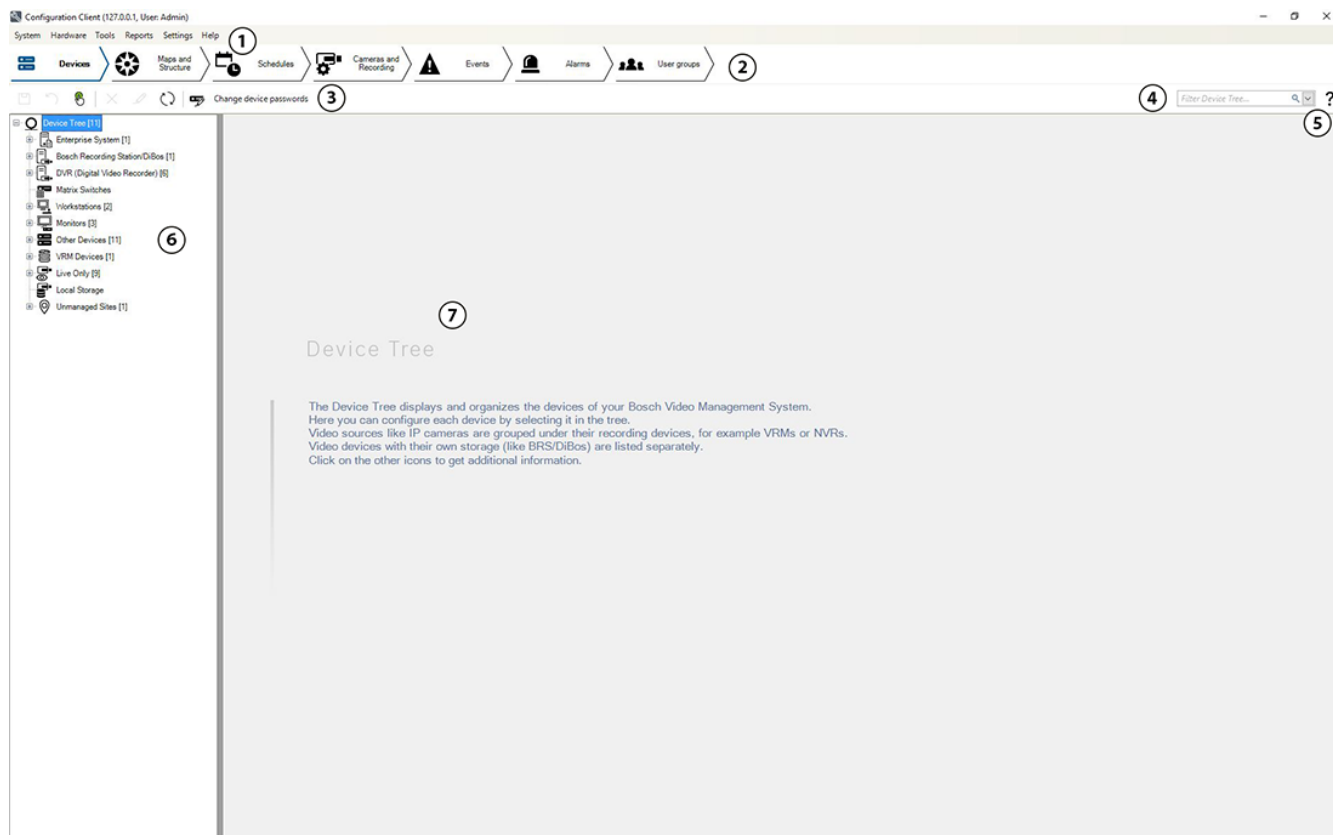
## 2 Введение

Нажмите ссылку, чтобы посмотреть, какие лицензии на программное обеспечение с открытым исходным кодом используются в BVMS и мобильном приложении:

<http://www.boschsecurity.com/oss/>



Подпадает под действие одного или нескольких патентов, перечисленных на [patentlist.hevcadvance.com](http://patentlist.hevcadvance.com).



1	Панель меню	Позволяет выбрать команду меню.
2	Панель вкладок	Позволяет настроить все необходимые действия слева направо.
3	Панель инструментов	Отображает доступные кнопки согласно активной вкладке. Наведите курсор мыши на значок, чтобы отобразить всплывающую подсказку.
4	Панель поиска	Позволяет выполнять поиск определенного устройства и соответствующих родительских элементов в дереве устройств.
5	Значок справки	Отображает интерактивную справку по BVMS Configuration Client.
6	Окно выбора	Иерархический список всех доступных устройств системы.
7	Окно конфигурации	Позволяет настроить выбранное устройство.

В настоящем руководстве приведены основные сведения о настройке и эксплуатации с помощью BVMS.

Более подробная информация и пошаговые инструкции находятся в руководстве по конфигурации и руководстве пользователя, а также в интерактивной справке.



BVMS интегрирует цифровые видео-, аудиопотоки и данные по любой IP-сети.

Система состоит из следующих программных модулей:


- Management Server
- VRM (Video Recording Manager)
- Operator Client
- Configuration Client

Для работы системы следует выполнить следующие задачи:

- Установить службы (Management Server и VRM)
- Установить Operator Client и Configuration Client
- Установить подключение к сети
- Подключить устройства к сети
- Базовая конфигурация:
  - Добавить устройства (например, поиском в сети)
  - Построить логическую структуру
  - Настроить расписания, камеры, события и тревоги
  - Настроить группы пользователей

BVMS Export Player отображает экспортированные записи.

Начать работу с BVMS Configuration Client лучше всего с настройки устройств и логического дерева. Затем на соответствующих страницах можно настроить расписания, записи, события и сигналы тревоги для устройств. Последний этап заключается в настройке групп пользователей на одноименной странице. После настройки всех страниц слева направо оператор может приступить к работе с Operator Client.

После настройки каждой страницы сохраните конфигурацию, нажав  в меню «Инструменты».

Чтобы отобразить изменения в BVMS Operator Client нажмите  .

## 3 Обзор системы

Если вы планируете установить и настроить систему BVMS, примите участие в обучении по системе BVMS.

Поддерживаемые версии аппаратного и микропрограммного обеспечения и другую важную информацию см. в замечаниях к выпуску текущей версии BVMS.

Сведения о компьютерах, на которые можно установить систему BVMS, см. в технических характеристиках рабочих станций и серверов Bosch.

Программные модули BVMS можно устанавливать на один компьютер.

### Важные компоненты

Компонент	Описание
Management Server (доступно для выбора при установке)	Управление потоком, обработка тревог, управление приоритетами, журнал Management, управление пользователями, управление состояниями устройств. Дополнительная лицензия Enterprise System: управление группами Enterprise User Groups и учетными записями Enterprise Accounts.
Config Wizard	Простая и быстрая настройка системы записи.
Configuration Client (доступно для выбора при установке)	Конфигурирование системы и администрирование для Operator Client.
Operator Client (доступно для выбора при установке)	Наблюдение в режиме реального времени, поиск сохраненных данных и воспроизведение, тревоги и доступ к нескольким компьютерам Management Server одновременно.
Video Recording Manager (доступно для выбора при установке)	Распределение объема хранилища на устройствах iSCSI по кодерам при одновременном распределении нагрузки между несколькими устройствами iSCSI. Потоковая передача видео- и аудиоданных с iSCSI на клиенты Operator Client.
Mobile Video Service (доступно для выбора при установке)	Предоставление службы транскодирования, которая транскодирует видеопоток в режиме реального времени и записанное видео с камеры, настроенной в системе BVMS в соответствии с доступной пропускной способностью сети. Эта служба позволяет видеоклиентам, таким как клиенты для iPhone или браузера, получать транскодированные потоки, например при ненадежном подключении к сети с низкой пропускной способностью.
Веб-клиент	Может использоваться для доступа к транслируемым видеоданным и воспроизведения видеозаписи через веб-браузер.
Мобильное приложение	Это приложение можно использовать на iPhone или iPad для доступа к транслируемым видеоданным и воспроизведения видеозаписи.

Компонент	Описание
Bosch Video Streaming Gateway (доступно для выбора при установке)	Обеспечивает интеграцию камер сторонних производителей и запись, аналогичную записи на сетевой видеорегистратор, например в сетях с низкой пропускной способностью.
Cameo SDK (доступно для выбора при установке)	Комплект Cameo SDK используется для встраивания областей изображений BVMS, как получаемых в режиме реального времени, так и записанных, во внешние приложения сторонних производителей. Области изображений используют разрешения пользователя на основе BVMS. Комплект Cameo SDK предоставляет набор функций BVMS Operator Client, позволяющий создавать приложения, сходные с Operator Client.
Client Enterprise SDK	Комплект Client Enterprise SDK используется для управления и мониторинга поведения Operator Client в системе Enterprise System с помощью внешних приложений. Этот комплект разработчика ПО позволяет просматривать устройства, доступные включенному и соединенному с сетью клиенту Operator Client, и управлять некоторыми функциями интерфейса пользователя.
Client SDK / Server SDK	Комплект Server SDK используется для управления и мониторинга сервера Management Server с помощью сценариев и внешних приложений. Эти интерфейсы можно использовать при наличии действующей учетной записи администратора. Комплект Client SDK используется для управления и мониторинга клиента Operator Client с помощью сценариев (часть конфигурации соответствующего сервера) и внешних приложений.

### 3.1 Требования к аппаратному оборудованию

См. технические характеристики для BVMS. Имеются также технические характеристики для различных платформ ПК.

### 3.2 Требования к программному обеспечению

См. технические характеристики для BVMS.

### 3.3 Лицензионные требования

Доступные лицензии указаны в технических характеристиках BVMS.

## 4 Понятия

В данном разделе содержится основная информация по данным вопросам.

### 4.1 Основы проектирования BVMS

#### **Система с одним сервером управления, Страница 20**

Одна система BVMS Management Server обеспечивает поддержку, мониторинг и управление до 2000 камер или кодеров.

#### **Enterprise System, Страница 21**

Enterprise Management Server обеспечивает одновременный доступ к нескольким Management Servers. Enterprise System позволяет получить полный доступ к событиям и тревогам из нескольких подсистем.

#### **Server Lookup, Страница 22**

Функция Server Lookup предоставляет список доступных BVMSManagement Servers для BVMSOperator Client. Оператор может выбрать сервер из списка доступных. При подключении к Management Server клиент имеет полный доступ к Management Server.

#### **Неуправляемый объект, Страница 23**

Устройства могут быть сгруппированы в unmanaged sites. Устройства группы unmanaged sites не контролируются при помощи Management Server. Management Server предоставляет список unmanaged sites для Operator Client. Оператор может по требованию подключаться к объекту и получать доступ к видеoinформации в режиме реального времени и записанным видеоданным. События и обработка тревог недоступны для функции unmanaged site.








#### 4.1.1 Система с одним сервером управления

- Один BVMSManagement Server может обслуживать до 2000 каналов.
- BVMS Management Server обеспечивает обслуживание, мониторинг и управление всей системы.
- BVMSOperator Client подключен к Management Server, принимает события и тревоги с BVMSManagement Server и отображает данные в режиме реального времени и воспроизведения записей.
- В большинстве случаев все устройства находятся в одной локальной сети с высокой пропускной способностью и низкой задержкой.

Функции

- Конфигурационные данные
- Журнал событий
- Профили пользователей
- Приоритеты пользователей
- Лицензирование
- Управление событиями и тревогами

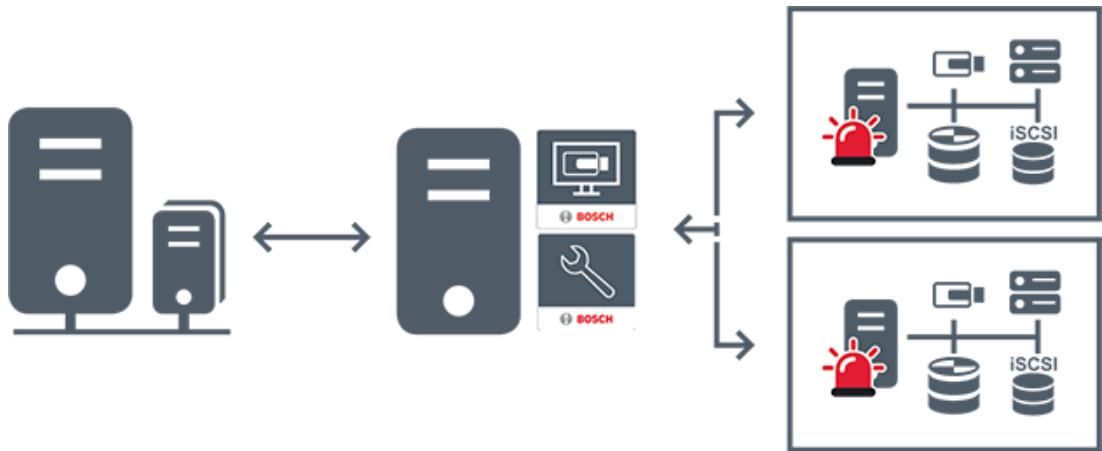






	Отображение в режиме реального времени, воспроизведение записей, события, тревоги
	Management Server
	Operator Client / Configuration Client
	Камеры
	VRM
	iSCSI
	Другие устройства.

#### 4.1.2

#### Enterprise System

- Назначением системы уровня BVMS Enterprise System предоставляет возможность пользователю программы Operator Client для одновременного доступа к нескольким Management Servers (подсистемам).
- Клиенты при подключении к серверу Enterprise имеют доступ ко всем камерам и записям из подсистем.
- При подключении к серверу Enterprise клиенты в реальном времени получают все события и тревоги от всех подсистем.
- Характерные области применения:
  - Метрополитены
  - Аэропорты



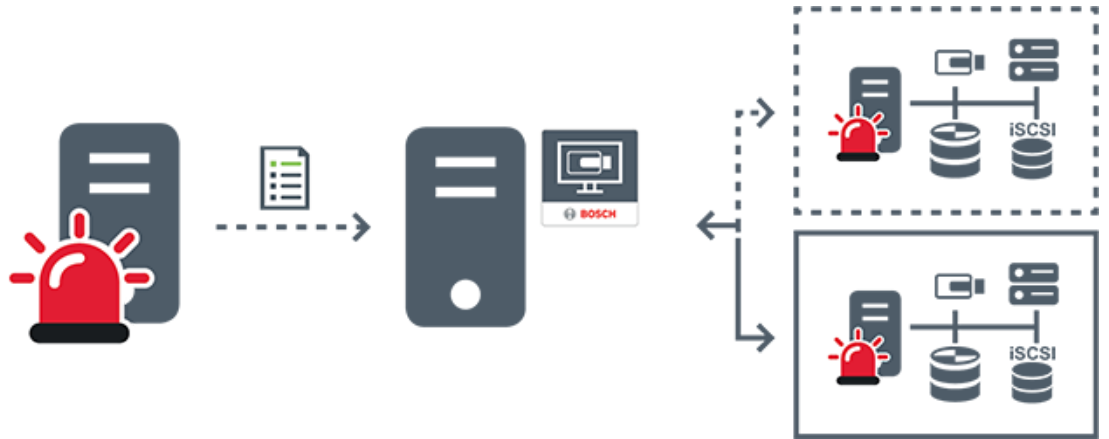
	Отображение в режиме реального времени, воспроизведение записей, события, тревоги
	BVMS Enterprise Management Server
	BVMS Operator Client / Configuration Client
	Подсистема BVMS

**См.**

- *Создание системы Enterprise, Страница 89*
- *Настройка списка серверов для корпоративной системы, Страница 89*
- *Настройка пользователей, разрешений и корпоративного доступа, Страница 364*
- *Доступ к системе, Страница 74*

**4.1.3****Server Lookup**

- Функция BVMS Server Lookup позволяет операторам подключаться к BVMSManagement Server из доступного списка серверов.
- Один пользователь Configuration Client или Operator Client может последовательно подключаться к нескольким системным точкам доступа.
- Системные точки доступа могут быть Management Server или Enterprise Management Server.
- Server Lookup использует специальный Management Server для размещения списка серверов.
- Функции Server Lookup и Management Server или Enterprise Management Server могут быть запущены на одном компьютере.
- Server Lookup поддерживает поиск системных точек доступа по имени или описанию.
- Operator Client, подключенный к Management Server, принимает события и тревоги с BVMS Management Server и отображает данные в режиме реального времени и воспроизведения записей.



	Отображение по требованию в режиме реального времени, воспроизведение записей, события, тревоги — подключено
	Отображение по требованию в режиме реального времени, воспроизведение записей, события, тревоги — не подключено
	Management Server
	Список серверов
	Operator Client
	Подключенная система BVMS из списка серверов
	Неподключенная система BVMS из списка серверов

**См.**

- *Настройка Server Lookup, Страница 128*
- *Страница «Список серверов/Адресная книга», Страница 127*
- *Использование просмотра сервера, Страница 74*
- *Экспорт списка серверов, Страница 129*
- *Импорт списка серверов, Страница 129*

**4.1.4**

**Неуправляемый объект**

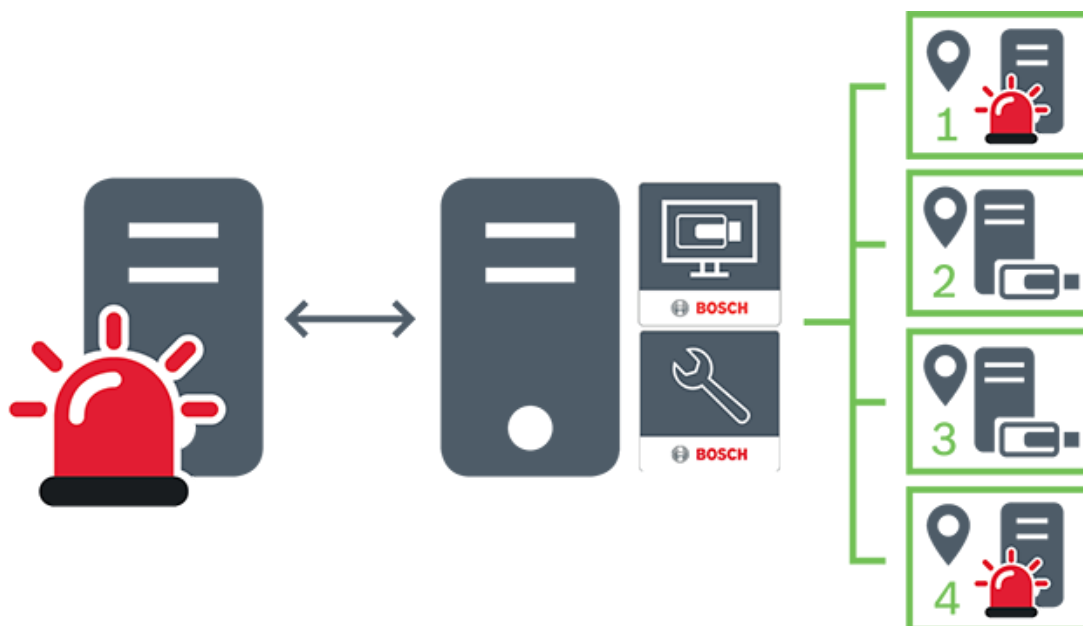
- Вариант построения системы BVMS со множеством небольших подсистем.
- Он позволяет настроить до 9999 местоположений в одном BVMS Management Server

- Операторы имеют доступ к видеоданным в реальном времени и записям с 20 sites одновременно.
- Для упрощения навигации объекты sites можно сгруппировать по папкам или расположить на картах. Предустановленные имя пользователя и пароль позволяют операторам быстро подключаться к site.

Функция unmanaged site поддерживает систему BVMS на основе IP, а также аналоговые решения DVR:

- Аналоговые регистраторы Bosch DIVAR AN 3000/5000
- Регистраторы DIVAR hybrid
- Регистраторы DIVAR network
- DIP 3000/7000 устройств записи на основе IP
- Отдельная система BVMS Management Server

Для добавления объекта site для централизованного мониторинга требуется только лицензия на каждый объект site; это не зависит от количества каналов на объекте site.



	Отображение в режиме реального времени, воспроизведение записей, события, тревоги
	Отображение в режиме реального времени по требованию и воспроизведение видеотрафика
	Management Server
	Operator Client / Configuration Client



	site
	DVR

См.

– *Добавление объекта unmanaged site вручную, Страница 223*

## 4.2

### Запись

В данной главе описываются различные функции системы, связанные с записью и воспроизведением.

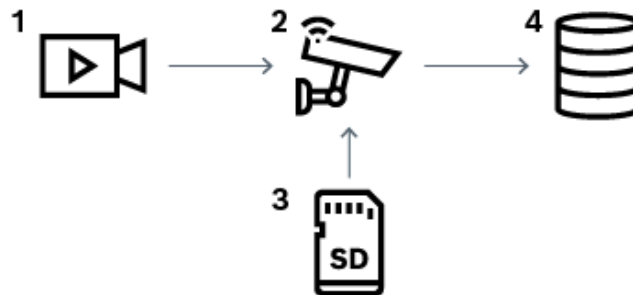
#### 4.2.1

### Автоматическая компенсация сети (ANR)

#### Использование по назначению

При сбое сети или центрального хранилища данных функция ANR обеспечивает передачу кодером записи, помещенной в локальный буфер, за недостающий период времени в центральное хранилище после устранения неполадки.

На следующем рисунке показана передача видеоданных после устранения неполадки сети или хранилища.



1	Видео
2	Кодер, IP-сеть
3	SD-карта (кольцевой буфер)
4	Получатель iSCSI (центральное хранилище)

#### Пример. Работа при сбое сети

Если возникает неожиданный сбой сети, функция ANR отправляет в центральное хранилище сохраненную в локальный буфер запись, когда доступ к сети восстанавливается.

#### Пример. Сохранение видеоданных при отсутствии доступа к сети

Поезд метро не имеет сетевого соединения с центральным хранилищем, когда он находится между станциями. Помещенную в буфер запись можно передавать в центральное хранилище только во время обычных остановок.

Проследите за тем, чтобы время, необходимое для передачи помещенной в буфер записи, не превышало продолжительность остановки.

#### **Пример. ANR для записи по тревоге**

Данные, предшествующие записи по тревоге, хранятся локально. Эти данные, предшествующие записи по тревоге, передаются в центральное хранилище только в случае срабатывания сигнала тревоги. Если сигнал тревоги не срабатывает, эти избыточные данные, предшествующие записи по тревоге, не передаются в центральное хранилище и, соответственно, не нагружают сеть.

#### **Ограничения**



#### **Замечание!**

Если в кодере заданы пароли для режимов user и live, воспроизведение с локальных носителей данных использовать невозможно. При необходимости снимите эти пароли.

Функция ANR работает только с записью VRM.

Функция ANR не работает с кодером, для которого настроено безопасное подключение для отображения в реальном времени.

Для использования функции ANR необходимо предварительно настроить носитель данных кодера.

Кодер, для которого выполняется настройка функции ANR, должен иметь версию микропрограммного обеспечения 5.90 или выше. Не все типы кодеров поддерживают функцию ANR.

Функцию ANR невозможно использовать с двойной записью.

Система хранения iSCSI должна быть настроена соответствующим образом.

В следующем перечне приводятся возможные причины, не позволяющие настроить функцию ANR.

- Кодер недоступен (неверный IP-адрес, сбой сети и т. п.).
- Носитель данных кодера недоступен или находится в режиме "только чтение".
- Неверная версия микропрограммного обеспечения.
- Тип кодера не поддерживает функцию ANR.
- Включена двойная запись.

#### **См.**

- *Настройка устройства iSCSI, Страница 202*
- *Настройка носителей данных кодера, Страница 88*
- *Настройка функции ANR, Страница 311*

## **4.2.2**

### **Двойная / резервная запись**

#### **Использование по назначению**

Основной VRM обеспечивает нормальную запись с камер, входящих в систему. Для выполнения двойной записи с камер используется дополнительный VRM.

Двойная запись позволяет записывать видеоданные с одной камеры в разных местах.

Двойная запись обычно выполняется с различными настройками потока и режимами записи. В качестве особого случая двойной записи можно настроить зеркальную запись, когда один и тот же видеосигнал записывается дважды в разных местах.

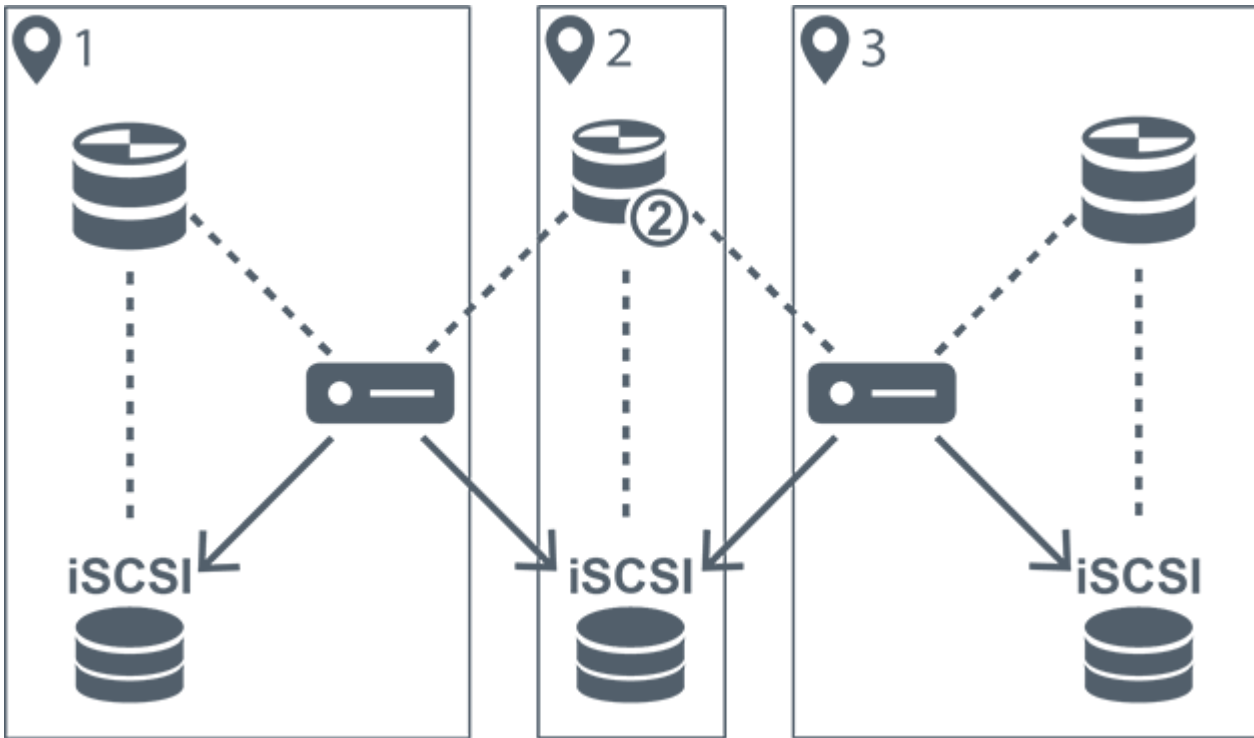
Двойная запись выполняется путем использования 2 серверов VRM, управляющих несколькими устройствами iSCSI, которые могут быть расположены в разных местах.

Дополнительный VRM может обеспечивать управление дополнительной записью для нескольких основных VRM.

Пользователь может выбрать из записей, выполненных с помощью основного диспетчера VRM, и записей, выполненных с помощью дополнительного диспетчера VRM. При работе с одной камерой пользователь может переключиться к записям дополнительного или основного VRM. Пользователь также может отобразить записи одной и той же камеры, выполненные с помощью основного VRM и дополнительного VRM, одновременно. Для двойной записи во время установки необходимо установить дополнительный диспетчер VRM.

Резервный диспетчер VRM используется для продолжения записи отказавшего компьютера основного VRM или дополнительного VRM.

На следующем рисунке приведен пример использования двойной записи.



1	Объект 1		Сервер
2	Центральный объект		Устройство хранения iSCSI
3	Объект 2	.....	Управляющее соединение
	Основной VRM	→	Видеопоток
	Вторичный VRM		

**Ограничения**

Двойную запись невозможно использовать с функцией ANR.

Sameo SDK поддерживает только воспроизведение основной записи.

**См.**

- *Настройка двойного режима записи в Таблице камер, Страница 311*
- *Добавление зеркального диспетчера VRM вручную, Страница 186*
- *Добавление резервного диспетчера VRM вручную, Страница 185*
- *Страница Камеры, Страница 292*

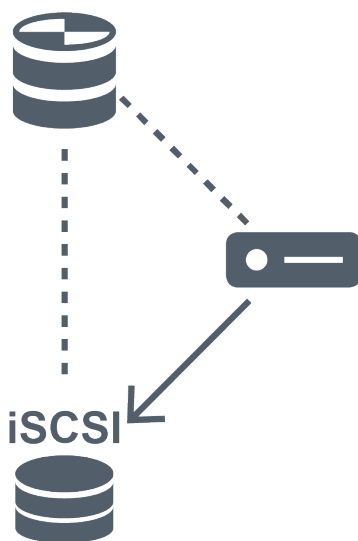
**4.2.3****Режимы записи VRM**




В этом разделе приведены рисунки, отображающие возможные режимы записи VRM.

Список возможных режимов записи VRM:

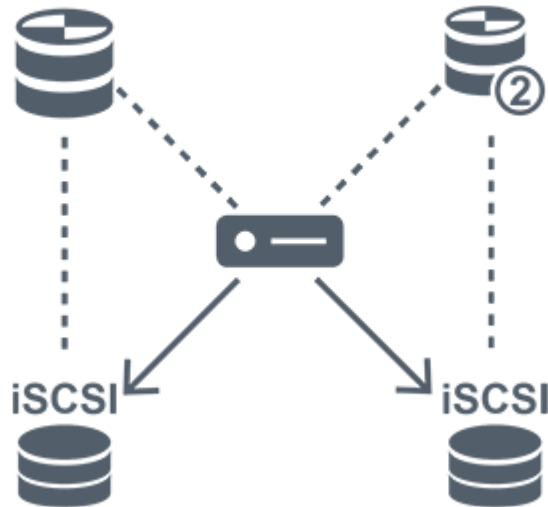
- Основная запись VRM
- Запись с зеркальным VRM
- Дополнительная запись VRM
- Резервная запись VRM

Сведения о записи ANR см. в разделе *Автоматическая компенсация сети (ANR), Страница 25.*

**Основная запись VRM**

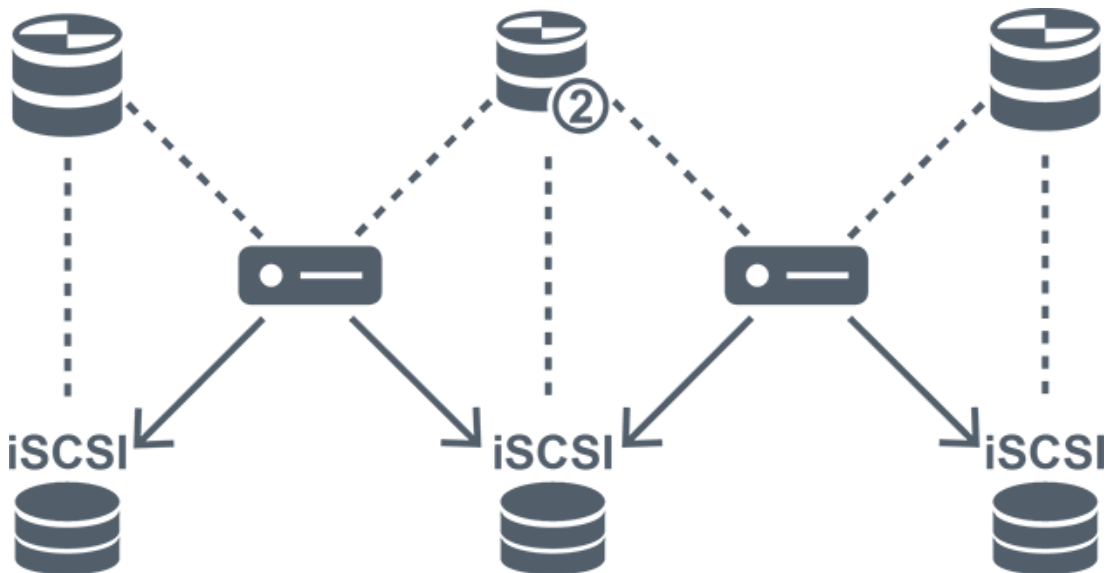
	Основной VRM	-----	Управляющее соединение
	Устройство хранения iSCSI	→	Видеопоток
	Кодер		

**Запись с зеркальным VRM**





	Основной VRM		Дополнительный VRM
	Устройство хранения iSCSI	.....	Управляющее соединение
	Кодер	→	Видеопоток

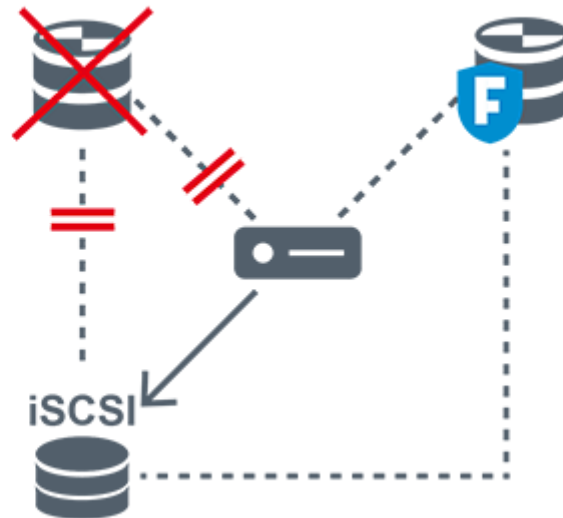
**Вторичная запись VRM**






	Основной VRM		Вторичный VRM
	Устройство хранения iSCSI	.....	Управляющее соединение

	Кодер		Видеопоток
---	-------	---	------------

### Резервная запись VRM



	Основной VRM		Первичный резервный VRM
	Устройство хранения iSCSI		Кодер
	Управляющее соединение		Видеопоток

## 4.2.4


### Воспроизведение источников записи VRM

На следующих рисунках показаны Области изображений с воспроизведением со всех возможных источников записи VRM. На каждом рисунке показано устройство хранения, экземпляр VRM (при наличии) и часть области изображений в качестве примера воспроизведения. Если это необходимо, источник записи указан соответствующим значком на Панели области изображений.

- *Воспроизведение одной записи, Страница 30*
- *Воспроизведение двойной записи VRM, Страница 31*
- *Воспроизведение записи основного диспетчера VRM с помощью дополнительного резервного диспетчера VRM., Страница 32*
- *Воспроизведение записи вторичного VRM с помощью дополнительного резервного VRM., Страница 33*
- *Автоматическая компенсация сети, Страница 34*

### Воспроизведение одной записи

Эта область изображений отображается, когда настроен только основной VRM. Выбрать другой источник записи невозможно.

: Если выполнена настройка для этой рабочей станции, воспроизведение обеспечивается непосредственно устройством хранения iSCSI.






	Устройство хранения iSCSI
	Основной VRM

**Воспроизведение двойной записи VRM**

Основной VRM и вторичный VRM настроены. Нажмите значок источника записи, чтобы отобразить первичное или вторичное воспроизведение.

Если выполнена настройка для этой рабочей станции, воспроизведение обеспечивается непосредственно устройством хранения iSCSI.



	Устройство хранения iSCSI
	Основной VRM
	Вторичный VRM

### Воспроизведение записи основного диспетчера VRM с помощью дополнительного резервного диспетчера VRM.

Когда основной VRM работает, он обеспечивает воспроизведение. Резервный VRM находится в неактивном состоянии.

Если выполнена настройка для этой рабочей станции, воспроизведение обеспечивается непосредственно устройством хранения iSCSI.

Если настроена запись вторичного VRM или ANR, можно переключить источник записи.




Если основной VRM не подключен, настроенный резервный VRM обеспечивает воспроизведение. Закройте область изображений и снова отобразите эту камеру в области изображений:



Если не подключен ни основной VRM, ни дополнительный основной резервный VRM, воспроизведение обеспечивается кодером. Закройте область изображений и снова отобразите эту камеру в области изображений.





	Устройство хранения iSCSI
	Основной VRM
	Основной резервный диспетчер VRM
	Кодер

При воспроизведении с помощью кодера доступ возможен только к ограниченной части записи.

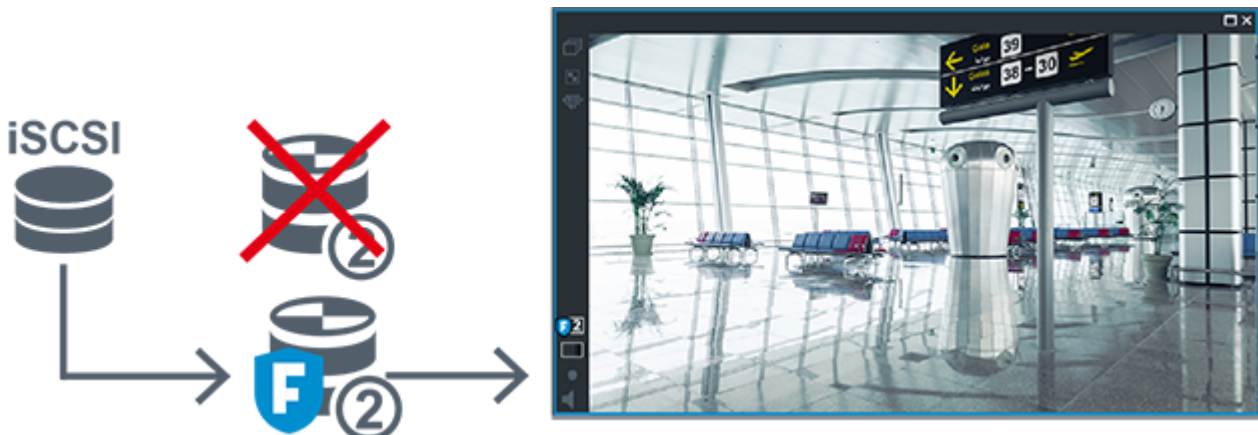
**Воспроизведение записи вторичного VRM с помощью дополнительного резервного VRM.**

Когда вторичный диспетчер VRM работает, он обеспечивает воспроизведение. Резервный VRM находится в неактивном состоянии.

Если выполнена настройка для этой рабочей станции, воспроизведение обеспечивается непосредственно устройством хранения iSCSI.







Если вторичный VRM не подключен, настроенный резервный VRM обеспечивает воспроизведение. Закройте область изображений и снова отобразите эту камеру в области изображений:



Если не подключен ни вторичный VRM, ни дополнительный вторичный резервный VRM, воспроизведение обеспечивается кодером. Закройте область изображений и снова перетащите эту камеру в область изображений.



	Устройство хранения iSCSI
	Основной VRM
	Вторичный резервный диспетчер VRM
	Кодер

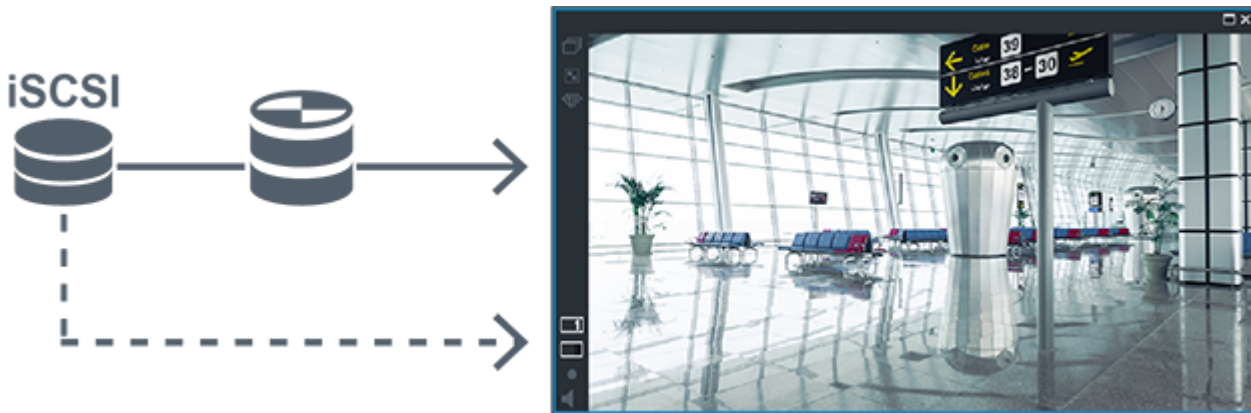
При воспроизведении с помощью кодера доступ возможен только к ограниченной части записи.




**Автоматическая компенсация сети**

Функция ANR не настроена. Нажмите значок источника записи для отображения основного воспроизведения (основное резервное воспроизведение, основное воспроизведение кодера) или воспроизведения ANR.

Если выполнена настройка для этой рабочей станции, воспроизведение обеспечивается непосредственно устройством хранения iSCSI.





	Устройство хранения iSCSI
	Основной VRM
	Карта SD

### 4.3 Обработка сигналов тревоги

Тревоги могут быть настроены индивидуально для обработки одной или несколькими группами пользователей. При срабатывании тревоги она появляется в списке тревожных сигналов всех пользователей, принадлежащих к тем пользовательским группам, настройки которых позволяют принимать этот тревожное событие. После того как один из этих пользователей начинает обработку данной тревоги, она исчезает из списка тревожных сигналов других пользователей.

Тревоги отображаются на тревожном мониторе рабочей станции. Это поведение описывается в следующих разделах.

#### Движение тревожного события

1. В системе возникает тревожное событие.
2. Уведомления о тревоге появляются в списках тревожных сигналов всех пользователей, которые настроены на эту тревогу. Тревожное видеоизображение немедленно отображается на настроенных мониторах. Если это тревожное событие является автоматически отображаемым (всплывающим), тревожное видеоизображение автоматически отображается также на тревожных мониторах рабочей станции Operator Client.  
 Если тревожное событие сконфигурирован как автоматически отключающийся, он удаляется из списка тревожных сигналов по истечении времени автоотключения (настраиваемого в Configuration Client).  
 В аналоговых мониторах режим квадрированного просмотра VIP XD временно заменяется полноэкранным режимом.
3. Один из пользователей принимает тревожное событие. На рабочей станции этого пользователя отображается тревожное видеоизображение (если оно еще не отображено автоматически). Тревожный сигнал удаляется из всех других списков тревожных сигналов и не отображается на экранах других операторов.

4. Пользователь, принявший тревожное событие, запускает поток заданий, который может включать в себя чтение плана действий и ввод комментариев. Этот шаг является факультативным: требования к потоку заданий могут быть настроены администратором.
5. В конечном итоге пользователь отключает тревожное событие. Это действие удаляет тревожное событие из списка тревожных сигналов, и он перестает отображаться на экране.  
В группе мониторов отображаются те камеры, которые отображались до возникновения тревожного события.

#### Окно тревожных изображений

1. Для отображения тревожного видеоизображения окно тревожных изображений занимает место окна изображения в режиме реального времени или окна воспроизведения записей на мониторе, который был настроен как монитор тревожных сигналов.
2. Каждому тревожному сигналу выделяется ряд Областей изображений. С каждым тревожным сигналом может быть связано до 5 областей изображений. Эти области изображений могут отображать видео в режиме реального времени, воспроизводить запись или отображать карту.  
В группе мониторов каждый тревожный сигнал может выводить камеры в ряду мониторов. Количество камер в каждом ряду ограничено количеством столбцов в группе мониторов. Мониторы в столбце, который не используется для отображения тревожных видеоизображений, могут быть настроены на отображение текущего изображения или пустого экрана.
3. Тревожные сигналы с более высоким приоритетом отображаются над тревожными сигналами с более низким приоритетом как в рядах мониторов, так и в рядах отображения тревожных сигналов рабочей станции Operator Client.
4. Если окно тревожных изображений полностью занято рядами тревожных изображений и при этом должен быть отображен дополнительный тревожный сигнал, в нижнем ряду окна тревожных изображений будет отображаться последовательность тревожных сигналов с наиболее низким приоритетом. Вы можете переключаться между тревожными сигналами в стеке при помощи элементов управления слева от строки тревожного сигнала.  
Можно переключаться между стеками тревожных сигналов в группе мониторов с помощью кнопок управления в окне **Мониторы** рабочей станции Operator Client. Мониторы с тревожными сигналами обозначены красными значками с мигающими "светодиодными" индикаторами.  
Название, время и дата тревожного сигнала могут быть отображены на всех мониторах или только на первом мониторе в тревожном ряду.
5. В отношении тревожных сигналов с одинаковым приоритетом система может быть настроена администратором одним из двух способов:
  - Режим "Last-in-First-out" (LIFO): при этой конфигурации новые тревожные сигналы помещаются над старыми тревожными сигналами с тем же приоритетом.
  - Режим "First-in-First-out" (FIFO); при этой конфигурации новые тревожные сигналы помещаются под старыми тревожными сигналами с тем же приоритетом.
6. Ряд тревожных изображений может отображаться в окне тревожных изображений одним из двух способов:
  - После его автоматического отображения (автоматического всплывания). Это происходит, когда приоритет тревожного сигнала выше приоритета дисплея.

- После принятия тревожного сигнала Это происходит, когда приоритет тревожного сигнала ниже приоритета дисплея.

#### **Автоматически всплывающие тревожные сигналы**

Тревожный сигнал может быть настроен как автоматически отображающийся (всплывающий) в окне тревожных сигналов, в соответствии с приоритетом. Дисплеям реального времени и воспроизведения каждой пользовательской группы также назначаются приоритеты. При получении тревожного сигнала с приоритетом, превышающим приоритет дисплея пользователя, этот тревожный сигнал автоматически отображает свой тревожный ряд в окне тревожных сигналов. Если окно тревожных сигналов не отображается в данный момент на экране, оно автоматически занимает место окна изображений в реальном времени или окна воспроизведения на мониторе, настроенном на отображение тревог.

Несмотря на то что всплывающие тревожные сигналы отображаются в окне тревожных сигналов, они не принимаются автоматически. Они могут одновременно отображаться на дисплеях нескольких пользователей. Когда пользователь принимает всплывающий тревожный сигнал, он удаляется из списка тревожных сигналов всех остальных пользователей и перестает отображаться на их дисплеях.

#### **Обработка тревог в случае выключения системы**

Все активные тревоги сохраняются по завершении работы сервера. Тревоги будут восстановлены и снова появятся в окне **Список тревожных сигналов**, когда система перезапустится.

Тревоги в состоянии **Принято** или **Поток заданий** автоматически переводятся обратно в состояние **Активно** после перезагрузки системы. Комментарии, введенные для тревог в состоянии **Поток заданий**, сохраняются.



#### **Замечание!**

Данные тревог сохраняются автоматически каждую минуту, поэтому максимально возможная потеря данных — это данные, накопленные за одну минуту.

См.

- *Настройка длительности до и после срабатывания тревожного сигнала, Страница 334*

## **4.4**

### **Сопоставление событий ONVIF**

#### **Использование по назначению**

Назначение — сопоставление событий ONVIF с событиями BVMS. События ONVIF могут запускать тревоги и запись BVMS.

Можно определить сопоставления событий по умолчанию только для определенного устройства ONVIF, для всех устройств ONVIF одного производителя и модели или для всех устройств ONVIF одного производителя. Сопоставления событий по умолчанию автоматически назначаются всем соответствующим кодерам ONVIF, добавляемым с помощью мастера сканирования BVMS или вручную.

При добавлении кодера ONVIF к конфигурации BVMS без подключения к этому кодеру ONVIF сопоставления событий не назначаются. Можно обновить такой кодер ONVIF, используя сопоставления событий с кодера ONVIF того же производителя или уже добавленной модели.

Задаются сопоставления событий для каждого из следующих источников:

- кодер ONVIF;
- камеры этого кодера ONVIF;
- реле этого кодера ONVIF;

- входы этого кодера ONVIF.

### Пример

На камере ONVIF происходит событие обнаружения движения. Это событие должно запускать событие **Обнаружено движение** в BVMS.

Чтобы это произошло, для этой камеры ONVIF выполняется следующая настройка:

- раздел ONVIF (*MotionDetection*);
- элемент данных ONVIF (*motion*);
- тип данных ONVIF (*boolean*);
- значение данных ONVIF (*true*).

**Примечание.** Недостаточно настроить только событие **Обнаружено движение**. Настройте также событие **Движение остановлено**. Необходимо всегда настраивать пару событий.

### Импорт и экспорт таблицы сопоставлений

Таблицу сопоставлений можно экспортировать на компьютер, на котором она создана, и импортировать ее на другой компьютер, на котором недоступна необходимая таблица сопоставлений.

### Устранение неисправностей

Для поиска и устранения неисправностей можно записывать файлы журнала.

### См.

- *Настройка таблицы сопоставления ONVIF, Страница 249*
- *Включение журнала для событий ONVIF, Страница 391*
- *Страница "События кодера ONVIF", Страница 245*

## 4.5

## Отключение при бездействии

### Использование по назначению

Отключение при бездействии предназначено для защиты клиента Operator Client или Configuration Client в отсутствие оператора или администратора.

Для каждой группы пользователей можно задать такие настройки, чтобы Operator Client автоматически отключался по истечении заданного времени бездействия.

Для Configuration Client пользовательские группы недоступны. Настройка отключения при бездействии действует только для **администратора**.

Все операции с использованием клавиатуры, мыши и клавиатуры CCTV влияют на заданное время отключения при бездействии. Автоматические действия Operator Client не влияют на это время. Такие автоматические действия Configuration Client, как загрузка микропрограммного обеспечения или настройка iSCSI предотвращают отключение при бездействии.

Также можно настроить отключение при бездействии для веб-клиента BVMS.

Незадолго до отключения при бездействии диалоговое окно напоминает пользователю, что отключение при бездействии можно предотвратить каким-либо действием.

В журнал вносится запись о произошедшем отключении при бездействии.

### Пример

Если рабочая станция находится в общественном месте, отключение при бездействии сводит к минимуму опасность получения несанкционированного доступа к Operator Client оставленной без присмотра рабочей станции.

Член группы администраторов должен автоматически отключаться по истечении времени бездействия, но дежурный (группа операторов) может просто смотреть видео без использования системы и не использовать отключение при бездействии.

### Ограничения

Активность Client SDK не поддерживает отключение при бездействии, что означает, что активность Client SDK не влияет на заданный период времени.

### См.

- *Диалоговое окно «Параметры» (меню «Настройки»), Страница 118*
- *Страница Свойства оператора, Страница 351*

## 4.6 Клиент Operator Client, независимый от версии

Для использования режима совместимости и на клиенте Operator Client, и на сервере Management Server должна быть версия выше 5.5.

Пользователь Operator Client может успешно подключиться к серверу Management Server, на котором используется программное обеспечение предыдущей версии.

Если сервер предоставляет конфигурацию новее, чем доступна на рабочей станции Operator Client, эта конфигурация автоматически копируется на рабочую станцию Operator Client. Пользователь может решить загрузить новую конфигурацию.

Клиент Operator Client предоставляет ограниченный набор функций и подключен к данному серверу Management Server.

Следующие функции, связанные с сервером Management Server, доступны после входа на сервер Management Server предыдущей версии:

- пользовательские настройки;
- запуск записи вручную;
- отображение состояний устройства;
- переключение состояний реле;
- поиск в журнале;  
Поиск событий невозможен.
- поиск сервера;
- удаленный экспорт.

### 4.6.1 Работа в режиме совместимости

Эта функция доступна в версиях выше 5.5.

Клиент BVMS Operator Client предоставляет визуальную и текстовую информацию о своем состоянии.

Возможны следующие состояния Operator Client.



Клиент Operator Client подключен к серверу Management Server.



Клиент Operator Client не подключен к серверу Management Server. Возможная причина — физическое отключение от сети сервера Management Server.



Это состояние отображается только после восстановления подключения к серверу Management Server. Все соответствующие функции снова можно использовать, но конфигурация клиента Operator Client оказывается устаревшей, так как в сети доступна более новая конфигурация. Войдите в систему снова, чтобы обновить конфигурацию.



Этот значок состояния отображается, если на сервере Management Server установлена более ранняя версия BVMS, чем на рабочей станции Operator Client.

## 4.7 Режимы просмотра панорамной камеры

В этом разделе показаны режимы просмотра изображения с панорамной камеры, которые доступны в системе BVMS.

Доступны следующие режимы просмотра:

- Круговое представление
- Панорамное представление
- Кадрированное представление

Панорамное и кадрированное представления создаются в результате операции устранения искажений в BVMS. Устранение искажений в камере не применяется.

Администратор должен настроить положение установки панорамной камеры в Configuration Client.

Размер области изображений можно изменить требуемым образом. Соотношение сторон области изображений не ограничено соотношениями 4:3 и 16:9.

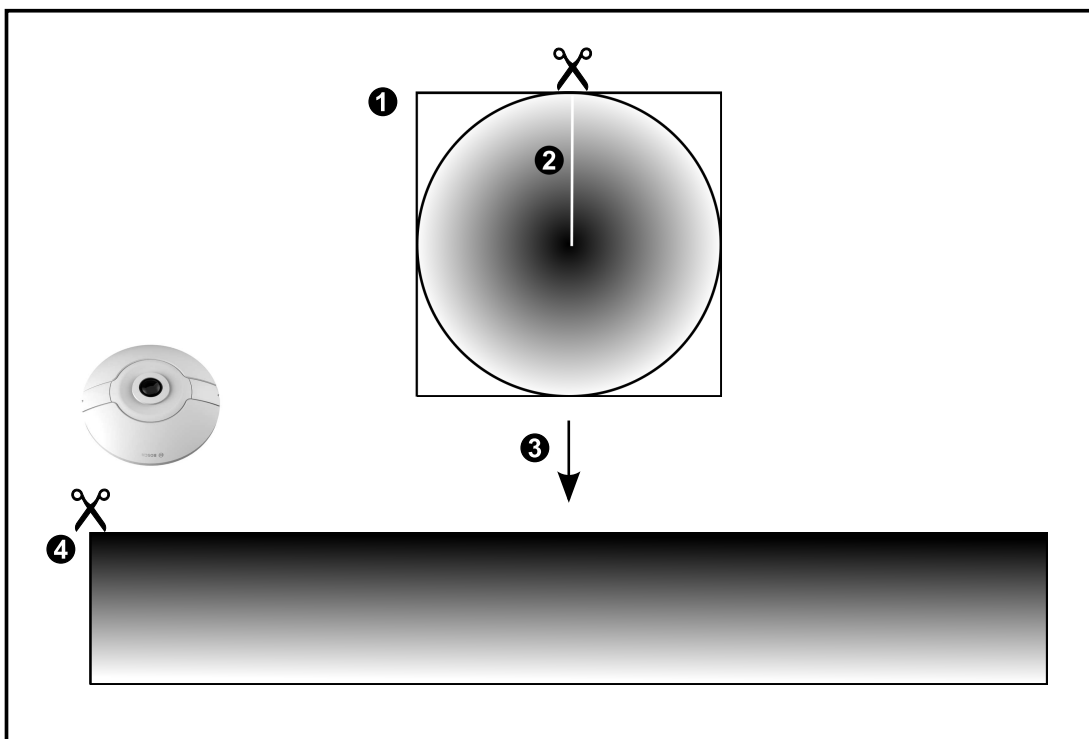
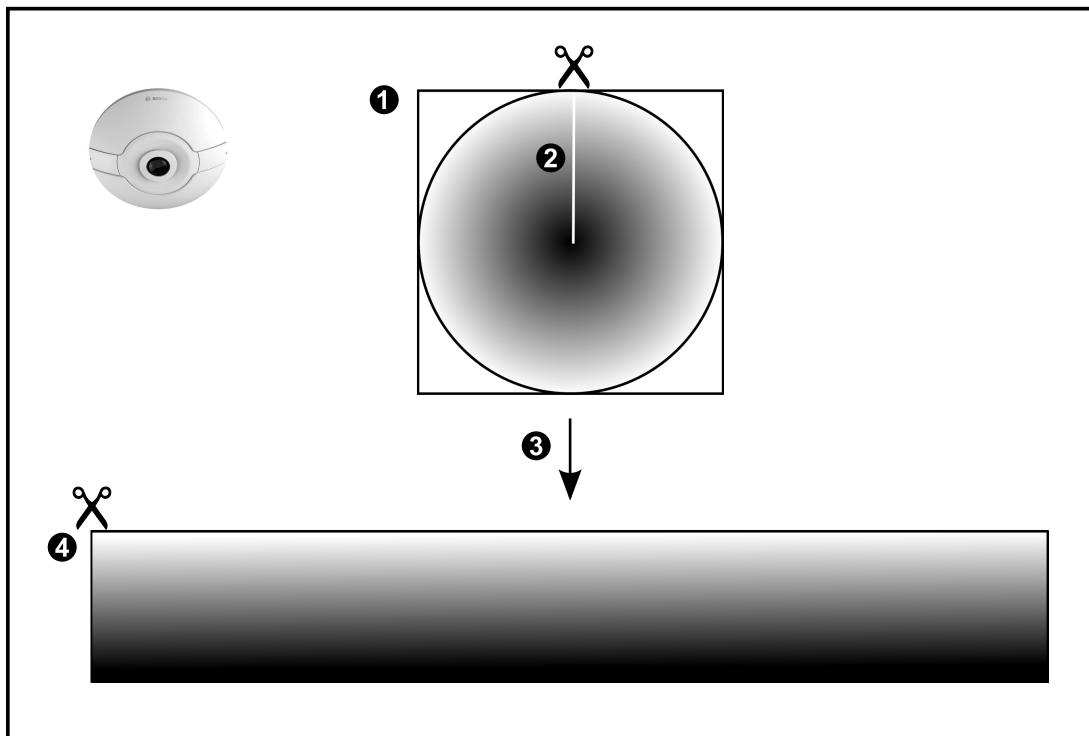
**См.**

- *Настройка предустановленных положений и дополнительных команд, Страница 307*

### 4.7.1 Панорамная камера 360°, монтируемая на полу или потолке

На рисунке ниже показана процедура устранения искажений для панорамной камеры 360°, монтируемой на полу или потолке.



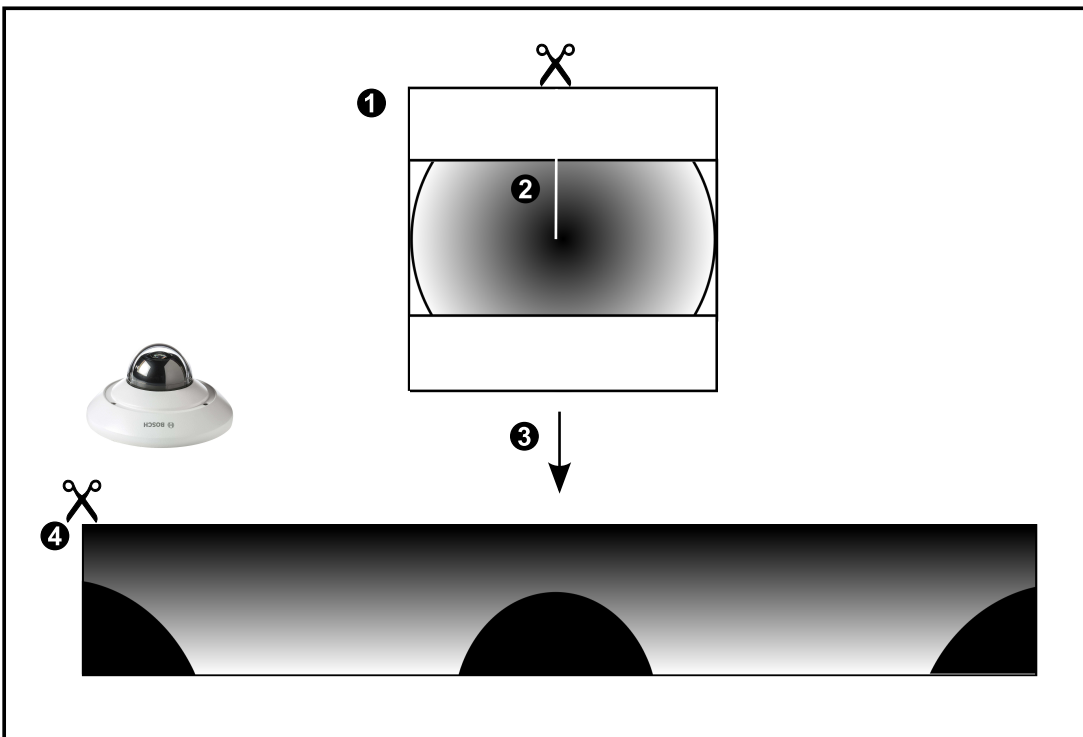
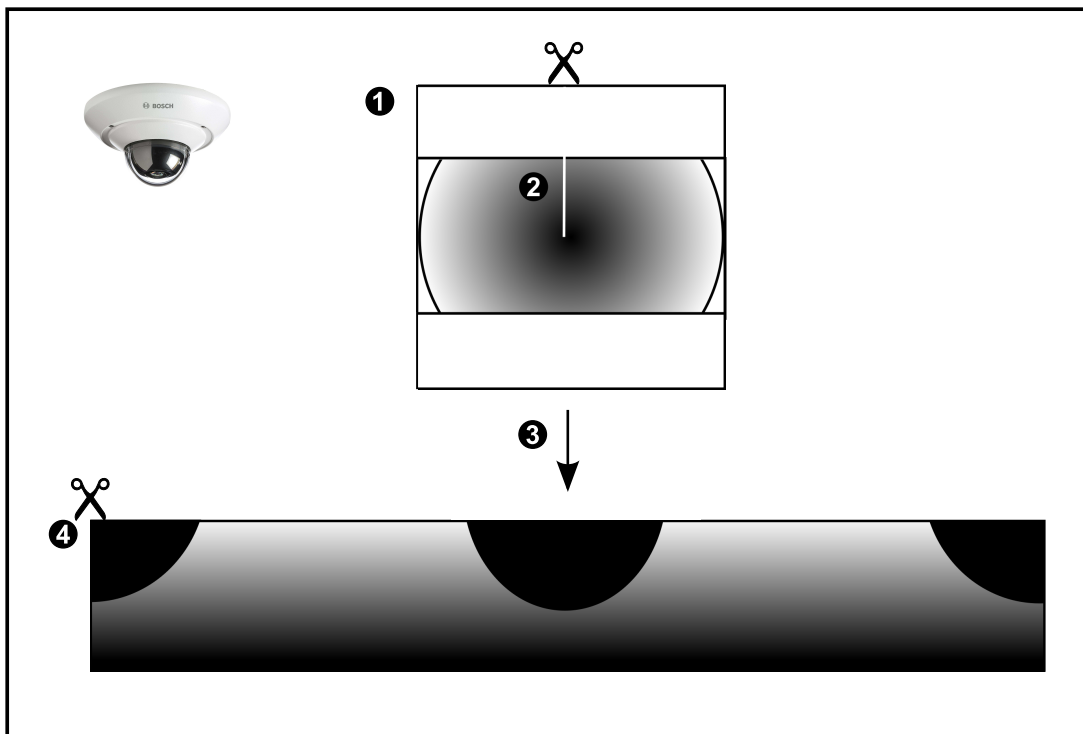


1	Изображение в виде целого круга	3	Устранение искажений
2	Линия разреза (оператор может изменять ее положение, если изображение не является увеличенным)	4	Панорамное представление

### 4.7.2

### Панорамная камера 180°, монтируемая на полу или потолке

На рисунке ниже показана процедура устранения искажений для панорамной камеры 180°, монтируемой на полу или потолке.



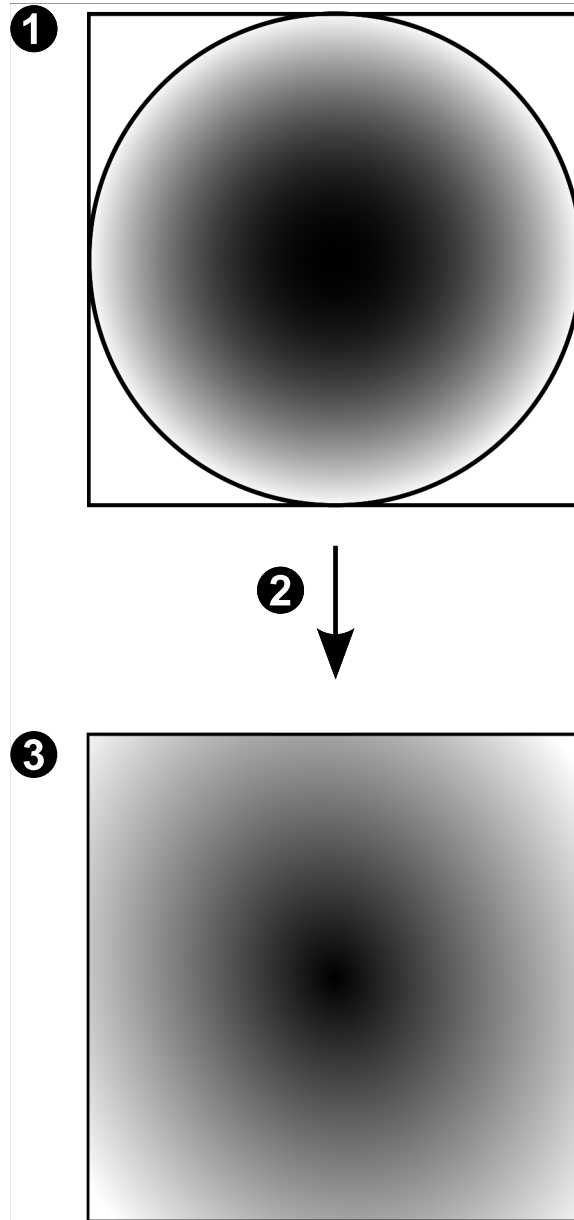
1 Изображение в виде целого круга	3 Устранение искажений
-----------------------------------	------------------------

2	Линия разреза (оператор может изменять ее положение, если изображение не является увеличенным)	4	Панорамное представление
---	--	---	--------------------------

### 4.7.3

#### Панорамная камера 360°, монтируемая на стене

На рисунке ниже показана процедура устранения искажений для панорамной камеры 360°, монтируемой на стене.

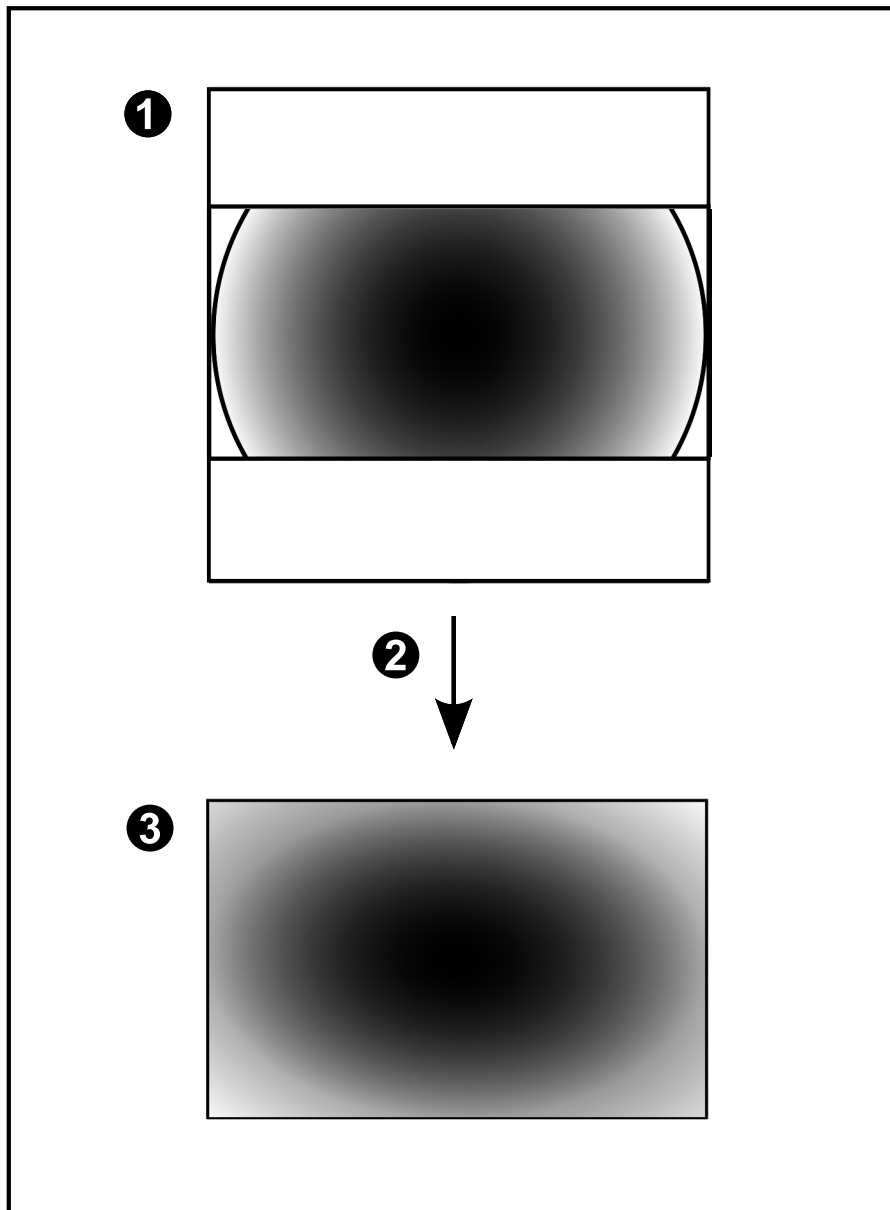


1	Изображение в виде целого круга	3	Панорамное представление
2	Устранение искажений		

#### 4.7.4

#### Панорамная камера 180°, монтируемая на стене

На рисунке ниже показана процедура устранения искажений для панорамной камеры 180°, монтируемой на стене.



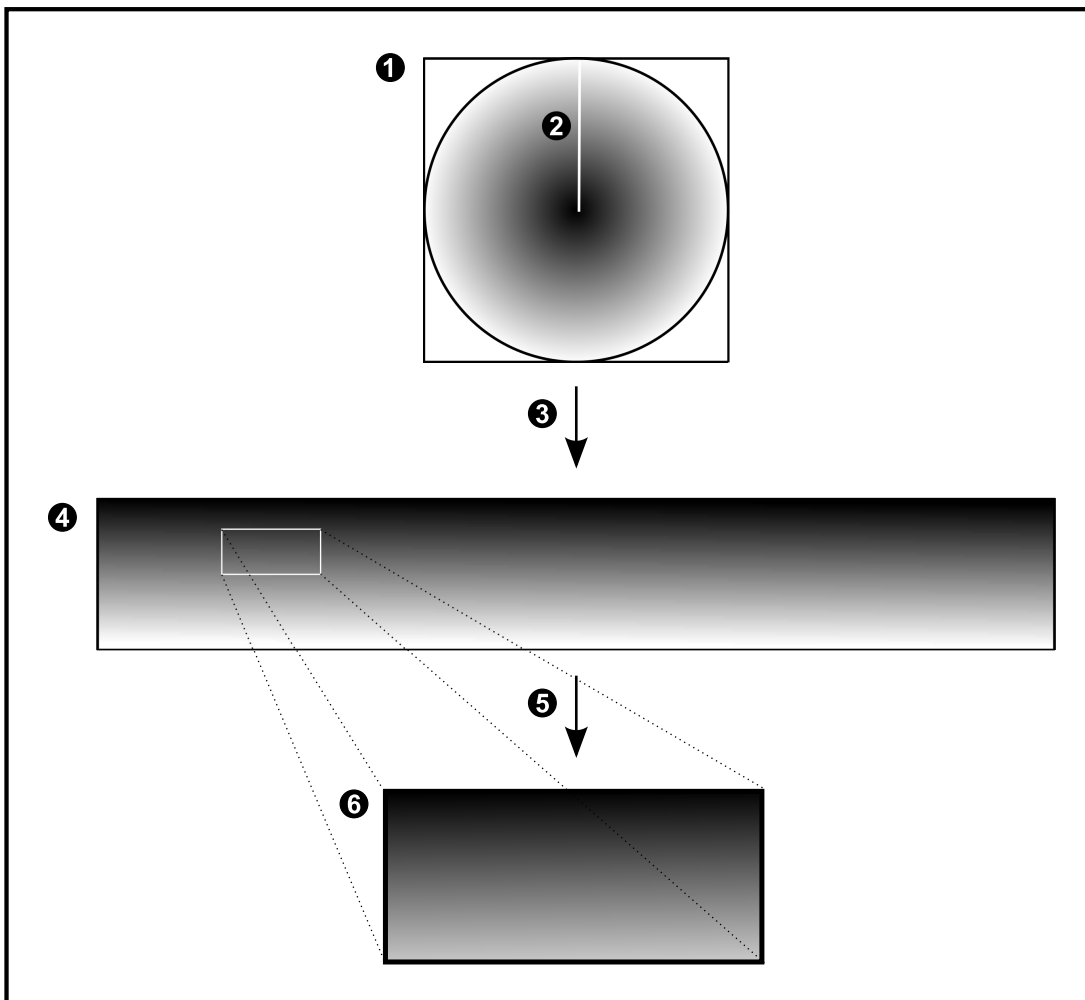
1	Изображение в виде целого круга	3	Панорамное представление
2	Устранение искажений		

### 4.7.5

#### Кадрированное представление изображения с панорамной камеры

На рисунке ниже показана процедура кадрирования изображения для панорамной камеры 360°, монтируемой на полу или потолке.

Применяемый для кадрирования прямоугольный фрагмент является фиксированным. Фрагмент можно изменить в области кадрированного изображения с помощью имеющихся средств управления PTZ.



1	Изображение в виде целого круга	4	Панорамное представление
2	Линия разреза (оператор может изменять ее положение, если изображение не является увеличенным)	5	Кадрирование
3	Устранение искажений	6	Кадрированная область изображений

## 4.8 Туннелирование SSH

BVMS обеспечивает удаленное подключение благодаря использованию технологии туннелирования Secure Shell (SSH).

Туннелирование SSH позволяет создать зашифрованный туннель с помощью подключения протокол/сокет SSH. Этот зашифрованный туннель может передавать как зашифрованные, так и незашифрованные данные. Реализация Bosch SSH также использует протокол Omni-Path — высокопроизводительный протокол связи с низкой задержкой от Intel.

### Ограничения и технические характеристики

- Туннелирование SSH использует порт 5322. Этот порт не может быть изменен.
- Служба SSH должна быть установлена на тот же сервер, что и Management Server BVMS.
- Для учетных записей пользователей (Enterprise) должен быть настроен пароль. Учетные записи пользователей (Enterprise) без пароля не могут выполнять вход при использовании соединения по протоколу SSH.
- Камеры с локальным устройством хранения не поддерживают соединение по протоколу SSH.
- Configuration Client не может подключаться удаленно по протоколу SSH. Соединение с Configuration Client должно осуществляться посредством сопоставления портов.
- Operator Client проверяет соединение со службой SSH каждые 15 секунд. В случае разрыва соединения Operator Client раз в минуту перепроверяет наличие соединения.

### Сопоставление портов

- ▶ Настройте один перенаправляющий порт для Management Server BVMS для использования порта 5322 для внутренних и внешних подключений. Это единственное сопоставление портов, которое необходимо выполнить для всей системы. Сопоставление портов BVMS не требуется.

### Шифрованная связь

После установления подключения через туннель SSH все соединения между Management Server BVMS и удаленным клиентом являются зашифрованными.

## 4.9 Многопутевой ввод-вывод

BVMS обеспечивает многопутевой ввод-вывод для систем с двойными контроллерами. Многопутевой ввод-вывод является устойчивой к ошибкам технологией, подходящей для более чем одного физического подключения между камерой и ее iSCSI хранилищами через резервные сетевые подключения. При использовании многопутевого ввода-вывода запись и воспроизведение видеоданных возможны даже в случае сбоя iSCSI контроллера.

### Необходимые условия и ограничения

- Установлен iSCSI модуль NetApp E2800 с двойным контроллером.
- Микропрограмма 6.43 позволяет устройствам, ведущими запись на E2800, использовать альтернативные пути.
- VRM 3.71 для мониторинга и ведения журнала устройств с включенным многопутевым входом-выходом.

- Два настроенных физических порта iSCSI на каждом контроллере: 2 x 2 RJ-45 или 2 x 2 оптических.
- Скорость соединения должна составлять 10 Гбит/с для обеспечения полноценной работы.
- Режим Dual—Simplex, используемый в E2700, больше не поддерживается.

Более подробные сведения об установке полного дуплекса DSA E2800 см. в Руководстве пользователя DSA E-Series E2800.



## 5 Поддерживаемое оборудование



### Замечание!

Не следует подключать устройство к нескольким BVMS! Это может привести к пропускам в записи и другим нежелательным последствиям.

К BVMS можно подключить следующее аппаратное оборудование.

- Мобильные видеоклиенты, такие как iPhone или iPad через DynDNS
- Различные IP-камеры. кодеры и ONVIF-камеры (только в режиме реального времени или через Video Streaming Gateway)  
Подключаются через сеть
- Кодеры, работающие только в режиме реального времени, с локальным хранилищем  
Подключаются через сеть
- Устройства хранения iSCSI  
Подключаются через сеть
- Компьютер VIDOS NVR  
Подключаются через сеть
- Аналоговые камеры  
Подключаются к кодерам, устройствам BRS/DiBos
- Декодеры  
Подключаются через сеть
- Мониторы  
Подключаются к декодеру, к матричному коммутатору Bosch Allegiant, к клиентской рабочей станции BVMS
- Устройства BRS/DiBos (см. технические характеристики для BVMS для поддерживаемых версий ПО)  
Подключаются через сеть
- матричный коммутатор Bosch Allegiant (версия микропрограммы: 8.75 или выше, версия MCS: 2.80 или выше)  
Подключается к COM-порту Management Server или к удаленному компьютеру и к IP-кодеру в сети.
- Клавиатура KBD-Universal XF  
Подключается к порту USB рабочей станции BVMS.
- Клавиатура Bosch IntuiKey  
Подключается к COM-порту рабочей станции BVMS (версия микропрограммного обеспечения 1.82 или выше) или к аппаратному декодеру (VIP XD).  
При подключении клавиатуры к рабочей станции пользователь может с клавиатуры управлять всей системой. При подключении клавиатуры к декодеру VIP XD пользователь может управлять с клавиатуры только мониторами.
- SMS-устройство  
Подключается к COM-порту Management Server
- Почтовый сервер SMTP  
Подключается через сеть
- POS  
Подключается через сеть
- АТМ  
Подключается через сеть
- Устройство мониторинга сети  
Подключается через сеть

- Модули ввода/вывода  
Подключается через сеть  
Поддерживаются только устройства ADAM.

Все устройства, подключаемые через сеть, подключаются к коммутатору. Компьютеры BVMS также подключаются к этому устройству.

## 5.1 Установка аппаратного оборудования

BVMS поддерживает следующие компоненты оборудования:

- Клавиатура KBD-Universal XF
- Клавиатура Bosch IntuiKey
- Матричный коммутатор Bosch Allegiant с камерами и монитором: подключен к COM-порту одного из компьютеров сети и к IP-кодерам, подключенным к сети.
- Кодеры с аналоговыми камерами
- Кодеры с локальными хранилищами
- IP-камеры и камеры IP AutoDome
- Мониторы, подключенные к декодеру (возможны группы мониторов для обработки тревог)
- Системы DiBos с камерами
- Системы DVR с камерами
- Устройства ATM / POS
- Модули ввода/вывода  
Поддерживаются только устройства ADAM.

## 5.2 Установка клавиатуры KBD Universal XF



### Замечание!

Ознакомьтесь с руководством, входящим в комплект вашей клавиатуры KBD-Universal XF и доступным в интернет-каталоге продуктов.

### Дополнительная информация

Для получения дополнительной информации, загрузки программного обеспечения и документации посетите страницу соответствующего продукта на веб-сайте [www.boschsecurity.com](http://www.boschsecurity.com).

К BVMS можно подключить следующее аппаратное оборудование.

- Мобильные видеоклиенты, такие как iPhone или iPad через DynDNS
- Различные IP-камеры, кодеры и ONVIF-камеры (только в режиме реального времени или через Video Streaming Gateway)  
Подключаются через сеть
- Кодеры, работающие только в режиме реального времени, с локальным хранилищем  
Подключаются через сеть
- Устройства хранения iSCSI  
Подключаются через сеть
- Компьютер VIDOS NVR  
Подключаются через сеть
- Аналоговые камеры  
Подключаются к кодерам, устройствам BRS/DiBos
- Декодеры  
Подключаются через сеть
- Мониторы

- Подключаются к декодеру, к матричному коммутатору Bosch Allegiant, к клиентской рабочей станции BVMS
- Устройства BRS/DiBos (см. технические характеристики для BVMS для поддерживаемых версий ПО)  
Подключаются через сеть
  - матричный коммутатор Bosch Allegiant (версия микропрограммы: 8.75 или выше, версия MCS: 2.80 или выше)  
Подключается к COM-порту Management Server или к удаленному компьютеру и к IP-кодеру в сети.

## 5.3 Подключение клавиатуры Bosch IntuiKey к BVMS

В данном разделе содержатся общие сведения о настройке клавиатуры Bosch IntuiKey.

### 5.3.1 Сценарии подключения клавиатур Bosch IntuiKey

Вы можете подключить клавиатуру Bosch IntuiKey к COM-порту рабочей станции BVMS (сценарий 1) или к аппаратному декодеру (напр., VIP XD, сценарий 2).

При подключении клавиатуры к рабочей станции BVMS пользователь может управлять всей системой. При подключении клавиатуры к декодеру пользователь может управлять только аналоговыми мониторами системы.

При подключении клавиатуры к Enterprise Operator Client вы можете управлять камерами определенного Management Server, сначала нажав клавишу сервера для ввода номера сервера, а затем номера камеры.

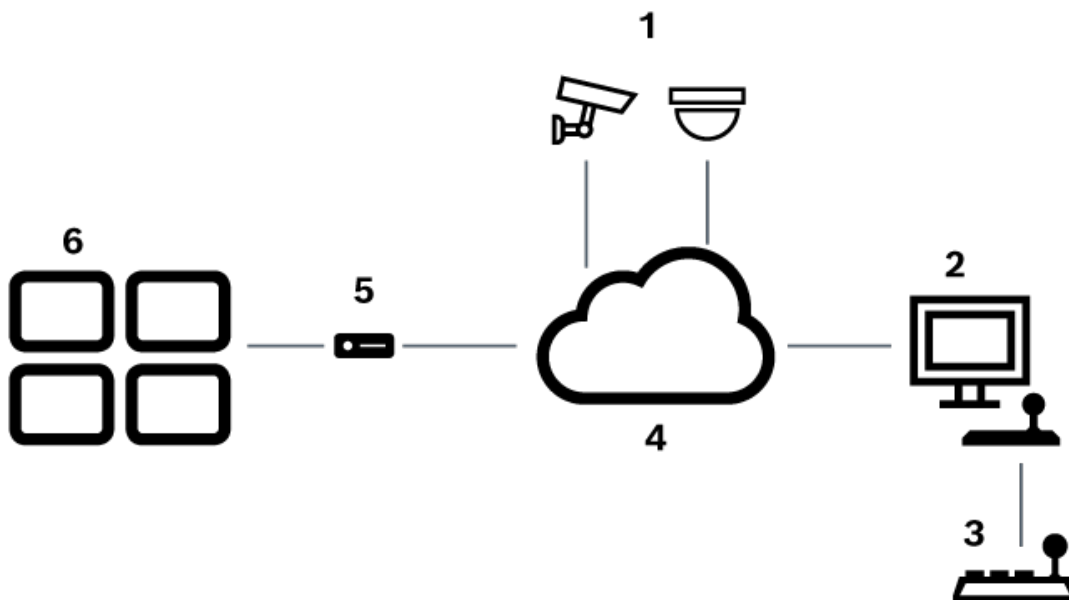
#### **Замечание!**



Для подключения клавиатуры Bosch IntuiKey к рабочей станции BVMS используйте специальный кабель Bosch.

Для подключения клавиатуры Bosch IntuiKey к декодеру VIP XD вам потребуется кабель, соединяющий последовательный COM-порт клавиатуры с последовательным интерфейсом декодера. Сведения о подключении см. в Подключение клавиатуры CCTV к декодеру.

### Поддерживается клавиатура Bosch IntuiKey, подключенная к рабочей станции BVMS



**Рис. 5.1:** Сценарий 1: клавиатура Bosch IntuiKey, подключенная к рабочей станции Bosch Video Management System

<b>1</b>	Различные камеры, подключенные к сети через кодеры
<b>2</b>	Рабочая станция BVMS
<b>3</b>	Клавиатура Bosch IntuiKey
<b>4</b>	Сеть BVMS
<b>5</b>	Декодер
<b>6</b>	Мониторы

### Клавиатура Bosch IntuiKey, подключенная к декодеру

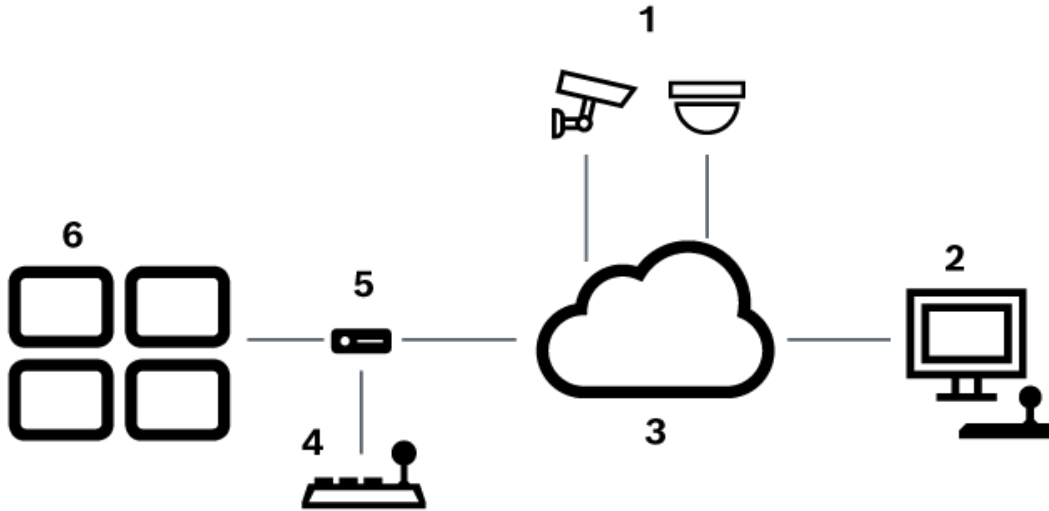


Рис. 5.2: Сценарий 2: клавиатура Bosch IntuiKey, подключенная к декодеру

1	Различные камеры, подключенные к сети через кодеры
2	Рабочая станция BVMS
3	Сеть BVMS
4	Клавиатура Bosch IntuiKey
5	Декодер
6	Мониторы

Подробные сведения обо всех окнах содержатся в следующих разделах:

– Страница "Назначить клавиатуру", Страница 163

Пошаговые инструкции содержатся в следующих разделах:

- Настройка клавиатуры Bosch IntuiKey (страница «Настройки») (рабочая станция), Страница 139
- Настройка клавиатуры Bosch IntuiKey (декодер), Страница 147
- Настройка декодера для использования с клавиатурой Bosch IntuiKey, Страница 148

См.

– Страница "Назначить клавиатуру", Страница 163

## 5.3.2

### Подключение клавиатуры Bosch IntuiKey к декодеру

#### Настройка декодера

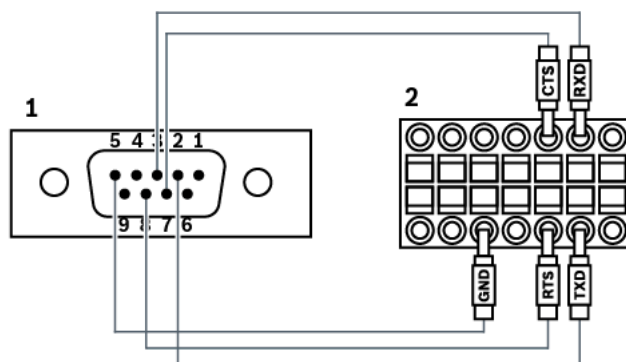
См. Настройка декодера для использования с клавиатурой Bosch IntuiKey, Страница 148 для получения подробных сведений.

### Соединение между COM-портом и декодером VIP XD

В следующей таблице перечислены соединения между адаптером RS232 и последовательным интерфейсом декодера VIP XD:

Адаптер RS232	Последовательный интерфейс декодера VIP XD
1	
2	TX
3	RX
4	
5	GND
6	
7	CTS
8	RTS
9	

На следующей иллюстрации показана схема расположения выводов стандартного адаптера RS232 (1) и схема расположения выводов последовательного адаптера декодера (2):



### 5.3.3

#### Обновление программного обеспечения клавиатуры Bosch IntuiKey

1. Установите на каком-либо ПК загрузчик IntuiKey.
2. Запустите служебную программу IntuiKey Firmware Upgrade.
3. При помощи последовательного кабеля (обратитесь в службу поддержки Bosch, если у вас нет такого кабеля) подключите клавиатуру к этому ПК.
4. На клавиатуре нажмите программную клавишу Keyboard Control, затем Firmware Upgrade.
5. Введите пароль: 0 и 1 одновременно.  
Клавиатура находится в режиме начального загрузчика.
6. На компьютере нажмите Browse для выбора файла ПО: например, kbd.s20
7. Настройте COM-порт.

8. Нажмите кнопку Download, чтобы загрузить микропрограмму.  
На дисплее клавиатуры отображается Programming.  
Пока не нажимайте Clr. В противном случае клавиатура будет не пригодна к использованию после перезагрузки (см. примечание ниже).
9. Нажмите Browse, чтобы выбрать язык: например, 8900\_EN\_..82.s20.  
На дисплее клавиатуры отображается Programming.
10. Закройте служебную программу IntuiKey Firmware Upgrade.
11. На клавиатуре нажмите клавишу Clr для выхода.  
Клавиатура будет перезапущена. Подождите несколько секунд, пока не появится меню выбора языка клавиатуры.
12. Выберите требуемый язык с помощью программной клавиши.  
Отображается стандартная стартовая страница.

**Замечание!**

Для непосредственного запуска режима начального загрузчика можно отключить питание от клавиатуры, одновременно нажать 0 и 1, снова включить питание и отпустить 0 и 1.

## 5.4

### Подключение матричного коммутатора Bosch Allegiant к BVMS

Матричный коммутатор BVMSAllegiant обеспечивает непрерывный доступ к аналоговым матричным камерам через интерфейс Operator Client. Камеры Allegiant выглядят почти так же, как и IP-камеры. Единственное различие заключается в небольшом значке с сеткой, указывающем на то, что это камера Allegiant. Вы можете отображать эти камеры, используя те же задания, что и для IP-камер. Они включены как в логическое дерево, так и на карты участков, и пользователи могут добавлять их в дерево избранного. При поддержке оконного управления видеоизображением с камеры PTZ, подключенной к Allegiant, эти камеры могут быть отображены на мониторах, подключенных к IP-декодерам. BVMS соединяется с матричным коммутатором посредством ПО Allegiant MCS (Master Control Software). Программа MCS запускается и работает в фоновом режиме. Это программное обеспечение представляет собой эффективный, событийно управляемый интерфейс для соединения с Allegiant. Оно обеспечивает быструю передачу в реальном времени от коммутатора Allegiant к BVMS. Например, если в результате повреждения кабеля возникла потеря сигнала в Allegiant, системе BVMS немедленно отправляется уведомление. Вы также можете запрограммировать BVMS таким образом, чтобы она реагировала на тревоги Allegiant.

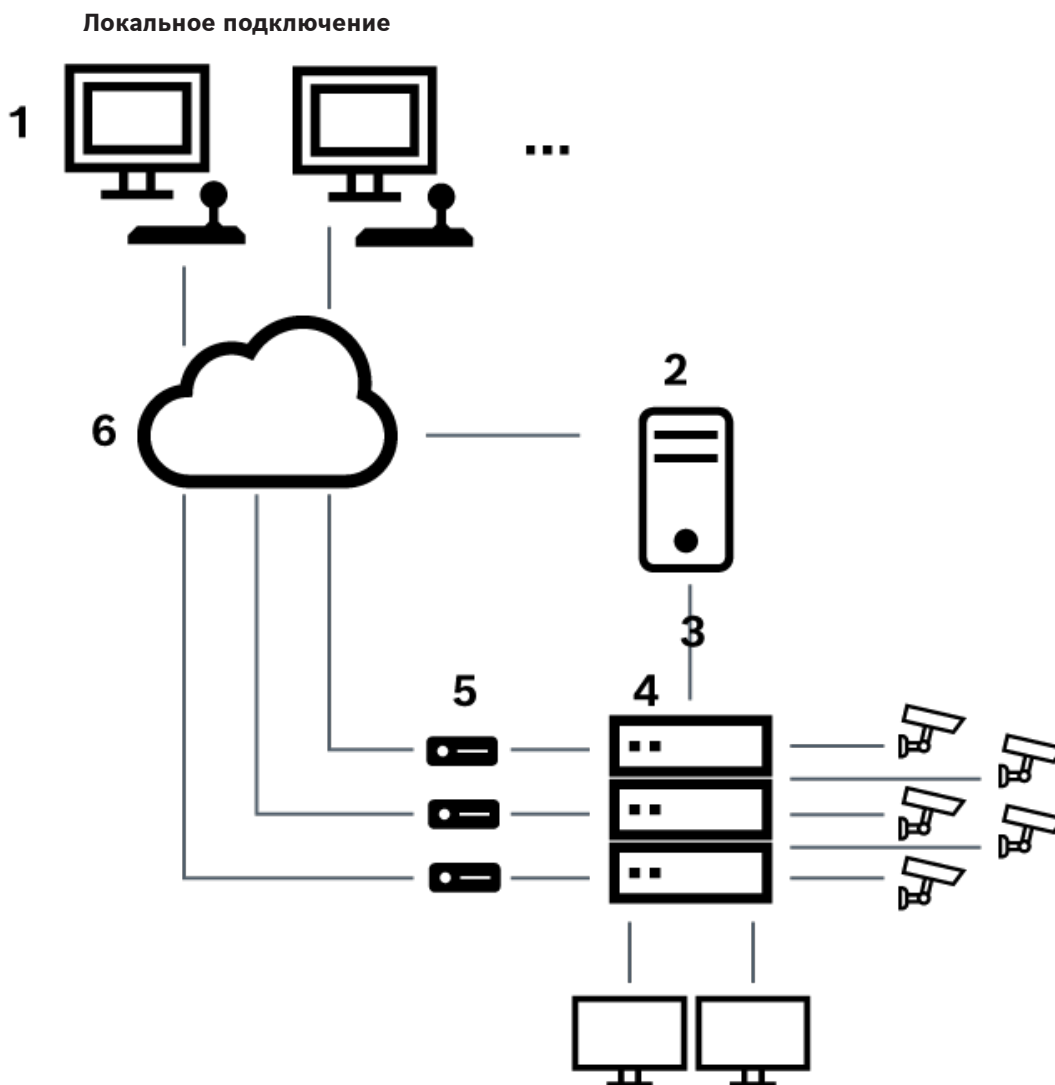
#### 5.4.1

#### Общие сведения о подключении Bosch Allegiant

Чтобы установить подключение между BVMS и системой матричных коммутаторов Allegiant, необходимо настроить канал управления между BVMS и матричным коммутатором Allegiant.

Возможны два сценария:

- Локальное подключение  
Management Server управляет коммутатором Allegiant.
- Удаленное соединение  
Специальный ПК Bosch Allegiant, подключенный к сети, контролирует матричный коммутатор Allegiant.

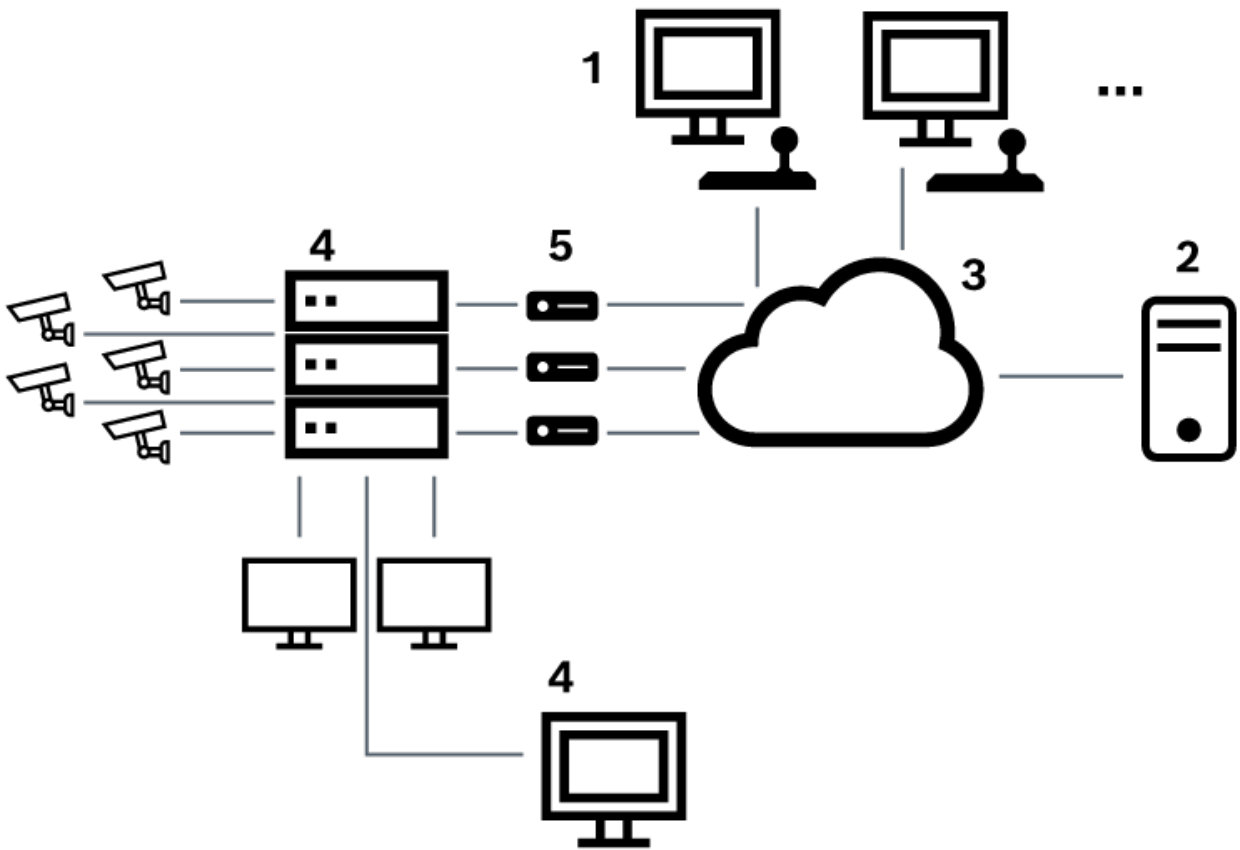


**Рис. 5.3:** Локальное подключение Bosch Video Management System к матричному коммутатору Bosch Allegiant

<b>1</b>	Клиентские рабочие станции BVMS
<b>2</b>	Management Server с ПО Master Control
<b>3</b>	Разъем RS-232
<b>4</b>	Матричный коммутатор Allegiant
<b>5</b>	Кодеры
<b>6</b>	Сеть



**Удаленное соединение**



**Рис. 5.4:** Удаленное подключение Bosch Video Management System к матричному коммутатору Bosch Allegiant

<b>1</b>	Клиентские рабочие станции BVMS
<b>2</b>	Management Server с ПО Master Control
<b>3</b>	Сеть
<b>4</b>	ПК Allegiant с программным обеспечением MCS
<b>5</b>	Разъем RS-232
<b>6</b>	Кодеры
<b>7</b>	Матричный коммутатор Allegiant

**5.4.2 Настройка контрольного канала**

Для настройки контрольного канала следует выполнить следующие действия:

- Подключения
- Установка программного обеспечения
- Создание файла конфигурации Allegiant
- Добавление матричного коммутатора Allegiant к BVMS
- Настройка имен пользователей

### Подключения

Для настройки контрольного канала между BVMS и матричным коммутатором Allegiant подключите один ПК через последовательный порт RS-232 к порту консоли Allegiant (используйте для подключения указанный кабель Bosch). Это может быть BVMS Management Server или любой другой компьютер в сети.

### Установка программного обеспечения Allegiant Master Control Software

1. Остановите службу Management Server, если она запущена (**Пуск > Контрольная панель > Службы > Щелчок правой кнопкой BVMS Management Server > Stop**)
2. Установите Allegiant Master Control Software на Management Server и на ПК Allegiant (при наличии).
3. На удаленном ПК Allegiant настройте запуск программы Allegiant Network Host (Id\_alghw.exe) при загрузке. В результате запускаются необходимые службы Allegiant, позволяющие другим компьютерам в сети получить доступ к Allegiant. Это ПО работает в фоновом режиме. Нет необходимости подключать к компьютеру защитный ключ.  
Чтобы служба запускалась на компьютере автоматически, следует скопировать ссылку на Id\_alghw.exe в папку "Автозагрузка".

### Создание файла конфигурации Bosch Allegiant

1. При помощи ПО Allegiant Master Control Software, создайте файл конфигурации Allegiant, в котором указан компьютер, подключенный к матричному коммутатору Allegiant. Для этого требуется защитный ключ Master Control.
2. В меню Transfer выберите Communication Setup. В списке Current Host введите DNS-имя компьютера, подключенного к матричному коммутатору Allegiant, и введите параметры последовательного порта (номер COM-порта, скорость передачи и т.д.), подключенного к Allegiant. Это позволит ПО Master Control Software на Management Server или ПК соединиться с системой Allegiant. В случае неудачи следует удостовериться, что ПО Master Control Software или программа Allegiant Network Host запущена на компьютере, подключенном к матричному коммутатору Allegiant, а параметры безопасности сети позволяют получить удаленный доступ к этому компьютеру.
3. В меню Transfer выберите пункт Upload. Выделите все таблицы и нажмите Upload. Чтобы сохранить файл конфигурации, выберите каталог.
4. Выйдите из Master Control Software.

### Добавление матричного коммутатора Bosch Allegiant к BVMS

1. Запустите службу BVMSManagement Server, запустите Configuration Client и добавьте устройство Allegiant, добавив файл конфигурации (для получения пошаговых инструкций см. Добавление устройства).
2. Удостоверьтесь, что файл конфигурации Allegiant Master Control Software, используемый в BVMS, соответствует текущей конфигурации Allegiant. BVMS запускает необходимые компоненты ПО Master Control Software в фоновом режиме.

### Настройка имени пользователя для подключения к службам Allegiant

Если матричный коммутатор Allegiant подключен к компьютеру в сети, а не к Management Server, следует удостовериться, что подключение к службам Allegiant на этом компьютере и на Management Server осуществляется с одной и той же учетной записи пользователя. Этот пользователь должен быть членом группы администраторов.

### Более подробные сведения содержатся в документации

Подробные сведения обо всех окнах содержатся в следующих разделах:

- Страница Матричные коммутаторы, Страница 135
- Пошаговые инструкции содержатся в следующих разделах:
- Настройка устройства Bosch Allegiant, Страница 136

**См.**

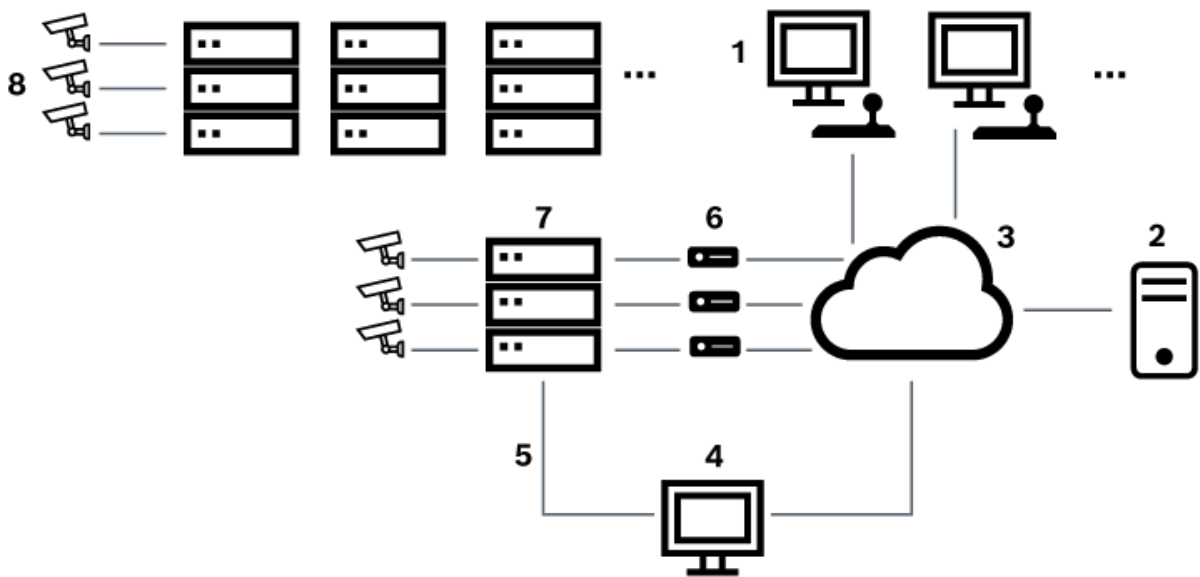
- Страница Матричные коммутаторы, Страница 135

### 5.4.3

#### Понятие о сателлитной конфигурации Allegiant компании Bosch

Матричные коммутаторы Allegiant позволяют объединить несколько систем Allegiant при помощи сателлитной конфигурации. В этом случае система BVMS рассматривает несколько систем Allegiant как одну большую систему, что обеспечивает доступ ко всем камерам во всех системах.

В сателлитной системе Allegiant выходы мониторов подчиненной системы Allegiant связаны с видеовходами главной системы Allegiant. Такое соединение называют магистральной линией. Кроме того, между главной и подчиненной системами устанавливается контрольный канал. При запросе камеры из подчиненной системы Allegiant главной системой Allegiant, в подчиненную систему отправляется команда, требующая перевести запрашиваемую камеру на магистральную линию. В это же время главная система Allegiant переключает вход магистральной линии на запрашиваемый выход монитора главной системы Allegiant. На этом видеоподключение подчиненной камеры к главному монитору завершается.



**Рис. 5.5:** Система Bosch Allegiant, расширенная за счет сателлитных коммутаторов

1	Клиентские рабочие станции BVMS
2	Management Server с ПО Master Control
3	Сеть
4	ПК Allegiant с программным обеспечением MCS
5	Разъем RS-232
6	Кодеры
7	Матричный коммутатор Allegiant

<b>8</b>	Сателлитный матричный коммутатор Allegiant
----------	--

Сателлитная концепция может быть применена таким образом, что система Allegiant может быть одновременно главной и подчиненной. Таким образом, каждая система Allegiant может просматривать камеры с других систем. Необходимо только подключить магистральные и контрольные линии в обоих направлениях и правильно сконфигурировать таблицы Allegiant.

Эта концепция может расширяться практически безгранично. Система Allegiant может иметь множество подчиненных систем и сама может быть подчиненной по отношению ко многим главным. Вы можете запрограммировать таблицы Allegiant таким образом, чтобы разрешить или запретить пользователям доступ к камерам в соответствии с требованиями конкретного участка.

## 5.5 Команды Allegiant CCL, поддерживаемые в системе BVMS

Чтобы использовать команды CCL, вам потребуется руководство пользователя CCL.

Данное руководство доступно в онлайн-каталоге продукции в разделе документации для каждого матричного коммутатора Allegiant LTC.

Поддерживаемые команды	Описание	Примечания
<b>Переключение/ последовательность</b>		
LCM	Переключение логической камеры на монитор	LCM, LCM+ и LCM-эквивалентны.
LCMP	Переключение логической камеры на монитор с вызовом препозиций	
MON+CAM	Переключение физической камеры на монитор	
MON-RUN	Запуск последовательности по номеру монитора	
MON-HOLD	Удержание последовательности по номеру монитора	
SEQ-REQ	Запрос последовательности	
SEQ-ULD	Выгрузка последовательности	
<b>Приемное/ исполнительное устройство</b>		

Поддерживаемые команды	Описание	Примечания
<b>Переключение/ последовательность</b>		
R/D	Основные команды управления	
REMOTE-ACTION	Одновременная команды управления панорамированием/ наклоном/ масштабированием	
REMOTE-TGL	Переключить команды управления панорамированием/ наклоном/ масштабированием	
PREPOS-SET	Установить препозицию	
PREPOS	Вызов препозиции	
AUX-ON AUX-OFF	Вспомогательные команды управления – Вспомогательные команды активированы – Вспомогательные команды деактивированы	
VARSPPEED_PTZ	Команды управления переменной скоростью	
<b>Тревога</b>		Используется для управления виртуальными входами. Например, «+тревога 1» закрывает виртуальный вход 1, «-тревога 1» открывает виртуальный вход 1
+ALARM	Активировать тревогу	Открывает виртуальный вход в BVMS.
-ALARM	Деактивировать тревогу	Закрывает виртуальный вход в BVMS.
<b>Система</b>		
TC8x00>HEX	Установить шестнадцатеричный режим	

<b>Поддерживаемые команды</b>	<b>Описание</b>	<b>Примечания</b>
<b>Переключение/ последовательность</b>		
TC8x00>DECIMAL	Установить десятичный режим	

## 6 Начало работы

В данном разделе содержится информация о том, как приступить к работе с BVMS.

### 6.1 Установка программных модулей



#### Замечание!

Не устанавливайте веб-клиент DiVos ни на какой компьютер BVMS.  
Установите на компьютер все необходимые модули программного обеспечения.

#### Установка

Закройте Configuration Client, прежде чем запустить установку BVMS.

1. запустите Setup.exe или запустите программу установки BVMS на экране приветствия.
2. В следующем диалоговом окне выберите модули, которые должны быть установлены на данном компьютере.
3. Следуйте инструкциям на экране.

### 6.2 Использование мастера настройки конфигурации

Config Wizard предназначен для простой и быстрой настройки небольших систем. Config Wizard помогает настроить конфигурацию системы, включая VRM, систему iSCSI, Mobile Video Service, камеры, профили записи и группы пользователей.

При стандартной установке программного обеспечения системы iSCSI необходимо добавлять вручную.

Группы пользователей и их разрешения настраиваются автоматически. Можно добавлять или удалять пользователей и задавать пароли.

Config Wizard может получить доступ к Management Server только на локальном компьютере.

Активированную конфигурацию можно сохранить в качестве резервной копии и импортировать эту конфигурацию позднее. После импорта импортированную конфигурацию можно изменить.

Config Wizard добавляет локальный VRM автоматически как при стандартной установке ПО, так и в случае DIVAR IP 3000 и DIVAR IP 7000.

В случае DIVAR IP 3000 и DIVAR IP 7000 локальное устройство iSCSI также добавляется автоматически, если оно еще не доступно.

В случае DIVAR IP 3000 и DIVAR IP 7000 локальная служба Mobile Video Service добавляется автоматически, если она еще не доступна.



#### Замечание!

Если в системе необходимо использовать декодеры, убедитесь, что все кодеры используют один и тот же пароль для уровня авторизации user.

#### Для запуска Config Wizard:

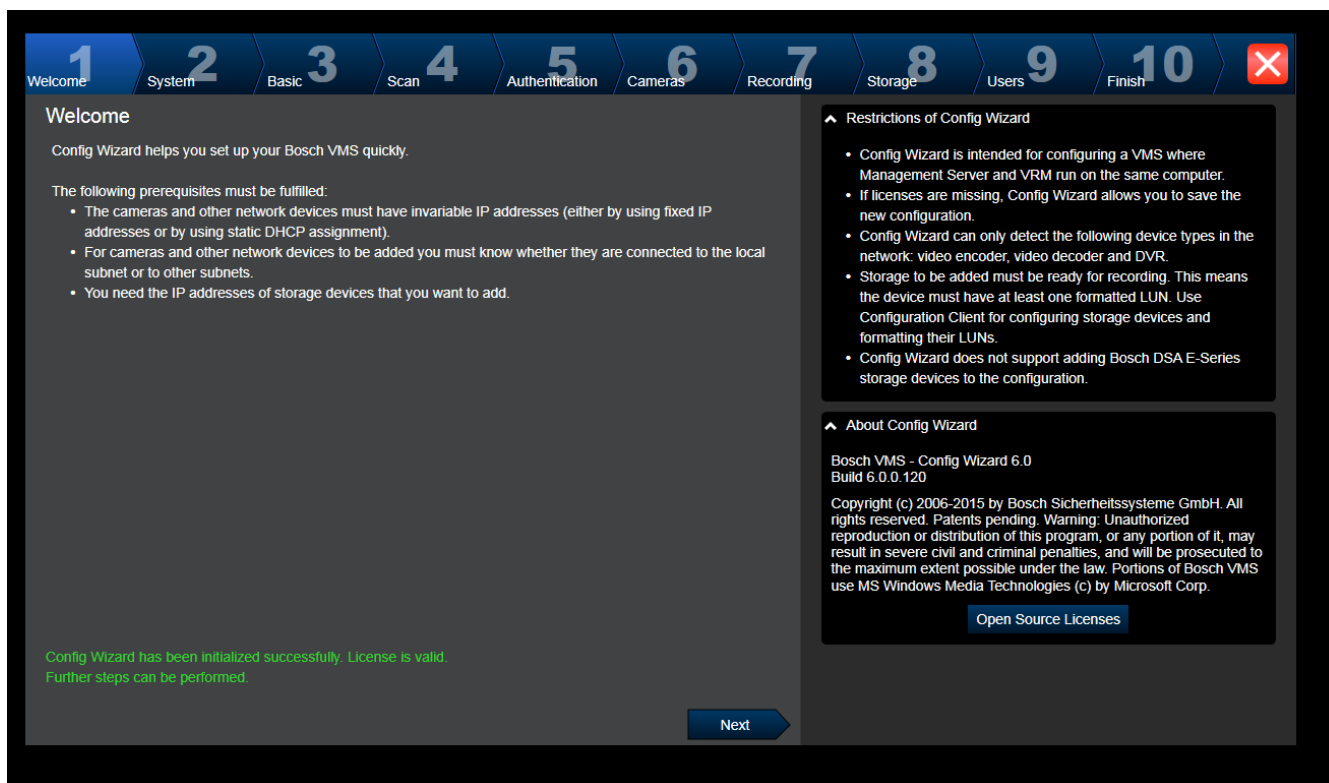
- ▶ нажмите **Пуск > Все программы > BVMS > Config Wizard**  
Откроется страница Welcome.

#### Доступные страницы

- *Страница Welcome, Страница 64*
- *Страница System, Страница 65*
- *Страница Basic, Страница 66*
- *Страница Scan, Страница 67*
- *Страница Authentication, Страница 68*

- Страница *Cameras*, Страница 69
- Страница *Recording*, Страница 69
- Страница *Storage*, Страница 70
- Страница *Users*, Страница 70
- Страница *Finish*, Страница 71

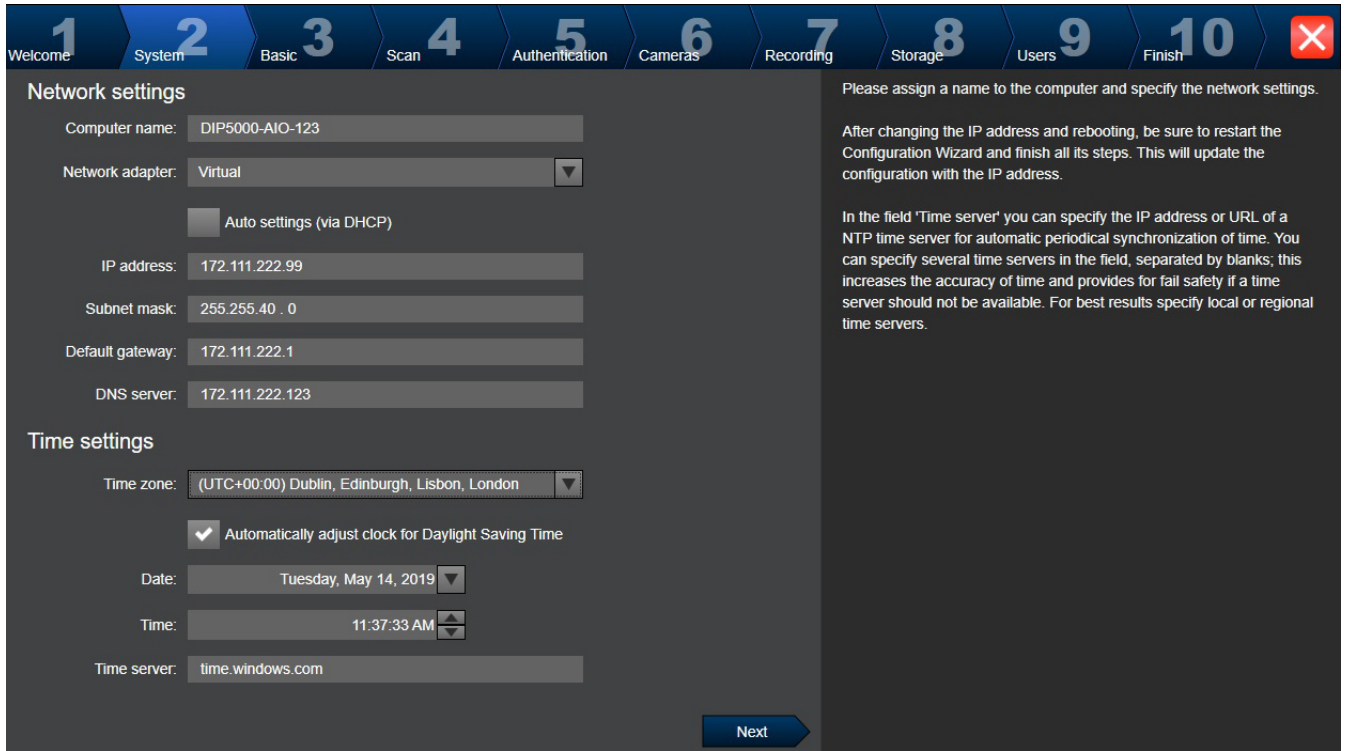
### Страница **Welcome**



- ▶ Нажмите **Next**, чтобы продолжить.



### Страница System



**Замечание!**

Доступно только для DIVAR IP 3000, DIVAR IP 7000, DIVAR IP all-in-one 5000, DIVAR IP all-in-one 6000 и DIVAR IP all-in-one 7000

Вы настраиваете сетевые параметры операционной системы.  
Вы настраиваете параметры времени операционной системы.

**Примечание.**

Настоятельно рекомендуем задать в среде видеонаблюдения сервер времени.  
После нажатия кнопки **Next** эти параметры активируются.

## Страница Basic

**Latest saved configuration**  
Devices and services included in the latest saved configuration

Network address	Device type	Recording Profile	Recorder
172.31.22.244	Dinion IP starlight 8000	Dauer-, Alarmaufzeichnung	VRM(172.30.11.54)
https://172.30.11.54/mv	Mobile Video Service		
172.30.11.54	VRM		
172.30.11.54	VRM Storage		

The active configuration is identical with the latest saved configuration.  
Video Recording Manager (VRM) service is found and is running.

Please select the network adapter for your local video network:  
LAN-Verbindung (Type: Ethernet; IPv4-Address: 172.30.11.54)

**Next**

**Import configuration**  
You can import an existing configuration. The imported configuration is saved immediately as a change to the local configuration. Import is only possible when the active configuration is identical with the latest saved configuration.  
Changes on the following pages are only saved and activated if you click the corresponding button on the last page of Configuration Wizard.  
**Import configuration ...**  
Changes on the following pages are only saved and activated if you apply them on the last page.

**Port Mapping**  
 Enable Port Mapping  
Remote access  
Port mapping allows a remote Operator Client to access the local VMS and its network devices via a single public IP address.  
Enter/change public network address:

На этой странице отображается последняя сохраненная конфигурация. Можно импортировать файл BVMS в качестве изменения для имеющейся конфигурации. Это изменение сохраняется, но не активируется при нажатии **Next**.

Можно выбрать сетевой адаптер своего компьютера, подключенного к видеоустройствам (IP-камеры, кодеры, декодеры, системы хранения iSCSI) системы. IP-адрес этого сетевого адаптера используется как IP-адрес системы VRM, VSG и локальной системы хранения iSCSI.

Нажмите **Port Mapping**, чтобы задать внешний IP-адрес или DNS-имя, если будет производиться доступ к системе через Интернет.

### Страница Scan

1 Welcome 2 System 3 Basic 4 Scan 5 Authentication 6 Cameras 7 Recording 8 Storage 9 Users 10 Finish

**Select video devices to be added** Selected 5 of 297

✓	Device name	IP address	MAC address	Device type
<input type="checkbox"/>	(172.31.22.235)	172.31.22.235	00-07-5f-72-0e-56	VIP X1600
<input type="checkbox"/>	VIP X16 XF E (CPP5)	172.31.22.232	00-07-5f-7e-90-af	VIP X16 XF E
<input type="checkbox"/>	VIP X1 XF IVA (172.31.22.231)	172.31.22.231	00-07-5f-75-a8-7f	VIP X1XF
<input checked="" type="checkbox"/>	DINION IP 7000 HD (172.31.22.230)	172.31.22.230	00-04-63-3f-0f-99	Dinion HD NBN-832VxP
<input type="checkbox"/>	NBC-255-P (172.31.22.229)	172.31.22.229	00-07-5f-74-99-2f	NBC-255-P
<input checked="" type="checkbox"/>	DINION IP bullet 5000 HD (172.31.22.228)	172.31.22.228	00-07-5f-7b-23-f9	IP bullet 5000 HD
<input type="checkbox"/>	FLEXIDOME NDN-921-P (172.31.22.226)	172.31.22.226	00-04-63-36-78-04	FlexiDome NDN-921-P
<input checked="" type="checkbox"/>	NDC-225-PI (172.31.22.225)	172.31.22.225	00-07-5f-74-b9-45	NDC-225-PI
<input type="checkbox"/>	VIP-X1600-XFM4 (172.31.22.224)	172.31.22.224	00-07-5f-74-ef-f1	VIP X1600 XFM4
<input type="checkbox"/>	VIP-X1600-XFM4 (172.31.22.223)	172.31.22.223	00-07-5f-75-40-6a	VIP X1600 XFM4
<input checked="" type="checkbox"/>	VIP-X1600-XFM4 (172.31.22.222)	172.31.22.222	00-07-5f-75-40-9a	VIP X1600 XFM4
<input type="checkbox"/>	(172.31.22.221)	172.31.22.221	00-07-5f-72-0e-71	VIP X1600
<input checked="" type="checkbox"/>	VIP-X1600-XFM4 (172.31.22.220)	172.31.22.220	00-07-5f-75-3d-29	VIP X1600 XFM4
<input type="checkbox"/>	FLEXIDOME IP corner 9000 M (172.31.22.216)	172.31.22.216	00-07-5f-7b-01-73	FlexiDome IP corner 9000 M
<input type="checkbox"/>	AUTODOME Jr 800 HD (172.31.22.215)	172.31.22.215	00-04-63-36-65-16	AutoDome Junior HD
<input type="checkbox"/>	FLEXIDOME IP panorami (172.31.22.214)	172.31.22.214	00-07-5f-88-76-44	FlexiDome panorama 5000 M

Next

You can select devices to be added to the configuration. The list contains all devices found by the network scan except the devices that are already contained in the configuration. Deselect the devices that should not be added.

**Scan options**

Range of network scan:

- Local subnet only (recommended)
- Across subnets

Rescan network

**Change network addresses**

Change the IP addresses of the selected encoders/decoders. Start with the following IP address:

Change IP Addresses

**Примечание.**

Поиск устройств может занять некоторое время. Поиск можно отменить. Все уже найденные устройства будут отображены в таблице.

На этой странице отображаются все видеоустройства, не включенные в последнюю сохраненную конфигурацию.

Снимите флажки для тех устройств, которые не должны быть добавлены в конфигурацию, а затем нажмите **Next**.

Если выбранное устройство находится в диапазоне IP-адресов, отличном от диапазона системы DIVAR IP, IP-адрес устройства можно изменить, задав начальный адрес диапазона IP-адресов устройства.

## Страница Authentication

**Enter passwords for devices**

Device name	IP address	User name	Password	Status
172.31.23.150	172.31.23.150	service		⚠
Decoder (172.31.21.204)	172.31.21.204	service	.....	🔒
NDC-284-P (172.31.23.15)	172.31.23.15	service		🔒
VIP10 (172.31.23.24)	172.31.23.24	service		🔒
VIPX-1600XFMD (172.31.22.4)	172.31.22.4	service		🔒
VIPX-1600XFMD (172.31.22.5)	172.31.22.5	service		🔒

You must authenticate at the devices of your system. To authenticate, enter the password for the user account of each device. An open green lock indicates a successful authentication. Devices with a status indicated by a yellow warning sign require an initial password; they do not allow logon with an empty password.

You can only click 'Next' to continue, when all locks are green.

To copy a password for authentication select a row with a shown password and press Ctrl + C. Then select the rows of the devices for which the copied password should be used. To paste the password press Ctrl + V.


▼ Change default password

Show passwords      Set Initial Passwords      Next

Эта страница используется для проверки подлинности всех видеоприборов, защищенных паролем. Для облегчения проверки подлинности с помощью одного пароля для нескольких устройств можно использовать буфер обмена (CTRL+C, CTRL+V).

1. Нажмите, чтобы включить **Show passwords**.
2. Выберите строку с успешно прошедшим проверку подлинности устройством (отображается зеленый замок), нажмите CTRL+C, выберите несколько строк с красным замком и нажмите CTRL+V).

Проверка пароля выполняется автоматически, если следующий символ в поле пароля не вводится в течение нескольких секунд или кнопка мыши нажимается вне поля пароля. Можно установить глобальный пароль по умолчанию для всех устройств, которые в данный момент не защищены паролем.

Если для устройства требуется начальный пароль, отображается .

**Для установки начального пароля:**

1. Введите пароль в поле **Password**.
2. Нажмите **Set Initial Passwords**.  
Установлен первоначальный пароль.

**Примечание:** пока вы не установили первоначальный пароль для всех устройств в списке, которые требуют начального пароля, вы не сможете продолжить работу.

3. Нажмите **Next**, чтобы продолжить.

### Страница Cameras

**Specify camera settings**

Camera name	IP address	Recording quality	Live quality
Camera 1 (172.31.22.227)	172.31.22.227	Bit Rate Optimized	Balanced
Camera 1 (172.31.22.229)	172.31.22.229	Bit Rate Optimized	Balanced

You can rename each camera in the 'Camera name' column.

You can configure recording quality and live quality for each camera. Fractional frame rates (FR) are indicated by the profile names and refer to the fraction of the maximum frame rate of the corresponding camera model.

You can change the settings of the 'Recording quality' and the 'Live quality' columns of multiple cameras simultaneously. To that end select those cameras and change the settings in one of the selected cameras. If the settings in a column are not identical for all selected cameras, you can click '<no change>' to avoid changing these settings unintentionally.

In the Preview pane, you can see a still image of the selected camera.

**Preview**

Camera 1 (172.31.22.227)

19. Feb 2016 14:31:38

Camera 1 (172.31.22.227)

Next

Эта страница используется для управления камерами системы.

### Страница Recording

**Specify recording settings**

Selected 0 of 2

Device name	IP address	Recording profile	Storage Min Time (days)	Storage Max Time (days)
VIP X1 (172.31.22.227)	172.31.22.227	Continuous, Alarm Re	1	unlimited
NBC-255-P (172.31.22.229)	172.31.22.229	Continuous, Alarm Re	1	unlimited

Alarm Recording  
 Alarm Recording Night and Weekend  
 Continuous Only  
 Continuous Only Night and Weekend  
 Continuous, Alarm Recording  
 No Recording

You can specify the recording profile and how long you want to store the recordings.

You can change the settings for several cameras in parallel. To that end select those cameras and change the settings in one of the selected cameras. If the settings in a column are not identical for all selected cameras, you can click '<no change>' to avoid changing these settings unintentionally.

Cameras recorded by DVR devices are not shown, because the recording settings for these cameras can only be set using the configuration application of the DVR device.

**Motion Alarm Recording in Recording Profiles**

Recording profile	Motion Triggered Alarm Recording
Alarm Recording	<input type="checkbox"/>
Alarm Recording Night and Weekend	<input type="checkbox"/>
Continuous Only	<input type="checkbox"/>
Continuous Only Night and Weekend	<input type="checkbox"/>
Continuous, Alarm Recording	<input checked="" type="checkbox"/>
No Recording	<input type="checkbox"/>

Next

На этой странице отображаются только новые добавленные камеры. После включения этой конфигурации невозможно изменить назначение профилей этих камер.

Можно включить запись по движению для профилей записи, для которых включена как запись, так и запись по тревоге. При необходимости настройте запись и запись по тревоге в Configuration Client (диалоговое окно **Настройки записи по расписанию**).

VCA активируется автоматически для всех новых добавляемых камер.

### Страница Storage

**Add storage**

You can add iSCSI storage devices currently available in the network for storing video recordings. More storage space allows longer storage of the video recordings.

Internal storage is already present in configuration.

Next

На этой странице можно добавлять дополнительные устройства хранения iSCSI

### Страница Users

**User accounts and passwords**

You can specify the names and passwords of users in predefined groups, and you can add further users to the predefined groups.

Different user groups have different permissions. These permissions define the operations allowed for users in this user group. You can add user groups and change permissions using Configuration Client.

For each user, you can enable a strong password policy. The following rules apply:

- Minimum 8 characters
- At least one upper-case letter (A through Z)
- At least one number (0 through 9)
- At least one special character (for example: ! \$ # %)
- Previous password must not be used.

The password is not set for some of the users, while strong password policy is applied for them.

Next

На этой странице можно добавить новых пользователей в существующие пользовательские группы.

- ▶ Введите имя пользователя и описание для каждого нового пользователя и задайте пароль.

### Strong password policy

Флажок **Strong password policy** предварительно установлен для всех вновь созданных пользовательских групп.

Мы настоятельно рекомендуем сохранить этот параметр в целях обеспечения защиты вашего компьютера от несанкционированного доступа.

Применяются следующие правила:

- Минимальная длина пароля соответствует указанной на странице **Политики учетных записей** для соответствующих групп пользователей.
- Не используйте один из предыдущих паролей.
- Используйте по крайней мере одну букву в верхнем регистре (A–Z).
- Используйте по крайней мере одну цифру (0–9).
- Используйте по крайней мере один специальный символ (например, ! \$ # %).
- ▶ Нажмите кнопку **Apply**, чтобы применить параметры, затем нажмите **Next** для продолжения.

**Примечание:** вы не сможете продолжить работу до тех пор, пока для всех пользователей, для которых установлен флажок **Strong password policy**, не будут заданы пароли. Чтобы продолжить, задайте недостающие пароли.

Используйте Configuration Client для добавления групп пользователей и изменения разрешений групп пользователей.

### Страница Finish

The screenshot shows the 'Finish' step of the configuration wizard. The progress bar at the top indicates steps 1 through 10, with 'Finish' being the current step. The main content area is titled 'Activate Configuration' and lists the settings for the new configuration: 1 Video Recording Manager(s) (VRM), 1 iSCSI Storage device(s) for video recordings, 1 Encoder(s) with 4 camera channels, 2 User group(s) with 1 user account(s), and 1 Mobile Video Service(s). There is a 'Details' button below this list. On the right side, there are two sections: 'Backup configuration' with a 'Save backup copy' button, and 'Licensing' which shows an active license for 'DIVAR IP Professional Editio' with a status of 'Activation valid'. A 'License Wizard' button is also present. At the bottom right, there is a large green 'Save and activate' button.

Прежде чем активировать конфигурацию, необходимо выполнить следующие действия:

- Установить глобальный пароль по умолчанию для всех устройств, которые в данный момент не защищены паролем.
- При необходимости активировать лицензию.

**Глобальный пароль по умолч.**

Если в клиенте Configuration Client отключен параметр **Принудительная защита паролем при активации (Параметры -> Параметры)**, для активации не обязательно предоставлять глобальный пароль по умолчанию.

**Лицензирование**

Разверните пункт **Licensing** и нажмите кнопку **License Wizard**, чтобы проверить или активировать пакет лицензий.

После нажатия кнопки **Save and activate** конфигурация активируется.

После успешной активации снова открывается страница **Finish**. Теперь при желании можно сохранить резервную копию данной конфигурации; для этого нажмите **Save backup copy**.

После нажатия кнопки **Save and activate** конфигурация активируется.

После успешной активации снова открывается страница **Готово**. Теперь при желании можно сохранить резервную копию данной конфигурации; для этого нажмите **Save backup copy**.

## 6.3 Запуск Configuration Client

**Замечание!**

Только пользователи группы администраторов могут подключиться к Configuration Client.

Предварительно настроенный пользователь группы администраторов по умолчанию — Admin. Только этот пользователь может подключиться к Configuration Client при первом запуске Configuration Client.

После запуска Configuration Client можно переименовать пользователя Admin и изменить пароль.

**Примечание.**

Невозможно запустить Configuration Client, если другой пользователь на другом компьютере в системе уже запустил модуль Configuration Client.

**Запуск Configuration Client**

1. В меню **Пуск** выберите **Программы > BVMS > Configuration Client**.  
Отобразится диалоговое окно для входа в систему.
2. Введите свое имя пользователя в поле **Имя пользователя:**.  
При первом запуске приложения введите в качестве имени пользователя Admin, пароль при этом не требуется.
3. Введите пароль в поле **Пароль:**.
4. Нажмите **ОК**.  
Приложение запустится.

При первом запуске пользователем Admin Configuration Client отображается диалоговое окно **Нарушена политика паролей** с предложением установить пароль для учетной записи администратора. Мы настоятельно рекомендуем сохранить этот параметр и задать надежный пароль для учетной записи Admin в соответствии с требованиями политики паролей.

**См.**

- *Строгая политика паролей*, Страница 364
- *Настройка группы администраторов*, Страница 370



## 6.4 Настройка языка Configuration Client

Настройка языка Configuration Client не зависит от языковых настроек Windows.




### Чтобы настроить язык:

1. В меню **Настройки** выберите пункт **Параметры...**  
Откроется диалоговое окно **Параметры**.
2. В списке **Язык** выберите нужный язык.  
При выборе **Системный язык** используется язык, настроенный в Windows.
3. Нажмите **ОК**.  
Языковые настройки вступают в силу после перезапуска приложения.

## 6.5 Настройка языка Operator Client

Настройка языка Operator Client не зависит от языковых настроек Windows и настроек модуля Configuration Client. Это действие выполняется в модуле Configuration Client.

### Чтобы настроить язык:

1. Нажмите **Группы пользователей** > . Перейдите на вкладку **Свойства пользовательской группы**. Перейдите на вкладку **Рабочие разрешения**.
2. В списке **Язык** выберите нужный язык.
3. Нажмите , чтобы сохранить настройки.
4. Нажмите  для активации конфигурации.  
Перезапуск Operator Client.

## 6.6 Поиск устройств



Главное окно > **Устройства**

Можно выполнять поиск следующих устройств для добавления с помощью диалогового окна **BVMS Scan Wizard**:

- Устройства VRM
- Кодеры
- Кодеры с локальным хранилищем и работающие только в режиме реального времени
- Кодеры ONVIF, работающие только в режиме реального времени
- Кодеры с локальными хранилищами
- Декодеры
- Устройства шлюза Video Streaming Gateway (VSG)
- Устройства DVR
- Устройства NVR VIDOS

Сведения о добавлении устройств путем поиска см. в разделе о соответствующем устройстве в главе *Страница Устройства, Страница 122*.

### См.

- *Добавление устройств VRM путем поиска, Страница 178*
- *Добавление устройства ONVIF, работающего только в режиме реального времени, путем сканирования, Страница 244*
- *Добавление устройств, работающих только в режиме реального времени, путем поиска, Страница 219*

- *Добавление устройства, Страница 124*

## 6.7 Доступ к системе

Для доступа к системе выполните следующие действия:

1. Выполните одно из следующих действий для выбора сетевого адреса нужной системы:
  - Нажмите заранее выбранный элемент списка.
  - Введите сетевой адрес вручную.
  - Выберите сетевой адрес с помощью Server Lookup.
2. Вход в нужную систему:
  - Система с одним сервером
  - Система Enterprise

## 6.8 Использование просмотра сервера

- Функция BVMS Server Lookup позволяет операторам подключаться к BVMSManagement Server из доступного списка серверов.
- Один пользователь Configuration Client или Operator Client может последовательно подключаться к нескольким системным точкам доступа.
- Системные точки доступа могут быть Management Server или Enterprise Management Server.
- Server Lookup использует специальный Management Server для размещения списка серверов.
- Функции Server Lookup и Management Server или Enterprise Management Server могут быть запущены на одном компьютере.
- Server Lookup поддерживает поиск системных точек доступа по имени или описанию.
- Operator Client, подключенный к Management Server, принимает события и тревоги с BVMS Management Server и отображает данные в режиме реального времени и воспроизведения записей.

### Доступ:

1. Запустите клиент Operator Client или Configuration Client.  
Откроется диалоговое окно входа в систему.
2. В списке **Соединение:** выберите пункт **<Адресная книга...>** для Configuration Client или **<Адресная книга...>** для Operator Client.  
Если для сервера задан внутренний и внешний IP-адреса, они будут указаны.  
При первом выборе **<Адресная книга...>** или **<Адресная книга...>** откроется диалоговое окно **Server Lookup**.
3. Введите допустимый сетевой адрес необходимого сервера в поле **Адрес (Enterprise) Management Server:**.
4. Введите допустимые имя пользователя и пароль.
5. При необходимости нажмите пункт **Запомнить параметры**.
6. Нажмите **ОК**.  
Откроется диалоговое окно **Server Lookup**.
7. Выберите необходимый сервер.
8. Нажмите **ОК**.
9. Если у выбранного сервера есть и внутренний, и внешний сетевые адреса, появится сообщение, спрашивающее, используете ли вы компьютер, расположенный во внутренней сети выбранного сервера.  
Имя сервера добавляется в список **Соединение:** в диалоговом окне входа.

10. Выберите этот сервер в списке **Соединение:** и нажмите кнопку **ОК**.  
Если вы установили флажок **Запомнить параметры**, при следующем доступе этот сервер можно выбрать напрямую.

## 6.9 Настройка удаленного доступа

Можно настроить удаленный доступ для одной системы без системы Enterprise или для Enterprise System.

### 6.9.1 Удаленный доступ



#### **Замечание!**

Для предотвращения несанкционированного доступа к видеоданным через Интернет настоятельно рекомендуется использовать защиту всех пользователей и устройств системы с помощью пароля.

Обеспечьте защиту всех уровней камеры/кодера (service/user/live) паролем.

#### **Дополнительная информация по изменению паролей**

- Страница *Свойства пользователей*, Страница 342
- Изменение пароля кодера / декодера
- *Изменение пароля устройства VRM*, Страница 184

Цель удаленного доступа в BVMS заключается в подключении различных частных сетей к общедоступным сетям.

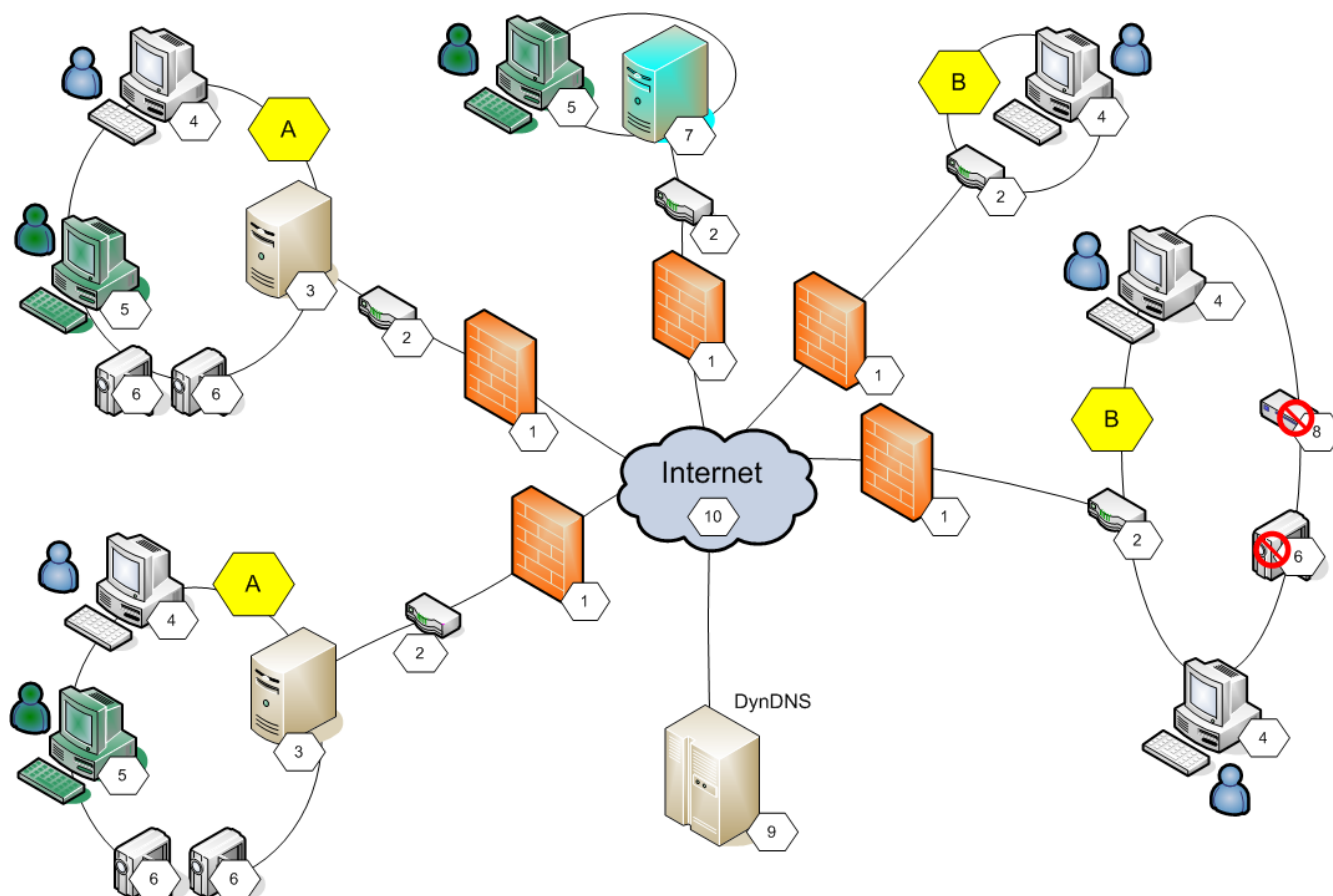
Компьютеры Operator Client могут получать доступ к нескольким сетям с частными (локальными) адресами одновременно или последовательно через открытые интерфейсы (маршрутизаторы). Задача маршрутизатора — перевести входящий общедоступный сетевой трафик на соответствующий частный сетевой адрес.

Пользователи Operator Client могут получить удаленный доступ к Management Server или Enterprise Management Server и их устройствам.

Невозможно получить удаленный доступ к следующим устройствам/функциям:

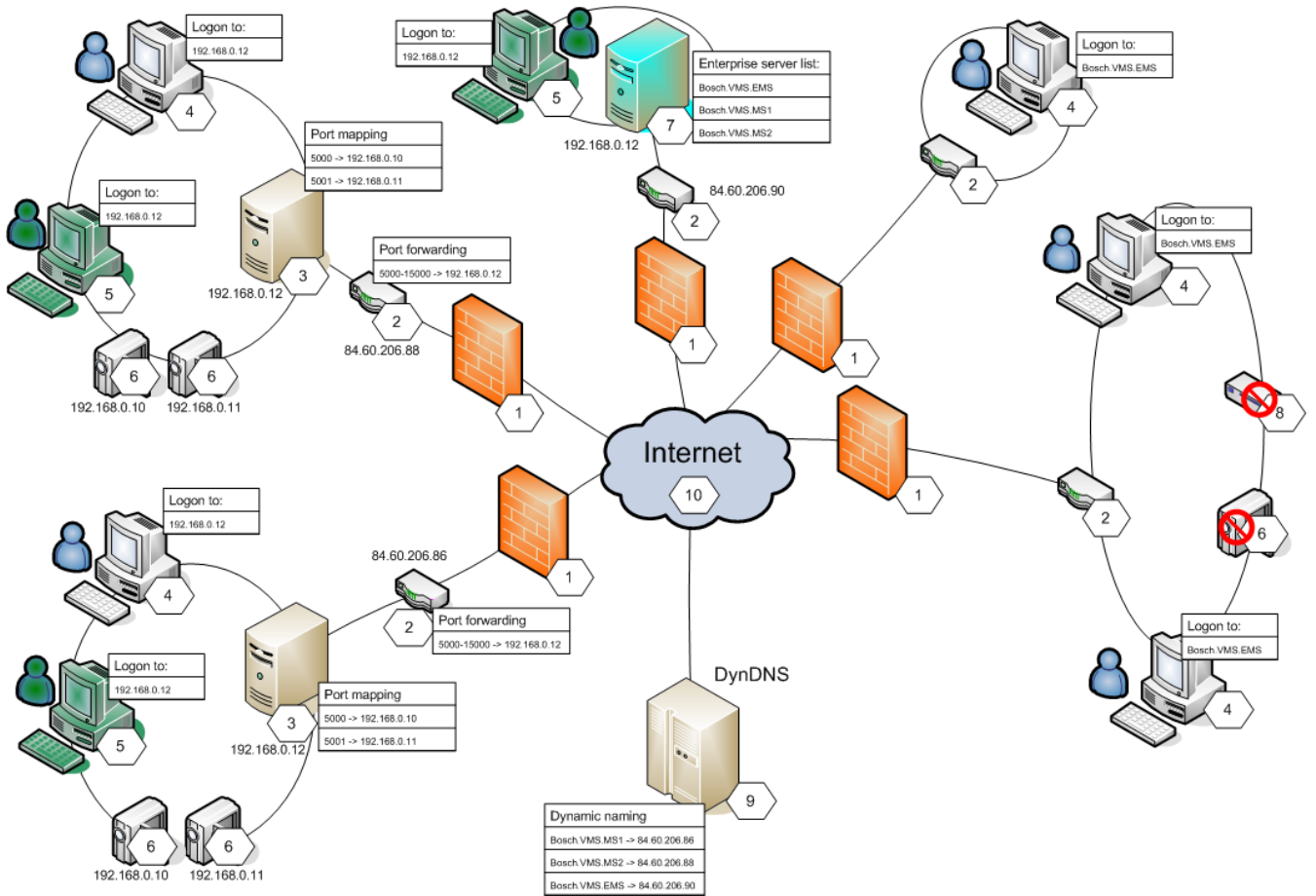
- Воспроизведение локального хранилища
- ONVIF
- DiBos
- Прямое воспроизведение ISCSI

На следующем изображении показан пример удаленного доступа к устройствам BVMS в одной системе:



<b>1</b>	Брандмауэр	<b>6</b>	IP-камера / кодер
<b>2</b>	Маршрутизатор	<b>7</b>	Enterprise Management Server
<b>3</b>	Management Server	<b>8</b>	Декодер
<b>4</b>	Operator Client	<b>9</b>	Сервер DynDNS
<b>5</b>	Configuration Client	<b>10</b>	World Wide Web
<b>A</b>	Удаленная сеть	<b>B</b>	Локальная сеть

На следующем изображении показан пример удаленного доступа из частной сети с Enterprise System к удаленным системам BVMS:



<b>1</b>	Брандмауэр	<b>6</b>	IP-камера / кодер
<b>2</b>	Маршрутизатор Переадресация портов	<b>7</b>	Enterprise Management Server Список корпоративных серверов
<b>3</b>	Management Server Сопоставление портов	<b>8</b>	Декодер
<b>4</b>	Operator Client Вход в	<b>9</b>	Сервер DynDNS Динамическое именование
<b>5</b>	Configuration Client Вход в	<b>10</b>	World Wide Web

Чтобы разрешить удаленный доступ Operator Client к устройствам в удаленной сети, каждому устройству назначается номер общедоступного порта в дополнение к общедоступному сетевому адресу маршрутизатора. Для доступа Operator Client использует этот номер общедоступного порта вместе с общедоступным сетевым адресом. В частной сети входящий трафик для данного номера общедоступного порта пересылается на адрес частной сети и номер порта соответствующего устройства. В Configuration Client настраивается сопоставление портов для использования в Operator Client.

**Замечание!**

Дополнительно сетевой администратор на маршрутизаторе частной сети должен настроить переадресацию портов. Сетевой администратор должен убедиться, что удаленный доступ через эти порты выполняется за пределами среды BVMS.

**См.**

- *Диалоговое окно «Параметры удаленного доступа» (меню «Настройки»), Страница 120*
- *Диалоговое окно «Таблица распределения портов», Страница 121*

**6.9.2****Настройка без корпоративной системы****Для настройки:**

1. Настройте параметры удаленного доступа в диалоговом окне **Параметры удаленного доступа**.
2. Настройте маршрутизатор.

**Дополнительная информация**

- *Диалоговое окно «Параметры удаленного доступа» (меню «Настройки»), Страница 120*

**6.9.3****Настройка с помощью корпоративной системы****Для настройки:**

1. Настройте список серверов.
2. Настройте Enterprise User Groups и Enterprise Accounts.
3. Настройте параметры удаленного доступа в диалоговом окне **Параметры удаленного доступа**.
4. Настройте маршрутизатор.

**Дополнительная информация**

- *Настройка списка серверов для корпоративной системы, Страница 89*
- *Создание группы или учетной записи, Страница 365*
- *Диалоговое окно «Параметры удаленного доступа» (меню «Настройки»), Страница 120*

**6.10****Активация лицензии на программное обеспечение**

При установке BVMS в первый раз, необходимо активировать лицензии на программные пакеты, которые вы заказали, включая базовый пакет и все расширения и/или дополнительные возможности.

**Необходимые условия**

- Номер авторизации, полученный от компании Bosch
- Компьютер с доступом в Интернет
- Учетная запись для Bosch Security Systems Software License Manager

**Процедура**

Для активации лицензии на программное обеспечение необходимо выполнить следующие действия.

1. *Получение цифровой подписи компьютера, Страница 79*
2. *Получение ключа активации, Страница 80*
3. *Активация системы, Страница 80*

**См.**

- *Диалоговое окно «Диспетчер лицензий» (меню «Инструменты»), Страница 114*

### 6.10.1 Скачать информационный файл Bundle Information

При заказе пакетов ПО BVMS, расширений и дополнительных функций компания Bosch пришлет вам номер авторизации и, как правило, файл пакета в формате XML, содержащий все лицензии на все пакеты, расширения и параметры, которые вы заказали. Информационный файл Bundle Information облегчает процесс активации лицензий ПО. Если не вы получили информационный файл Bundle Information от компании Bosch, вы можете скачать его из Bosch Security Systems Software License Manager.

#### Чтобы скачать файл Bundle Information:

1. На компьютере с доступом в Интернет введите следующий URL-адрес в строке обозревателя:  
https://activation.boschsecurity.com.
2. Войдите в Bosch Security Systems Software License Manager.  
Если у вас еще нет учетной записи, создайте новую.
3. Нажмите Download Bundle File.  
Откроется диалоговое окно Download Original Bundle File.
4. В поле Authorization Number введите номер авторизации, полученный вами от Bosch и нажмите кнопку Submit.
5. Сохраните информационный файл Bundle Information.

### 6.10.2 Получение цифровой подписи компьютера

#### Для получения цифровой подписи компьютера:

1. запустите BVMS Configuration Client.
2. В меню **Сервис** выберите пункт **Диспетчер лицензий...**  
Откроется диалоговое окно **Диспетчер лицензий**.
3. Установите флажки напротив программного обеспечения, функций и расширений, которые следует активировать. Для расширений введите количество лицензий.  
Или  
если вы получили информационный файл Bundle Information от Bosch, нажмите **Импортировать пакетную информацию**, чтобы импортировать его.  
Если не вы получили информационный файл Bundle Information, скачайте его из Bosch Security Systems Software License Manager, см. *Скачать информационный файл Bundle Information, Страница 79*.
4. Нажмите **Активировать**.  
Откроется диалоговое окно **Лицензионное соглашение Активация**.
5. Скопируйте подпись компьютера и вставьте ее в текстовый файл.

#### Замечание!

Подпись компьютера может измениться после замены аппаратного обеспечения на компьютере Management Server. После изменения подписи компьютера лицензия на базовый пакет становится недоступной.

Чтобы избежать проблем с лицензированием, настройку аппаратного и программного обеспечения необходимо завершить до генерирования подписи компьютера.

Базовая лицензия может оказаться недействительной при следующих изменениях аппаратного обеспечения:

Замена карты сетевого интерфейса.



Установка интерфейса VMWare или виртуальной сети VPN.

Установка или активация сетевого интерфейса WLAN.



### 6.10.3 Получение ключа активации

**Для получения** ключа активации:

1. На компьютере с доступом в Интернет введите следующий URL-адрес в строке обозревателя:  
`https://activation.boschsecurity.com`.
2. Войдите в Bosch Security Systems Software License Manager.  
Если у вас еще нет учетной записи, создайте новую.
3. Нажмите License Activation.  
Откроется диалоговое окно License Activation.
4. В поле Authorization Number введите номер авторизации, полученный вами от Bosch,  
  
и нажмите кнопку .  
Отобразится диалоговое окно License Activation.
5. В диалоговом окне License Activation заполните следующие поля.
  - Computer Signature : скопируйте цифровую подпись компьютера из текстового файла, в котором вы сохранили ее, и вставьте ее в данное поле.
  - Installation Site: введите сведения о месте установки.
  - Comment: при необходимости введите комментарий (не обязательно).
6. Нажмите кнопку Submit.  
Отобразится диалоговое окно License Activation, содержащее сводку активации вашей лицензии и ключ активации лицензии.
7. Скопируйте ключ активации и вставьте его в текстовый файл или отправьте ее по электронной почте по необходимому адресу.

### 6.10.4 Активация системы

**Для активации системы:**

1. запустите BVMS Configuration Client.
2. В меню **Сервис** выберите пункт **Диспетчер лицензий...**  
Откроется диалоговое окно **Диспетчер лицензий**.
3. Установите флажки напротив программного обеспечения, функций и расширений, которые следует активировать. Для расширений введите количество лицензий.  
Или  
если вы получили информационный файл Bundle Information от Bosch, нажмите **Импортировать пакетную информацию**, чтобы импортировать его.  
Если не вы получили информационный файл Bundle Information, скачайте его из Bosch Security Systems Software License Manager, см. *Скачать информационный файл Bundle Information, Страница 79*.
4. Нажмите **Активировать**.  
Откроется диалоговое окно **Лицензионное соглашение Активация**.
5. Скопируйте ключ активации лицензии из текстового файла, в котором вы сохранили его, и вставьте его в поле **License Activation Key**.
6. Нажмите кнопку **Активировать**.  
Активируются соответствующие программные пакеты.
7. Нажмите **Закреть** для закрытия диалогового окна **Диспетчер лицензий**.

## 6.11 Обслуживание BVMS

В данном разделе содержится информация об обслуживании недавно установленной или обновленной системы BVMS.

Для проведения обслуживания системы выполните следующие действия.



- Экпортируйте конфигурацию BVMS и настройки пользователя. История версий (все версии конфигурации, активированные ранее) не экспортируется. Рекомендуется активировать конфигурацию перед экспортом.
- Информацию об этой процедуре см. в разделе *Чтобы экспортировать параметры конфигурации.*, Страница 81.

или

- Выполните резервное копирование elements.bvms. Это необходимо, если требуется восстановить (Enterprise) Management Server, включая историю версий. Настройки пользователя не включаются.
- Информацию об этой процедуре см. в разделе *Выполнение резервного копирования.*, Страница 81.
- Сохраните файл конфигурации VRM (config.xml)
- Информацию об этой процедуре см. в разделе *Сохранение конфигурации VRM.*, Страница 82.

Экспортированная конфигурация не содержит историю системы. Откат конфигурации невозможен.

Вся конфигурация системы, включая полную историю изменений системы, сохраняется в одном файле.

C:\ProgramData\Bosch\VMS\Elements.bvms.

#### Чтобы экспортировать параметры конфигурации:

1. В меню **Система** нажмите кнопку **Конфигурация экспорта....**

Откроется диалоговое окно **Экспортировать файл конфигурации.**

**Примечание.** Если текущая рабочая копия конфигурации не активирована (активен



), экспортируется данная рабочая копия, а не активированная конфигурация.

2. Нажмите **Сохранить**.

3. Введите имя файла.

Экспортируется текущая конфигурация. Создается ZIP-файл с базой данных и данными пользователя.

#### Выполнение резервного копирования.

1. Остановите службу **Central Server** BVMS в (Enterprise) Management Server.
2. Скопируйте файл elements.bvms в требуемый каталог для резервного копирования.
3. Запустите службу **Central Server** BVMS в (Enterprise) Management Server.

Конфигурация VRM сохраняется в одном зашифрованном файле config.xml.

Этот файл можно скопировать и сохранить для создания резервной копии, когда служба VRM запущена и работает.

Этот файл зашифрован и содержит все необходимые данные VRM, такие как:

- Данные пользователя
- Все системные устройства и их соответствующие параметры VRM

Части конфигурации VRM также сохраняются в конфигурации BVMS. Если в эти данные вносятся какие-либо изменения, данные записываются в config.xml после активации конфигурации BVMS.

Следующие настройки не сохраняются в конфигурации BVMS:

- **Настройки VRM > Основные параметры**
- **Сеть > SNMP**
- **Обслуживание > Дополнительно**
- **Параметры записи**
- **Балансировка загрузки**

Если на одной из этих страниц вносятся какие-либо изменения, они незамедлительно записываются на сервер VRM и не сохраняются в конфигурации BVMS.

#### **Сохранение конфигурации VRM.**

- ▶ Скопируйте Config.xml в безопасное место.  
Этот файл можно найти в следующем каталоге для основного диспетчера VRM:  
C:\Program Files (x86)\Bosch\Video Recording Manager\primary\VRM Server
- Этот файл можно найти в следующем каталоге для вторичного диспетчера VRM:  
C:\Program Files (x86)\Bosch\Video Recording Manager\secondary\VRM Server

## 6.12 Замена устройства

В данном разделе содержится информация о способах восстановления системы, например, когда происходит сбой устройства и его необходимо заменить.

#### **Предварительное условие**

Операции обслуживания выполнены.

#### **См.**

- *Обслуживание BVMS, Страница 80*

### 6.12.1 Замена MS / EMS

Разницы между заменой Management Server и Enterprise Management Server нет.

Можно либо восстановить конфигурацию старого Management Server или Enterprise Management Server, а также можно импортировать экспортированную конфигурацию.

При восстановлении конфигурации идентификатор сервера остается неизменным.

При импорте конфигурации используется идентификатор сервера новой системы. Новый идентификатор сервера требуется, если необходимо создать Enterprise System с помощью экспортированной конфигурации, которая импортируется на каждом Management Server в качестве шаблона. Каждый Management Server в этой Enterprise System должен иметь уникальный идентификатор сервера.

Можно импортировать экспортированную конфигурацию и настройки пользователя этой конфигурации. Настройки пользователя содержат пользователей, которые были добавлены в эту конфигурацию и соответствующие им настройки в Operator Client, такие как размеры окон и закладки.

**Примечание.** Импорт конфигурации не восстанавливает историю версий старой конфигурации. При импорте конфигурации настройки пользователя не импортируются. Необходимо вручную восстанавливать экспортированные настройки пользователя.

#### **Чтобы импортировать конфигурацию:**

1. В меню **Система** выберите пункт **Импортировать конфигурацию...**  
Откроется диалоговое окно **Импортировать файл конфигурации**.
2. Выберите требуемый файл для импорта и нажмите кнопку **Открыть**.  
Откроется диалоговое окно **Импортировать конфигурацию...**
3. Введите соответствующий пароль и нажмите кнопку **ОК**.  
Клиент Configuration Client перезапускается. Необходимо повторить вход.  
Импортированная конфигурация не активируется, но ее можно изменить в клиенте Configuration Client.

#### **Восстановление экспортированной конфигурации.**

Доступ к этому файлу (копирование, удаление) возможен, только если служба **Central Server** BVMS остановлена.

1. Остановите службу **Central Server** BVMS в (Enterprise) Management Server.
2. При необходимости переименуйте резервный файл в Elements.bvms.

3. Замените существующий Elements.bvms.
4. Запустите службу **Central Server** BVMS в (Enterprise) Management Server.

**Примечание.** Для сброса настроек системы до пустой конфигурации остановите службу и удалите Elements.bvms.

Другие файлы конфигурации:

- Elements.bvms.bak (начиная с версии 2.2) — автоматически сохраненный резервный файл последней активации, включая историю версий. Последующие изменения конфигурации, которые не активировались, не включаются.
- Elements\_Backup\*\*\*\*\*.bvms: Конфигурация более ранней версии. Этот файл создается после обновления программного обеспечения.

#### Восстановление экспортированных настроек пользователя.

1. Разархивируйте zip-файл, созданный во время экспорта при обслуживании. Кнопка *файл export.bvms* и *каталог UserData* извлекаются из архива.
2. На требуемом (Enterprise) Management Server скопируйте *каталог UserData* каталог в `C:\ProgramData\Bosch\VMS\`.

## 6.12.2

### Замена VRM

#### Необходимые условия

- Установленная ОС с соответствующими сетевыми параметрами и надлежащей версией VRM.

#### Для замены устройства VRM из BVMS:

1. запустите BVMS Configuration Client.
2. В Дереве устройств выберите устройство VRM.
3. Задайте настройки на следующих страницах, затем сохраните и активируйте конфигурацию.

- Главное окно > **Устройства** > разверните  > разверните  > 
- Главное окно > **Устройства** > разверните  > разверните  > **Настройки VRM**
- Главное окно > **Устройства** > разверните  > разверните  > **Сеть** > **SNMP**
- Главное окно > **Устройства** > разверните  > разверните  > **Обслуживание** > **Дополнительно**
- Главное окно > **Устройства** > разверните  > разверните  >  >  > **Дополнительные параметры** > **Очередность записи**
- Главное окно > **Устройства** > разверните  > разверните  >  >  > **iSCSI** > **Балансировка загрузки**

#### Для замены устройства VRM без BVMS:

Используется исходный резервный файл config.xml с устройства VRM, содержащий все параметры конфигурации (дальнейшая настройка не требуется).

1. Остановите службу **Video Recording Manager**.
2. Скопируйте config.xml на новый сервер.
3. Запустите службу **Video Recording Manager**.

**Замена устройства iSCSI (запланированный резерв).**

1. Добавьте новое устройство iSCSI.
2. С помощью Configuration Manager на устройстве iSCSI, подлежащем замене, настройте все логические устройства как работающие только в режиме чтения.

**Примечание.** Можно удалить старое устройство iSCSI, когда старые записи более не требуются.

**Замечание!**

Во время настройки нового устройства iSCSI рекомендуется использовать тот же пароль CHAP, что и для старого устройства.

При использовании нового пароля CHAP обязательно установите новый пароль как общесистемный пароль CHAP и задайте его для всех устройств iSCSI и для VRM.

В противном случае вы не сможете проводить проверку подлинности на устройстве iSCSI и отображать непосредственное воспроизведение с устройства iSCSI.

**Дополнительная информация**

- *Общесистемный пароль CHAP*, Страница 182
- *Пароль для глобального подключения iSCSI (пароль CHAP):*, Страница 120

**6.12.3****Замена кодера или декодера****Замечание!**

Не удаляйте устройство из Дерева устройств, если необходимо сохранить его записи. Для замены устройства замените оборудование.

**Замена кодера/декодера такого же типа**

Необходимым условием является устройство с заводскими настройками по умолчанию (IP-адрес = 192.168.0.1).

1. Отключите старое устройство от сети.
2. Не удаляйте устройство из Дерева устройств в BVMS Configuration Client! При удалении устройства из VRM запись теряется.
3. Подключите новое устройство такого же типа к сети.

**Замечание!**

Для следующих шагов требуется указанный ранее IP-адрес по умолчанию. При использовании назначенных DHCP IP-адресов выполнение начального поиска устройства невозможно.

4. Configuration Client: в меню **Аппаратное обеспечение** нажмите **Первоначальный поиск устройств...**

Откроется диалоговое окно **Первоначальный поиск устройств**.

5. Щелкните ячейку, чтобы изменить нужный адрес. Для изменения нескольких адресов выберите нужные строки. Можно выбрать несколько устройств, нажав клавишу CTRL или SHIFT. Затем щелкните правой кнопкой мыши выбранные строки и нажмите **Установить IP-адреса...** или нажмите **Установить маску подсети...** для изменения соответствующих значений.

Необходимо ввести маску подсети и IP-адрес.

Маска подсети и IP-адрес должны соответствовать заменяемому устройству.

6. Нажмите **ОК**.
7. Через несколько секунд можно получить доступ к устройству в Дереве устройств.

8. Измените все необходимые настройки устройства, которыми не управляет система BVMS (см. информацию ниже).
9. Сохранить и активировать.

**Примечания.**

- Начальный поиск устройств находит только устройства, имеющие дублированные IP-адреса или IP-адрес по умолчанию (192.168.0.1).
- Не используйте поиск VRM или NVR для обнаружения устройств с параметрами по умолчанию, поскольку после этого вы не сможете изменить IP-адрес.



**Замена кодера с назначенным DHCP IP-адресом.**





Необходимым условием является кодер с заводскими настройками по умолчанию (IP-адрес заданный DHCP).




1. Подсоедините кодер напрямую к порту Ethernet своего компьютера.
2. Запишите параметры конфигурации сетевого адаптера TCP/IPv4, чтобы восстановить их в дальнейшем.
3. Для сетевого адаптера своего компьютера задайте следующий фиксированный IP-адрес и маску подсети:  
192.168.0.2  
255.255.255.0
4. Запустите Internet Explorer.
5. В строке **Адрес** введите 192.168.0.1.  
Отобразится веб-страница устройства.
6. Нажмите **Параметры**, затем нажмите **Сеть**.
7. На странице **Сеть** в списке **DHCP** выберите **Off (Выкл.)**.
8. В поле **IP-адрес**, поле **Маска подсети** и поле **Адрес шлюза** введите необходимые значения, действующие в вашей сети.
9. Нажмите **Уст. и перезагр..**
10. Восстановите конфигурацию сетевого адаптера.





**Замена кодера/декодера другого типа устройства**

- Отключите старое устройство от сети.
- Не удаляйте устройство из Древа устройств в BVMS Configuration Client! При удалении устройства из NVR запись теряется.
- Подключите новое устройство нового типа к сети.


 Главное окно  **Устройства** > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер** или


 Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер** или

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер** или

Главное окно >  **Устройства** > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить декодер** > диалоговое окно **Изменить декодер**

После замены устройства можно обновить его функциональные возможности. Текст сообщения информирует о том, соответствуют ли полученные возможности устройства возможностям, сохраненным в BVMS.

#### Для обновления:

1. Нажмите кнопку **ОК**.  
Отображается окно сообщения со следующим текстом:  
**Если применить данные возможности устройства, могут измениться настройки записи и событий для данного устройства. Проверьте эти настройки.**
2. Нажмите кнопку **ОК**.  
Выполняется обновление возможностей устройства.

#### Замена камеры VSG

При замене камеры VSG убедитесь, что используемая для замены камера имеет тот же тип, тот же IP-адрес и тот же профиль ONVIF, что и у старой камеры.

Кроме того необходимо задать следующие настройки на новой камере AXIS через веб-интерфейс камеры VSG перед заменой старой камеры AXIS:

- Задать пароль для основного пользователя
- Настроить синхронизацию времени
- Отключить адрес локального канала
- Создать пользователя ONVIF
- Отключить защиту атак повторного воспроизведения

#### Настройки, задаваемые системой BVMS

Кодеры и декодеры, настроенные в системе BVMS, управляются сервером BVMS и поэтому не могут использоваться совместно с другими приложениями.

Можно использовать BVMS Device Monitor для проверки того, какое устройство отображает несоответствующую конфигурацию, которая отличается от конфигурации BVMS.

BVMS Configuration Client содержит страницы конфигурации для всех устройств BVIP. Охват настроек зависит от конкретной модели BVIP (напр. VIPX 1600 XFM4).

BVMS обеспечивает управление всеми параметрами BVIP, необходимыми для полной интеграции в систему BVMS.

Настройки, задаваемые системой BVMS.

- Название камеры
- Настройки сервера времени
- Управление записями (профили, время хранения, графики)
- Определения настроек качества

- Пароли  
Хранятся в конфигурации BVMS, но не меняются на устройствах:
- IP-адрес (IP-адреса можно менять с помощью BVMS IP Device Configuration)
- Имена реле / вводов (отображаются различия имен устройств и имен, заданных в BVMS)

#### **Системные события для различающихся конфигураций устройств**

- События SystemInfo создаются после исправления конфигурации устройства во время периодической проверки.
- События SystemWarning создаются после обнаружения несоответствующей конфигурации на устройстве в первый раз. Последующие проверки не приводят к созданию такого события, пока конфигурация не будет исправлена путем активации или периодического исправления.
- События SytemError создаются после обнаружения ошибки конфигурации во время активации или периодических проверок. Последующие проверки не приводят к созданию такого события, пока конфигурация не будет исправлена путем активации или периодического исправления.

### **6.12.4**

#### **Замена клиента оператора**

##### **Замена рабочей станции Operator Client.**

1. Замените компьютер.
2. Запустите установку BVMS на новом компьютере.
3. В списке компонентов для установки выберите Operator Client.  
При необходимости выберите другие компоненты, которые были установлены на замененном компьютере.
4. Установите программное обеспечение.

### **6.12.5**

#### **Заключительные проверки**

##### **Проверка замены MS / EMS и замены Operator Client.**

1. Активируйте конфигурацию.
2. Запустите Operator Client.
3. Проверьте Логическое дерево в Operator Client.  
Оно должно быть идентичным Логическому дереву в Configuration Client.

##### **Проверка замены VRM.**

- ▶ Запустите VRM Monitor и проверьте активные записи.

### **6.12.6**

#### **Восстановление Divar IP 3000/7000**

См. руководства по установке для DIVAR IP 3000 или DIVAR IP 7000. В разделе по восстановлению устройства можно найти информацию по необходимым действиям.

### **6.13**





#### **Настройка синхронизации времени**

##### **Замечание!**



Убедитесь, что время на всех компьютерах системы BVMS синхронизировано с Management Server. В противном случае можно потерять записи. Настройте программное обеспечение сервера времени на Management Server. На других компьютерах настройте IP-адрес Management Server как сервера времени с использованием стандартных процедур Windows.

## 6.14 Настройка носителей данных кодера

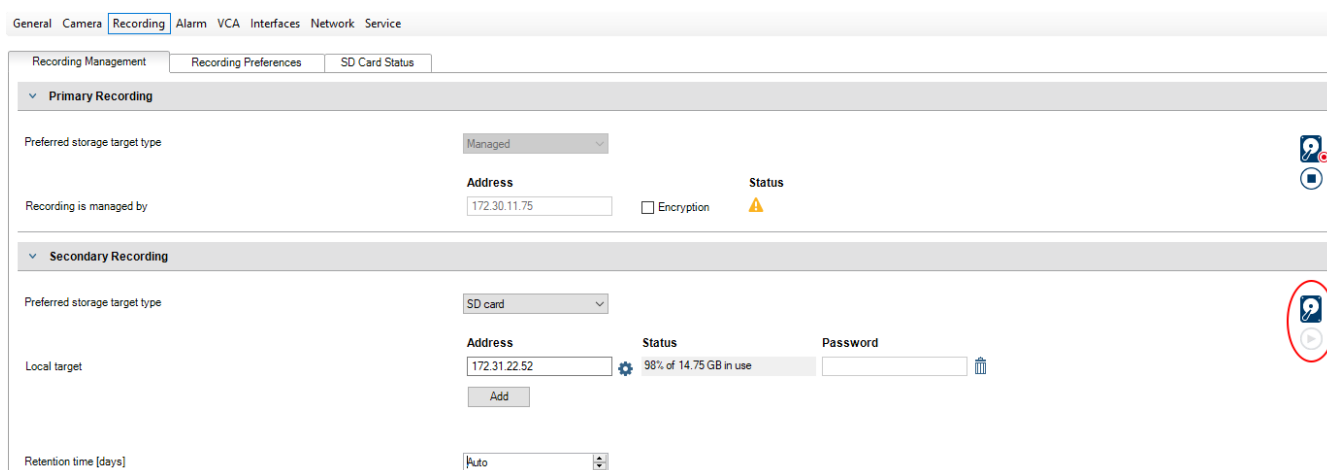
Главное окно >  **Устройства** > разверните  > разверните  >  >

 > **Дополнительные параметры** > **Управление записями**

**Примечание.** Убедитесь, что требуемые камеры этого кодера добавлены в Логическое дерево.

Для использования функции ANR необходимо настроить носитель данных кодера.

**Примечание.** Если необходимо настроить носитель данных кодера, который уже добавлен в систему и записан с помощью VRM, убедитесь, что остановлена вторичная запись:



Функция ANR работает только на кодерах с версией микропрограммного обеспечения 5.90 и выше. Не все типы кодеров поддерживают ANR, даже если установлена верная версия микропрограммного обеспечения.

### Настройка носителя данных кодера

1. В разделе **Вторичная запись** в списке **Предпочитаемый тип целевого хранилища** выберите носитель данных. В зависимости от типа устройства будут доступны разные носители.
2. При необходимости нажмите кнопку ..., чтобы отформатировать носитель данных. После успешного форматирования носитель данных будет готов к использованию с функцией ANR.
3. Настройте функцию ANR для этого кодера на странице **Камеры и запись**.

### См.

- Страница "Управление записью", Страница 242
- Настройка функции ANR, Страница 311



## 7 Создание системы Enterprise

Выполните следующие действия, чтобы создать Enterprise System на Enterprise Management Server и на нескольких компьютерах Management Server:

1. *Настройка списка серверов для корпоративной системы, Страница 89*
2. *Создание Enterprise User Group, Страница 90*
3. *Создание Enterprise Account, Страница 91*

Для использования корпоративной системы Enterprise System необходимо наличие действующих лицензий.

**См.**

- *Enterprise System, Страница 21*

### 7.1 Настройка списка серверов для корпоративной системы



Главное окно > **Устройства > Система Enterprise > Список серверов / адресная книга**

В списке серверов соответствующего Management Server можно настроить несколько компьютеров Management Server.




Для одновременного доступа необходимо настроить одну или несколько групп Enterprise User Group. В результате Management Server меняется на Enterprise Management Server. Пользователь Operator Client может войти в систему с именем пользователя Enterprise User Group, чтобы получить одновременный доступ к компьютерам Management Server, настроенным в списке серверов.



Рабочие привилегии настраиваются на Enterprise Management Server в **Группы пользователей**, на вкладке Enterprise User Group.



Привилегии для устройств настраиваются на каждом Management Server в **Группы пользователей**, на вкладке Enterprise Access.

- Нажмите  для сохранения настроек.
- Нажмите  для отмены последней настройки.
- Нажмите  для активации конфигурации.

**Добавление серверов.**

1. Нажмите **Добавить сервер**.  
Отображается диалоговое окно **Добавить сервер**.
2. Введите отображаемое имя сервера и адрес частной сети (DNS-имя или IP-адрес).  
**Примечание.** При использовании соединения по протоколу SSH введите адрес в следующем формате:  
ssh://IP-адрес или имя\_сервера:5322
3. При необходимости введите общедоступный сетевой адрес (DNS-имя или IP-адрес) для удаленного доступа.

4. Нажмите **ОК**.
5. Повторите эти действия для добавления всех необходимых компьютеров Management Server.

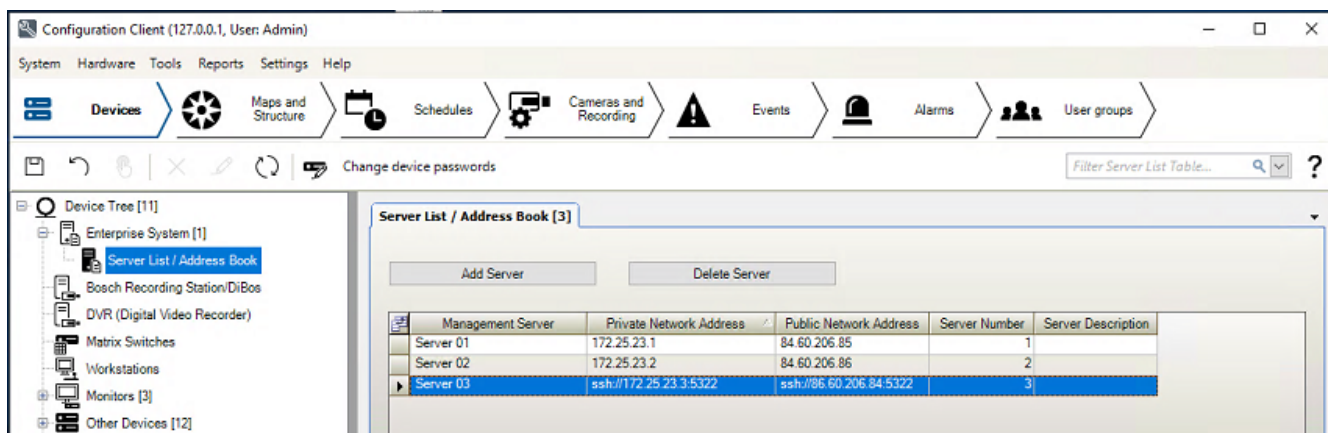
#### Чтобы добавить столбцы:

- ▶ Щелкните правой кнопкой мыши на заголовке таблицы, затем нажмите **Добавить столбец**.

Можно добавить до 10 столбцов.

Чтобы удалить столбец, щелкните на нем правой кнопкой мыши и нажмите **Удалить столбец**.

- ✓ При экспорте списка серверов также будут экспортированы добавленные столбцы. Компьютеры Management Server для вашей Enterprise System настроены. На следующем снимке экрана показан пример:



#### См.

- *Enterprise System, Страница 21*
- *Страница «Список серверов/Адресная книга», Страница 127*
- *Страница Пользовательские группы, Страница 339*
- *Использование просмотра сервера, Страница 74*

## 7.2

### Создание Enterprise User Group



Главное окно > **Группы пользователей**

Вы выполняете задачу создания Enterprise User Group для Enterprise System на Enterprise Management Server.

Вы создаете Enterprise User Group с пользователями для настройки их рабочих разрешений. Эти рабочие разрешения отображаются в Operator Client, подключенном к Enterprise Management Server. Примером рабочего разрешения является пользовательский интерфейс тревожного монитора.

#### Чтобы создать Enterprise User Group:

1. Нажмите вкладку **Enterprise User Groups**.

**Примечание.** Вкладка **Enterprise User Groups** доступна только при наличии соответствующей лицензии и при условии, что один или несколько компьютеров



Management Server настроены в **Устройства > Система Enterprise > Список серверов / адресная книга**.

2. Нажмите .  
Откроется диалоговое окно **Создать группу пользователей Enterprise User Group**.
3. Введите имя и описание.
4. Нажмите кнопку **ОК**.  
Enterprise User Group добавлена в соответствующее дерево.
5. Щелкните правой кнопкой по новой группе Enterprise и выберите **Переименовать**.
6. Введите нужное имя и нажмите клавишу ВВОД.
7. На странице **Рабочие разрешения** требуемым образом настройте рабочие разрешения и доступ к серверу для настроенных компьютеров Management Server.

**См.**

- *Страница Свойства пользовательской группы, Страница 341*
- *Страница Свойства оператора, Страница 351*
- *Страница Приоритеты, Страница 354*
- *Страница Интерфейс пользователя, Страница 354*
- *Страница Доступ к серверу, Страница 356*

## 7.3 Создание Enterprise Account



Главное окно &gt;

**Группы пользователей****Замечание!**

Прежде чем вы сможете добавить Enterprise Account, необходимо задать конфигурацию по меньшей мере одного устройства в дереве устройств.

Вы выполняете задачу создания Enterprise Account на Management Server. Повторите те же действия на каждом Management Server, являющемся элементом вашей Enterprise System. Вы создаете Enterprise Account для настройки разрешений для устройств Operator Client с помощью Enterprise System.

**Чтобы создать Enterprise Account:**

1. Перейдите на вкладку **Доступ Enterprise**.
2. Нажмите .  
Откроется диалоговое окно **Создать учетную запись Enterprise Account**.
3. Введите имя и описание.
4. Флажок **Пользователь должен изменить пароль при следующем входе в систему** предварительно установлен для всех вновь созданных учетных записей.  
Введите пароль в соответствии с требованиями к паролям и подтвердите его.
5. Нажмите кнопку **ОК**.  
Новая учетная запись Enterprise Account добавлена в соответствующее дерево.
6. Щелкните правой кнопкой по новой Enterprise Account и выберите **Переименовать**.
7. Введите нужное имя и нажмите клавишу ВВОД.
8. На странице **Разрешения для устройств** настройте, если требуется, учетные данные, а также разрешения устройств.




**См.**

- *Строгая политика паролей, Страница 364*

- *Страница Учетные данные, Страница 349*
- *Страница Логическое дерево, Страница 350*
- *Страница События и тревоги, Страница 347*
- *Страница Приоритеты управления, Страница 346*
- *Страница Разрешения камеры, Страница 344*
- *Страница Разрешения декодера, Страница 347*

## 8 Настройка командных сценариев

В этом разделе приводится описание способов настройки Командных сценариев. Командные сценарии располагаются в разных местах BVMS.

1. Нажмите  для сохранения настроек.
2. Нажмите  для отмены последней настройки.
3. Нажмите  для активации конфигурации.



### Замечание!

Серверные сценарии активируются во время перезапуска службы Management Server, даже если не выполняется активация из Configuration Client.

### 8.1 Управление командными сценариями

Главное окно


Командный сценарий можно создать при помощи следующих языков программирования сценариев:

- C#
- VB.Net

Вы не можете изменить язык сценария существующего командного сценария.

Вы можете создать клиентский сценарий или серверный сценарий.

К каждому сценарию вы можете добавлять скриплеты.

Чтобы получить справку по вводу кода, нажмите значок  в диалоговом окне **Редактор командных сценариев**. Отображается справка Bosch Script API.

#### Добавление скриплета сервера:

1. В меню **Сервис** выберите команду **Редактор командных сценариев...**  
Если командный сценарий еще не создан, откроется диалоговое окно **Выберите язык сценария**.
2. В списке **Язык сценария:** выберите необходимую запись.  
Откроется диалоговое окно **Редактор командных сценариев**.
3. На левой панели диалогового окна **Редактор командных сценариев** щелкните правой кнопкой мыши пункт **ServerScript** и выберите пункт **Создать команду**.  
Будет добавлен новый скриптлет.
4. Введите свой код.

#### Добавление скриплета клиента:

1. В меню **Сервис** выберите команду **Редактор командных сценариев...**  
Если командный сценарий еще не создан, откроется диалоговое окно **Выберите язык сценария**.
2. В списке **Язык сценария:** выберите необходимую запись.  
Откроется диалоговое окно **Редактор командных сценариев**.
3. На левой панели диалогового окна **Редактор командных сценариев** щелкните правой кнопкой мыши пункт **ClientScript** и выберите пункт **Создать команду**.  
Будет добавлен новый скриптлет.
4. Введите свой код.

#### Удаление скриплета:

1. Откройте диалоговое окно **Редактор командных сценариев**.

2. Откройте вкладку **Серверный сценарий** или **Клиентский сценарий**.
3. Щелкните правой кнопкой мыши нужное событие в дереве событий и выберите пункт



Скриптлет будет удален.

**Чтобы выйти из диалогового окна Редактор командных сценариев:**

- ▶ Нажмите .

**См.**

- *Диалоговое окно Редактор командных сценариев, Страница 316*

## 8.2

### Настройка автоматического запуска командного сценария



Главное окно > Тревожные сигналы > или > столбец **Параметры тревог** > ...

В результате данных настроек клиентский командный сценарий будет запущен в следующих случаях:

- Запуск рабочей станции.
- Прием тревожного сигнала пользователем.

**Чтобы настроить командный сценарий, выполняющийся при запуске рабочей станции:**

См Настройка командного сценария запуска.

**Чтобы настроить командный сценарий, выполняющийся после того, как пользователь принял тревожный сигнал:**

1. Щелкните вкладку **Поток заданий**.
2. Выберите соответствующий клиентский сценарий из списка **Выполнить следующий клиентский сценарий после принятия тревоги:**.  
Этот сценарий будет запущен сразу после приема пользователем тревожного сигнала.

**См.**

- *Диалоговое окно Параметры тревог, Страница 323*
- *Настройка командного сценария, выполняющегося при запуске (страница «Настройки»), Страница 95*

## 8.3

### Импорт командного сценария

Главное окно

Можно импортировать командные сценарии, созданные на другом компьютере. Файл должен быть составлен на том же языке сценариев, который используется в вашей системе.

**Чтобы импортировать командный сценарий:**

1. В меню **Сервис** выберите команду **Редактор командных сценариев...**.  
Откроется диалоговое окно **Редактор командных сценариев**.
2. Нажмите .  
Откроется диалоговое окно открытия файла.
3. Выберите нужный файл сценария и нажмите кнопку **ОК**.

**См.**


– *Диалоговое окно Редактор командных сценариев, Страница 316*

## 8.4 Экспорт командного сценария

Главное окно

Можно экспортировать командные сценарии, созданные на другом компьютере.

**Чтобы экспортировать командный сценарий:**




1. В меню **Сервис** выберите команду **Редактор командных сценариев...**  
Откроется диалоговое окно **Редактор командных сценариев**.
2. Нажмите .
3. Введите имя нужного файла сценария и нажмите кнопку **ОК**.

**См.**

– *Диалоговое окно Редактор командных сценариев, Страница 316*

## 8.5 Настройка командного сценария, выполняющегося при запуске (страница «Настройки»)



Главное окно >  **Устройства** > Разверните  >  > **Настройки**

Можно настроить командный сценарий, который будет запущен при запуске Operator Client на выбранной рабочей станции.

Вы должны создать соответствующий командный сценарий.

Сведения о создании командного сценария см. *Управление командными сценариями, Страница 93*.

**Чтобы настроить командный сценарий:**

- ▶ Выберите нужный командный сценарий из списка **Сценарий запуска**.

**См.**

– *Страница Рабочая станция, Страница 138*

## 9 Управление параметрами конфигурации




Главное окно

Вы должны активировать текущую конфигурацию, чтобы она вступила в силу для Management Server and Operator Client. Система напоминает вам о необходимости активации при выходе из Configuration Client.

Каждая активированная конфигурация сохраняется с датой и описанием (при необходимости).

Вы всегда можете восстановить последнюю активированную конфигурацию. Все конфигурации, сохраненные за это время, будут утрачены.

Текущую конфигурацию можно экспортировать в файл конфигурации и впоследствии импортировать этот файл. В результате этой операции восстанавливается экспортированная конфигурация. Все конфигурации, сохраненные за это время, будут утрачены.

- Нажмите  для сохранения настроек.
- Нажмите  для отмены последней настройки.
- Нажмите  для активации конфигурации.

### 9.1 Активация текущей конфигурации

Главное окно

Вы можете активировать текущую конфигурацию. Если пользователь принял ее, то Operator Client использует активированную конфигурацию после следующего запуска. Если активация была произведена принудительно, то все открытые экземпляры Operator Client закрываются и запускаются заново. Пользователю каждой копии Operator Client обычно не нужно выполнять вход заново.

Можно настроить время отложенной активации. Если настроено время отложенной активации, рабочая конфигурация активируется не сразу же, а в установленное время. При более поздней настройке времени активации (отложенной или нет), это время становится активным в данный момент. Первое настроенное время активации удаляется. При выходе из Configuration Client система напоминает вам о необходимости активации текущей рабочей копии конфигурации.

Невозможно активировать конфигурацию, содержащую устройство без защиты паролем.



#### Замечание!

Если активация была произведена принудительно, то каждый экземпляр Operator Client перезапускается при активации конфигурации. Избегайте ненужных активаций. Рекомендуется выполнять активацию ночью или в периоды низкой активности.



#### Замечание!

Если в системе содержатся устройства без защиты паролем, необходимо обеспечить безопасность этих устройств, чтобы можно было выполнить активацию. Это принудительное использование пароля можно отключить.



**Чтобы активировать текущую конфигурацию:**

1. Нажмите **Активировать конфигурацию**.  
Откроется диалоговое окно **Активировать конфигурацию**.  
Если конфигурация содержит устройства без защиты паролем, выполнение активации невозможно. В этом случае отображается диалоговое окно **Защита устройств паролем по умолчанию...**  
Выполните инструкции в этом диалоговом окне и нажмите кнопку **Применить**.  
Диалоговое окно **Активировать конфигурацию** снова откроется.
2. При необходимости введите время отложенной активации. По умолчанию текущее время устанавливается как время активации. Если не изменить время отложенной активации, активация выполняется немедленно.  
В случае необходимости установите флажок **Принудительная активация для всех модулей Operator Client**.
3. Введите описание и нажмите кнопку **ОК**.  
Текущая конфигурация активируется.  
Каждая рабочая станция Operator Client немедленно перезапускается, если имеется подключение к сети и выполняется принудительная активация. Если рабочая станция не подключена к сети, она перезапускается сразу после подключения.  
Если настроено время отложенной активации, конфигурация активируется позже.

**Примечание.** Отложенная активация не выполняется до тех пор, пока пользователь не выйдет из Configuration Client.

**См.**

- Диалоговое окно «Защита устройств с помощью всеобщего пароля по умолчанию» (меню «Оборудование»), Страница 109
- Диалоговое окно «Активировать конфигурацию» (меню «Система»), Страница 108

## 9.2 Активация конфигурации

Главное окно

Можно активировать предыдущую версию конфигурации, сохраненную ранее.

**Чтобы активировать конфигурацию:**

1. В меню **Система** выберите пункт **Диспетчер активации...**  
Откроется диалоговое окно **Диспетчер активации**.
2. Выберите из списка конфигурацию, которую вы хотите активировать.
3. Нажмите кнопку **Активировать**.  
Откроется окно сообщения.
4. Нажмите **ОК**.  
Откроется диалоговое окно **Активировать конфигурацию**.
5. При необходимости установите флажок **Принудительная активация для всех модулей Operator Client**. Каждая рабочая станция Operator Client автоматически перезапускается для активации новой конфигурации. Пользователь не может отклонить новую конфигурацию.  
Если не установлен флажок **Принудительная активация для всех модулей Operator Client**, на каждой рабочей станции Operator Client на несколько секунд появится диалоговое окно. Пользователи могут отказаться или принять новую конфигурацию. Диалоговое окно закрывается автоматически через несколько секунд, если пользователь не совершил никаких действий. В этом случае новая конфигурация не принимается.

**См.**

- Диалоговое окно «Активировать конфигурацию» (меню «Система»), Страница 108
- Диалоговое окно «Диспетчер активации» (меню «Система»), Страница 107

## 9.3

### Экспорт параметров конфигурации

Главное окно

Данные конфигурации устройства BVMS могут быть экспортированы в ZIP-файл. В этом ZIP-файле содержится файл базы данных (*Export.bvms*) и данных пользователя (*DAT*-файл).

Эти файлы можно использовать для восстановления конфигурации системы, ранее экспортированной на том же (Enterprise) Management Server, или импорта на другой (Enterprise) Management Server. Файл данных пользователя нельзя импортировать, но с его помощью можно вручную восстановить конфигурацию пользователя.

**Чтобы экспортировать параметры конфигурации:**

1. В меню **Система** нажмите кнопку **Конфигурация экспорта...**

Откроется диалоговое окно **Экспортировать файл конфигурации**.

**Примечание.** Если текущая рабочая копия конфигурации не активирована (активен



), экспортируется данная рабочая копия, а не активированная конфигурация.

2. Нажмите **Сохранить**.

3. Введите имя файла.

Экспортируется текущая конфигурация. Создается ZIP-файл с базой данных и данными пользователя.

**См.**

- *Импорт параметров конфигурации*, Страница 98

## 9.4

### Импорт параметров конфигурации

Главное окно

Рассматриваются следующие сценарии:

- импорт конфигурации, ранее экспортированной (выполнено резервное копирование) на том же сервере;
- импорт шаблона конфигурации, подготовленного и экспортированного на другом сервере;
- импорт конфигурации более ранней версии BVMS.

Конфигурацию можно импортировать, только если сохранены и активированы последние изменения текущей рабочей копии.

Для импорта данных конфигурации нужен соответствующий пароль.

Невозможно импортировать данные пользователя.

**Чтобы импортировать конфигурацию:**

1. В меню **Система** выберите пункт **Импортировать конфигурацию...**

Откроется диалоговое окно **Импортировать файл конфигурации**.

2. Выберите требуемый файл для импорта и нажмите кнопку **Открыть**.

Откроется диалоговое окно **Импортировать конфигурацию...**

3. Введите соответствующий пароль и нажмите кнопку **ОК**.

Клиент Configuration Client перезапускается. Необходимо повторить вход.

Импортированная конфигурация не активируется, но ее можно изменить в клиенте Configuration Client.

**Замечание!**

Чтобы продолжить редактировать конфигурацию, активированную для Management Server, выполните откат в диалоговом окне **Активировать конфигурацию**.

**См.**

– *Экспорт параметров конфигурации, Страница 98*

## 9.5

### Экспорт конфигурационных данных в OPC

Главное окно

Вы можете экспортировать конфигурационные данные устройства BVMS в файл XML для последующего импорта в приложение сервера OPC. Файл должен быть сохранен в директории bin установленного экземпляра BVMS.

Для настройки соединения между BVMS и BIS доступны руководство по подключению BVMS к BIS и технические примечания к BVMS OPC Server.

**Замечание!**

Установите сервер OPC и BVMS Management Server на разные компьютеры.

При установке обоих серверов на один компьютер производительность системы будет снижена. Кроме того, могут возникнуть серьезные проблемы с работой программного обеспечения.

**Чтобы экспортировать параметры конфигурации:**

1. В меню **Система** выберите пункт **Экспорт сведений об устройстве для OPC...**  
Откроется диалоговое окно **Экспорт файла со сведениями об устройстве**.
2. Введите имя файла и нажмите кнопку **Сохранить**.  
Файл будет сохранен.  
Этот файл может быть импортирован в приложение сервера OPC.

## 9.6

### Проверка состояния кодеров/декодеров

Главное окно > меню **Аппаратное обеспечение** > команда **Монитор устройств...** > диалоговое окно **Монитор устройств**

Состояние всех активированных кодеров/декодеров можно проверить в Дереве устройств.

**См.**

– *Диалоговое окно «Монитор устройств» (меню «Оборудование»), Страница 114*

## 9.7

### Настройка мониторинга SNMP

Главное окно

**Для настройки:**

1. В меню **Настройки** выберите пункт **Настройки SNMP...**  
Отображается диалоговое окно **Настройки SNMP**.
2. Установите требуемые параметры и нажмите **ОК**.

**Отключение SNMP GetRequest.**

- ▶ Удалите содержимое поля **Порт SNMP GET**.  
BVMS более не принимает данные SNMP GetRequest.

**См.**

– *Диалоговое окно «Настройки SNMP» (меню «Настройки»), Страница 117*

## 9.8 Создание отчета

Главное окно

Можно создавать отчеты, собирающие сведения о текущей конфигурации.

### Создание отчета:

1. В меню **Отчеты** выберите необходимую команду.  
Откроется соответствующее диалоговое окно.
2. Нажмите **Экспорт CSV**.
3. Введите путь и имя файла для нового отчета.
4. Откройте CSV-файл в Microsoft Excel или другом приложении для работы с электронными таблицами, чтобы проверить его содержимое.

### См.

- Диалоговое окно "Расписания записей", Страница 115
- Диалоговое окно "Расписания задач", Страница 115
- Диалоговое окно "Камеры и параметры записи", Страница 115
- Диалоговое окно "Параметры качества потока", Страница 116
- Диалоговое окно "Настройки событий", Страница 116
- Диалоговое окно "Настройки составных событий", Страница 116
- Диалоговое окно "Настройки тревог", Страница 116
- Диалоговое окно "Настроенные пользователи", Страница 116
- Диалоговое окно "Группы пользователей и учетные записи", Страница 116
- Диалоговое окно "Рабочие разрешения", Страница 116

## 10 примеры конфигурации

В данном разделе содержатся примеры конфигурации выбранных устройств в BVMS.

### 10.1 Добавление моста Bosch ATM/POS




В данном примере описано, как настроить мост Bosch ATM/POS.


#### Настройка моста ATM/POS



1. Убедитесь, что устройство подключено к сети.
2. Чтобы настроить IP-адрес и маску подсети устройства, подключите его к COM-порту компьютера при помощи кабеля RS232 (используйте для подключения кабель, указанный в спецификациях Bosch). Подробные сведения содержатся в руководстве по установке моста Bosch ATM/POS.
3. Запустите на компьютере сеанс работы программы Hyperterminal (обычно: **Пуск > Программы > Стандартные > Связь > Hyper Terminal**).
4. Введите имя сеанса и нажмите кнопку **ОК**.
5. Выберите номер COM-порта и нажмите **ОК**.
6. Введите следующие параметры COM-порта:
  - 9600 бит/с
  - 8 бит данных
  - без проверки четности
  - 1 стоповый бит
  - аппаратное управление потоком
 Нажмите **ОК**.
7. Нажмите F1 для отображения меню системных параметров устройства.
8. Введите 1 для установки IP-адреса и маски подсети.
9. Оставьте стандартные значения для портов:
  - port1: **4201**
  - port2: **4200**





#### Добавление моста ATM/POS к BVMS

1. Подключите устройство к сети BVMS.
2. Запустите Configuration Client.

3. Нажмите  **Устройства**, разверните логическое дерево, разверните , щелкните правой кнопкой мыши , нажмите **Добавить мост ATM/POS Bosch**. Откроется диалоговое окно **Добавить мост ATM/POS Bosch**.
4. Введите имя и ранее установленные настройки.
5. Перейдите на вкладку **Входы** и выберите нужные входы.

6. Нажмите , чтобы сохранить настройки.



7. Нажмите  **События**.
8. Разверните , разверните **Вход моста POS**, нажмите **Ввод данных**.
9. В списке **Активировать тревогу** выберите **Всегда**, чтобы данное событие всегда активировало тревогу. При необходимости активации тревоги событием только в течение определенного периода времени, выберите расписание.

10. Нажмите , чтобы сохранить настройки.
11. Нажмите  **Тревожные сигналы**.
12. Установите нужные настройки тревоги для данного события.
13. Нажмите , чтобы сохранить настройки и нажмите , чтобы включить конфигурацию.
14. Выполните тест, чтобы убедиться, что тревожный сигнал работает должным образом.

## 10.2 Добавление входа сигнализации Bosch Allegiant

После добавления устройства Bosch Allegiant в BVMS следует добавить тревожные входы Allegiant.

1. В дереве устройств нажмите запись устройства Allegiant.
2. Выберите вкладку **Входы** и нажмите **Добавить вход**.
3. Добавьте нужные тревожные входы.
4. Нажмите **События**.
5. В дереве событий разверните **Устройства Allegiant**, разверните **Вход Allegiant** и нажмите **Вход закрыт** или **Вход открыт** (в зависимости от приложения).
6. В списке **Активировать тревогу** выберите **Всегда**, чтобы данное событие всегда активировало тревогу. При необходимости активации тревоги событием только в течение определенного периода времени, выберите расписание.

7. Нажмите , чтобы сохранить настройки и нажмите , чтобы включить конфигурацию.
8. Выполните тест, чтобы убедиться, что тревожный сигнал работает должным образом.

## 10.3 Добавление и настройка 2 камер Dinion IP для записи VRM

В данном разделе описываются способы добавления 2 камер Dinion IP для записи VRM, способы настройки различных параметров записи и способы настройки поиска для этих камер.

### Предварительные условия.

Диспетчер видеозаписи и устройства iSCSI настроены правильно.

Это означает следующее.

- Диспетчер видеозаписи добавлен в логическое дерево.
- Устройство iSCSI с настроенным получателем и LUN назначено данному диспетчеру видеозаписи.

### Чтобы добавить IP-камеры к существующему диспетчеру видеозаписи (VRM):

Главное окно >  **Устройства** > развернуть 

1. Щелкните правой кнопкой мыши  и выберите команду **Добавить кодер**. Откроется диалоговое окно **Добавить кодер**.

- Введите IP-адрес IP-камеры и выберите тип кодера (Dinon IP).  
Нажмите **ОК**.  
Повторите это же действие для другой IP-камеры.

**Чтобы добавить IP-камеры в логическое дерево, выполните следующие действия.**



Главное окно > **Карты и структура**

- ▶ Перетащите камеры в логическое дерево.


**Чтобы изменить свойства камеры:**



Главное окно > **Камеры и запись** >  > вкладка 

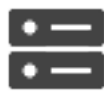
- В столбце **Видеоизображение в реальном времени** настройте параметры качества отображения изображений в реальном времени. Для этих устройств можно настроить параметры качества только для каждой камеры, но не в соответствии с расписанием.
- Установите соответствующие параметры в других столбцах.

**Чтобы настроить параметры записи для камер, выполните следующие действия.**


- Перейдите на вкладку расписания, например .

- Выберите ячейку в столбце  и выберите соответствующее качество потока.
- В поле **Непрерывная запись или запись перед тревожным сигналом** в столбце **Выбрать** выберите необходимый режим записи.  
При выборе **До тревоги**: щелкните ячейку в столбце **Продолжительность** для выбора времени записи перед тревожным сигналом в секундах.
- В поле **Запись по тревоге** в столбце **Продолжительность** нажмите на ячейку и введите необходимое время записи.
- Повторите эти действия, чтобы настроить параметры записи для другой камеры.

**Чтобы активировать поиск на рабочей станции, выполните следующие действия:**



Главное окно > **Устройства** > Развернуть 

- Нажмите значок  вашей рабочей станции.
- Перейдите на вкладку **Настройки**.
- Установите флажок **Включить Forensic Search**.

## 11 Главные окна Configuration Client







В данном разделе содержится информация о некоторых основных окнах приложения, имеющихся в BVMSConfiguration Client.

### 11.1 Окно Конфигурация


Главное окно

Используется для настройки системы. Кнопки на панели инструментов представляют собой ссылки на различные страницы, которые вы должны настроить для работы системы. Они расположены в той последовательности, в которой рекомендуется осуществлять настройки.

- ▶ нажмите на элемент дерева для отображения всех доступных страниц свойств.

 <p><b>Устройства</b></p>	Нажмите для отображения страницы <b>Устройства</b> со всеми устройствами, подключенными к системе.
 <p><b>Карты и структура</b></p>	Нажмите для отображения страницы <b>Карты и структура</b> с логическим деревом, деревом устройств и картами.
 <p><b>Расписания</b></p>	Нажмите для отображения страницы <b>Расписания записей и Расписания задач</b> .
 <p><b>Камеры и запись</b></p>	Нажмите для отображения страницы <b>Камеры и запись</b> с таблицей камер и параметрами записи для всех камер.
 <p><b>События</b></p>	Нажмите для отображения страницы <b>События</b> .
 <p><b>Тревожные сигналы</b></p>	Нажмите для отображения страницы <b>Тревожные сигналы</b> .
 <p><b>Группы пользователей</b></p>	Нажмите для отображения страницы <b>Группы пользователей</b> со всеми пользователями.
	нажмите для сохранения параметров активного окна.
	нажмите для восстановления сохраненных параметров активного окна.



	Нажмите для отображения диалогового окна <b>Активировать конфигурацию</b> .
	нажмите для удаления выделенного элемента. (Доступно не на всех страницах).
	нажмите для переименования выделенного элемента. (Доступно не на всех страницах).
	Нажмите для отображения справочной информации, относящейся к активному окну.
	Нажмите, если нужно обновить информацию о состояниях для всех устройств и сведения о возможностях устройств (доступно не на каждой странице). Можно обновить состояние отдельного устройства: щелкните устройство правой кнопкой мыши и выберите <b>Обновить состояние</b> . <b>Примечание.</b> Если у вас крупная система с несколькими тысячами настроенных устройств, процесс обновления состояний и возможностей устройств может занять длительное время.

## 11.2

### Команды меню

#### Команды меню Система

<b>Сохранить изменения</b>	Сохраняет изменения, сделанные на данной странице.
<b>Отменить все изменения на странице</b>	Восстанавливает последние сохраненные параметры на странице.
<b>Диспетчер активации...</b>	Отображает диалоговое окно <b>Диспетчер активации</b> .
<b>Конфигурация экспорта...</b>	Отображает диалоговое окно <b>Экспортировать файл конфигурации</b> .
<b>Импортировать конфигурацию...</b>	Отображает диалоговое окно <b>Импортировать файл конфигурации</b> .
<b>Экспорт сведений об устройстве для ОРС...</b>	Отображает диалоговое окно создания файла конфигурации, который можно импортировать в систему управления сторонних производителей.
<b>Выход</b>	Выход из программы.

#### Команды меню Аппаратное обеспечение

<b>Первоначальный поиск устройств...</b>	Отображает диалоговое окно <b>Первоначальный поиск устройств</b> .
--	--

<b>Защита устройств паролем по умолчанию...</b>	Отображает диалоговое окно <b>Защита устройств всеобщим паролем по умолчанию.</b>
<b>Изменить пароли устройств...</b>	Отображает диалоговое окно <b>Изменить пароли устройств.</b>
<b>Обновить микропрограмму устройства...</b>	Отображает диалоговое окно <b>Обновить микропрограмму устройства.</b>
<b>Изменить IP-адрес устройства и сетевые параметры...</b>	Отображает диалоговое окно <b>Изменить IP-адрес и сетевые параметры устройства.</b>
<b>Монитор устройств...</b>	Отображает диалоговое окно <b>Монитор устройств.</b>

#### Команды меню Сервис

<b>Редактор командных сценариев...</b>	Отображает диалоговое окно <b>Редактор командных сценариев</b>
<b>Диспетчер ресурсов...</b>	Отображает диалоговое окно <b>Диспетчер ресурсов.</b>
<b>Конструктор последовательностей...</b>	Отображает диалоговое окно <b>Конструктор последовательностей.</b>
<b>Конвертор ресурсов</b>	При наличии ресурсов карты отображает диалоговое окно <b>Конвертор ресурсов.</b>
<b>Конфигурация RRAS...</b>	Отображает диалоговое окно <b>Конфигурация RRAS.</b>
<b>Диспетчер лицензий...</b>	Отображает диалоговое окно <b>Диспетчер лицензий.</b>
<b>Инспектор лицензий...</b>	Отображает диалоговое окно <b>Инспектор лицензий.</b>

#### Команды меню Отчеты

<b>Расписания записи...</b>	Отображает диалоговое окно отчета <b>Расписания записей.</b>
<b>Параметры записи по расписанию...</b>	Отображает диалоговое окно отчета <b>Параметры записи по расписанию.</b>
<b>Расписания задач...</b>	Отображает диалоговое окно отчета <b>Расписания задач.</b>
<b>Камеры и параметры записи...</b>	Отображает диалоговое окно отчета <b>Параметры камер и записи.</b>
<b>Параметры качества потока...</b>	Отображает диалоговое окно отчета <b>Параметры качества потока.</b>
<b>Параметры событий...</b>	Отображает диалоговое окно отчета <b>Настройки событий.</b>
<b>Параметры составного события...</b>	Отображает диалоговое окно отчета <b>Настройки сложных событий.</b>
<b>Параметры тревог...</b>	Отображает диалоговое окно отчета <b>Настройки тревог.</b>

<b>Настроенные пользователи...</b>	Отображает диалоговое окно отчета <b>Настроенные пользователи.</b>
<b>Группы пользователей и учетные записи...</b>	Отображает диалоговое окно отчета <b>Группы пользователей и учетные записи.</b>
<b>Разрешения устройства...</b>	Отображает диалоговое окно отчета <b>Разрешения для устройств.</b>
<b>Разрешения для операторов</b>	Отображает диалоговое окно отчета <b>Рабочие разрешения.</b>
<b>Разрешения конфигурировании...</b>	Отображает диалоговое окно отчета <b>Разрешения конфигурирования.</b>
<b>Разрешения группы пользователей</b>	Отображает диалоговое окно отчета <b>Разрешения группы пользователей.</b>
<b>Параметры безопасности...</b>	Отображает диалоговое окно отчета <b>Параметры безопасности.</b>
<b>Обойденные устройства...</b>	Отображает диалоговое окно отчета <b>Обойденные устройства.</b>

#### Команды меню Настройки

<b>Настройки тревог...</b>	Отображает диалоговое окно <b>Настройки тревог.</b>
<b>Настройки SNMP...</b>	Отображает диалоговое окно <b>Настройки SNMP.</b>
<b>Установить качество записи...</b>	Отображает диалоговое окно <b>Параметры качества потока .</b>
<b>Параметры...</b>	Отображает диалоговое окно <b>Параметры.</b>
<b>Параметры удаленного доступа...</b>	Отображает диалоговое окно <b>Параметры удаленного доступа.</b>

#### Команды меню Справка

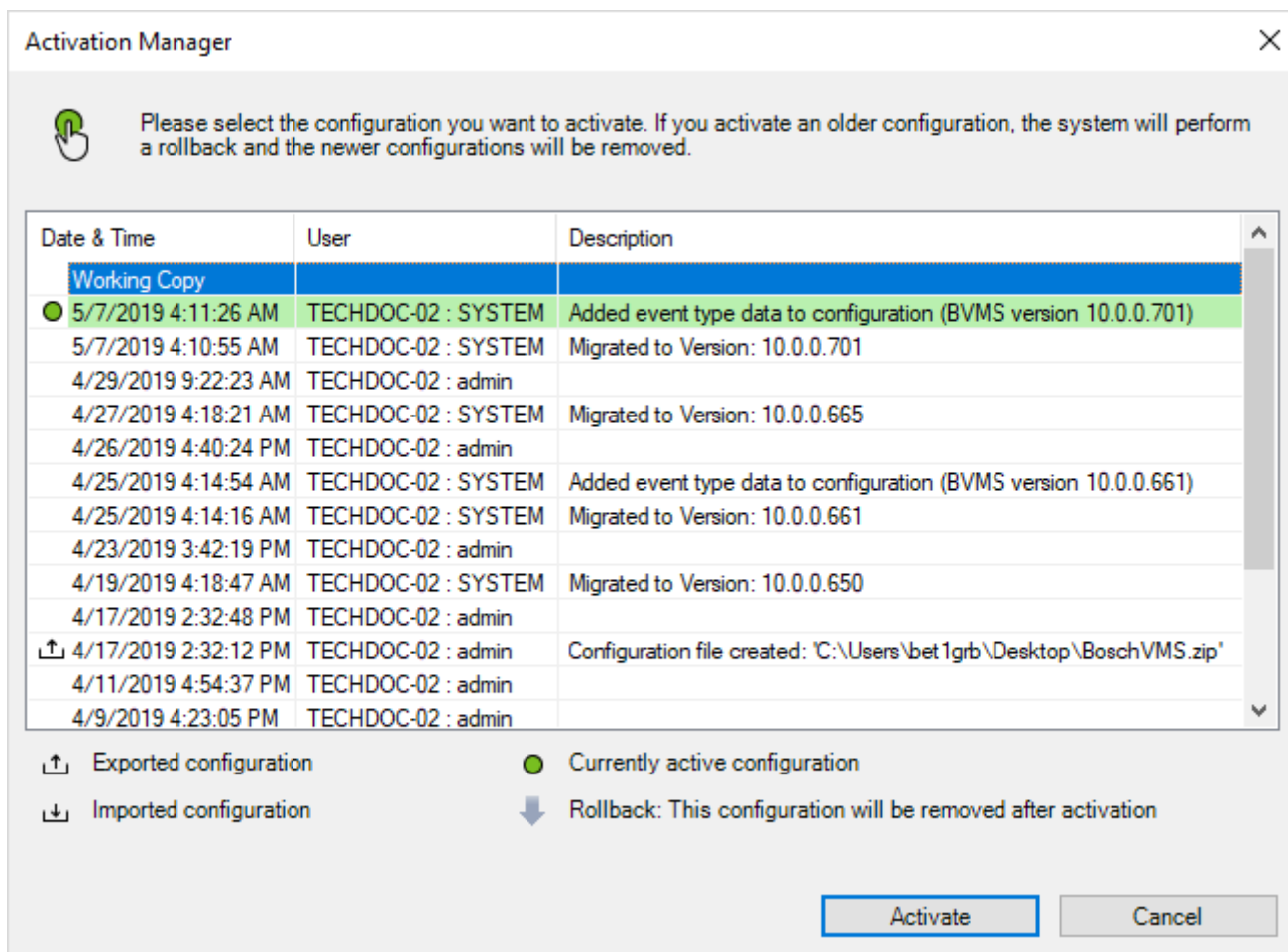
<b>Показать справку</b>	Отображает справку приложения BVMS.
<b>О программе...</b>	Отображает диалоговое окно, содержащее информацию об установленной системе, например, номер версии.

## 11.3

### Диалоговое окно «Диспетчер активации» (меню «Система»)

Главное окно > Меню **Система** > Команда **Диспетчер активации...**

Позволяет активировать текущую конфигурацию или вернуться к предыдущей конфигурации.

**Активировать**

Нажмите для отображения диалогового окна **Активировать конфигурацию**.

**См.**

- Активация текущей конфигурации, Страница 96
- Активация конфигурации, Страница 97

**11.4****Диалоговое окно «Активировать конфигурацию» (меню «Система»)**

Главное окно >

Позволяет ввести описание текущей копии конфигурации, которая должна быть активирована.

**Установить время отложенной активации**

Нажмите для выбора времени отложенной активации.

**Примечание.** Отложенная активация не выполняется до тех пор, пока пользователь не выйдет из Configuration Client.

**Принудительная активация для всех модулей Operator Client**

Если флажок установлен, каждая рабочая станция Operator Client автоматически перезапускается для активации новой конфигурации. Пользователь не может отказаться от новой конфигурации.

Если не установлен флажок, то на каждой рабочей станции Operator Client на несколько секунд появится диалоговое окно. Пользователи могут отказаться или принять новую конфигурацию. Диалоговое окно закрывается автоматически через несколько секунд, если пользователь не совершил никаких действий. В этом случае новая конфигурация не принимается.

#### **Перед активацией настройте службу RRAS**

Это возможно, только если включен параметр **Включить сопоставление портов** в диалоговом окне **Параметры удаленного доступа**.

Если флажок установлен, перед выполнением активации отображается диалоговое окно **Конфигурация RRAS**.

См.

– *Активация текущей конфигурации, Страница 96*

## 11.5

### **Диалоговое окно «Первоначальный поиск устройств» (меню «Оборудование»)**

Главное окно > Меню **Аппаратное обеспечение** > Команда **Первоначальный поиск устройств...**

Отображает устройства, имеющие двойные IP-адреса или IP-адрес по умолчанию (192.168.0.1).

Позволяет изменять эти IP-адреса и маски подсети.

Прежде чем изменять IP-адрес, вы должны ввести правильную маску подсети.

## 11.6

### **Диалоговое окно «Защита устройств с помощью всеобщего пароля по умолчанию» (меню «Оборудование»)**

Главное окно > Меню **Аппаратное обеспечение** > Команда **Защита устройств паролем по умолчанию...**

или



Главное окно >

Это диалоговое окно появляется, если ожидается выполнение активации и если конфигурация содержит устройства без защиты паролем. Оно позволяет ввести всеобщий пароль по умолчанию, применяемый ко всем затрагиваемым устройствам.

#### **Обновить состояния и функции**

Нажмите для повторного сканирования сети для поиска устройств, не защищенных паролем.

#### **Всеобщий пароль по умолч.**

Введите пароль, используемый для всех не защищенных в данный момент устройств.

#### **Показать пароли**

Нажмите, чтобы все пароли в этом диалоговом окне стали видимы.

#### **Принудительная защита паролем при активации**

Установите этот флажок. Если функция включена, необходимо применить всеобщий пароль по умолчанию для устройств, которые не защищены паролем.

#### **Применить**

Нажмите, чтобы применить всеобщий пароль по умолчанию.

Откроется диалоговое окно **Изменение паролей**. Перечисляются изменения паролей.

Нажмите **ОК**, чтобы закрыть окно.


Если началась активация конфигурации, отображается диалоговое окно **Диспетчер активации**.

**См.**

– *Активация текущей конфигурации, Страница 96*

## 11.7

### Диалоговое окно «Изменить пароли устройств» (меню «Оборудование»)

Главное окно >  **Устройства** >  **Изменить пароли устройств** > диалоговое окно **Изменить пароли устройств**

или

Главное окно > меню **Аппаратное обеспечение** > команда **Изменить пароли устройств...** > диалоговое окно **Изменить пароли устройств**



Нажмите, чтобы обновить информацию о состоянии всех устройств. Можно обновить состояние отдельного устройства: щелкните устройство правой кнопкой мыши и выберите **Обновить состояние**.

**Примечание.** Если у вас большая система с несколькими тысячами настроенных устройств, процесс обновления состояния может занять длительное время.



Нажмите, чтобы выбрать все доступные устройства сразу.


#### Показать пароли

Установите флажок, если вы хотите, чтобы настроенные пароли отображались в читаемой форме.



Введите строку и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы. Отображаются только элементы, содержащие введенную строку, и их соответствующие родительские элементы (только в деревьях).

Указывается число отфильтрованных элементов и совокупное число элементов. На

активный фильтр указывает значок . Для поиска точных фраз строки следует заключать в кавычки, например, в случае строки "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

Чтобы отменить фильтрацию, нажмите .

**Примечание.** Только если флажок **Показать пароли** установлен, можно также выполнить поиск паролей.

В этой таблице можно установить следующие свойства доступных IP-устройств:

- Пароль сервиса
- Пароль пользователя
- Пароль Live

- Пароль пункта назначения

**Чтобы изменить пароль для IP-устройств:**

1. Выберите требуемое устройство.
2. Щелкните правой кнопкой мыши выбранное устройство и щелкните **Изменить пароль...**  
Отобразится диалоговое окно **Изменить пароли устройств**.
3. Выберите требуемый тип пароля.
4. Введите новый пароль.
5. Нажмите **ОК**.  
Новый пароль будет применен для выбранного устройства.

**Чтобы изменить параметры для нескольких устройств:**

См *Настройка нескольких кодеров / декодеров, Страница 239*.

## 11.8

### Диалоговое окно «Обновить микропрограммное обеспечение устройства» (меню «Оборудование»)

Главное окно > меню **Аппаратное обеспечение** > команда **Обновить микропрограмму устройства...** > диалоговое окно **Обновить микропрограмму устройства**



Нажмите, чтобы обновить информацию о состоянии всех устройств. Можно обновить состояние отдельного устройства: щелкните устройство правой кнопкой мыши и выберите **Обновить состояние**.

**Примечание.** Если у вас большая система с несколькими тысячами настроенных устройств, процесс обновления состояния может занять длительное время.



Нажмите, чтобы выбрать все доступные устройства сразу.



Нажмите для обновления версии микропрограммы.



Введите строку и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы. Отображаются только элементы, содержащие введенную строку, и их соответствующие родительские элементы (только в деревьях). Указывается число отфильтрованных элементов и совокупное число элементов. На активный фильтр указывает значок . Для поиска точных фраз строки следует заключать в кавычки, например, в случае строки "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

Чтобы отменить фильтрацию, нажмите .

**Порядок обновления микропрограммы:**

1. Выберите требуемое устройство.

2. Нажмите **Обновить микропрограмму**.  
Открывается информационное окно Configuration Client.
3. Нажмите **ОК**.  
Открывается проводник.
4. Выберите файл с обновлением.
5. Нажмите **Открыть**.  
Открывается окно **Состояние отправки программного обеспечения**.
6. Чтобы начать загрузку, нажмите **Начало**.
7. Нажмите **Заккрыть**.  
Микропрограмма обновлена.

#### Чтобы изменить параметры для нескольких устройств:

См *Настройка нескольких кодеров / декодеров*, Страница 239.

## 11.9

### Диалоговое окно «Изменить IP-адрес и сетевые параметры устройства» (меню «Оборудование»)

Главное окно > меню **Аппаратное обеспечение** > команда **Изменить IP-адрес устройства и сетевые параметры...** > диалоговое окно **Изменить IP-адрес и сетевые параметры устройства**



Нажмите, чтобы обновить информацию о состоянии всех устройств. Можно обновить состояние отдельного устройства: щелкните устройство правой кнопкой мыши и выберите **Обновить состояние**.

**Примечание.** Если у вас большая система с несколькими тысячами настроенных устройств, процесс обновления состояния может занять длительное время.



Нажмите, чтобы выбрать все доступные устройства сразу.



Введите строку и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы. Отображаются только элементы, содержащие введенную строку, и их соответствующие родительские элементы (только в деревьях). Указывается число отфильтрованных элементов и совокупное число элементов. На активный фильтр указывает значок **X**. Для поиска точных фраз строки следует заключать в кавычки, например, в случае строки "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201 .

Чтобы отменить фильтрацию, нажмите **X**.

В этой таблице можно установить следующие свойства доступных IP-устройств:

- Краткое имя
- IP-адрес
- Маска подсети
- IP-адрес шлюза



**Замечание!**

Вместо использования команд вы можете ввести соответствующие параметры в нужном поле.

**Чтобы задать отображаемые имена для IP-устройств:**

1. Выберите требуемое устройство.
2. Щелкните правой кнопкой мыши выбранное устройство и щелкните **Задать краткие имена....** Отображается диалоговое окно **Задать краткие имена.**
3. В поле **Начинать с:** введите первую строку.
4. Нажмите **Рассчитать.** В поле **Заканчивать:** отображается последняя из ряда строк для выбранного устройства.
5. Нажмите **ОК.**
6. В диалоговом окне **Изменить IP-адрес и сетевые параметры устройства** нажмите **Применить.**  
Вычисляемое имя будет обновлено в выбранном устройстве.

**Диалоговое окно Задать отображаемые имена****Начинать с:**

Введите первое имя.

**Заканчивать:**

Отображает последнее имя для выбранных устройств после нажатия кнопки **Рассчитать.**

**Рассчитать**

Нажмите для расчета диапазона кратких имен выбранных устройств.

**Чтобы задать IP-адреса для IP-устройств:**

1. Выберите требуемое устройство.
2. Щелкните правой кнопкой мыши выбранное устройство и выберите **Установить IP-адреса....** Отображается диалоговое окно **Установить IP-адреса.**
3. В поле **Начинать с:** введите первый IP-адрес.
4. Нажмите **Рассчитать.** В поле **Заканчивать:** отображается последний из ряда IP-адресов для выбранного устройства.
5. Нажмите **ОК.**
6. В диалоговом окне **Изменить IP-адрес и сетевые параметры устройства** нажмите **Применить.**  
Новый IP-адрес вступит в силу в выбранном устройстве.

**Диалоговое окно Установить IP-адреса****Начинать с:**

Введите первый IP-адрес.

**Заканчивать:**

Отображает последний IP-адрес для выбранных устройств после нажатия кнопки

**Рассчитать.****Рассчитать**

Нажмите для расчета диапазона IP-адресов выбранных устройств.

**Чтобы задать маску подсети/идентификатор шлюза для IP-устройств:**

1. Щелкните нужное поле.
2. Введите соответствующее значение.
3. Нажмите **Применить**.  
Новое значение будет применено для выбранного устройства.

**Применить**

Нажмите для применения введенных значений без закрытия диалогового окна.

**Чтобы изменить параметры для нескольких устройств:**

См *Настройка нескольких кодеров / декодеров, Страница 239*.

**11.10****Диалоговое окно «Монитор устройств» (меню «Оборудование»)**

Главное окно > меню **Аппаратное обеспечение** > команда **Монитор устройств...** > диалоговое окно **Монитор устройств**

Позволяет проверять состояние кодеров и декодеров в Дереве устройств, которые активны в системе BVMS.

**Отобразить имя**

Имя устройства, заданное в BVMS.

**Сетевой адрес**

IP-адрес устройства.

**Состояние**

Возможно отображение следующих состояний.

- **Настроенные** — конфигурация этого устройства активирована.
- **Несоответствие конфигурации** — конфигурация этого устройства не активирована.
- **Неизвестно** — определение состояния невозможно.
- **Не подключено** — не подключено.

**Последняя проверка**

Дата и время начала работы диалогового окна и выполнения проверки. Пока диалоговое окно отображается, устройства не повторяются повторно.

**См.**

- *Проверка состояния кодеров/декодеров, Страница 99*

**11.11****Диалоговое окно «Исследователь лицензий» (меню «Инструменты»)**

Главное окно > меню **Сервис** > команда **Инспектор лицензий...** > диалоговое окно **Инспектор лицензий**

Можно проверить, не превышает ли количество установленных лицензий BVMS количество приобретенных лицензий.

**11.12****Диалоговое окно «Диспетчер лицензий» (меню «Инструменты»)**

Главное окно > Меню **Сервис** > Команда **Диспетчер лицензий...**

Позволяет лицензировать заказанный пакет BVMS и обновлять его дополнительными возможностями.

**Базовые пакеты**

Отображает доступные базовые пакеты.

**Номер типа**

Отображает Коммерческое название (CTN) выбранного пакета, функции или расширения.

**Состояние**

Отображает лицензионный статус (если применимо).

**Дополнительные возможности**

Отображает доступные функции.

**Расширение**

Отображает доступные расширения и их количество. Чтобы изменить количество, поместите указатель мыши справа от флажка и нажмите стрелку вверх или вниз.

**Активировать**

Нажмите для отображения диалогового окна **Лицензионное соглашение Активация**.

**Импортировать пакетную информацию**

Нажмите для импорта XML-файла, содержащего информацию Bundle, полученную от компании Bosch.

**Добавить новый пакет**

Нажмите для отображения диалогового окна выбора нового файла лицензии.

**См.**

– *Активация лицензии на программное обеспечение, Страница 78*

**11.13****Диалоговые окна «Отчеты» (меню «Отчеты»)**

В этой главе описаны все диалоговые окна, доступные для отчетов о конфигурации.

**См.**

– *Создание отчета, Страница 100*

**11.13.1****Диалоговое окно "Расписания записей"**

Главное окно > Меню **Отчеты** > Команда **Расписания записи...**

Открывает список настроенных расписаний записей.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

**11.13.2****Диалоговое окно Настройки записи по расписанию**

Главное окно > Меню **Отчеты** > Команда **Параметры записи по расписанию...**

Открывает список параметров настроенных расписаний записей.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

**11.13.3****Диалоговое окно "Расписания задач"**

Главное окно > Меню **Отчеты** > Команда **Расписания задач...**

Открывает список настроенных расписаний задач.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

**11.13.4****Диалоговое окно "Камеры и параметры записи"**

Главное окно > Меню **Отчеты** > Команда **Камеры и параметры записи...**

Открывает список параметров записи, настроенных в таблице камер и таблице записи.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

### 11.13.5 **Диалоговое окно "Параметры качества потока"**

Главное окно > Меню **Отчеты** > Команда **Параметры качества потока...**

Открывает список настроенных параметров качества потока для всех камер.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

### 11.13.6 **Диалоговое окно "Настройки событий"**

Главное окно > Меню **Отчеты** > Команда **Параметры событий...**

Открывает список событий, для которых настроено расписание вызова тревожного сигнала.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

### 11.13.7 **Диалоговое окно "Настройки составных событий"**

Главное окно > Меню **Отчеты** > Команда **Параметры составного события...**

Открывает список всех составных событий.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

### 11.13.8 **Диалоговое окно "Настройки тревог"**

Главное окно > Меню **Отчеты** > Команда **Настройки тревог...**

Открывает список всех настроек тревог для настроенных тревог, включая параметры в диалоговом окне **Параметры тревог**.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

### 11.13.9 **Диалоговое окно "Настроенные пользователи"**

Главное окно > Меню **Отчеты** > Команда **Настроенные пользователи...**

Открывает список пользователей, которым разрешен вход в Operator Client.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

### 11.13.10 **Диалоговое окно "Группы пользователей и учетные записи"**

Главное окно > Меню **Отчеты** > Команда **Группы пользователей и учетные записи...**

Открывает список настроенных групп пользователей, Enterprise Accounts, Enterprise User Groups и групп двойной авторизации.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

### 11.13.11 **Диалоговое окно "Разрешения для устройств"**

Главное окно > Меню **Отчеты** > Команда **Разрешения устройства...**

Открывает список разрешений на использование настроенных устройств для каждой группы пользователей.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

### 11.13.12 **Диалоговое окно "Рабочие разрешения"**

Главное окно > Меню **Отчеты** > Команда **Разрешения для операторов**

Открывает список разрешений на использование Operator Client для каждой группы пользователей.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

### 11.13.13 Диалоговое окно «Разрешения конфигурации»

Главное окно > меню **Отчеты** > команда **Разрешения конфигурировании...**

Открывает список разрешений на использование Configuration Client для каждой группы пользователей.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

### 11.13.14 Диалоговое окно «Разрешения групп пользователей»

Главное окно > меню **Отчеты** > команда **Разрешения группы пользователей**

Открывает список разрешений для настройки групп пользователей для каждой группы пользователей.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

### 11.13.15 Диалоговое окно «Параметры безопасности»

Главное окно > меню **Отчеты** > команда **Параметры безопасности...**

Открывает список настроенных параметров безопасности для каждой группы пользователей и Enterprise User Groups.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

### 11.13.16 Диалоговое окно «Обход устройств»

Главное окно > меню **Отчеты** > команда **Обойденные устройства...**

Открывает список всех настроенных устройств, а также тех, которые обходятся.

- ▶ Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

## 11.14 Диалоговое окно «Настройки тревог» (меню «Настройки»)

См. *Диалоговое окно Настройки тревог*, Страница 320 для получения подробных сведений.

## 11.15 Диалоговое окно «Настройки SNMP» (меню «Настройки»)

Главное окно > Меню **Настройки** > Команда **Настройки SNMP...**

Позволяет настроить мониторинг SNMP на компьютере Management Server. Пользователь задает, для какого события отправляется ловушка SNMP, какую-либо дополнительную информацию о системе и IP-адреса компьютеров, которые будут получать ловушки SNMP от BVMS.

Сервер отправляет ловушки SNMP, когда события происходят. Эти ловушки можно получать используя приемник SNMP в Configuration Client с помощью инструмента **Журнал регистрации запросов SNMP**. Также можно использовать другое программное обеспечение, которое может получать ловушки SNMP.

Агент SNMP в BVMS поддерживает SNMP GetRequest. Когда управляющее ПО SNMP (например, iReasoning MIB Browser) отправляет SNMP GetRequest в адрес BVMS Management Server, Management Server отправляет соответствующее ответное сообщение. Файл MIB расположен в следующем файле:

`<installation_directory>\Bosch\VMS\bin\BVMS.mib`

Поддерживаются только SNMPv1 и v2.

**Примечания.** SNMPv1 и SNMPv2 не являются полностью совместимыми. Поэтому не рекомендуется использовать SNMPv1 и SNMPv2 совместно.

#### **Порт SNMP GET**

Введите номер порта для SNMP GetRequest. Это порт, где агент SNMP системы BVMS Management Server ожидает SNMP GetRequest.

**Примечание.** BVMS не использует стандартный номер порта 161 для SNMP GetRequest, поскольку этот порт может использоваться агентом SNMP компьютера, где установлено ПО BVMS Management Server.

Значение по умолчанию: `12544`.

#### **Контакт системы**

Введите контактные данные для системы BVMS. Эту информацию можно получить с помощью SNMP GetRequest, используя OID `.1.3.6.1.2.1.1.4`.

#### **Описание системы**

Введите описание своей системы BVMS. Эту информацию можно получить с помощью SNMP GetRequest, используя OID `.1.3.6.1.2.1.1.4`.

#### **Расположение системы**

Введите расположение своей системы BVMS. Эта строка должна указывать физическое расположение сервера, например здание, номер помещения, номер стойки и т. п. Эту информацию можно получить с помощью SNMP GetRequest, используя OID `.1.3.6.1.2.1.1.6`.

#### **Приемники запросов**

Введите IP-адрес компьютера, куда система BVMS должна отправлять ловушки SNMP.

#### **Фильтр запросов**

Щелкните, чтобы выбрать события в дереве событий и отфильтровать отправляемые ловушки SNMP.

#### **См.**

– *Настройка мониторинга SNMP, Страница 99*

## **11.16**

### **Диалоговое окно «Параметры» (меню «Настройки»)**

Главное окно > Меню **Настройки** > Команда **Параметры...**

#### **Язык**

Позволяет вам настроить язык Configuration Client. При выборе **Системный язык** используется язык, настроенный в Windows.

Этот параметр включается при перезапуске клиента Configuration Client.

#### **Параметры сканирования**

Позволяет вам настроить, если это возможно, поиск устройств в соответствующей подсети или по подсетям.

#### **Настройки группы мониторов**

Позволяет указать, что пользователи могут управлять всеми группами мониторов с каждого клиентского компьютера BVMS. Впоследствии не понадобится настраивать этот компьютер как рабочую станцию в дереве устройств.

Этот параметр включается после активации конфигурации.

**Декодеры автоматически выбирают поток при подключении к камере**

Позволяет настроить таким образом, чтобы все декодеры в системе использовали совместимый поток, который не обязательно должен быть потоком реального времени. Этот параметр включается после активации конфигурации.

**Конфигурация журнала**

Позволяет настроить строку подключения для базы данных журнала.

**Замечание!**

Эту строку следует изменять только в тех случаях, когда вы хотите настроить удаленный сервер SQL для журнала, и только если вы знакомы с технологией сервера SQL.

Позволяет вам задать максимальный срок хранения записей в журнале. По истечении заданного срока хранения записи будут автоматически удаляться.

Этот параметр включается после активации конфигурации.

**Расширенное отображение состояния****Отключить цвет активных точек на картах**

Позволяет вам настроить отключение мигающих активных точек на картах.

**Включить расширенное отображение состояний (цвет активных точек на картах в зависимости от состояния)**

Позволяет указать для всех событий состояния, что активные точки устройств, принадлежащих этому событию, при возникновении настроенного события выделяются цветом фона и миганием.

**Включить расширенное отображение тревог (цвет активных точек на картах в зависимости от тревоги)**

Позволяет указать для всех тревог, что активные точки устройств, принадлежащих этой тревоге, при возникновении настроенной тревоги выделяются цветом фона и миганием. Настроить отображение дополнительного состояния можно после сохранения конфигурации. Активные точки отображаются на карте в Operator Client после активации конфигурации.

**Автоматический выход из системы****Принудительно выйти из системы на Configuration Client после следующего периода бездействия**

Позволяет настраивать автоматический выход из клиента Configuration Client. По истечении заданного времени будет выполнен выход из клиента Configuration Client. Изменения на страницах конфигурации следующих устройств на странице **Устройства** не сохраняются автоматически и теряются после выхода из системы после периода бездействия:

- Кодеры
- Декодеры
- Устройства VRM
- Устройства iSCSI
- Устройства VSG

Все остальные новые изменения конфигурации сохраняются автоматически.

**Примечание.** Изменения в диалоговых окнах, не подтвержденные нажатием кнопки **ОК**, не сохраняются.

Этот параметр включается после активации конфигурации.

**Разрешить несколько раз входить в систему с использованием одного имени пользователя**

Позволяет указать, что пользователи BVMS SDK, веб-клиента BVMS, мобильного приложения BVMS или Operator Client могут выполнять одновременно несколько входов с использованием одного имени пользователя.

**Пароль для глобального подключения iSCSI (пароль CHAP):**

Введите пароль CHAP iSCSI, необходимый для проверки подлинности устройства хранения iSCSI и активации прямого воспроизведения с iSCSI.

**Примечание.** Пароль CHAP iSCSI и общесистемный пароль CHAP должны совпадать. См. *Общесистемный пароль CHAP*, Страница 182

**Отобразить пароль**

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог посмотреть этот пароль.

См.

– *Общесистемный пароль CHAP*, Страница 182

**11.17****Диалоговое окно «Параметры удаленного доступа» (меню «Настройки»)**

Главное окно > Меню **Настройки** > Команда **Параметры удаленного доступа...**

Позволяет настроить сопоставление портов для удаленного доступа.

Следует добавить один или несколько диапазонов портов. BVMS автоматически назначает каждый частный IP-адрес настроенных устройств разным номерам общедоступных портов из одного из этих диапазонов.

В маршрутизаторе, соединяющем частную сеть с общедоступной, необходимо настроить такое же сопоставление портов. Затем маршрутизатор будет пересылать каждый пакет с номером общедоступного порта из общедоступной сети по частным IP-адресу и номеру порта. Частные IP-адрес и номер порта настроены в таблице сопоставления портов для данного номера общедоступного порта.

**Замечание!**

В маршрутизаторе также необходимо вручную настроить переадресацию портов в соответствии с настройками в таблице сопоставления портов.

**Включить сопоставление портов**

Щелкните, чтобы включить / отключить сопоставление портов.

**Добавить**

Нажмите, чтобы добавить диапазон портов в список **Диапазоны портов**.

**Правка**

Нажмите, чтобы изменить выбранный элемент в списке **Диапазоны портов**.

**Удалить**

Нажмите, чтобы удалить выбранный элемент из списка **Диапазоны портов**.

**Частный IP-адрес (для доступа в пределах LAN)**

Выберите частный IP-адрес своего локального сетевого адаптера Management Server.



**Общедоступный сетевой адрес (IP-адрес или имя DNS для доступа из внешних сетей, например, через Интернет)**

Введите общедоступный сетевой адрес данной частной сети. Удаленный клиент Operator Client осуществляет вход по этому общедоступному сетевому адресу, чтобы получить доступ к устройствам этого Management Server.

**Показать сопоставление портов...**

Нажмите для отображения диалогового окна **Таблица сопоставления портов**.

**См.**

– *Удаленный доступ, Страница 75*

**11.17.1****Диалоговое окно "Таблица распределения портов"**

Главное окно > меню **Настройки** > команда **Параметры удаленного доступа...** > кнопка

**Показать сопоставление портов...** > диалоговое окно **Таблица сопоставления портов**

Отображает распределение портов для IP-адресов настроенных устройств в системе BVMS.

Можно скопировать эту таблицу в буфер обмена и добавить элементы, которые не находятся под управлением BVMS.

**Копировать в буфер обмена**

Нажмите, что скопировать таблицу распределения в буфер обмена. Это поможет создать сценарий конфигурации для распределения портов в маршрутизаторе (например, служба RRAS).

**Протокол**

Отображает используемый сетевой протокол для этого устройства.

Это значение можно изменить вручную.

**Частный порт**

Отображает частный номер порта, используемый в частной сети для этого устройства.

Это значение можно изменить вручную.

**Общедоступный порт**

Отображает общедоступный номер порта, используемый Operator Client из общей сети для доступа к этому устройству.

Это значение можно изменить вручную.

**Фиксированное**

Установите флажок для изменения назначенного вручную номера порта.

Снимите флажок для включения автоматического назначения номера порта.

## 12 Страница Устройства



Главное окно > **Устройства**

Отображает Дерево устройств и страницы настроек.

Количество элементов под записью отображается в квадратных скобках.

Позволяет настроить все доступные устройства, например мобильные видеосервисы, кодеры ONVIF, устройства Bosch Video Streaming Gateway, кодеры, декодеры, диспетчеры видеозаписи, кодеры с локальными хранилищами, аналоговые матрицы или такие периферийные устройства, как мосты ATM/POS.

### Примечание.

Устройства отображаются в дереве и группируются в соответствии с физической сетевой структурой и категориями устройств.

Видеоисточники, например, кодеры, группируются по диспетчерам видеозаписи.

Цифровые видеорегистраторы, например, DiBos перечислены в списке отдельно.



Введите строку и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы. Отображаются только элементы, содержащие введенную строку, и их соответствующие родительские элементы (только в деревьях).

Указывается число отфильтрованных элементов и совокупное число элементов. На

активный фильтр указывает значок **x**. Для поиска точных фраз строки следует заключать в кавычки, например, в случае строки "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

Чтобы отменить фильтрацию, нажмите **x**.

- ▶ Щелкните элемент дерева для отображения соответствующей страницы.

### 12.1 Обновление состояний и возможностей устройств



Главное окно > **Устройства**

Например, после обновления микропрограммы может потребоваться синхронизировать возможности всех настроенных декодеров, кодеров и устройств VSG. С помощью этой функции возможности каждого устройства сравниваются с возможностями, уже хранящимися в BVMS. В дереве устройств можно обновить возможности сразу всех устройств одновременно.

Можно также скопировать в буфер обмена список устройств, чьи возможности изменились. Затем этот список можно вставить, например, в текстовый редактор для детального анализа изменений.

Список устройств вставляется из буфера обмена в формате CSV (значения, разделенные запятыми) и содержит следующую информацию:

- устройство;
- тип устройства;
- IP-адрес.

**Примечание.** Если у вас крупная система с несколькими тысячами настроенных устройств, процесс обновления состояний и возможностей устройств может занять длительное время.

**Замечание!**

Сведения о возможностях извлекаются только для доступных устройств. Узнать, доступно устройство или нет, можно, проверив состояние устройства.

**Чтобы обновить состояния и возможности устройств:**

1. Нажмите .  
Откроется диалоговое окно **Обновить возможности устройства**. Для всех устройств будет обновлена информация о состоянии, будут получены сведения о возможностях устройств.  
При наличии устройств, сведения о возможностях которых не актуальны, соответствующие устройства отобразятся в списке и станет доступна кнопка **Обновить**.
  2. При необходимости нажмите **Скопируйте список устройств в буфер обмена**.
  3. Нажмите **Обновить**.
  4. Нажмите **ОК**.
- ✓ Сведения о возможностях устройств будут обновлены.

**Замечание!**

Информация о состояниях всех устройств будет обновлена в любом случае, даже если вы отмените диалоговое окно **Обновление возможностей устройств**.

## 12.2

### Изменение пароля для IP-устройств



Главное окно > **Устройства** > **Изменить пароли устройств** > диалоговое окно **Изменить пароли устройств**

или

Главное окно > меню **Аппаратное обеспечение** > команда **Изменить пароли устройств...** > диалоговое окно **Изменить пароли устройств**

**Чтобы изменить пароль для IP-устройств:**

1. Выберите требуемое устройство.
2. Щелкните правой кнопкой мыши выбранное устройство и щелкните **Изменить пароль...**  
Отобразится диалоговое окно **Изменить пароли устройств**.
3. Выберите требуемый тип пароля.
4. Введите новый пароль.
5. Нажмите **ОК**.

Новый пароль будет применен для выбранного устройства.

Подробную информацию см. в разделе *Диалоговое окно «Изменить пароли устройств» (меню «Оборудование»)*, Страница 110.

**Чтобы изменить параметры для нескольких устройств:**

См *Настройка нескольких кодеров / декодеров*, Страница 239.

**См.**

- *Диалоговое окно «Изменить пароли устройств» (меню «Оборудование»)*, Страница 110

## 12.3 Добавление устройства



Главное окно > **Устройства**

Следующие устройства добавляются в дерево устройств вручную. Это означает, что для добавления необходимо знать сетевой адрес устройства.

- IP-видеоустройства производства Bosch
- Система Bosch Recording Station/DiBos
- Аналоговый матричный коммутатор  
Чтобы добавить устройство Bosch Allegiant, необходим правильный файл конфигурации Allegiant.
- Рабочая станция BVMS  
На рабочей станции должно быть установлено программное обеспечение Operator Client.
- Устройство связи
- Мост ATM/POS Bosch, устройство DTP
- Виртуальный вход
- Устройство мониторинга сети
- Клавиатура Bosch IntuiKey
- Клавиатура KBD-Universal XF
- Группа мониторов
- Модуль ввода/вывода
- Эмуляция CCL Allegiant
- Охранная панель производства Bosch
- Устройство для анализа на стороне сервера
- Системы контроля и управления доступом компании Bosch

Можно выполнять поиск следующих устройств для добавления с помощью диалогового окна **BVMS Scan Wizard**:

- Устройства VRM
- Кодеры
- Кодеры с локальным хранилищем и работающие только в режиме реального времени
- Кодеры ONVIF, работающие только в режиме реального времени
- Кодеры с локальными хранилищами
- Декодеры
- Устройства шлюза Video Streaming Gateway (VSG)
- Устройства DVR
- Устройства NVR VIDOS



### Замечание!




После добавления устройства нажмите  для сохранения настроек








### Замечание!



Добавьте DVR с помощью учетной записи администратора устройства. Использование учетной записи пользователя DVR с ограниченными разрешениями может привести к тому, что некоторые возможности не будут доступны в BVMS, например использование управления камерой PTZ.





#### Диалоговое окно BVMS Scan Wizard

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Поиск кодеров** > диалоговое окно **BVMS Scan Wizard**

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Поиск шлюзов Video Streaming Gateway** > диалоговое окно **BVMS Scan Wizard**

Главное окно >  **Устройства** > щелкните правой кнопкой мыши  > нажмите **Поиск кодеров, работающих только в реальном времени** > диалоговое окно **BVMS Scan Wizard**

Главное окно >  **Устройства** > щелкните правой кнопкой мыши  > нажмите **Поиск кодеров локального хранилища** > диалоговое окно **BVMS Scan Wizard**

Главное окно >  **Устройства** > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Поиск декодеров** > диалоговое окно **BVMS Scan Wizard**

Это диалоговое окно позволяет выполнить поиск доступных устройств в сети, настроить их и добавить их в систему в рамках одной процедуры.

#### Использовать

Нажмите для выбора устройства, которое необходимо добавить в систему.

#### Тип (недоступно для устройств VSG)

Отображает тип устройства.

#### Краткое имя

Отображает имя устройства, которое было введено в Дереве устройств.

#### Сетевой адрес

Отображает IP-адрес устройства.

#### Имя пользователя

Отображает имя пользователя, настроенное на устройстве.

**Пароль**

Введите действующий пароль для проверки подлинности на этом устройстве.

**Состояние**



Отображает состояние проверки подлинности.



— успешно



— неудачно

Главное окно >  **Устройства** > щелкните правой кнопкой мыши  > нажмите **Выполнить поиск устройств VRM** > диалоговое окно BVMS Scan Wizard

**Замечание!**

Для настройки конфигурации вторичной системы VRM необходимо сначала установить соответствующее ПО на требуемый компьютер. Запустите Setup.exe и выберите **Вторичный VRM**.

**Роль**

Выберите нужное значение в списке.

В следующей таблице перечислены функции, которые может выполнять каждый тип VRM:

Функция / тип	Основной VRM	Дополнительный VRM
Основная (стандарт)	X	
Дополнительная (стандарт)		X
Основная резервная	X	
Дополнительная резервная		X
Зеркальный		X

Основному диспетчеру VRM можно добавить устройство VRM со следующими функциями:

- Резервный VRM
- Зеркальный VRM

Дополнительному диспетчеру VRM можно добавить устройства VRM со следующими функциями:

- Резервный VRM

**Ведущий VRM**

Выберите нужное значение в списке.

**Имя пользователя**

Отображает имя пользователя, настроенное на устройстве VRM.

При необходимости можно ввести другое имя пользователя.

**См.**

- *Добавление устройств VRM путем поиска, Страница 178*
- *Добавление кодера в пул VRM, Страница 228*
- *Добавление кодера, работающего только в режиме реального времени, Страница 228*
- *Добавление кодера локального хранилища, Страница 228*
- *Поиск устройств, Страница 73*

## 12.4

### Страница «Список серверов/Адресная книга»




Главное окно > **Устройства > Система Enterprise > Список серверов / адресная книга**

Можно добавить несколько компьютеров Management Server для одновременного доступа в BVMS Enterprise System. Также можно добавить несколько компьютеров Management Server для последовательного доступа к Server Lookup.

Можно добавить дополнительные столбцы в список серверов. Это позволяет добавлять дополнительные сведения, которые пользователь может использовать для поиска с помощью Server Lookup. Добавленные столбцы также будут отображаться на странице



**Доступ к серверу** (главное окно > **Группы пользователей > вкладка Enterprise**

**User Groups** >  > вкладка **Доступ к серверу**).

#### Добавить сервер

Нажмите для отображения диалогового окна **Добавить сервер**.

#### Удалить сервер:

Нажмите, чтобы удалить записи Management Server.

#### Management Server

Отображаются имена всех добавленных компьютеров Management Server. Каждую запись можно изменить.

**Примечание:** при использовании подключения SSH введите адрес в следующем формате: **ssh://IP или servername:5322**

#### Частный сетевой адрес

Отображаются частные сетевые адреса всех добавленных компьютеров Management Server. Каждую запись можно изменить.

#### Общедоступный сетевой адрес

Отображаются общедоступные сетевые адреса всех добавленных компьютеров Management Server. Каждую запись можно изменить. Данный общедоступный сетевой адрес необходим для удаленного доступа к этому компьютеру Management Server.

#### Номер сервера

Отображаются логические номера всех добавленных компьютеров Management Server. Каждую запись можно изменить.

#### Описание сервера

Введите описание для Management Server. Это описание необходимо, чтобы найти его в списке всех доступных серверов, если требуется монопольный доступ к Management Server, например, чтобы очистить тревожный сигнал, поступающий из другой системы управления.

#### Нажмите для получения пошаговых инструкций:

- *Настройка списка серверов для корпоративной системы, Страница 89*
- *Настройка Server Lookup, Страница 128*
- *Экспорт списка серверов, Страница 129*
- *Импорт списка серверов, Страница 129*

См.

– *Туннелирование SSH, Страница 47*

## 12.4.1 Диалоговое окно Добавить сервер



Главное окно > **Устройства > Система Enterprise > Список серверов / адресная книга**

### Имя сервера

Введите отображаемое имя сервера Management Server.

**Примечание:** при использовании подключения SSH введите адрес в следующем формате:  
**ssh://IP или servername:5322**

### Частный сетевой адрес

Введите частный IP-адрес или DNS-имя Management Server.

### Общедоступный сетевой адрес

Введите адрес общедоступной сети или DNS-имя для маршрутизируемого доступа.

### Описание сервера

Введите описание Management Server.

## 12.4.2 Настройка Server Lookup

Для просмотра сервера пользователь Operator Client или Configuration Client входит в систему с именем пользователя из обычной группы пользователей, а не как пользователь Enterprise User Group.

См.

– *Server Lookup, Страница 22*

– *Страница «Список серверов/Адресная книга», Страница 127*

– *Использование просмотра сервера, Страница 74*

## 12.4.3 Настройка списка серверов



Главное окно > **Устройства > Система Enterprise > Список серверов / адресная книга**

### Добавление серверов.

1. Нажмите **Добавить сервер**.  
Отображается диалоговое окно **Добавить сервер**.
2. Введите отображаемое имя сервера и адрес частной сети (DNS-имя или IP-адрес).  
**Примечание.** При использовании соединения по протоколу SSH введите адрес в следующем формате:  
ssh://IP-адрес или имя\_сервера:5322
3. При необходимости введите общедоступный сетевой адрес (DNS-имя или IP-адрес) для удаленного доступа.
4. Нажмите **ОК**.
5. Повторите эти действия для добавления всех необходимых компьютеров Management Server.



**Чтобы добавить столбцы:**

- ▶ Щелкните правой кнопкой мыши на заголовке таблицы, затем нажмите **Добавить столбец**.  
Можно добавить до 10 столбцов.  
Чтобы удалить столбец, щелкните на нем правой кнопкой мыши и нажмите **Удалить столбец**.
- ✓ При экспорте списка серверов также будут экспортированы добавленные столбцы.

**См.**

- *Настройка списка серверов для корпоративной системы, Страница 89*

**12.4.4****Экспорт списка серверов**

Главное окно > **Устройства > Система Enterprise > Список серверов / адресная книга**

Можно экспортировать список серверов со всеми настроенными свойствами для редактирования и дальнейшего импорта.

При внесении изменений в экспортированный файл CSV во внешнем редакторе обратите внимание на ограничения, описанные в разделе Список серверов.

**Порядок выполнения экспорта:**

1. Щелкните заголовок таблицы правой кнопкой мыши и нажмите **Экспорт списка серверов...**
  2. Введите имя для экспортного файла и нажмите **Сохранить**.
- ✓ Все столбцы списка серверов экспортируются в виде файла CSV.

**Дополнительная информация**

- *Server Lookup, Страница 22*
- Список серверов
- *Страница «Список серверов/Адресная книга», Страница 127*

**12.4.5****Импорт списка серверов**

Главное окно > **Устройства > Система Enterprise > Список серверов / адресная книга**

Если вы внесли изменения в экспортированный файл CSV во внешнем редакторе, обратите внимание на ограничения, описанные в разделе Список серверов.

**Импорт.**

1. Щелкните заголовок таблицы правой кнопкой мыши и нажмите **Импорт списка серверов...**
2. Нажмите нужный файл, затем нажмите **Открыть**.



**Дополнительная информация**

- *Server Lookup, Страница 22*
- Список серверов
- *Страница «Список серверов/Адресная книга», Страница 127*

## 12.5 Страница про сетевые видеорегистраторы NVR, резервные сетевые видеорегистраторы NVR и избыточные сетевые видеорегистраторы NVR

В версии 5.0 системы BVMS сетевые видеорегистраторы NVR, резервные сетевые видеорегистраторы NVR и избыточные сетевые видеорегистраторы NVR больше не поддерживаются.

## 12.6 Страница DiBos

Главное окно >  **Устройства** >  > .  
Отображает страницы свойств выбранной системы DiBos.  
Позволяет интегрировать систему DiBos в вашу систему.



### Замечание!



В данном случае вы настраиваете не систему DiBos, а соответствующие параметры BVMS.

- ▶ нажмите вкладку для перехода к соответствующей странице свойств.


### См.

- *Настройка интеграции системы DiBos, Страница 131*

### 12.6.1 Добавление системы DiBos путем поиска

Главное окно >  **Устройства** > щелкните правой кнопкой мыши  > команду **Добавить систему BRS/DiBos**  
Позволяет добавить систему DiBos к системе BVMS.

#### Чтобы добавить систему DiBos:

1. Щелкните правой кнопкой мыши .
2. Нажмите **Добавить систему BRS/DiBos**.  
Откроется диалоговое окно **Добавить систему BRS/DiBos**.
3. Введите соответствующие значения.
4. Нажмите **Сканировать**.  
Система DiBos будет добавлена в систему.
5. В появившемся окне нажмите кнопку **ОК** для подтверждения.

#### Диалоговое окно «Добавить систему DiBos»

##### Сетевой адрес

Введите имя DNS или IP-адрес системы DiBos.

##### Имя пользователя:



Введите имя пользователя для входа в систему DiBos.

##### Пароль:

Введите пароль для входа в систему DiBos.

## 12.6.2 Страница Настройки





Главное окно > **Устройства** > разверните  >  > вкладка **Настройки**  
Отображает сетевые параметры системы DiBos, подключенной к вашей системе.  
Позволяет при необходимости изменять настройки.

**См.**

– *Настройка интеграции системы DiBos, Страница 131*

## 12.6.3 Страница Камеры





Главное окно > **Устройства** > разверните  >  > вкладку **Камеры**  
Отображает все камеры системы DiBos, подключенной к вашей системе.  
Позволяет вам удалять камеры.

**См.**

– *Настройка интеграции системы DiBos, Страница 131*

## 12.6.4 Страница Входы





Главное окно > **Устройства** > разверните  >  > вкладку **Входы**  
Отображает все входы системы DiBos, подключенной к вашей системе.  
Позволяет вам удалять элементы.

**См.**

– *Настройка интеграции системы DiBos, Страница 131*

## 12.6.5 Страница Реле



Главное окно > **Устройства** > разверните  >  > вкладку **Реле**  
Отображает все реле системы DiBos, подключенной к вашей системе.  
Позволяет вам удалять элементы.

**См.**

– *Настройка интеграции системы DiBos, Страница 131*

## 12.6.6 Настройка интеграции системы DiBos



Главное окно > **Устройства** > разверните  > 



### **Замечание!**

В данном случае вы настраиваете не систему DiBos, а ее интеграцию в BVMS.

**Поиск новых устройств DiBos:**

- ▶ Щелкните правой кнопкой мыши  и выберите команду **Повторить поиск систем BRS/DiBos**.

Выполняется поиск и подключение новых устройств в системе DiBos.

**Удаление элемента:**

1. Перейдите на вкладку **Камеры, Реле** или **Входы**.
2. Щелкните элемент правой кнопкой мыши и выберите **Удалить**. Элемент будет удален из системы.

**Переименование устройства DiBos:**

1. Щелкните устройство DiBos правой кнопкой мыши и нажмите **Переименовать**.
2. Введите новое имя.

**12.7****Страница DVR (цифровой видеорегистратор)**

Главное окно >  **Устройства** >  > 

Отображает страницы свойств выбранного цифрового видеорегистратора.

Позволяет интегрировать цифровой видеорегистратор в вашу систему.

- ▶ Щелкните вкладку для перехода к соответствующей странице свойств.

**Замечание!**

В данном случае вы настраиваете не систему DVR, а только интеграцию устройства DVR в BVMS.

**Замечание!**

Добавьте DVR с помощью учетной записи администратора устройства. Использование учетной записи пользователя DVR с ограниченными разрешениями может привести к тому, что некоторые возможности не будут доступны в BVMS, например использование управления камерой PTZ.

**См.**

- *Цифровые видеорегистраторы, Страница 132*
- *Настройка интеграции цифрового видеорегистратора, Страница 135*

**12.7.1****Цифровые видеорегистраторы**

В этой главе предоставляются общие сведения о цифровых видеорегистраторах, которые можно интегрировать в BVMS.

Некоторые модели цифровых видеорегистраторов (например, DHR-700) поддерживают запись с кодеков / IP-камер. Другие модели цифровых видеорегистраторов поддерживают только аналоговые камеры.

Кодеры / IP-камеры не следует интегрировать в конфигурацию двух видеосистем (цифровые видеорегистраторы или системы управления видео).

Если кодеры / IP-камеры подключены к цифровому видеорегистратору, который уже интегрирован в BVMS, такие кодеры / IP-камеры не обнаруживаются при поиске сетевых устройств BVMS в сети. Это также верно для поиска в сети, запущенного из Configuration Client или Config Wizard.

Если цифровой видеореги­стратор с подключенными кодерами / IP-каме­рами интегрирован в BVMS и эти кодеры / IP-каме­ры уже добавлены в BVMS, отображается предупреждение. Удалите такие кодеры / IP-каме­ры из данного цифрового видеореги­стратора или BVMS.

Config Wizard не добавляет в конфигурацию цифровые видеореги­страторы с конфликтующими IP-каме­рами.

Цифровые видеореги­страторы поддерживают ограниченное число одновременных подключений. Это число определяет максимальное количество пользователей Operator Client, которые могут одновременно отображать видео с цифрового видеореги­стратора без отображения черных областей изображений.



#### **Замечание!**

Добавьте DVR с помощью учетной записи администратора устройства. Использование учетной записи пользователя DVR с ограниченными разрешениями может привести к тому, что некоторые возможности не будут доступны в BVMS, например использование управления камерой PTZ.



#### **Замечание!**

DIVAR AN 3000/5000: обратите внимание, что при удалении видеоданных с цифрового видеореги­стратора всегда удаляется не менее полного часа видеоданных. Например, если выбрать период времени с 6:50 до 7:05, фактически будут удалены все видеоданные с 6:00 до 8:00.

Гибридные и сетевые HD-видеореги­страторы Bosch серии 700: удаление всегда начинается с точки начала записи на всех камерах, которые отображаются в Operator Client, и заканчивается в указанной вами точке во времени.

#### **См.**

- *Страница DVR (цифровой видеореги­стратор), Страница 132*
- *Настройка интеграции цифрового видеореги­стратора, Страница 135*

## 12.7.2


### **Добавление устройств DVR путем поиска**

**Для добавления цифровых видеореги­страторов с помощью поиска выполните следующие действия.**

1. Щелкните правой кнопкой мыши  и выберите команду **Выполнить поиск устройств DVR**.  
Откроется диалоговое окно **BVMS Scan Wizard**.
2. Установите флажки для устройств, которые необходимо добавить.
3. Нажмите **Далее >>**.  
Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.  
Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.  
Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.  
Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в**

столбец.

В столбце **Состояние** успешные входы в систему обозначены значком .

Неудачные попытки входа обозначены значком .

5. Нажмите **Готово**.

Устройство добавлено в дерево устройств.

### 12.7.3

#### Диалоговое окно "Добавить цифровой видеорегистратор"



Главное окно >

**Устройства** > Разверните



> **Добавить цифровой**

**видеорегистратор**

Позволяет вручную добавить цифровой видеорегистратор.

##### Сетевой адрес / порт

Введите IP-адрес вашего цифрового видеорегистратора. При необходимости измените номер порта.

##### Имя пользователя:

Введите имя пользователя для подключения к цифровому видеорегистратору.

##### Пароль:

Введите пароль для подключения к цифровому видеорегистратору.

##### Безопасность

Флажок **Безопасное соединение** установлен по умолчанию.

Если безопасное подключение невозможно, отображается соответствующее сообщение.

Нажмите, чтобы снять флажок.



##### Замечание!

Если флажок **Безопасное соединение** установлен, подключения команд и управления защищены. Поточковая передача видеоданных не защищена.

См.

– *Добавление устройства, Страница 124*

### 12.7.4

#### Вкладка "Настройки"



Главное окно >

**Устройства** >



>



>

вкладка **Настройки**

Отображает сетевые параметры цифрового видеорегистратора, подключенного к вашей системе. Позволяет при необходимости изменять настройки.

### 12.7.5

#### Вкладка "Камера"



Главное окно >

**Устройства** >



>





>

вкладка **Камеры**



Все видеоканалы цифрового видеорегистратора отображаются как камеры. Позволяет вам удалять камеры.

Видеовход, отключенный в цифровом видеорегистраторе, отображается в BVMS как активная камера, так как для этого входа существуют более ранние записи.

## 12.7.6 Вкладка "Входы"

Главное окно > **Устройства** >  >  > вкладка **Входы**  
 Отображаются все выходы цифрового видеорегистратора.  
 Позволяет вам удалять элементы.

## 12.7.7 Вкладка "Реле"

Главное окно > **Устройства** >  >  > вкладка **Реле**  
 Отображаются все реле цифрового видеорегистратора. Позволяет вам удалять элементы.

## 12.7.8 Настройка интеграции цифрового видеорегистратора

Главное окно >  **Устройства** > Разверните  > 



### Замечание!

Добавьте DVR с помощью учетной записи администратора устройства. Использование учетной записи пользователя DVR с ограниченными разрешениями может привести к тому, что некоторые возможности не будут доступны в BVMS, например использование управления камерой PTZ.



### Замечание!

В данном случае вы настраиваете не систему DVR, а только интеграцию устройства DVR в BVMS.

### Удаление элемента:

1. Нажмите вкладку **Настройки**, вкладку **Камеры**, вкладку **Входы** или вкладку **Реле**.
2. Щелкните элемент правой кнопкой мыши и выберите **Удалить**. Элемент будет удален из системы.



### Замечание!

Для восстановления удаленного элемента щелкните правой кнопкой мыши по устройству DVR и нажмите **Повторить сканирование устройства DVR**.


### Переименование устройства DVR.

1. Щелкните устройство DVR правой кнопкой мыши и нажмите **Переименовать**.
2. Введите новое имя.

### См.

- *Добавление устройства, Страница 124*
- *Страница DVR (цифровой видеорегистратор), Страница 132*

## 12.8 Страница Матричные коммутаторы

Главное окно >  **Устройства** >  >   
 Отображает страницы свойств устройства Bosch Allegiant.

В данном случае вы настраиваете не устройство Bosch Allegiant, а соответствующие параметры BVMS. Сведения о подключении устройств Allegiant к BVMS содержатся в разделе **Понятия** настоящей справки. В данном разделе содержится основная информация по данным вопросам.

Дополнительно можно настроить приоритеты управления для магистральных линий Allegiant.

- ▶ нажмите вкладку для перехода к соответствующей странице свойств.


**См.**

- *Настройка устройства Bosch Allegiant, Страница 136*
- *Подключение матричного коммутатора Bosch Allegiant к BVMS, Страница 55*

## 12.8.1

### Добавление устройства Bosch Allegiant

**Чтобы добавить устройство Bosch Allegiant:**

1. Щелкните правой кнопкой мыши  и выберите команду **Добавить Allegiant**. Откроется диалоговое окно **Открыть**.
2. Выберите соответствующий файл конфигурации Allegiant и нажмите кнопку **ОК**. Устройство Bosch Allegiant будет подключено к системе.

**Примечание.** Можно добавить только один матричный коммутатор Bosch Allegiant.

## 12.8.2

### Настройка устройства Bosch Allegiant

Главное окно >  **Устройства** > Разверните  > 

В данном случае вы настраиваете не устройство Bosch Allegiant, а соответствующие параметры BVMS.

**Чтобы назначить выход кодеру:**

1. Перейдите на вкладку **Выходы**.
2. В столбце **Использование** щелкните **Цифровая магистраль** в нужных ячейках.
3. В столбце **Кодер** выберите требуемый кодер.

**Добавление входа к устройству Bosch Allegiant:**

1. Перейдите на вкладку **Входы**.
2. Нажмите **Добавить входы**. В таблицу будет добавлена новая строка.
3. Введите в ячейки требуемые параметры.

**Удаление входа:**

1. Перейдите на вкладку **Входы**.
2. Выберите нужную строку таблицы.
3. Нажмите **Удалить вход**. Строка будет удалена из таблицы.

**См.**

- *Подключение клавиатуры Bosch IntuiKey к BVMS, Страница 51*
- *Страница Соединение, Страница 138*
- *Страница Камеры, Страница 138*
- *Страница Выходы, Страница 137*
- *Страница Входы, Страница 137*



### 12.8.3 Страница Выходы



Главное окно > **Устройства** > Разверните  >  > вкладка **Выходы**

Позволяет настроить использование выхода устройства Bosch Allegiant и назначить выходу кодер.

Для сохранения видеоданных с выхода устройства Bosch Allegiant в системе BVMS вы должны назначить выходу кодер. Этот кодер должен быть подключен к выходу.

#### **№**

Отображает номер выхода.

#### **Логический № Allegiant**

Отображает логический номер выхода в пределах Allegiant.

#### **Логический номер BVMS**

Позволяет изменить логический номер выхода в пределах BVMS. Если вы введете номер, который уже используется, появляется соответствующее сообщение.

#### **Имя**

Отображает имя выхода.

#### **Использование**

Позволяет изменить использование выхода.

При выборе **Цифровая магистраль** можно назначить кодер этому выходу в поле **Кодер**.

Выход Allegiant становится совместимым с сетью.

При выборе **Монитор Allegiant** в Operator Client пользователь может назначить сигнал камеры аппаратному монитору. Управление PTZ возможно, если камера настроена как камера PTZ. В Operator Client пользователь не может перетащить эту камеру в область изображений.

При выборе **Не используется** пользователь не может назначить монитор камере Allegiant.

#### **Кодер**



Позволяет назначить выход кодеру. Можно выбрать кодер только в том случае, если вы установили флажок **Цифровая магистраль**. Кодер блокируется для логического дерева. Если вы назначили кодер, уже присутствующий в логическом дереве, он удаляется оттуда. В Operator Client пользователь не может перетащить камеру на область изображений.

#### **См.**

– *Настройка устройства Bosch Allegiant, Страница 136*

### 12.8.4 Страница Входы



Главное окно > **Устройства** > Разверните  >  > вкладка **Входы**

Позволяет добавлять входы к устройству Bosch Allegiant.

#### **Добавить вход**

Нажмите, чтобы добавить в таблицу строку для указания нового входа.

#### **Удалить вход**

Нажмите для удаления строки из таблицы.

#### **№ входа**

Введите номер входа. Если вы введете номер, который уже используется, появляется соответствующее сообщение.


**Имя входа**

Введите имя входа.

**См.**

– *Настройка устройства Bosch Allegiant, Страница 136*

**12.8.5****Страница Соединение**

Главное окно > **Устройства** > Разверните  >  > вкладка **Соединение**

Отображает имя файла конфигурации Bosch Allegiant.

BVMS может считывать информацию из файла конфигурации, имеющего формат структурированного хранилища, содержащего имена и информацию о конфигурации всех камер, подключенных к устройству Bosch Allegiant.


**Обновить конфигурацию**

Нажмите для выбора файла конфигурации BoschAllegiant.

**См.**

– *Настройка устройства Bosch Allegiant, Страница 136*

**12.8.6****Страница Камеры**

Главное окно > **Устройства** > Разверните  >  > вкладка **Камеры**

Отображает таблицу камер, подключенных к устройству Bosch Allegiant.

**№**

Отображает последовательный номер камеры.

**Логический № Allegiant**

Отображает логический номер камеры.

**Название камеры**

Отображает название камеры.

**См.**

– *Настройка устройства Bosch Allegiant, Страница 136*

**12.9****Страница Рабочая станция**

Главное окно > **Устройства** > разверните  > 

На рабочей станции должно быть установлено программное обеспечение Operator Client.

Позволяет настроить следующие параметры рабочей станции:

- Добавьте CCTV клавиатуру, подключенную к рабочей станции Bosch Video Management System.
- Выберите командный сценарий, исполняемый при запуске рабочей станции.
- Выберите поток по умолчанию для отображения в реальном времени.
- Включите функцию аналитического поиска.

**Примечание.** Невозможно настроить клавиатуру CCTV для рабочей станции по умолчанию. Это возможно только для определенно настроенных рабочих станций.

Чтобы добавить клавиатуру Bosch IntuiKey, которая подключена к декодеру, разверните



и нажмите

**См.**

- *Добавление рабочей станции вручную, Страница 139*
- *Настройка командного сценария, выполняющегося при запуске (страница «Настройки»), Страница 140*

## 12.9.1

### Добавление рабочей станции вручную


Чтобы добавить рабочую станцию BVMS:

1. Щелкните правой кнопкой мыши .
2. Нажмите **Добавить рабочую станцию**.  
Откроется диалоговое окно **Добавить рабочую станцию**.
3. Введите соответствующее значение.
4. Нажмите **ОК**.

Рабочая станция  будет добавлена в систему.

Чтобы добавить рабочую станцию BVMS по умолчанию:

- ▶ Щелкните правой кнопкой мыши .
- Нажмите **Добавить рабочую станцию по умолчанию**.

Рабочая станция  будет добавлена в систему.



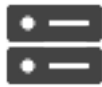
#### Замечание!

Вы можете добавить только одну рабочую станцию по умолчанию.

Если рабочая станция по умолчанию настроена, параметры применяются для каждой рабочей станции, которая подключена к данному серверу и не настраивается отдельно. Если рабочая станция настроена, применяются параметры данной рабочей станции, а не рабочей станции по умолчанию.

## 12.9.2

### Настройка клавиатуры Bosch IntuiKey (страница «Настройки») (рабочая станция)



Главное окно >  **Устройства** > Разверните  > 

Чтобы настроить клавиатуру Bosch IntuiKey, подключенную к рабочей станции:

1. Перейдите на вкладку **Настройки**.
2. В поле **Keyboard Settings** введите необходимые параметры.



Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

**См.**

- *Страница Рабочая станция, Страница 138*

### 12.9.3 Активация поиска на рабочей станции (страница «Настройки»)



Главное окно > **Устройства** > Развернуть  >  > страница **Настройки**  
Необходимо включить функцию Forensic Search на рабочей станции.

#### Примечание



Активируйте анализ видеоданных на каждом кодере. Воспользуйтесь страницей кодера VCAв логическом дереве.

#### Чтобы включить функцию Forensic Search:

- ▶ Установите флажок **Включить Forensic Search**.

### 12.9.4 Настройка командного сценария, выполняющегося при запуске (страница «Настройки»)



Главное окно > **Устройства** > Разверните  >  > **Настройки**

Можно настроить командный сценарий, который будет запущен при запуске Operator Client на выбранной рабочей станции.

Вы должны создать соответствующий командный сценарий.

Сведения о создании командного сценария см. *Управление командными сценариями, Страница 93*.

#### Чтобы настроить командный сценарий:



- ▶ Выберите нужный командный сценарий из списка **Сценарий запуска**.

#### См.

- *Страница Рабочая станция, Страница 138*

### 12.9.5 Страница Настройки



Главное окно > **Устройства** > разверните  >  > вкладка **Настройки**

Позволяет настроить сценарий, который будет выполняться при запуске Operator Client на рабочей станции.

Позволяет настроить TCP или UDP в качестве протокола передачи для всех камер, которые отображаются в режиме реального времени на рабочей станции.

Позволяет указать, какой поток IP-устройства используется для отображения в реальном времени.

Позволяет включить поиск для данной рабочей станции.

Можно также настроить клавиатуру, подключенную к данной рабочей станции.

#### Сетевой адрес:

Введите DNS-имя или IP-адрес вашей рабочей станции.

#### Сценарий запуска:

Выберите сценарий, который должен запускаться при запуске Operator Client рабочей станции. Этот сценарий можно создать или импортировать на странице **События**.

#### Протокол камеры по умолчанию:

Выберите протокол передачи данных по умолчанию, используемый для всех камер, назначенных логическому дереву на данной рабочей станции.

**Переопределить настройки со страницы "Камеры и запись"**

Установите флажок, чтобы активировать выбор нужного потока для отображения в реальном времени.

**Примечание.** Для цифровых видеорегистраторов, которые предоставляют более 1 потока (например, DIVAR AN 3000/5000), здесь также изменяется параметр "Поток просмотра в реальном времени" этого цифрового видеорегистратора. Параметры потоков просмотра в реальном времени для цифровых видеорегистраторов недоступны на странице **Камеры и запись**.

**Поток в реальном времени**

Выберите необходимый поток для просмотра в реальном времени.

При выборе **Оптимизирован размер области изображения** разрешение каждой отображаемой камеры настраивается автоматически в соответствии с размером области изображений в зависимости от разрешения используемого монитора. Это полезно для отображения нескольких камер с большим разрешением, например, камер 4K ultra HD. Только камеры с потоками, разрешение которых можно настроить независимо друг от друга, могут регулировать разрешение в соответствии с областью изображения. Пользователь Operator Client может изменить выбор потока для каждой камеры отдельно.

**Использовать вместо этого транскодированный поток (если доступен)**

Установите флажок, чтобы включить использование транскодированного потока, если он доступен. Этот транскодированный поток используется для просмотра в реальном времени вместо выбранного потока.

Чтобы в BVMS был доступен транскодированный поток, необходимо установить MVS, либо на компьютере VRM должен быть встроенный аппаратный транскодер.

При отображении камеры в режиме реального времени используется набор потоков по умолчанию для рабочей станции. Если у камеры нет потока 2 или сервис транскодирования (программный и аппаратный) недоступен, будет использоваться поток 1, даже если в параметрах рабочей станции настроен другой параметр.

**Включить Forensic Search**

Нажмите, чтобы включить поиск для данной рабочей станции.

**Использовать прямое воспроизведение из системы хранения данных**

Установите флажок для отправки видеопотока непосредственно с устройства хранения на эту рабочую станцию. Теперь поток не передается через VRM. Рабочей станции все равно требуется подключение к VRM, чтобы обеспечить правильное воспроизведение.

**Примечание.** Прямое воспроизведение с устройства хранения iSCSI можно использовать только в случае, если вы установили глобальный пароль CHAP iSCSI.

См. *Пароль для глобального подключения iSCSI (пароль CHAP):*, Страница 120

**Получать видеоизображение в реальном времени со шлюза Video Streaming Gateway вместо камеры**

Отображает список устройств Video Streaming Gateway. Выберите нужные записи, чтобы активировать передачу видеоданных через сегменты с низкой полосой пропускания между источником видеосигнала и данной рабочей станцией.

**Тип клавиатуры:**

Выберите тип клавиатуры, подключенной к рабочей станции.

**Порт:**

Выберите COM-порт, который используется для подключения клавиатуры.

**Скорость (бит/с):**

Выберите максимальную скорость передачи (в битах в секунду), с которой данные должны передаваться через этот порт. Обычно это значение соответствует максимальной скорости, поддерживаемой компьютером или устройством, с которым осуществляется связь.

**Информационные биты:**

Отображает количество битов, используемых для каждого передаваемого и принимаемого символа.

**Стоповые биты:**

Отображает время между каждым передаваемым символом (если время измеряется в битах).

**Четность:**

Отображает тип контроля четности, используемый для данного порта.

**Тип порта:**

Отображает тип соединения, которое используется для подключения клавиатуры Bosch IntuiKey к рабочей станции.


**См.**

- *Настройка командного сценария, выполняющегося при запуске (страница «Настройки»), Страница 140*
- *Активация поиска на рабочей станции (страница «Настройки»), Страница 140*
- *Пароль для глобального подключения iSCSI (пароль CHAP):, Страница 120*


**12.9.6****Изменение сетевого адреса рабочей станции**

Главное окно >  **Устройства** > Развернуть 

**Для изменения IP-адреса:**

1. Щелкните правой кнопкой мыши  и выберите команду **Изменить сетевой адрес**. Откроется диалоговое окно **Изменить сетевой адрес**.
2. Измените список в поле в соответствии с вашими требованиями.

**12.10****Страница Декодеры**

Главное окно >  **Устройства** > Разверните  > 

Позволяет добавлять и настраивать декодеры.

**Замечание!**

Если в системе необходимо использовать декодеры, убедитесь, что все кодеры используют один и тот же пароль для уровня авторизации user.

**См.**

- *Поиск устройств, Страница 73*
- *Страница «Кодер/декодер/камера Bosch», Страница 226*

## 12.10.1








### Добавление кодера и декодера вручную

Позволяет добавить кодер или декодер вручную. Это особенно полезно, если необходимо добавить какое-либо IP-видеоустройство производства Bosch (только для VRM).




#### Внимание.


Если добавляется IP-видеокодер или декодер Bosch с выбранным параметром **<Автоопределение>**, это устройство должно быть доступно в сети.



#### Добавление IP-видеоустройства производства Bosch:




- Разверните , разверните , щелкните правой кнопкой мыши .  
Или  
щелкните правой кнопкой мыши .  
Или  
щелкните правой кнопкой мыши .
- Нажмите **Добавить кодер**.  
Откроется диалоговое окно **Добавить кодер**.
- Введите соответствующий IP-адрес.
- В списке выберите **<Автоопределение>**.
- Нажмите **ОК**.  
Устройство будет добавлено в систему.
- Если для устройства требуется начальный пароль, отображается .  
Чтобы установить начальный пароль, щелкните правой кнопкой мыши значок устройства и нажмите **Задать первоначальный пароль....** Отобразится диалоговое окно  
**Введите пароль**.  
Введите пароль для пользователя service и нажмите **ОК**.  
 закроется; вы можете использовать устройство.

#### Диалоговое окно Добавить кодер

Главное окно >  **Устройства** > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Добавить кодер** > диалоговое окно **Добавить кодер**  
или

Главное окно >  **Устройства** > щелкните правой кнопкой мыши  > нажмите **Добавить кодер** > диалоговое окно **Добавить кодер**  
или

Главное окно >  **Устройства** > щелкните правой кнопкой мыши  > нажмите **Добавить кодер** > диалоговое окно **Добавить кодер**  
или

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Добавить декодер** > диалоговое окно **Добавить кодер**

**IP-адрес:**

Введите действительный IP-адрес.




**Тип кодера:/Тип декодера:**




Для устройства с известным типом выберите соответствующий элемент. Устройство не обязательно должно быть доступно в сети.




Если требуется добавить какое-либо IP-видеоустройство производства Bosch, выберите **<Автоопределение>**. Это устройство должно быть доступно в сети.

**12.10.2****Диалоговое окно «Изменить кодер / Изменить декодер»**

Главное окно  **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**  
или

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**  
или

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**  
или

Главное окно >  **Устройства** > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить декодер** > диалоговое окно **Изменить декодер**

Позволяет проверить и обновить возможности устройства. Устройство подключается при открытии этого диалогового окна. Запрашивается пароль, и возможности устройства сравниваются с возможностями устройства, сохраненными в BVMS.



**Имя**

Отображает имя устройства. При добавлении IP-видеоустройства производства Bosch имя устройства генерируется системой. При необходимости измените значение.

**Сетевой адрес / порт**

Введите сетевой адрес устройства. При необходимости измените номер порта.

**Имя пользователя**

Отображает имя пользователя, используемое для аутентификации на устройстве.

**Пароль**

Введите действующий пароль для аутентификации на устройстве.

**Отобразить пароль**

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог посмотреть этот пароль.

**Проверить подлинность**

Нажмите для аутентификации на устройстве с использованием введенных выше учетных данных.

**Безопасность**

Флажок **Безопасное соединение** установлен по умолчанию.

Если безопасное подключение невозможно, отображается соответствующее сообщение.

Нажмите, чтобы снять флажок.

**Следующие декодеры поддерживают безопасное соединение:**

- VID 7000
- VID 8000
- VIP XD HD

**Замечание!**

Соединение между декодером и кодером безопасно, только если они настроены с использованием безопасного соединения.

**Возможности устройства**

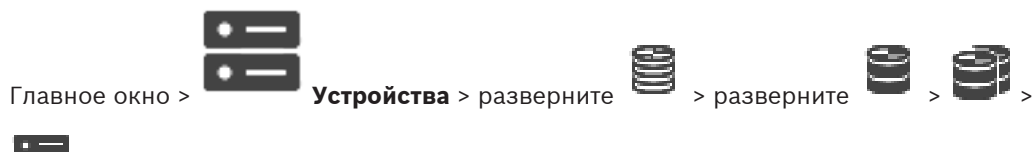
Отображаемые возможности устройства можно упорядочивать по категориям или по алфавиту.

Текст сообщения информирует о том, соответствуют ли автоматически определенные возможности устройства возможностям данного устройства.

Нажмите **ОК** для применения изменений возможностей устройства после обновления устройства.

**См.**

- *Шифрование видео в режиме реального времени («Изменение кодера»), Страница 229*
- *Обновление возможностей устройства («Изменение кодера»), Страница 230*

**12.10.3****Изменение пароля кодера и декодера («Изменить пароль»/«Введите пароль»)**

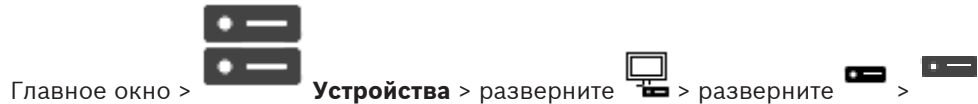
или



или




или



Определите или измените отдельный пароль для каждого уровня. Введите пароль (не более 19 символов; без специальных символов) для выбранного уровня.

**Для изменения пароля выполните следующие действия.**

1. щелкните правой кнопкой мыши  и нажмите **Изменить пароль....**  
Откроется диалоговое окно **Введите пароль**.
  2. Из списка **Введите имя пользователя** выберите пользователя, для которого необходимо изменить пароль.
  3. В поле **Введите пароль для пользователя** введите новый пароль.
  4. Нажмите **ОК**.
- ✓ Пароль на устройстве изменится незамедлительно.

Пароль препятствует несанкционированному доступу к устройству. Для ограничения доступа могут быть использованы различные уровни авторизации.

Надлежащая защита паролем обеспечивается только в тех случаях, когда все более высокие уровни авторизации также защищены паролем. Таким образом, всегда следует начинать с самого высокого уровня авторизации при назначении паролей.

Можно задать и изменить пароль для каждого уровня авторизации, если вы вошли в учетную запись пользователя «service».

Устройство имеет три уровня авторизации: service, user и live.

- service представляет собой высший уровень авторизации. Ввод правильного пароля дает доступ ко всем функциям и позволяет изменять все параметры конфигурации.
- user представляет собой средний уровень авторизации. На этом уровне можно эксплуатировать устройство, воспроизводить записи и управлять камерой, однако невозможно изменять конфигурацию.
- live представляет собой низший уровень авторизации. На этом уровне можно только просматривать видеоизображения в реальном времени и переключаться между различными экранами изображений в реальном времени.

Для декодера уровень авторизации live заменяется следующим уровнем авторизации:

- destination password (доступно только для декодеров)  
Используется для доступа к кодеру.

**См.**

- *Предоставление пароля пункта назначения декодеру («Проверка подлинности...»), Страница 222*

**12.10.4****Профиль декодера**

Позволяет настроить различные параметры отображения видео на мониторе VGA.

**Название монитора**

Введите название монитора. Название монитора позволяет дистанционно идентифицировать местонахождение монитора. Используйте название, которое позволит максимально просто и однозначно идентифицировать местонахождение.

Нажмите , чтобы обновить имя в дереве устройств.

**Стандартный**

Выберите выходной сигнал используемого монитора. Имеется восемь предварительно настроенных профилей параметров для мониторов VGA, кроме параметров PAL и NTSC для аналоговых видеомониторов.

**Замечание!**

Выбор параметра VGA со значениями, выходящими за пределы спецификаций монитора, может привести к серьезному повреждению монитора. Обратитесь к технической документации используемого вами монитора.

**Компоновка окна**

Выберите компоновку изображений по умолчанию для монитора.

**Размер VGA-экрана**

В данном поле введите соотношение сторон экрана (например, 4 x 3) или физические размеры экрана в миллиметрах. Устройство будет использовать эту информацию для точного масштабирования, не вносящего искажений в видеоизображение.

**12.10.5****Данные на мониторе**

Устройство распознает помехи передачи и отображает предупреждающее сообщение на мониторе.

**Показывать помехи передачи**

Выберите **Включено**, если на мониторе должно отображаться предупреждающее сообщение в случае возникновения помех передачи.

**Чувствительность к помехам**

Переместите ползунок, чтобы отрегулировать уровень помех, при котором отображается предупреждающее сообщение.

**Текст уведомления о помехах**

Введите текст предупреждения, которое отображается на мониторе при потере связи. Максимальная длина сообщения составляет 31 символ.

**12.10.6****Настройка клавиатуры Bosch IntuiKey (декодер)**

Главное окно >  **Устройства** > разверните  > 

**Замечание!**

Клавиатуру KBD-Universal XF невозможно подключить к декодеру.

**Чтобы настроить клавиатуру Bosch IntuiKey, подключенную к декодеру:**

- Щелкните ячейку в столбце **Соединение** и выберите соответствующий декодер. Вы также можете выбрать рабочую станцию, если к ней подключена клавиатура Bosch IntuiKey.




Рабочую станцию необходимо настроить на странице .

- В поле **Параметры подключения** введите необходимые параметры. Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

**См.**

- Страница "Назначить клавиатуру", Страница 163
- Сценарии подключения клавиатур Bosch IntuiKey, Страница 51
- Подключение клавиатуры Bosch IntuiKey к декодеру, Страница 53

**12.10.7****Настройка декодера для использования с клавиатурой Bosch IntuiKey**

Главное окно >  **Устройства** > Разверните  > Разверните .  
Выполните следующие действия для настройки декодера VIP XD, подключенного к клавиатуре Bosch IntuiKey.

**Чтобы настроить декодер:**

- Выберите соответствующий декодер, используемый для подключения к клавиатуре Bosch IntuiKey.
- Перейдите на вкладку **Периферия**.
- Убедитесь, что установлены следующие параметры:
  - Функция последов. порта:: **Прозрачный**
  - Скорость обмена данными:: **19200**
  - Стоповые биты: **1**
  - Контроль четности: **Нет**
  - Режим интерфейса: **RS232**
  - Полудуплексный режим:: **Выкл.**

**См.**

- Сценарии подключения клавиатур Bosch IntuiKey, Страница 51
- Подключение клавиатуры Bosch IntuiKey к декодеру, Страница 53
- Обновление программного обеспечения клавиатуры Bosch IntuiKey, Страница 54

**12.10.8****Удалить логотип декодера**

Нажмите для удаления логотипа, который был установлен на веб-странице декодера.

**12.11****Страница «Группы мониторов»**

Главное окно >  **Устройства** > разверните  > .  
Позволяет добавить и настроить группы мониторов. Группа мониторов назначается рабочей станции BVMS в .



**Замечание!**

Невозможно управлять группой мониторов в Operator Client, если соединение с Management Server потеряно.

**См.**

- *Добавление группы мониторов вручную, Страница 149*
- *Настройка группы мониторов, Страница 149*
- *Настройка предустановленных положений и дополнительных команд, Страница 307*
- *Настройка тревоги, Страница 333*
- *Диалоговое окно Параметры тревог, Страница 323*
- *Диалоговое окно «Выбрать содержимое области изображений» (MG), Страница 322*

**12.11.1****Добавление группы мониторов вручную**

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши






> нажмите **Добавить группу мониторов**

1. Нажмите **Добавить группу мониторов**.  
Отобразится диалоговое окно **Добавить группу мониторов**. Введите имя новой группы мониторов.
2. Нажмите «ОК».  
Группа мониторов добавлена в систему.



3. Нажмите **Карты и структура**.
4. Перетащите группу мониторов в Логическое дерево.

**12.11.2****Настройка группы мониторов**

Главное окно >  **Устройства** > разверните  >  > 

**Замечание!**

Невозможно управлять группой мониторов в Operator Client, если соединение с Management Server потеряно.

Вы можете настроить мониторы в группе мониторов логически по столбцам и строкам. Это расположение не обязательно должно соответствовать реальному расположению мониторов.

**Для настройки группы мониторов выполните следующие действия.**

1. Перетащите соответствующие мониторы из вкладки **Не назначенные мониторы** в поле группы мониторов.
2. На вкладке **Схема** выберите соответствующую схему.

3. Перетащите любую доступную камеру из вкладки **Камеры** в область мониторов слева. Логический номер камеры отображается черным цветом в области мониторов, а цвет этой области меняется.
4. Измените логические номера областей изображений соответствующим образом. Если ввести номер, который уже используется, появляется соответствующее сообщение.
5. На вкладке **Параметры** можно выбрать, будут ли отображаться имя и номер камеры в области мониторов. Вы также можете выбрать расположение этой информации.

#### Изображение монитора

Номер, выделенный полужирным шрифтом черного цвета, если он присутствует, обозначает логический номер первоначальной камеры. Номер светло-черного цвета является логическим номером монитора.

Чтобы отменить назначение камеры, щелкните правой кнопкой мыши в области мониторов и выберите **Очистить область** или перетащите камеру за пределы области изображений.

См.

– *Добавление группы мониторов вручную, Страница 149*

## 12.12

### Страница Настенная панель мониторов



Позволяет добавить приложение видеостены. Это приложение позволяет управлять оборудованием видеостены из Operator Client. При управлении видеостеной сервер не используется. Это означает, что пользователь Operator Client всегда может управлять видеостеной, даже если Management Server отключен.

#### Имя

Введите отображаемое имя для видеостены.

#### Монитор

Выберите монитор, подключенный к декодеру.

Если добавляется декодер, к которому подключено 2 монитора, необходимо открыть диалоговое окно **Изменить декодер** декодера и обновить возможности устройства для этого декодера. Для каждого монитора добавляйте дополнительную видеостену.

#### Максимальное количество камер для подключения

Введите максимальное число камер, которое может отображаться на видеостене. Если оставить это поле пустым, оператор может отображать столько камер, сколько есть доступных областей изображения в раскладке видеостены.

#### Включить миниатюры

Нажмите, чтобы установить флажок, если необходимо отобразить снимок в Operator Client для каждого монитора. Этот снимок периодически обновляется.

#### Начальная последовательность

Выберите последовательность камер, которая будет отображаться на видеостене при ее запуске оператором.

**Замечание!**

Если последовательность удалена в диалоговом окне **Конструктор последовательностей**, она автоматически удаляется из списка **Начальная последовательность** видеостены, если она задана в нем.

См.

– *Диалоговое окно Конструктор последовательностей, Страница 276*

**12.12.1****Добавление видеостены вручную**

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Добавить группу мониторов**.


Добавьте нужный декодер к BVMS, прежде чем добавлять настенную панель мониторов. После добавления видеостены пользователь Operator Client может ей управлять. Пользователь может изменить схему расположения мониторов и назначить кодеры мониторам.

**Добавление**

1. Выберите требуемый декодер.
2. При необходимости введите максимальное количество камер и настройте миниатюры.
3. Нажмите **ОК**.

4. Нажмите  .

5. Нажмите  **Карты и структура**.

6. Нажмите  **Структура**.
7. Перетащите видеостену в Логическое дерево.
8. При необходимости настройте доступ к видеостене с помощью соответствующих разрешений групп пользователей.

**Диалоговое окно Добавить группу мониторов****Имя**

Введите отображаемое имя для видеостены.

**Монитор**

Выберите монитор, подключенный к декодеру.

Если добавляется декодер, к которому подключено 2 монитора, необходимо открыть диалоговое окно **Изменить декодер** декодера и обновить возможности устройства для этого декодера. Для каждого монитора добавляйте дополнительную видеостену.

**Максимальное количество камер для подключения**

Введите максимальное число камер, которое может отображаться на видеостене. Если оставить это поле пустым, оператор может отображать столько камер, сколько есть доступных областей изображения в раскладке видеостены.

**Включить миниатюры**

Нажмите, чтобы установить флажок, если необходимо отобразить снимок в Operator Client для каждого монитора. Этот снимок периодически обновляется.

**Начальная последовательность**

Выберите последовательность камер, которая будет отображаться на видеостене при ее запуске оператором.

## 12.13 Страница Устройства связи



Позволяет добавлять и настраивать устройства связи.

Можно настроить следующие устройства связи:


- Электронная почта
- SMS (провайдер GSM или SMSC)

**См.**

- *Настройка устройства связи, Страница 154*

### 12.13.1 Добавление сервера электронной почты/SMTP

**Чтобы добавить устройство связи:**

1. Разверните , щелкните правой кнопкой мыши  и нажмите **Добавить устройство E-mail/SMTP**.

Откроется диалоговое окно **Добавить устройство E-mail/SMTP**.

2. Введите соответствующие параметры.
3. Нажмите **ОК**.

Устройство связи будет добавлено в систему.



#### **Диалоговое окно Добавить устройство E-mail/SMTP**

**Имя:**

Введите отображаемое имя сервера электронной почты.

### 12.13.2 Добавление устройства SMS

**Чтобы добавить устройство связи:**

1. Разверните , щелкните правой кнопкой мыши  и нажмите **Добавить устройство SMS**.

Отобразится диалоговое окно **Добавить устройство SMS**.

2. Введите соответствующие параметры.
3. Нажмите **ОК**.

Устройство связи будет добавлено в систему.

#### **Диалоговое окно Добавить устройство SMS**

**Имя:**

Введите имя сервера SMS, которое будет отображаться на экране.

**Модем GSM**

Нажмите, чтобы добавить модем GSM.



### Коммутируемый доступ SMSC

Нажмите, чтобы добавить модем, совместимый с Hayes, который может подключаться к провайдеру SMSC.

## 12.13.3

### Страница Сервер SMTP



Главное окно >

**Устройства** > разверните



> разверните



Позволяет настроить параметры электронной почты вашей системы. На странице **События** можно назначить событие электронному сообщению. Когда это событие происходит, система отправляет электронное сообщение. Вы можете получать электронную почту в BVMS.

#### Имя сервера SMTP

Введите имя сервера электронной почты. Информацию об этом вы можете получить у своего провайдера. Обычно это IP-адрес или DNS-имя вашего почтового сервера.

#### Адрес отправителя

Введите адрес электронной почты, который используется системой в качестве адреса отправителя сообщений электронной почты, например в случае тревоги.

#### SSL/TLS

Установите флажок, чтобы включить использование защищенного соединения SSL/TLS. В этом случае автоматически выбирается сетевой порт 587.

#### Порт

Введите номер сетевого порта для исходящей почты. Информацию об этом вы можете получить у своего провайдера.

Если параметр **SSL/TLS** отключен, автоматически выбирается порт 25.

При необходимости можно выбрать другой порт.

#### Время ожидания при соединении (сек)

Введите количество секунд бездействия, после которых подключение будет прервано.

#### Проверка подлинности

Установите флажок напротив нужного способа аутентификации. Информацию об этом вы можете получить у своего провайдера.

#### Имя пользователя

Введите имя пользователя для аутентификации на сервере электронной почты.

Информацию об этом вы можете получить у своего провайдера.

#### Пароль:

Введите пароль для аутентификации на сервере электронной почты. Информацию об этом вы можете получить у своего провайдера.




#### Отправить тестовое электронное сообщение

Нажмите для отображения диалогового окна **Отправить тестовое электронное сообщение**.



#### См.

– *Настройка устройства связи, Страница 154*

### 12.13.4 Настройка устройства связи

Главное окно >  **Устройства** > разверните  > разверните 

**Чтобы настроить устройство связи:**





1. Выберите нужное устройство:  или .
2. Установите необходимые параметры.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

**См.**

- *Добавление сервера электронной почты/SMTP, Страница 152*
- *Добавление устройства SMS, Страница 152*
- *Страница Сервер SMTP, Страница 153*
- *Страница Настройки GSM / Настройки SMSC, Страница 154*

### 12.13.5 Диалоговое окно Отправить тестовое электронное сообщение

Главное окно >  **Устройства** > разверните  > разверните  >  >

кнопка **Отправить тестовое электронное сообщение**

Позволяет отправить тестовое электронное сообщение.

**От:**

Введите адрес электронной почты отправителя.

**Кому**

Введите адрес электронной почты получателя.

**Тема**

Введите тему электронного сообщения.

**Сообщение**

Введите текст сообщения.





**Отправить тестовое электронное сообщение**

Нажмите для отправки сообщения.

**См.**

- *Настройка устройства связи, Страница 154*

### 12.13.6 Страница Настройки GSM / Настройки SMSC

Главное окно >  **Устройства** > разверните  > разверните  > 

Позволяет настроить параметры SMS-сообщений вашей системы BVMS. На странице **События** можно назначить событие SMS-сообщению. Когда это событие происходит, система отправляет SMS-сообщение. Если количество введенных символов превышает установленный уровень (обычно 160 символов), SMS-сообщение будет разбито на несколько частей.

**Устройство:**

Выберите COM-порт, к которому подключен внешний модем. Если ваш компьютер имеет внутренний модем, выберите соответствующий пункт.

**Скорость**

Выберите скорость передачи.

**PIN (только для устройств GSM)**

Введите личный идентификационный номер для аутентификации на устройстве.

**Формат данных (только для устройств SMSC)**

Выберите нужный формат даты. Информацию об этом вы можете получить у своего провайдера.

**Юникод (только для устройств GSM)**

Установите флажок для включения символов Unicode. Это сокращает максимально допустимое количество символов до 80.

**Строка набора (только для устройств SMSC)**

Введите телефонный номер для подключения к провайдеру SMSC. Этот номер вы можете получить у своего провайдера.

**Пароль: (только для устройств SMSC)**

Если требуется, введите пароль, необходимый устройству для телефонного подключения к провайдеру SMSC. Информацию об этом вы можете получить у своего провайдера.

**Протокол (только для устройств SMSC)**

Выберите протокол, используемый устройством для подключения к провайдеру SMSC. Информацию об этом вы можете получить у своего провайдера.

**Получатель**

Введите номер мобильного телефона получателя SMS-сообщений. Введите префикс страны без знака "+" (например, 49170123456).

**Сообщение (макс. 160 символов)**

Введите текст SMS-сообщения.

**Тестовое SMS-сообщение**

Нажмите для отправки тестового SMS-сообщения.

**См.**

– *Настройка устройства связи, Страница 154*

## 12.14

### Страница ATM/POS



Главное окно >

**Устройства** > разверните



>




Позволяет добавлять и настраивать периферийные устройства, например мост Bosch ATM/POS.

Чтобы добавить несколько мостов к одному серверу необходимо использовать разные порты.

**См.**



- *Добавление моста Bosch ATM/POS, Страница 101*
- *Настройка периферийных устройств, Страница 157*

## 12.14.1 Добавление моста Bosch ATM/POS вручную

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > команда **Добавить мост ATM/POS Bosch**.

Позволяет добавить мост Bosch ATM/POS.

**Чтобы добавить периферийное устройство:**

1. Разверните , щелкните правой кнопкой мыши  и нажмите **Добавить мост ATM/POS Bosch**.  
Отобразится диалоговое окно **Добавить мост ATM/POS Bosch**.
2. Введите соответствующие параметры.
3. Нажмите кнопку **ОК**.  
Периферийное устройство будет добавлено в систему.

**Диалоговое окно Добавить мост ATM/POS Bosch**

**Имя:**

Введите соответствующее имя устройства.

**IP-адрес:**

Введите IP-адрес устройства.

**Порт 1:**

Введите соответствующий номер порта, используемого как порт прослушивания моста ATM/POS.

**Порт 2:**

Введите номер порта, используемый как слушающий порт BVMS Management Server.







**Замечание!**

При добавлении нескольких мостов ATM/POS в систему убедитесь, что номера порта 2 на каждом из устройств отличаются. Использование одного номера для порта 2 несколько раз может привести к потере данных ATM/POS.

**См.**

– *Добавление моста Bosch ATM/POS, Страница 101*

## 12.14.2 Страница Мост ATM/POS Bosch

Главное окно >  **Устройства** > Разверните  > Разверните  >  >  
Вкладка **Мост ATM/POS Bosch**

Позволяет настраивать Bosch ATM/POS Bridge.

**IP-адрес:**

Введите IP-адрес устройства.

**Порт 1:**

Введите соответствующий номер порта, используемого как порт прослушивания моста ATM/POS.

**Порт 2:**

Введите номер порта, используемый как слушающий порт BVMS Management Server.

**Замечание!**






При добавлении нескольких мостов ATM/POS в систему убедитесь, что номера порта 2 на каждом из устройств отличаются. Использование одного номера для порта 2 несколько раз может привести к потере данных ATM/POS.

**См.**

- *Настройка периферийных устройств, Страница 157*
- *Добавление моста Bosch ATM/POS, Страница 101*

**12.14.3****Настройка периферийных устройств**

Главное окно >  **Устройства** > разверните  > разверните  >  **Мост ATM/POS Bosch**  
или

Главное окно >  **Устройства** > разверните  > разверните  >   
 **Устройство DTP** >

**Чтобы настроить периферийное устройство:**





- ▶ Измените требуемые параметры.

Для получения подробной информации о различных полях щелкните ссылку на соответствующее окно приложения ниже.

**См.**

- *Страница Настройки банкомата, Страница 157*
- *Страница Мост ATM/POS Bosch, Страница 156*
- *Страница "Настройки DTP", Страница 157*

**12.14.4****Страница "Настройки DTP"**

Главное окно >  **Устройства** > разверните  > разверните  >   
Позволяет настраивать устройство DTP с не более чем 4 устройствами ATM, подключенными к этому устройству DTP.






**Последовательный порт**

Выберите соответствующий порт из списка.

**См.**

- *Страница Настройки банкомата, Страница 157*
- *Настройка периферийных устройств, Страница 157*

**12.14.5****Страница Настройки банкомата**

Главное окно >  **Устройства** > разверните  > разверните  >  >   
Позволяет настраивать устройство ATM, подключенное к DTP.

**Номер входа устройства DTP**

Выберите требуемый номер ввода. Если этот номер уже используется другим устройством ATM, можно поменять номера вводов.

**Время ожидания подключения [часы]**

Введите необходимое количество часов. Если во время этого периода устройство ATM не отправило никаких данных транзакций, система BVMS делает допущение, что связь прервана. Запускается соответствующее событие. Событие **Не авторизовано** доступно для устройства ATM, но не имеет к нему отношения.

Ввод значения **0** означает, что проверка соединения не выполняется.





**Входы данных**

Нажмите, чтобы включить необходимые входы и введите требуемое имя для вводов.

**См.**

– *Настройка периферийных устройств, Страница 157*

**12.14.6****Страница Входы**

Главное окно >  **Устройства** > разверните  > разверните  >  > вкладка **Входы**




Позволяет настраивать входы моста ATM/POS Bosch.

**См.**

– *Настройка периферийных устройств, Страница 157*

– *Добавление моста Bosch ATM/POS, Страница 101*

**12.15****Устройства чтения кредитных карточек**

Главное окно >  **Устройства** > Разверните  >  > Вкладка **Глобальные настройки для устройств чтения кредитных карточек**

Можно настроить параметры, которые будут действительны для всех устройств чтения кредитных карточек в системе.

**Последовательный порт**

Выберите последовательный порт, к которому подключено устройство чтения кредитных карточек.

**Заблокировано**

Позволяет добавлять коды банковской маршрутизации для блокировки. Это означает, что карточки с введенными здесь характеристиками не обладают авторизацией для доступа. Доступ блокируется устройством чтения кредитных карточек. Необходимо установить следующий режим по умолчанию отпираания электрического замка двери для устройства чтения кредитных карточек: **Автоматически**

Этот список может содержать элементы с подстановочными символами.

?: означает любой символ или отсутствие символа в этой позиции.

\*: означает последовательность (один или несколько символов) любых символов или их отсутствие (исключение: отдельный символ \* означает, что все коды банковской сортировки блокируются).

### Игнорировать код страны на картах ЕС

Нажмите, чтобы включить режим, в котором система BVMS не анализирует используемые данные карточки для определения страны, в которой карта была выпущена. Доступ возможен для карточек с другим кодом страны.

## 12.15.1

### Диалоговое окно "Добавление устройства чтения кредитных карточек"

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > команда **Добавить устройство чтения кредитных карточек**  
Можно добавить устройство чтения кредитных карточек.

#### Имя





Введите имя для устройства.

#### Идентификатор устройства

Выберите уникальный номер для устройства. Если доступных номеров нет, в систему уже добавлено максимальное количество устройств чтения кредитных карточек.

## 12.15.2

### Страница "Параметры устройства чтения кредитных карточек"

Главное окно >  **Устройства** > разверните  >  >  > вкладка **Настройки для устройства чтения кредитных карт**  
Можно настроить устройство чтения кредитных карточек.

#### Идентификатор устройства

Отображает уникальный номер устройства.

#### Включить защиту от скимминга

Нажмите, чтобы включить режим, в котором система BVMS запускает событие, когда подключенный скиммер обнаруживает скимминг. Этот режим поддерживается не всеми типами устройств чтения кредитных карточек.

#### Режим открывания электрического замка двери по умолчанию

**Открыть:** дверь открыта и любой человек может получить доступ без карты.

**Закрыто:** дверь закрыта независимо от того, какая карта вставляется.

**Автоматически:** дверь открывается, только когда в считыватель вставляется карта с авторизацией для доступа.

#### Включить управление на основе расписания

Нажмите, чтобы включить режим, в котором можно назначать расписание для выбранного режима отпирания замка двери.

Когда расписание становится активным, BVMS переключает устройство чтения кредитных карточек в соответствующий режим отпирания.

Если выбранные расписания накладываются друг на друга, действительный режим отпирания двери определяется по следующему приоритету режимов: 1. **Открыть** 2.

**Закрыто** 3. **Автоматически**

## 12.16

### Страница Виртуальные входы

Главное окно >  **Устройства** > разверните  > 

Отображает виртуальные входы, сконфигурированные в вашей системе. Позволяет добавить новые виртуальные входы и удалить существующие.

#### Добавить входы

Нажмите для отображения диалогового окна добавления новых виртуальных входов.

#### Удалить входы

Нажмите для удаления выбранного виртуального входа.

#### №

Отображает номер виртуального входа.


#### Имя

Щелкните ячейку, чтобы изменить имя виртуального входа.

### 12.16.1

#### Добавление виртуальных входов вручную



Главное окно > **Устройства** > разверните  > кнопка **Добавить входы**

Позволяет добавить новые виртуальные входы.

**Для добавления виртуального входа выполните следующие действия.**

1. Разверните  и щелкните  .  
Откроется соответствующая страница.
2. Нажмите **Добавить входы**.  
В таблицу будет добавлена новая строка.
3. Настройте необходимые параметры.
4. Нажмите **Добавить**.  
Виртуальный вход будет подключен к системе.

#### Диалоговое окно Добавить входы

##### Начало:

Выберите первый номер новых виртуальных входов.

##### Конец:

Выберите последний номер новых виртуальных входов.

##### Имя:

Введите имя каждого нового виртуального входа. Добавляется последовательный номер.



##### Добавить

Нажмите для добавления новых виртуальных входов.

### 12.17

#### Страница SNMP





Главное окно > **Устройства** > разверните  >   
Позволяет добавить и настроить измерения SNMP для поддержания качества сети.

#### См.

- *Настройка приемника запросов SNMP (страница приемника запросов SNMP), Страница 161*





## 12.17.1 Добавление SNMP вручную

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > команда **Добавить SNMP**

Позволяет добавить систему сетевого мониторинга к системе BVMS.

**Для добавления устройства мониторинга сети выполните следующие действия.**

1. Разверните , щелкните правой кнопкой мыши  и нажмите **Добавить SNMP**.  
Откроется диалоговое окно **Добавить SNMP**.
2. Введите имя устройства SNMP.  
Устройство мониторинга сети будет подключено к системе.

### Диалоговое окно Добавить SNMP

#### Имя:

Введите имя устройства мониторинга сети.


#### См.

- *Настройка приемника запросов SNMP (страница приемника запросов SNMP),  
Страница 161*

## 12.17.2 Настройка приемника запросов SNMP (страница приемника запросов SNMP)


Главное окно >  **Устройства** > разверните 

**Чтобы настроить SNMP trap receiver, выполните следующие действия.**

1. Нажмите  для отображения страницы **Приемник запросов SNMP**.
2. Установите требуемые параметры.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

### Страница Приемник запросов SNMP.

Главное окно >  **Устройства** > разверните  > разверните 

Позволяет выбрать устройства для мониторинга и выбрать OID trap SNMP, которые запускают событие для выбранного устройства при получении.



#### Замечание!

Следует ввести IP-адрес Bosch Video Management System Management Server в качестве trap-приемника мониторируемых устройств.

#### Устройства отправки запросов SNMP:

Позволяет ввести диапазон IP-адресов отслеживаемых сетевых устройств. Для мониторинга отдельного устройства введите соответствующий IP-адрес в ячейке **Диапазон от**.

Будьте внимательны при изменении этих адресов. При вводе неверного адреса мониторинг устройства прекращается.

#### **Правила фильтров запросов SNMP:**

Позволяют ввести идентификаторы объектов и соответствующие значения. Для расширения диапазона фильтра можно использовать такие подстановочные знаки, как «\*» и «?». При вводе идентификаторов объектов и значений в нескольких строках эти правила фильтра должны соблюдаться одновременно, чтобы событие было активировано. В каждом из столбцов можно ввести регулярное выражение в фигурных скобках {}. Если эти символы находятся вне скобок, выражение не считается регулярным.



#### **Показать средство регистрации запросов**

Нажмите, чтобы отобразить диалоговое окно **Журнал регистрации запросов SNMP** для отслеживания идентификаторов запросов SNMP.

### 12.17.3

#### **Диалоговое окно Журнал регистрации запросов SNMP**



Главное окно > **Устройства** > разверните  > разверните  > выберите универсальный приемник ловушек SNMP > нажмите **Показать средство регистрации запросов**

Позволяет отслеживать OIDловушкиSNMP. Можно получать ловушки от всех устройств в сети или только от выбранных. Можно фильтровать получаемые запросы и добавлять идентификаторы объектов и значения выбранных запросов в таблицу **Правила фильтров запросов SNMP**.

#### **Старт/Пауза**

Нажмите для запуска или остановки процесса отслеживания.

#### **Только запросы отправителя**

Введите IP-адрес или DNS-имя устройства. Отслеживаются только запросы данного устройства.

#### **Только запросы, содержащие**

Введите строку, которую должен содержать запрос. Пользуйтесь подстановочными символами \* и ?. Строки в фигурных скобках {} рассматриваются как регулярные выражения. Отслеживаются только запросы, содержащие данную строку.

#### **Полученные запросы**

Отображаются запросы, полученные в процессе отслеживания.



Нажмите, чтобы удалить все записи в поле **Полученные запросы**.




#### **Подробные сведения о запросе**

Отображаются подробные сведения о запросе. Можно скопировать идентификатор объекта и значение в таблицу **Правила фильтров запросов SNMP**.

#### **См.**



- *Настройка приемника запросов SNMP (страница приемника запросов SNMP), Страница 161*

## 12.18 Страница "Назначить клавиатуру"

Главное окно >  **Устройства** > Разверните  >  .  
 Позволяет добавить клавиатуру KBD-Universal XF (подключенную к рабочей станции BVMS) или клавиатуру Bosch IntuiKey (подключенную к рабочей станции BVMS или декодеру).

**Для добавления клавиатуры CCTV выполните следующие действия.**

**Примечание.** Для добавления клавиатуры необходимо сначала добавить рабочую станцию.

1. Разверните  и щелкните  .  
Откроется соответствующая страница.
2. Нажмите **Добавить клавиатуру**.  
В таблицу будет добавлена новая строка.
3. В соответствующем поле столбца **Тип клавиатуры** выберите нужный тип клавиатуры:  
**Клавиатура IntuiKey**  
**KBD-Universal XF Keyboard**
4. В соответствующем поле столбца **Соединение** выберите рабочую станцию, к которой подключена клавиатура.
5. Настройте необходимые параметры.  
Клавиатура будет добавлена в систему.

### Добавить клавиатуру

Нажмите, чтобы добавить в таблицу строку для настройки клавиатуры.

### Удалить клавиатуру

Нажмите, чтобы удалить выделенную строку.

### Тип клавиатуры



Отображает тип клавиатуры, подключенной к рабочей станции или декодеру.

Нажмите ячейку, чтобы выбрать необходимый тип клавиатуры.

- **IntuiKey**  
Выберите этот тип, если вы подключили клавиатуру IntuiKey производства Bosch.
- **KBD-Universal XF Keyboard**  
Выберите этот тип, если вы подключили клавиатуру KBD-Universal XF.

### Соединение

Выберите в ячейке тип устройства, к которому подключена клавиатура. При выборе

рабочей станции клавиатура также добавляется на страницу  >  .

### Порт

Выберите в ячейке соответствующий COM-порт.

### Скорость (бит/с)

Выберите в ячейке максимальную скорость передачи (в битах в секунду), с которой данные должны передаваться через этот порт. Обычно это значение соответствует максимальной скорости, поддерживаемой компьютером или устройством, с которым осуществляется связь.

### Информационные биты

Отображает количество информационных битов, используемых для каждого передаваемого и принимаемого символа.

**Стоповые биты**

Отображает время между каждым передаваемым символом (если время измеряется в битах).

**Четность**

Отображает тип контроля четности, используемый для данного порта.




**Тип порта**

Отображает тип соединения, которое используется для подключения клавиатуры Bosch IntuiKey к рабочей станции.

**См.**

- *Настройка декодера для использования с клавиатурой Bosch IntuiKey, Страница 148*
- *Настройка клавиатуры Bosch IntuiKey (страница «Настройки») (рабочая станция), Страница 139*
- *Настройка клавиатуры Bosch IntuiKey (декодер), Страница 147*

**12.19****Страница Модули ввода/вывода**



Главное окно >  **Устройства** > разверните  >   
 Позволяет добавить и настроить модули ввода/вывода.  
 В настоящее время поддерживаются только устройства ADAM.

**См.**

- *Настройка модуля ввода/вывода, Страница 164*

**12.19.1****Добавление модуля ввода/вывода вручную**





**Чтобы добавить модуль ввода/вывода:**

1. Разверните , щелкните правой кнопкой мыши  и нажмите **Добавить новое устройство ADAM**.  
 Отображается диалоговое окно **Добавить ADAM**.
2. Введите IP-адрес устройства.
3. Выберите тип устройства.  
 Отобразится соответствующая страница.
4. Если нужно, перейдите на вкладку **ADAM**, чтобы изменить краткие имена входов.
5. Если нужно, перейдите на вкладку **Имя**, чтобы изменить краткие имена реле.

**Замечание!**

Вы также можете выполнить поиск устройств ADAM (**Выполнить поиск устройств ADAM**). Будут определены IP-адреса устройств. При доступности тип устройства выбран заранее. Вы должны подтвердить этот выбор.

**12.19.2****Настройка модуля ввода/вывода**

Главное окно >  **Устройства** > Разверните  > Разверните  > 

**Чтобы настроить модуль ввода/вывода:****Замечание!**

Избегайте изменения типа устройства.

При уменьшении количества входов или реле удаляются все данные конфигурации удаленных входов или реле.

1. Перейдите на вкладку **ADAM**.
2. Выберите соответствующий тип устройства из списка **Тип ADAM**.
3. Перейдите на вкладку **Входы**.
4. В столбце **Имя** при необходимости измените краткое имя входа.
5. Перейдите на вкладку **Реле**.
6. При необходимости измените имя реле в столбце **Реле**.



**Изменение IP-адреса:**

1. В дереве устройств щелкните правой кнопкой мыши устройство ADAM.
2. Выберите **Изменить сетевой адрес**.
3. Введите новый IP-адрес и нажмите **ОК**.
4. Активируйте конфигурацию.
- ✓ Новый IP-адрес используется для доступа к устройству.

**См.**

– *Страница Модули ввода/вывода, Страница 164*

**12.19.3****Страница ADAM**

Главное окно > **Устройства** > Разверните  >  > Вкладка **ADAM**

Отображается информация о выбранном устройстве ADAM.

Позволяет изменить краткое имя устройства ADAM.

**Тип ADAM:**

Выберите соответствующий тип устройства.


**Входов всего:**

Отображает общее количество входов, доступных для этого типа устройства.

**Реле/выходов всего:**

Отображает общее количество реле, доступных для этого типа устройства.

**12.19.4****Страница Входы**

Главное окно > **Устройства** > Разверните  >  > Вкладка **Входы**

Позволяет изменять краткие имена входов выбранного устройства ADAM.

**Номер**

Отображает логический номер входа.

**Имя**

Щелкните ячейку, чтобы изменить краткое имя входа.

## 12.19.5 Страница Реле



Главное окно > **Устройства** > Разверните > > Вкладка **Реле**

Позволяет изменять краткие имена реле выбранного устройства ADAM.

### Номер

Щелкните ячейку, чтобы изменить логический номер реле.

### Имя

Введите краткое имя реле.

## 12.20 Страница Эмуляция Allegiant CCL



Главное окно > **Устройства** > Разверните > >

Позволяет активировать эмуляцию Allegiant CCL.

*Команды Allegiant CCL, поддерживаемые в системе BVMS, Страница 60* содержит команды CCL, поддерживаемые в Bosch Video Management System.

### Примечание.

Не настраивайте эмуляцию Allegiant CCL и устройство Allegiant на один и тот же COM-порт. Если для обоих устройств настроить один и тот же COM-порт, будет работать устройство Allegiant. В доступе устройству эмуляции Allegiant CCL отказывается с выводом соответствующего сообщения.

Для решения данной проблемы Management Server необходимо оснастить двумя разными COM-портами или подключить устройство Allegiant к другому компьютеру.

### Включить эмуляцию Allegiant CCL

Установите флажок, чтобы включить эмуляцию

### Скорость в бодах

Введите значение скорости передачи в бит/сек.

### Стоповые биты

Выберите количество стоповых битов на символ.

### Контроль четности

Выберите тип контроля четности.

### Подтверждение связи

Выберите необходимый метод для управления потоком.

### Модель

Выберите модель Allegiant, которую необходимо эмулировать.

### См.

– *Настройка эмуляции Allegiant CCL, Страница 167*

## 12.20.1 Добавление эмуляции Allegiant CCL вручную

**Для добавления эмуляции Allegiant CCL выполните следующие действия.**

1. Разверните , нажмите .  
Откроется вкладка **Эмуляция Allegiant CCL**.
2. Установите флажок **Включить эмуляцию Allegiant CCL**.

3. Настройте необходимые параметры.  
Сервис эмуляции Allegiant CCL будет запущен на устройстве Management Server.

## 12.20.2

### Команды Allegiant CCL

Можно использовать команды CCL для переключения IP-камер или кодеров на IP-декодеры, если оба типа устройств настроены в BVMS. Команды CCL невозможно использовать для прямого управления аналоговыми камерами или самой матрицей Allegiant.

Эмуляция Allegiant CCL запускается как внутренняя служба BVMS, которая транслирует команды CCL матричного коммутатора в BVMS. Следует настроить COM-порт Management Server для прослушивания этих команд CCL. Эмуляция CCL способствует обмену между существующими устройствами Allegiant и Bosch Video Management System или использованию Bosch Video Management System с приложениями, поддерживающими команды Allegiant CCL. Управление старым оборудованием Allegiant, настроенным в BVMS, с помощью этих команд невозможно.

## 12.20.3

### Настройка эмуляции Allegiant CCL

Главное окно >  **Устройства** > Разверните  > 

Для использования команд CCL требуется руководство пользователя CCL. Это руководство доступно в интернет-каталоге продукции в разделе документации каждого матричного коммутатора LTC Allegiant.

Кнопка *Команды Allegiant CCL, поддерживаемые в системе BVMS, Страница 60* перечислены команды CCL, поддерживаемые в Bosch Video Management System.

#### Чтобы настроить эмуляцию Allegiant CCL:

1. Нажмите **Enable Allegiant CCL Emulation**.
2. Установите параметры связи в соответствии с потребностями.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

#### См.

– *Страница Эмуляция Allegiant CCL, Страница 166*

## 12.21

### Страница Мобильный видеосервис

Главное окно >  **Устройства** > 

Позволяет добавить в BVMS одну или несколько записей служб транскодирования. Эта служба транскодирования приспособливает видеопоток с камеры, настроенной в BVMS, к доступной пропускной способности сети. Благодаря этому мобильные видеоклиенты, такие как iPhone, iPad или веб-клиент, могут получать видеоданные в режиме реального времени или воспроизведения через ненадежные сетевые соединения с ограниченной пропускной способностью.

#### См.

– *Добавление Mobile Video Service вручную, Страница 168*

## 12.21.1

### Mobile Video Service

Mobile Video Service транскодирует видеопотоки от источника в соответствии с полосой пропускания, доступной подключенным клиентам. Интерфейсы Mobile Video Service предназначены поддерживать клиенты на нескольких платформах, например мобильные устройства (IOS: iPad, iPhone) и HTML-клиент Windows Internet Explorer.

Mobile Video Service основан на Microsoft Internet Information Service.

Одна мобильная служба может синхронно обслуживать несколько клиентов.

В отношении ограничений см. лист данных и Технические заметки Mobile Video Service, доступные в интернет-каталоге изделий для BVMS.

#### Служба Internet Information Service

Настройте параметры службы Internet Information Service на компьютере, на котором планируете установить MVS для BVMS.

#### Замечания по установке

Нельзя добавлять Mobile Video Service (MVS) в Configuration Client, если время между компьютером Configuration Client и компьютером Mobile Video Service не синхронизировано. Убедитесь в том, что время между задействованными компьютерами синхронизировано.

Перед установкой службы Mobile Video Service установите и задайте конфигурацию службы Internet Information Service (IIS). Если служба IIS не установлена, установка Mobile Video Service на BVMS будет прервана.

Во время установки BVMS выберите компонент Mobile Video Service для выполнения его установки.

Нельзя установить VRM и Mobile Video Service на одном компьютере.

Не рекомендуется устанавливать Mobile Video Service на компьютер, на который установлен Management Server.

С помощью мобильного приложения можно выполнять следующие действия:

- Отображение видео
  - Живой просмотр
  - Воспроизведение
- Контроль состояния сети и сервера

См.

- *Добавление Mobile Video Service вручную, Страница 168*

## 12.21.2

### Добавление Mobile Video Service вручную



Главное окно > **Устройства** > > щелкните правой кнопкой мыши  > нажмите

#### Добавить Mobile Video Service

Вы можете добавить одну или несколько записей Mobile Video Service в систему BVMS.

#### Для добавления выполните следующие действия.

1. Введите URI системы Mobile Video Service.
  2. Нажмите **ОК**.
- ✓ Теперь Mobile Video Service и Management Server знают друг о друге, а Mobile Video Service может принимать данные конфигурации от Management Server.

#### Диалоговое окно Добавить Mobile Video Service

##### URI

Введите URI своего Mobile Video Service. Следуйте синтаксическим правилам, приведенным в примере:



<https://www.MyDomain.org/mvs>

Такая запись всегда должна начинаться с `https://`, даже если не настроен шифрованный доступ к вашему веб-серверу.

## 12.22 Страница "Охранные панели"

Главное окно >  **Устройства** > Разверните  > 

Позволяет добавлять и настраивать охранные панели производства Bosch. Устройство должно быть подключено и доступно.

После добавления охранной панели в дереве устройств в иерархическом порядке отображаются области, точки, двери и реле.

Можно удалить или переименовать панель, любую область, точку, дверь и реле.

После изменения конфигурации охранной панели необходимо повторить сканирование устройства, чтобы отобразить изменения в BVMS.



### Замечание!

Все тревожные события, которые могут возникать в точке, автоматически конфигурируются как тревога BVMS.




Пример: пожарная тревога



### Замечание!

Если дверь не назначена точке в конфигурации охранной панели, добавленной к BVMS, тревога с этой двери не вызывает событие BVMS, а следовательно, событие BVMS не возникает.

### 12.22.1 Добавление тревожной панели вручную

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > команда **Добавить панель**

Позволяет добавить тревожную панель производства Bosch.

**Для добавления тревожной панели выполните следующие действия.**

1. Разверните , щелкните правой кнопкой мыши  и нажмите **Добавить панель**.

Откроется диалоговое окно **Добавление тревожной панели**.

2. Введите соответствующее значения.
3. Нажмите **ОК**.

В систему будет добавлена тревожная панель.

**Диалоговое окно Добавление тревожной панели**

#### Сетевой адрес

Введите IP-адрес устройства.





#### Сетевой порт

Выберите номер порта, настроенный на устройстве.

**Код доступа автоматизации**

Введите пароль для проверки подлинности на устройстве.

**12.22.2****Страница "Настройки"**

Главное окно >  **Устройства** > разверните  > разверните  >  > вкладка **Настройки**

Позволяет изменять настройки подключения тревожной панели.

**12.23****Страница «Системы контроля и управления доступом»**

Главное окно >  **Устройства** > разверните  > 

Позволяет добавлять и настраивать системы контроля и управления доступом от Bosch. Устройство должно быть подключено и доступно. После добавления системы контроля и управления доступом контроллер, входы, считывающие устройства и двери отображаются в дереве устройств иерархически.

Контроллер, входы, считывающие устройства и двери можно удалить или переименовать на странице **Карты и структура**.

После изменения конфигурации или иерархии контроллеров, считывателей или дверей в системе контроля и управления доступом необходимо повторно сканировать устройство, чтобы применить изменения в BVMS.

**Сертификат HTTPS для Client**

Для обеспечения безопасности соединения между системой контроля и управления доступом и BVMS необходимо экспортировать сертификат клиента из системы контроля и управления доступом и импортировать его в BVMS. Этот процесс описан в разделе **Сертификат HTTPS для Client** документации по системе контроля и управления доступом.


**Замечание!**

Если сертификат не добавлен, системы не смогут обмениваться данными.

**12.23.1****Добавление системы контроля и управления доступом**

Главное окно >  **Устройства** > разверните  > 

**Для добавления системы контроля и управления доступом выполните следующие действия.**

1. Щелкните правой кнопкой мыши .
2. Нажмите **Добавить систему контроля доступа**.  
Откроется диалоговое окно **Добавить систему контроля доступа**.

**Примечание.** При добавлении системы контроля и управления доступом настроенные двери, считыватели, входы и реле отображаются в дереве устройств на странице **Карты и структура**.

### Диалоговое окно Добавить систему контроля доступа

#### Сетевой адрес/порт HTTPS

Введите сетевой адрес устройства. При необходимости измените номер порта.

#### Имя пользователя

Отображает имя пользователя, используемое для аутентификации на устройстве.

#### Пароль

Введите действующий пароль для аутентификации на устройстве.

#### Для проверки подключения выполните следующие действия.


1. Нажмите кнопку «Подключиться».  
Система BVMS Configuration Client попытается подключиться к системе контроля и управления доступом и получить необходимую информацию.
2. Нажмите «ОК».  
Система контроля и управления доступом будет добавлена в систему на основе показанной информации.

## 12.23.2

### Изменение системы контроля и управления доступом





Главное окно  > **Устройства** > разверните  >  > 

**Для изменение системы контроля и управления доступом выполните следующие действия.**

1. Щелкните правой кнопкой мыши .
2. Нажмите **Изменить систему контроля доступа**.  
Откроется диалоговое окно **Изменить систему контроля доступа**.

## 12.23.3

### Страница «Настройки»

Главное окно  > **Устройства** > разверните  >  >  > вкладка

#### Параметры

Позволяет изменить настройки подключения системы контроля и управления доступом.

## 12.24





### Страница Video Analytics

Главное окно  > **Устройства** > Разверните  > 

Позволяет добавлять устройства Video Analytics, Person Identification (PID) и LPR.

### 12.24.1

#### Страница параметров видеоаналитики

Главное окно  > **Устройства** > разверните  > разверните  > 

#### Video Analytics > страница Параметры Video Analytics

Можно добавить устройство видеоаналитики на стороне сервера.

Должны быть доступны учетные данные и путь установки приложения для просмотра аналитики, используемого для устройства видеоаналитики.

**Сетевой адрес**

Введите IP-адрес устройства видеоаналитики. Имена DNS запрещены.

**Имя пользователя**

Введите имя пользователя в соответствии с настройками в устройстве видеоаналитики.

**Пароль**

Введите пароль, настроенный на устройстве для анализа на стороне сервера.

**Путь к приложению для просмотра аналитики**

Введите относительный путь установки приложения для просмотра аналитики.

Указывается путь относительно *C:\Program Files (x86)\* на компьютере, на котором используется приложение для просмотра.



Пример. Приложение для просмотра аналитики (*AnalyticsViewer.exe*) установлено в следующем каталоге:

```
C:\Program Files (x86)\VideoAnalytics\
```

Укажите следующий путь в поле **Путь к приложению для просмотра аналитики**:



```
VideoAnalytics\AnalyticsViewer.exe
```

**12.24.2****Добавление устройства Video Analytics**

Главное окно  **Устройства** > щелкните правой кнопкой мыши  > команда **Добавить устройство Video Analytics** > диалоговое окно **Добавить устройство Video Analytics**

При добавлении устройства для анализа на стороне сервера необходимо указать учетные данные для нового устройства.

**Добавление устройства серверной аналитики**

1. Разверните , щелкните правой кнопкой мыши  и выберите пункт **Добавить устройство Video Analytics**.

Отображается диалоговое окно **Добавить устройство Video Analytics**.

2. Введите соответствующее значения.

3. Нажмите кнопку **ОК**.

Устройство добавлено в систему.

**Диалоговое окно Добавить устройство Video Analytics****Сетевой адрес**

Введите IP-адрес устройства видеоаналитики. Имена DNS запрещены.





**Имя пользователя**

Введите имя пользователя в соответствии с настройками в устройстве видеоаналитики.

**Пароль**

Введите пароль, настроенный на устройстве для анализа на стороне сервера.

**12.24.3****Страница устройств Person Identification**

Главное окно  > **Устройства** > развернуть  > развернуть  > 

страница устройств Person Identification

Позволяет добавить устройство Person Identification. Устройство должно быть подключено и доступно. Вы можете добавить камеры к устройству Person Identification и настроить события и тревоги Person Identification.

#### Группы лиц

На вкладке **Группы лиц** можно добавлять и настраивать группы людей.

#### Камеры

На вкладке **Камеры** можно добавить камеры к устройству Person Identification.

Добавленные камеры отображаются в списке.

**Примечание.** Сначала добавьте соответствующие камеры в логическое дерево.

## 12.24.4

### Добавление Person Identification Device (PID)



#### Замечание!

В случае сбоя центрального сервера необходимо восстановить конфигурацию BVMS и сертификат Bosch VMS CA. В противном случае вы не сможете использовать существующее устройство PID без перезапуска, что приведет к удалению всех сохраненных лиц.

Рекомендуется создать резервную копию конфигурации BVMS и сертификата Bosch VMS CA.



При добавлении устройства Person Identification убедитесь, что сертификат, отображаемый в диалоговом окне **Добавить устройство Person Identification Device**, соответствует добавляемому PID.

Начиная с BVMS 10.1, можно добавлять несколько устройств PID.

Первое добавленное устройство PID становится ведущим устройством, которое подключается к системе BVMS. На значке в дереве устройств отображается точка красного цвета. Это первое устройство PID устанавливает соединение с другими устройствами PID, и в этом устройстве хранится база данных людей.

**Примечание.** Прежде чем удалять первое добавленное устройство PID, необходимо удалить все остальные настроенные устройства PID.

#### Чтобы добавить устройство Person Identification:

1. Разверните .
2. Щелкните правой кнопкой мыши .
3. Нажмите **Добавить устройство Person Identification Device**.  
Отображается диалоговое окно **Добавить устройство Person Identification Device**.
4. Введите соответствующие значения.
5. Нажмите **Посмотреть сертификат...**, чтобы проверить, соответствует ли сертификат PID.
6. Чтобы подтвердить выбор, нажмите кнопку **ОК**.
7. Нажмите **ОК**.  
Устройство будет добавлено в систему.

#### Диалоговое окно Добавить устройство Person Identification Device

##### Сетевой адрес

Введите IP-адрес устройства.






**Номер порта**

Введите номер порта устройства.

**См.**

- *Восстановление доступа к PID после сбоя центрального сервера BVMS, Страница 174*
- *Чтобы экспортировать параметры конфигурации., Страница 98*

**12.24.5****Страница PID**

Главное окно >  **Устройства** > развернуть  > развернуть  >   
 страница устройств Person Identification  PID

**Подключение**

На вкладке **Подключение** отображаются сетевой адрес и номер порта Person Identification Device. Параметры подключения Person Identification Device доступны только для чтения.

**12.24.6****Восстановление доступа к PID после сбоя центрального сервера BVMS****Замечание!**

В случае сбоя центрального сервера необходимо восстановить конфигурацию BVMS и сертификат Bosch VMS CA. В противном случае вы не сможете использовать существующее устройство PID без перезапуска, что приведет к удалению всех сохраненных лиц.

Рекомендуется создать резервную копию конфигурации BVMS и сертификата Bosch VMS CA.

Дополнительные сведения о сохранении конфигурации BVMS см. в разделе *Чтобы экспортировать параметры конфигурации., Страница 81*. Управление сертификатами осуществляется вне BVMS в приложении для Windows **Управление сертификатами компьютеров**.

**Замечание!**

Сертификаты содержат конфиденциальную информацию. Для их защиты выполните следующие действия.

- Установите надежный пароль.
- Сохраните сертификат в ограниченной зоне, например на сервере, не являющемся общедоступным.
- Убедитесь, что только уполномоченный персонал может получить доступ к сертификату.

**Чтобы создать резервную копию сертификата Bosch VMS CA:**

1. Откройте приложение для Windows **Управление сертификатами компьютеров**.
2. В папке **Доверенные корневые центры сертификации** выберите сертификат Bosch VMS CA.
3. Экпортируйте сертификат с закрытым ключом, выбрав **Да, экспортировать закрытый ключ**.
4. Используйте формат Personal Information Exchange.
5. Введите надежный пароль.

6. Сохраните сертификат как PFX-файл.

**Чтобы восстановить доступ к PID с нового установленного центрального сервера BVMS:**

1. Откройте приложение для Windows **Управление сертификатами компьютеров**.
2. Импортируйте PFX-файл, содержащий сертификат Bosch VMS CA, в папку **доверенных корневых центров сертификации** нового центрального сервера. Включить все расширенные свойства.
3. Импортируйте резервную копию конфигурации BVMS.

**См.**




– *Экспорт параметров конфигурации, Страница 98*

## 12.24.7

### Добавление камер к Person Identification Device (PID)

Вы можете добавить камеры к устройству Person Identification, если они уже добавлены в логическое дерево.

**Чтобы добавить камеры к устройству Person Identification:**

1. Разверните .
2. Разверните .
3. Нажмите .
4. Перейдите на вкладку **Камеры**.
5. Перетащите нужные камеры из окна **Логическое дерево** в окно **Камеры**.

Или

дважды нажмите нужные камеры в окне **Логическое дерево**.

Камеры добавляются в устройство Person Identification и отображаются в списке **Камеры**.

## 12.24.8

### Настройка параметров камеры для тревог Person Identification

Для каждой доступной камеры можно настроить параметры тревог Person Identification, чтобы сократить количество ложных тревог.

**Параметр камеры**

Название	Информация о значении	Описание
Вероятность порога (%)	По умолчанию: 55 % Мин.: 0 % Макс.: 100 %	Минимальная вероятность положительной идентификации лица для создания события Person Identification.
Размер лица (%)	По умолчанию: 7,5 % Мин.: 5 % Макс.: 100 %	Минимальный размер обнаруживаемого лица по сравнению с размером всего видеокadra.



Название	Информация о значении	Описание
Мин. число кадров	По умолчанию: 4 Мин.: 1	Минимальное количество последовательных видеок кадров, на которых должно появиться лицо для его обнаружения.
Анализируемые кадры (%)	По умолчанию: 100 % Мин.: 10 % Макс.: 100 %	Процент кадров, анализируемых для идентификации людей. Значение 50 % означает, что анализируется каждый второй кадр.

## 12.24.9

**Настройка групп людей**

Главное окно >  > **Устройства** > Разверните  > 

**Чтобы настроить группы людей:**

1. Выберите вкладку **Группы лиц**.
2. Нажмите  для добавления новой группы лиц.
3. Введите соответствующее значения.
4. Нажмите  для удаления группы лиц.

**Замечание!**

Вы не можете удалить или изменить значения группы по умолчанию.

**Таблица групп лиц**

<b>Группа лиц</b>	Введите имя группы лиц.
<b>Цвет тревоги</b>	Дважды щелкните для выбора цвета тревоги.
<b>Название тревоги</b>	Введите название тревоги, которое будет отображаться в модуле Operator Client.

**Чтобы изменить значения в таблице групп лиц:**

1. Дважды щелкните соответствующее поле таблицы.
2. Измените значение.

**Приоритет тревожного сигнала**

На **Тревожные сигналы** странице можно установить приоритет тревог Person Identification.



**Замечание!**

Для каждой камеры соответствующей группы лиц можно установить различные приоритеты тревоги.

Вы также можете изменить приоритет тревоги для группы лиц по умолчанию.

**См.**

– *Страница Тревожные сигналы, Страница 319*

**12.24.10****Добавление устройства LPR**

Главное окно > > **Устройства** > развернуть



Устройства LPR идентифицируют и распознают номерные знаки. Можно настроить соответствующие события и сигналы тревоги LPR.

Если устройство LPR должно распознавать конкретные номерные знаки, сначала нужно настроить список соответствующих номерных знаков непосредственно в устройстве LPR. Более подробную информацию см. в пользовательской документации к устройству.

**Замечание!**

Устройство должно быть подключено и доступно.

Система BVMS подключается только в том случае, если на устройстве LPR активирована проверка подлинности, а также указаны имя пользователя и пароль. Имя пользователя и пароль не могут быть пустыми.

**Чтобы добавить устройство LPR:**

1. Щелкните правой кнопкой мыши .
2. Нажмите **Добавить устройство распознавания номеров**.  
Откроется диалоговое окно **Добавить устройство распознавания номеров**.
3. Введите соответствующие значения.
4. Нажмите **Проверить подлинность**.
5. Нажмите **ОК**.  
Устройство будет добавлено в систему.

**Замечание!**

В конфигурации устройства LPR необходимо указать IP-адрес сервера Management Server системы BVMS. В противном случае система BVMS не будет получать события от этого устройства LPR.

**Диалоговое окно Добавить устройство распознавания номеров****Сетевой адрес**

Введите IP-адрес устройства.

**Номер порта**

Введите номер порта устройства.

**Имя пользователя**

Введите действительное имя пользователя для проверки подлинности в устройстве.

**Пароль**

Введите действующий пароль для аутентификации на устройстве.

**Проверить подлинность**

Нажмите для аутентификации на устройстве с использованием введенных выше учетных данных.

**12.25****Страница Устройства VRM**

Главное окно >

**Устройства** > Разверните



>

Позволяет добавлять и настраивать устройства VRM. Устройству VRM необходимы, по крайней мере, кодер, iSCSI-устройство, LUN, назначенное данному iSCSI-устройству, и пул хранения. Текущие версии микропрограммного обеспечения см. в замечаниях к версии и технических характеристиках.

**Замечание!**

После того как вы добавили устройство iSCSI с соответствующими кодерами в свою систему BVMS, вы должны добавить IQN каждого кодера к данному устройству iSCSI (действительно для некоторых типов устройств iSCSI).

Подробную информацию см. в разделе *Настройка устройства iSCSI, Страница 202*.

**Замечание!**

Убедитесь, что время на компьютере VRM синхронизировано с Management Server. В противном случае можно потерять видеозаписи.

Настройте программное обеспечение сервера времени на сервере Management Server. На компьютере VRM настройте IP-адрес сервера Management Server в качестве сервера времени, используя стандартные процедуры Windows.

**См.**

- *Настройка многоадресной передачи, Страница 242*
- *Синхронизация конфигурации BVMS, Страница 188*
- *Страница Настройки VRM, Страница 182*
- *Страница "Пул", Страница 188*
- *Страница устройства iSCSI, Страница 198*
- *Изменение пароля устройства VRM, Страница 184*

**12.25.1****Добавление устройств VRM путем поиска**

Главное окно >

**Устройства** >



В сети необходима служба VRM, запущенная на компьютере, и устройство iSCSI.





**Замечание!**

При добавлении устройства iSCSI без настроенных целевых объектов и устройств LUN запустите конфигурацию по умолчанию и добавьте IQN каждого кодера к данному устройству iSCSI.

При добавлении устройства iSCSI с настроенными целевыми объектами и устройствами LUN добавьте IQN каждого кодера к данному устройству iSCSI.

Подробную информацию см. в разделе *Настройка устройства iSCSI, Страница 202*.

**Для добавления устройств VRM путем поиска выполните следующие действия.**

1. Щелкните правой кнопкой мыши  и выберите команду **Выполнить поиск устройств VRM**.  
Откроется диалоговое окно **BVMS Scan Wizard**.
2. Установите флажки для устройств, которые необходимо добавить.
3. В списке **Роль** выберите нужную роль.  
Доступная для выбора новая роль зависит от текущего типа устройства VRM.  
Если выбрать **Зеркальный** или **Резервный**, потребуется выполнить дополнительное действие.
4. В списке **Роль** выберите нужную роль.  
Новая роль, которую вы можете выбрать, зависит от текущего типа устройства VRM.
5. Нажмите **Далее >>**
6. В списке **Ведущий VRM** выберите ведущий VRM для выбранного зеркального или резервного VRM.
7. Нажмите **Далее >>**.  
Откроется диалоговое окно мастера **Проверки подлинности устройств**.
8. Введите пароль для каждого устройства, защищенного паролем.  
Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.  
Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.  
Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.  
  
В столбце **Состояние** успешные входы в систему обозначены значком .  
Неудачные попытки входа обозначены значком .
9. Нажмите **Готово**.  
Устройство добавлено в дерево устройств.

**Примечание.** Все устройства VRM добавляются по умолчанию с безопасным соединением.

**Чтобы изменить безопасное/небезопасное соединение:**

1. Щелкните правой кнопкой мыши .
2. Нажмите **Изменить устройство VRM**.  
Откроется диалоговое окно **Изменить устройство VRM**.
3. Установите флажок **Безопасное соединение**.  
Используемый порт автоматически меняется на порт HTTPS.  
Или  
снимите флажок **Безопасное соединение**.  
Используемый порт автоматически меняется на порт RCPP.

**См.**

- *Добавление устройства, Страница 124*
- *Страница Устройства VRM, Страница 178*
- *Настройка устройства iSCSI, Страница 202*
- *Двойная / резервная запись, Страница 26*

## 12.25.2 Добавление основного или вторичного VRM вручную



Главное окно > **Устройства** > щелкните правой кнопкой мыши > нажмите **Добавить VRM** > диалоговое окно **Добавить VRM**

Позволяет добавить устройство VRM. Можно выбрать тип устройства и ввести учетные данные.

Назначить резервный диспетчер VRM основному VRM можно, только когда оба диспетчера подключены к сети и успешно прошли проверку подлинности. Затем синхронизируются пароли.

Можно добавить основной VRM вручную, если вам известны IP-адрес и пароль.

**Для добавления основного устройства VRM выполните следующие действия.**

1. Настройте необходимые параметры для устройства VRM.
2. В списке **Тип** выберите элемент **Первичный**.
3. Нажмите **ОК**.

Будет добавлено устройство VRM.

Можно добавить вторичный VRM вручную, если вам известны IP-адрес и пароль.



### **Замечание!**

Для настройки конфигурации вторичной системы VRM необходимо сначала установить соответствующее ПО на требуемый компьютер. Запустите Setup.exe и выберите **Вторичный VRM**.

**Для добавления вторичного VRM выполните следующие действия.**

1. Настройте необходимые параметры для устройства VRM.
2. В списке **Тип** выберите элемент **Вторичный**.
3. Нажмите **ОК**.

Будет добавлено устройство VRM.

Теперь можно настроить вторичный VRM, как любой другой основной VRM.

### **Диалоговое окно Добавить VRM**

#### **Имя**

Введите отображаемое имя устройства.

#### **Сетевой адрес / порт**

Введите IP-адрес своего устройства.

Если флажок **Безопасное соединение** установлен, порт автоматически меняется на порт HTTPS.

Вы можете изменить номер порта, если порты по умолчанию не используются.

#### **Тип**

Выберите необходимый тип устройства.

#### **Имя пользователя**

Введите имя пользователя для проверки подлинности.

#### **Пароль**

Введите пароль для проверки подлинности.

#### **Показать пароль**

Нажмите, чтобы пароль в этом диалоговом окне стал виден.

**Безопасность**

По умолчанию флажок **Безопасное соединение** установлен, если поддерживается протокол HTTPS.

**Замечание!**

При переходе к версии BVMS 10.0 и выше флажок **Безопасное соединение** не установлен по умолчанию, а соединение не защищено (RCPP).

Чтобы изменить безопасное или небезопасное соединение, используйте команду

**Изменить устройство VRM** и установите или снимите флажок **Безопасное соединение**.

**Тест**

Нажмите, чтобы проверить, подключено ли устройство и успешно ли выполнена проверка подлинности.

**Свойства**

При необходимости измените номера портов для порта HTTP и порта HTTPS. Это возможно только в тех случаях, когда добавляется или изменяется диспетчер VRM, который не подключен. Если диспетчер VRM подключен, эти значения поступают из сети, и их невозможно изменить.

В строке таблицы **Ведущий VRM** указывается выбранное устройство, если это возможно.

**См.**

- *Редактирование устройства VRM, Страница 181*
- *Добавление зеркального диспетчера VRM вручную, Страница 186*
- *Добавление резервного диспетчера VRM вручную, Страница 185*

**12.25.3****Редактирование устройства VRM**

Главное окно > **Устройства**

Позволяет изменить устройство VRM.

**Чтобы изменить безопасное/небезопасное соединение:**

1. Щелкните правой кнопкой мыши .
2. Нажмите **Изменить устройство VRM**.  
Откроется диалоговое окно **Изменить устройство VRM**.
3. Установите флажок **Безопасное соединение**.  
Используемый порт автоматически меняется на порт HTTPS.  
Или  
снимите флажок **Безопасное соединение**.  
Используемый порт автоматически меняется на порт RCPP.

**Замечание!**

После обновления до новой версии рекомендуется изменить включить безопасное соединение.




Подробные сведения о параметрах диалогового окна **Изменить устройство VRM** см. в главе «Добавление основного или вторичного VRM вручную».

**См.**

– *Добавление основного или вторичного VRM вручную, Страница 180*

## 12.25.4

### Страница Настройки VRM

Главное окно >  **Устройства** > разверните  >  > **Основные параметры** > **Настройки VRM**

#### Имя инициатора на сервере

Отображает имя инициатора iSCSI-сервера VRM Server.

#### Общесистемный пароль CHAP

Введите пароль, настроенный в устройстве хранения iSCSI. Пароль CHAP действителен для VRM и автоматически отправляется на все устройства. Клиентам воспроизведения не требуется дополнительная настройка. Систему iSCSI необходимо настраивать вручную и задавать пароль CHAP. При использовании пароля CHAP все системы хранения необходимо настроить для использования пароля CHAP. Система VRM поддерживает только один системный пароль.

См. *Пароль для глобального подключения iSCSI (пароль CHAP):*, Страница 120

## 12.25.5

### Страница SNMP

Главное окно >  **Устройства** > разверните  > разверните  > **Сеть** > **SNMP**

#### 1. Адрес узла SNMP 2. Адрес узла SNMP

VRM поддерживает SNMP (Simple Network Management Protocol) для управления сетевыми компонентами и может отправлять SNMP-сообщения (запросы) по IP-адресам. Устройство поддерживает SNMP MIB II в стандартизированном коде. Чтобы посылать запросы SNMP, введите в данном поле IP-адреса одного или двух устройств назначения. Некоторые события отправляются только как запросы SNMP. Описание содержится в файле MIB.

## 12.25.6

### Страница "Учетные записи"

Чтобы настроить размещение изображений и экспортировать видеотреггеры в формате файла MP4, необходимо создать учетную запись для сохранения и доступа к ним. Можно создать не более четырех (4) учетных записей.

#### Тип

Выберите тип учетной записи: **FTP** или **Dropbox**.

#### IP-адрес

Введите IP-адрес сервера, на котором требуется сохранять изображения.

#### Имя пользователя

Введите имя пользователя для сервера.

#### Пароль

Введите пароль, который дает вам право доступа к серверу. Чтобы проверить пароль, нажмите **Проверить** справа.

#### Проверить




Нажмите, чтобы проверить пароль.

#### Путь

Введите точный путь для размещения изображений и видеотреггеров на сервере.

## 12.25.7

**Страница Дополнительно**

Главное окно >  **Устройства** > разверните  > разверните  > **Обслуживание** > **Дополнительно**

**Регистрация RCP+ / Регистрация данных отладки / Регистрация данных воспроизведения / Регистрация данных VDP / Регистрация данных производительности**

Включите различные журналы для VRM Server и Configuration Manager.  
 Файлы журнала для VRM Server хранятся в компьютере, на котором запущен сервер VRM Server, и их можно просмотреть или загрузить при помощи VRM Monitor.  
 Файлы журнала для Configuration Manager хранятся локально в следующем каталоге:  
 %USERPROFILE%\My Documents\Bosch\Video Recording Manager\Log

**Срок хранения (в днях)**

Укажите срок хранения для файлов журнала в днях.

**Полный дамп-файл памяти**

Включайте этот параметр только в случае необходимости, например, если в службе технической поддержки потребуют полную сводку состояния основной памяти.

**Поддержка Telnet**

Включайте этот параметр, если требуется поддержка доступа по протоколу Telnet.  
 Включайте только в случае необходимости.

**Замечание!**

Для интенсивной регистрации в журналах необходимы значительные ресурсы центрального процессора и емкость жесткого диска.  
 Не пользуйтесь интенсивной регистрацией постоянно.

## 12.25.8

**Шифрование записи для VRM**

Зашифрованная запись для кодеров VRM не включена по умолчанию.

Вам необходимо включить зашифрованную запись для основного или вторичного VRM отдельно.

**Замечание!**

Перед тем как включить шифрование видеозаписи в первый раз, необходимо создать резервный ключ (резервную копию сертификата). Для каждого устройства VRM требуется лишь один раз создать резервный ключ.

Если обычный ключ шифрования будет потерян, видеозаписи можно будет расшифровать с помощью резервного ключа.

Мы рекомендуем хранить копию резервного ключа в надежном месте (например, в сейфе).

**Для создания резервного ключа:**

1. Выберите соответствующее устройство VRM.
2. Откройте вкладку **Обслуживание**.
3. Откройте вкладку **Шифрование видеозаписи**.
4. Нажмите **Резервный ключ**.
5. Выберите расположение хранилища сертификатов.
6. Введите пароль, отвечающий требованиям к сложности пароля, и подтвердите его.

7. Нажмите **Создать**.  
Будет создан резервный ключ (резервная копия сертификата).

**Чтобы активировать/деактивировать шифрование видеозаписи:**

1. Выберите соответствующее устройство VRM.
2. Откройте вкладку **Обслуживание**.
3. Откройте вкладку **Шифрование видеозаписи**.
4. Установите/снимите флажок **Включить шифрование видеозаписи**.

5. Нажмите  .

**Примечание.** Шифрование активируется только после изменения следующего блока. Для этого может потребоваться некоторое время.

Убедитесь, что кодеры выполняют шифрование.

**Чтобы убедиться, что кодеры VRM выполняют шифрование:**

1. Выберите соответствующее устройство VRM.
2. Откройте вкладку **Обслуживание**.
3. Откройте вкладку **Шифрование видеозаписи**.

**Примечание.** Это также можно посмотреть на вкладке **Monitoring** в VRM Monitor.



**Замечание!**

Все кодеры VRM, поддерживающие шифрование, автоматически шифруют видеозапись после активации шифрования в VRM.

Для каждого кодера шифрование может быть отключено.

Кодеры VSG всегда выполняют шифрование, если шифрование активировано в VRM.

**Чтобы активировать или деактивировать шифрование видеозаписи для одного кодера VRM:**

1. Выберите соответствующий кодер VRM.
2. Откройте вкладку **Запись**.
3. Откройте вкладку **Управление видеозаписью**.
4. Установите/снимите флажок **Шифрование**.


5. Нажмите  .

## 12.25.9

### Изменение пароля устройства VRM

Главное окно >  **Устройства** > Разверните  > 

**Изменение пароля:**

1. Щелкните  правой кнопкой мыши, затем щелкните **Изменить пароль VRM**.  
Отображается диалоговое окно **Изменить пароль**.
2. В поле **Старый пароль** введите необходимый пароль.
3. В поле **Новый пароль** введите новый пароль, нажмите второе поле **Новый пароль** и снова введите новый пароль.

Нажмите **ОК**.

- ▶ Подтвердите введенные данные в следующем диалоговом окне.
- ✓ Пароль на устройстве изменяется незамедлительно.



## 12.25.10 Добавления пула VRM

Главное окно >  **Устройства** > Развернуть 

### Добавление пула VRM:

- ▶ Щелкните правой кнопкой мыши  или  и выберите команду **Добавить пул**. В систему добавляется новый пул.

См.

– Пул хранения iSCSI, Страница 198

## 12.25.11 Добавление резервного диспетчера VRM вручную

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Добавить резервный VRM** > диалоговое окно **Добавить резервный VRM**



### Замечание!

Для настройки конфигурации вторичной системы VRM необходимо сначала установить соответствующее ПО на требуемый компьютер. Запустите Setup.exe и выберите **Вторичный VRM**.

Как основной VRM, так и вторичный VRM могут взять на себя функции резервного VRM. Основной резервный VRM добавляется к основному VRM, а вторичный резервный VRM — ко вторичному VRM.

Можно добавить устройство резервного VRM вручную, если известны IP-адрес и пароль. Изначально выбранный VRM является ведущим VRM для этого избыточного VRM.

Вы можете добавить устройство резервного VRM. Вы можете добавить его вручную или выбрать устройство из списка просканированных устройств VRM.

Назначить резервный диспетчер VRM основному VRM можно, только когда оба диспетчера подключены к сети и успешно прошли проверку подлинности. Затем синхронизируются пароли.

### Добавление устройства резервного VRM

1. Задайте необходимые параметры для устройства VRM.
  2. Убедитесь, что выбран верный основной диспетчер VRM. Если это не так, отмените процедуру.
  3. Нажмите **ОК**.
- ✓ Устройство резервного VRM добавляется к выбранному основному VRM.

### Диалоговое окно Добавить резервный VRM

#### Сетевой адрес

Введите IP-адрес устройства или выберите сетевой адрес в списке **Просканированные VRM**.

#### Просканированные VRM

Отображает список просканированных компьютеров VRM. Для повтора сканирования закройте диалоговое окно и снова отобразите диалоговое окно.




**Замечание!**

Резервное устройство VRM наследует параметры, настроенные в ведущем устройстве VRM. При изменении параметров ведущего устройства VRM соответствующим образом меняются параметры резервного устройства VRM.

**См.**

– *Двойная / резервная запись, Страница 26*

**12.25.12****Добавление зеркального диспетчера VRM вручную**

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Добавить зеркальный VRM** > диалоговое окно **Добавить VRM**

**Замечание!**

Для настройки конфигурации вторичной системы VRM необходимо сначала установить соответствующее ПО на требуемый компьютер. Запустите Setup.exe и выберите **Вторичный VRM**.

Только дополнительный VRM может взять на себя функцию зеркального VRM. Можно добавить зеркальный VRM к основному VRM. Устройство зеркального VRM можно добавить вручную, если известны IP-адрес и пароль. Изначально выбранный VRM является основным VRM для этого зеркального VRM.

**Добавление устройства зеркального VRM:**

1. Задайте необходимые параметры для устройства VRM.
2. Убедитесь, что выбран верный основной диспетчер VRM. Если это не так, отмените процедуру.
3. Нажмите **ОК**.

Устройство зеркального VRM добавляется к выбранному основному VRM.

**Диалоговое окно Добавить VRM****Имя**

Введите отображаемое имя устройства.

**Сетевой адрес / порт**

Введите IP-адрес своего устройства.

Если флажок **Безопасное соединение** установлен, порт автоматически меняется на порт HTTPS.

Вы можете изменить номер порта, если порты по умолчанию не используются.

**Тип**

Выберите необходимый тип устройства.

**Имя пользователя**

Введите имя пользователя для проверки подлинности.

**Показать пароль**

Нажмите, чтобы пароль в этом диалоговом окне стал виден.

**Пароль**

Введите пароль для проверки подлинности.

**Безопасность**

По умолчанию флажок **Безопасное соединение** установлен, если поддерживается протокол HTTPS.

**Замечание!**

При переходе к версии BVMS 10.0 и выше флажок **Безопасное соединение** не установлен по умолчанию, а соединение не защищено (RCPP).

Чтобы изменить безопасное или небезопасное соединение, используйте команду

**Изменить устройство VRM** и установите или снимите флажок **Безопасное соединение**.

**Тест**

Нажмите, чтобы проверить, подключено ли устройство и успешно ли выполнена проверка подлинности.

**Свойства**

При необходимости измените номера портов для порта HTTP и порта HTTPS. Это возможно только в тех случаях, когда добавляется или изменяется диспетчер VRM, который не подключен. Если диспетчер VRM подключен, эти значения поступают из сети, и их невозможно изменить.

В строке таблицы **Ведущий VRM** указывается выбранное устройство, если это возможно.

**См.**


- *Добавление основного или вторичного VRM вручную, Страница 180*
- *Двойная / резервная запись, Страница 26*

**12.25.13****Добавление кодеров путем поиска**

Для добавления кодеров путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск кодеров**. Откроется диалоговое окно **BVMS Scan Wizard**.
2. Выберите необходимые кодеры, выберите необходимый пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.
3. Нажмите **Далее >>**.  
Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.  
Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.  
Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.  
Затем щелкните это поле правой кнопкой мыши и выберите **Копировать ячейку в столбец**.

В столбце **Состояние** успешные подключения обозначены значком .

Неудачные подключения обозначены значком .

, что означает, что для устройства требуется начальный пароль.

Для установки начального пароля введите его в поле **Пароль**.

Статус изменится на .

Повторите эти действия для всех устройств, которые требуют первоначальный пароль.

**Примечание:** пока вы не установили первоначальный пароль для всех устройств в списке, которые требуют начальный пароль, вы не сможете продолжить работу.

5. Нажмите **Готово**.  
Устройство добавлено в дерево устройств.

## 12.25.14

### Добавление устройств VSG путем поиска

Для добавления устройств VSG путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск шлюзов Video Streaming Gateway**.  
Откроется диалоговое окно **BVMS Scan Wizard**.
2. Выберите необходимые устройства VSG, выберите пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.
3. Нажмите **Далее >>**.  
Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.  
Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.  
Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.  
Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.




В столбце **Состояние** успешные входы в систему обозначены значком .

Неудачные попытки входа обозначены значком .

5. Нажмите **Готово**.  
Устройство добавлено в дерево устройств.

## 12.25.15

### Синхронизация конфигурации BVMS





Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > команда **Синхронизация конфигурации BVMS**

В версии BVMS 6.0 поддерживается версия VRM 3.50. Если вы не обновите VRM до версии 3.50 во время обновления системы BVMS до версии 6.0, запись продолжится, однако вы не можете изменить конфигурацию старого VRM.

Если вы обновили программное обеспечение VRM до версии 3.50, необходимо вручную синхронизировать конфигурацию BVMS.

## 12.26

### Страница "Пул"

Главное окно >  **Устройства** > Разверните  > Разверните  >   
Позволяет настраивать запись для всех устройств, собираемых данным пулом хранилищ.

#### Идентификация пула

Отображает номер пула.

### Режим настроек записи

#### – При отказе

Записи сохраняются только на первичный целевой объект. Если сохранение на этот целевой объект невозможно, запись будет сохранена на объект, указанный как вторичный.

Ситуация отказа возникает, если основная система по какой-либо причине не предоставляет блоки хранения: система отключена, сетевая ошибка, не осталось места.

Второй список можно оставить пустым. В этом случае резервирование невозможно, однако количество необходимых сеансов iSCSI сокращается, на вторичном целевом объекте не выделяется дисковое пространство. Это снижает нагрузку на систему и увеличивает время хранения системы.

#### – Автоматический

Балансировка нагрузки настраивается автоматически. Каждому кодеру автоматически назначаются 2 целевых объекта iSCSI и их блоки.

### Период проверки работоспособности (дн.)

Требуемый период времени настраивается путем перемещения ползунка. По истечении заданного периода времени целевой объект iSCSI проверяется и при необходимости блоки выделяются повторно.

### Использование второстепенной цели

Включите или отключите использование вторичного целевого объекта.

### Резервирование блоков на время простоя

Введите число дней, в течение которых будет производиться запись с назначенных кодеров, когда сервер VRM отключен.

Например, если установить значение 4, запись будет производиться в течение приблизительно 4 дней простоя сервера VRM.

Если в системе имеются устройства с низким значением потока, можно существенно снизить предварительно выделенное пространство на диске. Это обеспечивает правильное распределение емкости хранилища и увеличивает время хранения.

### Разрешить LUN более 2 ТБ

Нажмите, чтобы включить использование устройств LUN больше 2 ТБ.

Устройства LUN больше 2 ТБ («большие устройства LUN») не поддерживаются следующими устройствами:

- Устройства VRM версии ниже 3.60
- Устройства VSG с версией микропрограммного обеспечения ниже 6.30
- Кодеры с версией микропрограммного обеспечения ниже 6.30

BVMS не позволяет выполнять следующие действия:

- Добавлять или перемещать устройства с версией микропрограммного обеспечения ниже 6.30 в пул, допускающий использование больших устройств LUN.
- Добавлять или перемещать устройства, которые в данный момент не подключены к сети, к пулу, допускающему использование больших устройств LUN.
- Добавлять или перемещать устройство iSCSI, содержащее большие устройства LUN, в пул, который не поддерживает использование больших устройств LUN.
- Разрешать использование больших устройств LUN в пуле, содержащем устройства с версией микропрограммного обеспечения ниже 6.30.
- Отключать использование больших устройств LUN в пуле с устройством iSCSI, содержащим большие устройства LUN.





Переместите устройства с версией микропрограммного обеспечения ниже 6.30 в пул, не поддерживающий большие устройства LUN.

**См.**

- *Добавление устройства LUN, Страница 206*
- *Добавления пула VRM, Страница 185*

## 12.26.1

### Настройка автоматического режима записи в пуле

Главное окно >  **Устройства** > Разверните  > Разверните  > 

**Примечание.**

Если ранее был настроен резервный режим записи, эта настройка будет перезаписана.

**Настройка**

- ▶ В списке **Режим настроек записи** выберите **Автоматически**. После активации конфигурации активируется **Автоматически** режим записи. На странице **Очередность записи** кодера отображаются списки первичных и вторичных целевых объектов.

**Дополнительная информация**

- *Настройка резервного режима записи на кодере, Страница 241*

## 12.26.2







### Добавление кодера и декодера вручную

Позволяет добавить кодер или декодер вручную. Это особенно полезно, если необходимо добавить какое-либо IP-видеоустройство производства Bosch (только для VRM).

**Внимание.**

Если добавляется IP-видеокодер или декодер Bosch с выбранным параметром **<Автоопределение>**, это устройство должно быть доступно в сети.

**Добавление IP-видеоустройства производства Bosch:**

1. Разверните  , разверните  , щелкните правой кнопкой мыши  .  
Или  
щелкните правой кнопкой мыши  .  
Или  
щелкните правой кнопкой мыши  .
2. Нажмите **Добавить кодер**.  
Откроется диалоговое окно **Добавить кодер**.
3. Введите соответствующий IP-адрес.
4. В списке выберите **<Автоопределение>**.
5. Нажмите **ОК**.  
Устройство будет добавлено в систему.
6. Если для устройства требуется начальный пароль, отображается  .  
Чтобы установить начальный пароль, щелкните правой кнопкой мыши значок устройства и нажмите **Задать первоначальный пароль...** . Отобразится диалоговое окно


**Введите пароль.**



Введите пароль для пользователя service и нажмите **ОК**.








закрывается; вы можете использовать устройство.

**Диалоговое окно Добавить кодер**

Главное окно >  **Устройства** > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Добавить кодер** > диалоговое окно **Добавить кодер**  
или

Главное окно >  **Устройства** > щелкните правой кнопкой мыши  > нажмите **Добавить кодер** > диалоговое окно **Добавить кодер**  
или

Главное окно >  **Устройства** > щелкните правой кнопкой мыши  > нажмите **Добавить кодер** > диалоговое окно **Добавить кодер**  
или

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Добавить декодер** > диалоговое окно **Добавить кодер**

**IP-адрес:**


Введите действительный IP-адрес.

**Тип кодера:/Тип декодера:**

Для устройства с известным типом выберите соответствующий элемент. Устройство не обязательно должно быть доступно в сети.

Если требуется добавить какое-либо IP-видеоустройство производства Bosch, выберите **<Автоопределение>**. Это устройство должно быть доступно в сети.

**12.26.3****Добавление устройства iSCSI вручную**

Главное окно >  **Устройства** >  > разверните  > щелкните правой кнопкой мыши  > **Добавить устройство iSCSI** > диалоговое окно **Добавить устройство iSCSI**

Позволяет добавить устройства iSCSI в VRM.

**Добавление устройства iSCSI:**

- Щелкните правой кнопкой мыши  и выберите команду **Добавить устройство iSCSI**.  
Откроется диалоговое окно **Добавить устройство iSCSI**.
- Введите требуемое имя для отображения, сетевой адрес устройства iSCSI и тип устройства и нажмите **ОК**.  
Устройство iSCSI добавляется к выбранному пулу VRM.  
При необходимости добавьте целевые объекты и устройства LUN.

**Диалоговое окно Добавить устройство iSCSI****Имя**

Введите отображаемое имя устройства.

**Сетевой адрес**

Введите действительный сетевой адрес устройства.

**Тип устройства iSCSI**

Выберите соответствующий тип устройства.




**Пароль**

Введите пароль для проверки подлинности на устройстве.

**Дополнительная информация**


- *Добавление устройств VRM путем поиска, Страница 178*

**12.26.4****Добавление Video Streaming Gateway вручную**


Главное окно >  **Устройства** > Разверните  > 

Можно добавлять устройства VSG в пул VRM.

**Для добавления устройства VSG вручную выполните следующие действия.**

- Щелкните правой кнопкой мыши  и щелкните **Добавить шлюз Video Streaming Gateway**.  
Откроется диалоговое окно **Добавить шлюз Video Streaming Gateway**.
- Задайте необходимые параметры для устройства VSG.
- Нажмите **Добавить**.  
✓ Устройство VSG будет добавлено в систему. Изображения с камер, назначенных этому устройству VSG, будут записываться.

**Диалоговое окно Добавить шлюз Video Streaming Gateway**

Щелкните правой кнопкой мыши  > **Добавить шлюз Video Streaming Gateway** > диалоговое окно **Добавить шлюз Video Streaming Gateway**

**Имя**

Введите необходимое отображаемое имя для устройства.

**Имя пользователя**

Введите имя пользователя, используемое для аутентификации на устройстве. Обычно: service

**Сетевой адрес / порт**

Введите IP-адрес устройства.



Если флажок **Безопасное соединение** установлен, порт автоматически меняется на порт HTTPS.

Можно изменить номер порта, если порты по умолчанию не используются или если экземпляры VSG настроены в другом порядке.

#### Порты по умолчанию

Экземпляр VSG	Порт RCPP	Порт HTTPS
1	8756	8443
2	8757	8444
3	8758	8445
4	8759	8446
5	8760	8447
6	8761	8448
7	8762	8449

#### Пароль

Введите действующий пароль для аутентификации на устройстве.

#### Show password

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

#### Безопасность

По умолчанию флажок **Безопасное соединение** установлен, если поддерживается протокол HTTPS.

Начиная с VSG версии 7.0, VSG поддерживает безопасное соединение.



#### Замечание!

При переходе к версии BVMS 10.0 и выше флажок **Безопасное соединение** не установлен по умолчанию, а соединение не защищено (RCPP).

Чтобы изменить безопасное или небезопасное соединение, используйте команду

**Изменить шлюз Video Streaming Gateway** и установите или снимите флажок **Безопасное соединение**.

#### Тест

Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

#### См.

– *Изменение шлюза Video Streaming Gateway, Страница 211*

## 12.26.5

### Добавление устройства iSCSI DSA E-Series вручную



Главное окно >

Устройства >



> разверните



>

Вы можете добавить устройство iSCSI серии E-Series, которое уже инициализировано, или устройство iSCSI серии E-Series, которое не инициализировано.

вы можете добавить устройства LUN больше 2 ТБ, если пул настроен для использования больших устройств LUN.

Устройства LUN больше 2 ТБ («большие устройства LUN») не поддерживаются следующими устройствами:


- Устройства VRM версии ниже 3.60
- Устройства VSG с версией микропрограммного обеспечения ниже 6.30
- Кодеры с версией микропрограммного обеспечения ниже 6.30

BVM5 не позволяет выполнять следующие действия:


- Добавлять или перемещать устройства с версией микропрограммного обеспечения ниже 6.30 в пул, допускающий использование больших устройств LUN.
- Добавлять или перемещать устройства, которые в данный момент не подключены к сети, к пулу, допускающему использование больших устройств LUN.
- Добавлять или перемещать устройство iSCSI, содержащее большие устройства LUN, в пул, который не поддерживает использование больших устройств LUN.
- Разрешать использование больших устройств LUN в пуле, содержащем устройства с версией микропрограммного обеспечения ниже 6.30.
- Отключать использование больших устройств LUN в пуле с устройством iSCSI, содержащим большие устройства LUN.



Переместите устройства с версией микропрограммного обеспечения ниже 6.30 в пул, не поддерживающий большие устройства LUN.

#### для добавления инициализированного устройства iSCSI:





1. Щелкните  правой кнопкой мыши и выберите пункт **Добавить устройство серии DSA E-Series**.  
Отображается диалоговое окно **Добавить устройство серии DSA E-Series**.
2. Введите IP-адрес управления и пароль.
3. Нажмите **Подключиться**.  
. Если подключение установлено, поля в группе **Контроллер** и/или в группе **2-й контроллер** заполняются.
4. Нажмите **ОК**.  
Устройство будет добавлено в систему.  
Автоматически сканируются доступные целевые объекты, и отображаются устройства LUN.  
Вы можете использовать устройство iSCSI.  
Если пул настроен для использования больших устройств LUN и для устройства iSCSI настроены большие устройства LUN, в столбце **Большой LUN** отображается флажок для соответствующих устройств LUN.

#### Чтобы добавить не инициализированное устройство iSCSI:

1. Щелкните  правой кнопкой мыши и выберите пункт **Добавить устройство серии DSA E-Series**.  
Отображается диалоговое окно **Добавить устройство серии DSA E-Series**.
2. Введите IP-адрес управления и пароль.
3. Нажмите **Подключиться**.  
. Если подключение установлено, поля в группе **Контроллер** и/или в группе **2-й контроллер** заполняются.
4. Нажмите **ОК**.  
Устройство будет добавлено в систему.

5. Нажмите , затем нажмите .
6. Перейдите на вкладку **Базовая конфигурация**.
7. Введите требуемый объем устройства LUN.  
Если вы введете значение больше 2 ТБ, потребуется настроить пул для использования устройств LUN больше 2 ТБ.
8. Нажмите кнопку **Инициализировать**.  
Создаются устройства LUN.
9. Нажмите **Закреть**.
10. Щелкните правой кнопкой мыши значок устройства iSCSI и выберите команду **Сканировать целевой объект**.  
Устройства LUN отображаются с неизвестным состоянием.
11. Сохраните и активируйте конфигурацию.
12. Форматирование всех устройств LUN.
13. После добавления устройства iSCSI с двойным контроллером удалите требуемые устройства LUN из первого контроллера, правой кнопкой мыши щелкните второй контроллер и выберите **Сканировать целевой объект** для добавления этих устройств LUN.

#### Диалоговое окно Добавить устройство серии DSA E-Series

Главное окно >  **Устройства** >  > разверните  > щелкните правой кнопкой мыши  > **Добавить устройство серии DSA E-Series** > диалоговое окно

#### Добавить устройство серии DSA E-Series

Позволяет добавить устройство iSCSI DSA E-Series. IP-адрес управления этого типа устройства отличается от IP-адреса хранилища iSCSI. Этот IP-адрес управления используется для автоматического обнаружения и настройки устройства.

#### Имя

Введите отображаемое имя устройства.

#### Адрес управления

Введите IP-адрес для автоматической настройки устройства.

#### Пароль:

Введите пароль для данного устройства.

#### Тип DSA E-Series

Отображает тип устройства.

#### Сетевой адрес канала iSCSI

Отображает IP-адрес или порт iSCSI устройства. При наличии можно выбрать другой IP-адрес.

#### Адрес управления

Отображает IP-адрес для автоматической конфигурации второго контроллера при его наличии. При наличии можно выбрать другой IP-адрес.

#### Сетевой адрес канала iSCSI

Отображает IP-адрес порта iSCSI второго контроллера при его наличии. При наличии можно выбрать другой IP-адрес.

**Подключиться**

Нажмите, чтобы определить параметры устройства.

Если подключение установлено, поля в группе **Контроллер** и в группе **Второй контроллер** заполняются.


**См.**

- Страница "Базовая конфигурация", Страница 204
- Форматирование LUN, Страница 208

**12.26.6****Добавление кодеров путем поиска**

Для добавления кодеров путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск кодеров**. Откроется диалоговое окно **BVMS Scan Wizard**.
2. Выберите необходимые кодеры, выберите необходимый пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.
3. Нажмите **Далее >>**. Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем. Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля. Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**. Затем щелкните это поле правой кнопкой мыши и выберите **Копировать ячейку в столбец**.

В столбце **Состояние** успешные подключения обозначены значком .

Неудачные подключения обозначены значком .



, что означает, что для устройства требуется начальный пароль.

Для установки начального пароля введите его в поле **Пароль**.



Статус изменится на .


Повторите эти действия для всех устройств, которые требуют первоначальный пароль.

**Примечание:** пока вы не установили первоначальный пароль для всех устройств в списке, которые требуют начальный пароль, вы не сможете продолжить работу.

5. Нажмите **Готово**. Устройство добавлено в дерево устройств.

**12.26.7****Добавление устройств VSG путем поиска**

Для добавления устройств VSG путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск шлюзов Video Streaming Gateway**. Откроется диалоговое окно **BVMS Scan Wizard**.
2. Выберите необходимые устройства VSG, выберите пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.

3. Нажмите **Далее >>**.  
Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.  
Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.  
Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.  
Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.



В столбце **Состояние** успешные входы в систему обозначены значком



Неудачные попытки входа обозначены значком

5. Нажмите **Готово**.  
Устройство добавлено в дерево устройств.

## 12.26.8

### Настройка двойного режима записи в Дереве устройств



Главное окно >

**Устройства** > разверните



Для настройки двойной записи функцию ANR необходимо отключить.

Если выполняется настройка двойной записи для одной камеры многоканального кодера, система следит за тем, чтобы все камеры этого кодера были настроены на один и тот же получатель записи.

Двойную запись можно настроить путем назначения кодеров, запись которых обеспечивается основным диспетчером VRM, вторичному VRM. Это может быть полезно, если требуется назначить только часть кодеров, запись которых обеспечивается основным VRM.

Вторичный VRM должен быть уже настроен.

#### Настройка



1. Щелкните правой кнопкой мыши, затем щелкните **Добавить кодер с первичного VRM**.

Отображается диалоговое окно **Добавить кодеры**.

2. Выберите необходимые кодеры.  
При выборе пула или VRM автоматически выбираются все дочерние элементы.
3. Нажмите **ОК**.  
Выбранные кодеры будут добавлены во вторичный VRM.

#### См.

- *Настройка двойного режима записи в Таблице камер, Страница 311*
- *Настройка функции ANR, Страница 311*
- *Двойная / резервная запись, Страница 26*

## 12.27

### Страница «Кодер/декодер Bosch»

Сведения о настройке кодера/декодера Bosch см. в разделе *Страница «Кодер/декодер/камера Bosch», Страница 226*.

## 12.28 Страница устройства iSCSI



Можно добавить либо устройство iSCSI серии E, либо другое поддерживаемое устройство iSCSI.

### См.

- *Добавление устройства iSCSI вручную, Страница 199*
- *Добавление устройства iSCSI DSA E-Series вручную, Страница 200*
- *Настройка устройства iSCSI, Страница 202*
- *Добавление устройства LUN, Страница 206*
- *Форматирование LUN, Страница 208*

### 12.28.1 Пул хранения iSCSI

Пул хранилищ — это контейнер для одной или нескольких систем хранения iSCSI, которые используют одинаковые свойства балансировки нагрузки. IP-камеры и кодеры, назначенные пулу хранилищ, производят запись с этими общими настройками балансировки нагрузки.

Пул хранилищ можно использовать так, чтобы сохранялось логическое сопоставление между топологией сети и VRM. Например, если есть два здания, в каждом из которых есть свое хранилище и устройства, то можно исключить маршрутизацию сетевого трафика из одного здания в другое.

Пулы хранилищ также можно использовать для группировки камер и систем хранения по определенному важному полю обзора. Пусть, к примеру, система содержит несколько очень важных камер и большое число менее важных. В этом случае можно сгруппировать камеры в два пула хранилищ: один с большим количеством функций резервирования, а второй — с меньшей степенью резервирования.

Для пула хранилищ можно настроить следующие свойства балансировки нагрузки:

- Настройки видеозаписи (**Автоматически** или **При отказе**).
- Использование вторичного целевого объекта.  
 Вторичный целевой объект используется в режиме **При отказе** в случае сбоя назначенного первичного целевого объекта. Если эта функция отключена, при сбое первичного целевого объекта видеозапись со всех назначенных ему устройств прекращается.  
 В режиме **Автоматически**: если происходит сбой одного целевого объекта, сервер VRM Server автоматически переназначает связанные с этим объектом устройства другим хранилищам. Если во время сбоя целевого объекта отключен сервер VRM Server, видеозапись с устройств, производивших запись на отказавший целевой объект, прекращается.
- Резервирование блоков на время простоя
- Период проверки работоспособности

Каждый пул можно настроить таким образом, чтобы он допускал использование устройств LUN больше 2 ТБ.

Устройства LUN больше 2 ТБ («большие устройства LUN») не поддерживаются следующими устройствами:

- Устройства VRM версии ниже 3.60

- Устройства VSG с версией микропрограммного обеспечения ниже 6.30
  - Кодеры с версией микропрограммного обеспечения ниже 6.30
- BVMS не позволяет выполнять следующие действия:
- Добавлять или перемещать устройства с версией микропрограммного обеспечения ниже 6.30 в пул, допускающий использование больших устройств LUN.
  - Добавлять или перемещать устройства, которые в данный момент не подключены к сети, к пулу, допускающему использование больших устройств LUN.
  - Добавлять или перемещать устройство iSCSI, содержащее большие устройства LUN, в пул, который не поддерживает использование больших устройств LUN.
  - Разрешать использование больших устройств LUN в пуле, содержащем устройства с версией микропрограммного обеспечения ниже 6.30.
  - Отключать использование больших устройств LUN в пуле с устройством iSCSI, содержащим большие устройства LUN.

Переместите устройства с версией микропрограммного обеспечения ниже 6.30 в пул, не поддерживающий большие устройства LUN.




Если основной VRM имеет пул, поддерживающий использование больших устройств LUN, соответствующий зеркальный VRM наследует этот параметр, и вы не можете установить или снять флажок **Разрешить LUN более 2 ТБ** в соответствующем пуле зеркального VRM. После добавления устройства iSCSI с большими устройствами LUN к зеркальному VRM вы не можете снять флажок **Разрешить LUN более 2 ТБ** в соответствующем пуле основного VRM.

**См.**

- *Страница "Пул", Страница 188*

## 12.28.2

### Добавление устройства iSCSI вручную

Главное окно >  **Устройства** >  > разверните  > щелкните правой кнопкой мыши  > **Добавить устройство iSCSI** > диалоговое окно **Добавить устройство iSCSI**

Позволяет добавить устройства iSCSI в VRM.

#### Добавление устройства iSCSI:

1. Щелкните правой кнопкой мыши  и выберите команду **Добавить устройство iSCSI**.  
Откроется диалоговое окно **Добавить устройство iSCSI**.
2. Введите требуемое имя для отображения, сетевой адрес устройства iSCSI и тип устройства и нажмите **ОК**.  
Устройство iSCSI добавляется к выбранному пулу VRM.  
При необходимости добавьте целевые объекты и устройства LUN.

#### Диалоговое окно **Добавить устройство iSCSI**

##### **Имя**

Введите отображаемое имя устройства.

##### **Сетевой адрес**

Введите действительный сетевой адрес устройства.

**Тип устройства iSCSI**

Выберите соответствующий тип устройства.

**Пароль**

Введите пароль для проверки подлинности на устройстве.

**Дополнительная информация**

- *Добавление устройств VRM путем поиска, Страница 178*

**12.28.3****Добавление устройства iSCSI DSA E-Series вручную**

Главное окно >  > **Устройства** >  > разверните  > 

Вы можете добавить устройство iSCSI серии E-Series, которое уже инициализировано, или устройство iSCSI серии E-Series, которое не инициализировано.

вы можете добавить устройства LUN больше 2 ТБ, если пул настроен для использования больших устройств LUN.

Устройства LUN больше 2 ТБ («большие устройства LUN») не поддерживаются следующими устройствами:


- Устройства VRM версии ниже 3.60
- Устройства VSG с версией микропрограммного обеспечения ниже 6.30
- Кодеры с версией микропрограммного обеспечения ниже 6.30

BVMs не позволяет выполнять следующие действия:

- Добавлять или перемещать устройства с версией микропрограммного обеспечения ниже 6.30 в пул, допускающий использование больших устройств LUN.
- Добавлять или перемещать устройства, которые в данный момент не подключены к сети, к пулу, допускающему использование больших устройств LUN.
- Добавлять или перемещать устройство iSCSI, содержащее большие устройства LUN, в пул, который не поддерживает использование больших устройств LUN.
- Разрешать использование больших устройств LUN в пуле, содержащем устройства с версией микропрограммного обеспечения ниже 6.30.
- Отключать использование больших устройств LUN в пуле с устройством iSCSI, содержащим большие устройства LUN.

Переместите устройства с версией микропрограммного обеспечения ниже 6.30 в пул, не поддерживающий большие устройства LUN.




**для добавления инициализированного устройства iSCSI:**

- Щелкните  правой кнопкой мыши и выберите пункт **Добавить устройство серии DSA E-Series**.  
Отображается диалоговое окно **Добавить устройство серии DSA E-Series**.
- Введите IP-адрес управления и пароль.
- Нажмите **Подключиться**.  
. Если подключение установлено, поля в группе **Контроллер** и/или в группе **2-й контроллер** заполнятся.
- Нажмите **ОК**.  
Устройство будет добавлено в систему.  
Автоматически сканируются доступные целевые объекты, и отображаются устройства LUN.  
Вы можете использовать устройство iSCSI.







Если пул настроен для использования больших устройств LUN и для устройства iSCSI настроены большие устройства LUN, в столбце **Большой LUN** отображается флажок для соответствующих устройств LUN.

#### Чтобы добавить не инициализированное устройство iSCSI:

1. Щелкните  правой кнопкой мыши и выберите пункт **Добавить устройство серии DSA E-Series**.  
Отображается диалоговое окно **Добавить устройство серии DSA E-Series**.
2. Введите IP-адрес управления и пароль.
3. Нажмите **Подключиться**.  
. Если подключение установлено, поля в группе **Контроллер** и/или в группе **2-й контроллер** заполнятся.
4. Нажмите **ОК**.  
Устройство будет добавлено в систему.
5. Нажмите , затем нажмите .
6. Перейдите на вкладку **Базовая конфигурация**.
7. Введите требуемый объем устройства LUN.  
Если вы введете значение больше 2 ТБ, потребуется настроить пул для использования устройств LUN больше 2 ТБ.
8. Нажмите кнопку **Инициализировать**.  
Создаются устройства LUN.
9. Нажмите **Заккрыть**.
10. Щелкните правой кнопкой мыши значок устройства iSCSI и выберите команду **Сканировать целевой объект**.  
Устройства LUN отображаются с неизвестным состоянием.
11. Сохраните и активируйте конфигурацию.
12. Форматирование всех устройств LUN.
13. После добавления устройства iSCSI с двойным контроллером удалите требуемые устройства LUN из первого контроллера, правой кнопкой мыши щелкните второй контроллер и выберите **Сканировать целевой объект** для добавления этих устройств LUN.

#### Диалоговое окно Добавить устройство серии DSA E-Series

Главное окно >  **Устройства** >  > разверните  > щелкните правой кнопкой мыши  > **Добавить устройство серии DSA E-Series** > диалоговое окно **Добавить устройство серии DSA E-Series**

Позволяет добавить устройство iSCSI DSA E-Series. IP-адрес управления этого типа устройства отличается от IP-адреса хранилища iSCSI. Этот IP-адрес управления используется для автоматического обнаружения и настройки устройства.

#### Имя

Введите отображаемое имя устройства.

#### Адрес управления

Введите IP-адрес для автоматической настройки устройства.

**Пароль:**

Введите пароль для данного устройства.

**Тип DSA E-Series**

Отображает тип устройства.

**Сетевой адрес канала iSCSI**

Отображает IP-адрес или порт iSCSI устройства. При наличии можно выбрать другой IP-адрес.

**Адрес управления**

Отображает IP-адрес для автоматической конфигурации второго контроллера при его наличии. При наличии можно выбрать другой IP-адрес.

**Сетевой адрес канала iSCSI**

Отображает IP-адрес порта iSCSI второго контроллера при его наличии. При наличии можно выбрать другой IP-адрес.

**Подключиться**

Нажмите, чтобы определить параметры устройства.

Если подключение установлено, поля в группе **Контроллер** и в группе **Второй контроллер** заполняются.

**См.**

- Страница "Базовая конфигурация", Страница 204
- Форматирование LUN, Страница 208

**12.28.4****Настройка устройства iSCSI**

Главное окно >

**Устройства** > разверните



> разверните



>



После добавления устройств VRM, устройств iSCSI и кодеров выполните следующие действия для обеспечения того, чтобы все видеоданные сохранялись на устройствах iSCSI и видеоданные можно было получить с этих устройств iSCSI.

- Активируйте конфигурацию по умолчанию, чтобы создать номера LUN на каждом целевом объекте устройства iSCSI.  
Это действие не является обязательным. Его не обязательно выполнять на устройстве iSCSI с предварительно настроенными номерами LUN.
- Просканируйте устройство iSCSI, чтобы добавить целевые объекты и номера LUN в логическое дерево после активации конфигурации по умолчанию.



**Примечание**

Не все устройства iSCSI поддерживают конфигурацию по умолчанию и автоматическое сопоставление IQN.

**Предварительные условия:**

Устройство iSCSI должно быть сконфигурировано с действительными IP-адресами.

**Чтобы выполнить базовую конфигурацию устройства DSA E-Series iSCSI:**

- ▶ разверните соответствующее устройство  и , щелкните соответствующее

устройство iSCSI .

1. Перейдите на вкладку **Базовая конфигурация**.
2. Введите требуемый объем устройства LUN.







Если вы введете значение больше 2 ТБ, потребуется настроить пул для использования устройств LUN больше 2 ТБ.

3. Нажмите кнопку **Инициализировать**.  
Создаются устройства LUN.
4. Нажмите **Заккрыть**.
5. Щелкните правой кнопкой мыши значок устройства iSCSI и выберите команду **Сканировать целевой объект**.  
Устройства LUN отображаются с неизвестным состоянием.
6. Сохраните и активируйте конфигурацию.
7. Форматирование всех устройств LUN.
8. После добавления устройства iSCSI с двойным контроллером удалите требуемые устройства LUN из первого контроллера, правой кнопкой мыши щелкните второй контроллер и выберите **Сканировать целевой объект** для добавления этих устройств LUN.

#### Чтобы выполнить базовую конфигурацию на других устройствах iSCSI:

1. перейдите на вкладку **Базовая конфигурация**.
2. Введите необходимое количество устройств LUN.
3. Нажмите **Установить**.  
Создаются устройства LUN.
4. Нажмите **Заккрыть**.
5. Щелкните правой кнопкой мыши значок устройства iSCSI и выберите команду **Сканировать целевой объект**.  
Устройства LUN отображаются с неизвестным состоянием.
6. Сохраните и активируйте конфигурацию.
7. Форматирование всех устройств LUN.

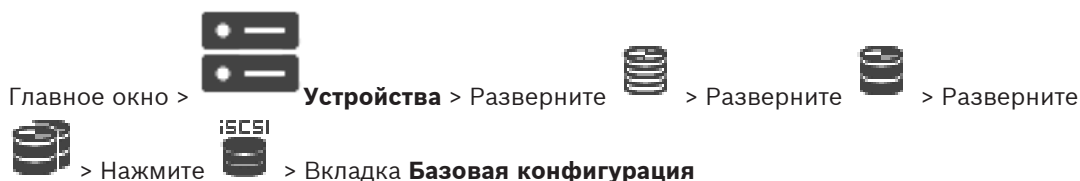
#### Для выполнения сопоставления IQN для других устройств iSCSI:

1. Разверните соответствующее устройство  и , щелкните соответствующее устройство iSCSI  .
2. Щелкните правой кнопкой мыши  и нажмите **Сопоставить IQN**. Отображается диалоговое окно *iqn-Mapper*, и процесс запускается.  
Кодеры, назначенные выбранному устройству VRM, анализируются, а их имена IQN добавляются к данному устройству iSCSI.
3. Нажмите , чтобы сохранить настройки.
4. Нажмите  для активации конфигурации.

#### См.

- *Страница "Базовая конфигурация", Страница 204*
- *Диалоговое окно "Распределение нагрузки", Страница 205*
- *Диалоговое окно iqn-Mapper, Страница 208*
- *Форматирование LUN, Страница 208*

## 12.28.5 Страница "Базовая конфигурация"



Отображаемые параметры могут зависеть от используемого типа системы хранения iSCSI. Позволяет выполнить базовую настройку устройства iSCSI. На жестком диске iSCSI создаются и форматируются устройства LUN. Отображается, только если устройство представляет собой систему хранения iSCSI, поддерживаемую Bosch, например DSA или DLS 1x00.



### Замечание!

После базовой настройки серии E-Series для инициализации системы требуется много часов (или даже дней). На этом этапе полная производительность недоступна, а на этапе 1,5 возможен сбой форматирования.

### Физическая емкость (ГБ)

Информация об общей емкости системы хранения.

### Количество логических устройств

Можно изменить количество устройств LUN.



### Замечание!

При изменении количества устройств LUN вся система iSCSI будет реорганизована, а все сохраненные в системе видеопоследовательности будут утрачены. Поэтому прежде чем вносить изменения, проверьте записи и сделайте резервные копии всех важных видеопоследовательностей.

### Емкость для новых логических устройств (ГБ)

Этот параметр отображается только для E-Series.

Так как в массиве хранилищ не может быть более 256 устройств LUN, нельзя задавать слишком маленький размер LUN (в противном случае в будущем нельзя будет создать дополнительные LUN при установке дополнительной полки).

### Целевые свободные диски

Количество свободных дисков, которые пользователь хочет оставить в системе.

### Фактическое кол-во свободных дисков

Количество свободных дисков, присутствующих в системе в настоящий момент. Это число может отличаться от указанного выше числа, например если система хранения перенастроена вручную или часть дисков сломана.

### Состояние инициализации (%)

Дополнительные сведения отображаются при инициализации. По завершении инициализации (100 %) будет еще одна возможность удалить все устройства LUN.

**Примечание.** В системах хранения FAS полное удаление всех устройств LUN может занять несколько часов. В течение этого времени общая производительность вновь созданных устройств LUN может быть снижена. Новые устройства LUN с полной производительностью можно создать только после полного удаления всех старых LUN.

**RAID-DP (обеспечение надежности)**

Активируйте этот параметр, если вы не хотите использовать указанный тип RAID — RAID-4, а предпочитаете использовать более надежный RAID-DP.

**RAID 6 (приоритет надежности)**

Активируйте этот параметр, если вы не хотите использовать указанный тип RAID — RAID-5, а предпочитаете использовать более надежный RAID-6.






**Дополнительная информация**

Здесь отображается дополнительная информация, например сведения о том, что система хранилища настроена неправильно и по этой причине настройка невозможна.

**См.**

– *Добавление устройства iSCSI DSA E-Series вручную, Страница 200*

**12.28.6****Диалоговое окно "Распределение нагрузки"**





Главное окно >  **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > команда **Балансировка нагрузки...** > диалоговое окно **Балансировка загрузки**

**Предварительные условия:** настройка режима записи **Автоматически**.

Установка верхних пределов допустимой скорости передачи и количества одновременных подключений iSCSI для каждой системы iSCSI. Если эти пределы превышены, данные перестают записываться в систему iSCSI и будут утеряны.




Для поддерживаемых систем (например, Bosch RAID, NetApp, DLA) используйте значения по умолчанию. В случае использования других устройств см. соответствующую документацию. Начинать тестирование с малых значений.

**12.28.7****Перемещение системы iSCSI в другой пул («Изменение пула...»)**

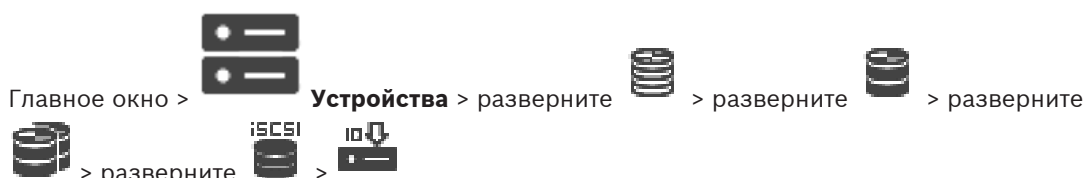
Главное окно > **Устройства** > разверните  > разверните  > разверните  > 

Устройство можно переместить из одного пула в другой в пределах одного устройства VRM без потерь записи.

**Для перемещения:**

- Щелкните правой кнопкой мыши  /  /  и выберите команду **Изменить пул...**  
Откроется диалоговое окно **Изменить пул**.
- В списке **Новый пул:** выберите необходимый пул.
- Нажмите **ОК**.  
Устройство перейдет к выбранному пулу.

## 12.28.8 Страница устройств LUN



Позволяет добавлять, удалять или форматировать устройства LUN, а также просматривать информацию об устройствах LUN.

### Добавить

Нажмите для отображения диалогового окна **Добавить LUN**.

### Удалить

Нажмите, чтобы удалить выбранные строки. Для выбора строки нажмите заголовок строки с левой стороны. Каждая строка представляет LUN.

Отображается окно сообщения.

### Форматировать LUN

Нажмите для форматирования выбранного устройства LUN. Отображается окно сообщения.

### Формат

Установите флажок, чтобы выбрать устройство LUN и нажмите кнопку **Форматировать LUN**.

### Логическое устройство

Отображает имя устройства LUN.

### Размер [ГБ]

Отображает максимальную емкость устройства LUN.

### Большой LUN

Каждая ячейка отображает, является ли это устройство LUN устройством больше 2 ТБ.

### Состояние

Отображает состояние устройства LUN.

### Ход выполнения

Отображает ход выполнения процесса форматирования.

### См.

- *Страница "Пул", Страница 188*
- *Добавление устройства LUN, Страница 206*
- *Добавление устройств VRM путем поиска, Страница 178*

## 12.28.9 Добавление устройства LUN

Главное окно > **Устройства** > разверните > разверните > разверните

Обычно нужные устройства iSCSI с их получателями и номерами LUNs добавляются в результате сканирования сети автоматически. Если сканирование сети не приводит к нужным результатам или требуется настройка устройства iSCSI в автономном режиме перед его интегрированием в сеть, следует настроить получателя в устройстве iSCSI, а в этом получателе настроить один или несколько номеров LUN.

вы можете добавить устройства LUN больше 2 ТБ, если пул настроен для использования больших устройств LUN.

Устройства LUN больше 2 ТБ («большие устройства LUN») не поддерживаются следующими устройствами:

- Устройства VRM версии ниже 3.60
- Устройства VSG с версией микропрограммного обеспечения ниже 6.30
- Кодеры с версией микропрограммного обеспечения ниже 6.30

BVMS не позволяет выполнять следующие действия:

- Добавлять или перемещать устройства с версией микропрограммного обеспечения ниже 6.30 в пул, допускающий использование больших устройств LUN.
- Добавлять или перемещать устройства, которые в данный момент не подключены к сети, к пулу, допускающему использование больших устройств LUN.
- Добавлять или перемещать устройство iSCSI, содержащее большие устройства LUN, в пул, который не поддерживает использование больших устройств LUN.
- Разрешать использование больших устройств LUN в пуле, содержащем устройства с версией микропрограммного обеспечения ниже 6.30.
- Отключать использование больших устройств LUN в пуле с устройством iSCSI, содержащим большие устройства LUN.

Переместите устройства с версией микропрограммного обеспечения ниже 6.30 в пул, не поддерживающий большие устройства LUN.

#### Для добавления выполните следующие действия.

1. При необходимости выберите **Разрешить LUN более 2 ТБ**.

2. Щелкните  правой кнопкой мыши и выберите **Сканировать целевой объект**.


Целевой объект  добавлен.

3. Выберите целевой объект.  
Отобразится страница **Устройства LUN**.
4. Нажмите **Добавить**.  
Откроется диалоговое окно **Добавить LUN**.
5. Введите нужный номер LUN и нажмите кнопку **ОК**.  
Номер LUN будет добавлен в новой строке таблицы.  
Повторите эти действия для каждого выбранного LUN.

#### Примечания

- Чтобы удалить LUN, нажмите **Удалить**.  
Видеоданные не удаляются с этого LUN.
- Чтобы отформатировать LUN, нажмите **Форматировать LUN**.  
Все данные с этого LUN будут удалены!

#### Диалоговое окно Добавить LUN

Главное окно >  **Устройства** > развернуть  > развернуть  > развернуть  > развернуть  >  > нажмите **Добавить**

Позволяет добавить LUN.

#### Id

Введите идентификатор требуемого LUN.

**См.**

- Страница "Пул", Страница 188
- Страница устройств LUN, Страница 206

### 12.28.10

#### Форматирование LUN



Устройство LUN форматируется для подготовки к первому использованию.



#### Замечание!

После форматирования все данные на устройстве LUN удаляются.

#### Настройка

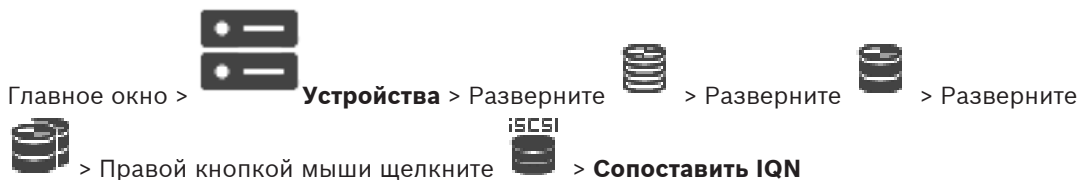
1. Выберите нужное устройство LUN и установите флажок в столбце **Формат**.
2. Нажмите **Форматировать LUN**.
3. Внимательно прочтите появившееся сообщение и подтвердите его.  
Выбранное устройство LUN будет отформатировано. Все данные с этого LUN будут удалены.

**См.**

- Страница устройств LUN, Страница 206

### 12.28.11

#### Диалоговое окно iqn-Маркер



Позволяет начать процесс сопоставления IQN.

**См.**

- Добавление устройств VRM путем поиска, Страница 178
- Настройка устройства iSCSI, Страница 202

### 12.29

#### Страница устройства Video Streaming Gateway



В данном разделе содержится информация о настройке устройства VSG в системе. Позволяет добавлять и настраивать следующие типы кодеров.

- Кодеры Bosch
- Кодеры ONVIF
- Кодеры JPEG



- Кодеры RTSP

#### Добавление устройств VSG путем поиска.

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск шлюзов Video Streaming Gateway**.  
Откроется диалоговое окно **BVMS Scan Wizard**.
2. Выберите необходимые устройства VSG, выберите необходимый пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.
3. Нажмите **Далее >>**.  
Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.  
Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.  
Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.  
Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.

В столбце **Состояние** успешные входы в систему обозначены значком .

Неудачные попытки входа обозначены значком .




5. Нажмите **Готово**.  
Устройство добавлено в дерево устройств.  
При добавлении нового VSG версии 7.0 или выше флажок **Безопасное соединение** устанавливается по умолчанию.  
Чтобы изменить безопасное или небезопасное соединение, используйте команду **Изменить шлюз Video Streaming Gateway** и установите или снимите флажок **Безопасное соединение**.

#### См.

- *Изменение шлюза Video Streaming Gateway, Страница 211*
- *Страница "ONVIF", Страница 244*

## 12.29.1

### Добавление Video Streaming Gateway вручную

Главное окно >  **Устройства** > Разверните  >   
Можно добавлять устройства VSG в пул VRM.

**Для добавления устройства VSG вручную выполните следующие действия.**

1. Щелкните правой кнопкой мыши  и щелкните **Добавить шлюз Video Streaming Gateway**.  
Откроется диалоговое окно **Добавить шлюз Video Streaming Gateway**.
2. Задайте необходимые параметры для устройства VSG.
3. Нажмите **Добавить**.  
✓ Устройство VSG будет добавлено в систему. Изображения с камер, назначенных этому устройству VSG, будут записываться.

### Диалоговое окно Добавить шлюз Video Streaming Gateway

Щелкните правой кнопкой мыши  > **Добавить шлюз Video Streaming Gateway** > диалоговое окно **Добавить шлюз Video Streaming Gateway**

#### Имя

Введите необходимое отображаемое имя для устройства.

#### Имя пользователя

Введите имя пользователя, используемое для аутентификации на устройстве. Обычно: service

#### Сетевой адрес / порт

Введите IP-адрес устройства.

Если флажок **Безопасное соединение** установлен, порт автоматически меняется на порт HTTPS.

Можно изменить номер порта, если порты по умолчанию не используются или если экземпляры VSG настроены в другом порядке.

#### Порты по умолчанию

Экземпляр VSG	Порт RCPP	Порт HTTPS
1	8756	8443
2	8757	8444
3	8758	8445
4	8759	8446
5	8760	8447
6	8761	8448
7	8762	8449

#### Пароль

Введите действующий пароль для аутентификации на устройстве.

#### Show password

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

#### Безопасность

По умолчанию флажок **Безопасное соединение** установлен, если поддерживается протокол HTTPS.

Начиная с VSG версии 7.0, VSG поддерживает безопасное соединение.



#### Замечание!

При переходе к версии BVMS 10.0 и выше флажок **Безопасное соединение** не установлен по умолчанию, а соединение не защищено (RCPP).

Чтобы изменить безопасное или небезопасное соединение, используйте команду

**Изменить шлюз Video Streaming Gateway** и установите или снимите флажок **Безопасное соединение**.

#### Тест

Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

См.

– *Изменение шлюза Video Streaming Gateway, Страница 211*

## 12.29.2

### Изменение шлюза Video Streaming Gateway



**Чтобы изменить безопасное/небезопасное соединение:**

1. Щелкните правой кнопкой мыши .
2. Нажмите **Изменить шлюз Video Streaming Gateway**.  
Откроется диалоговое окно **Изменить шлюз Video Streaming Gateway**.
3. Установите флажок **Безопасное соединение**.  
Используемый порт автоматически меняется на порт HTTPS.  
Или  
снимите флажок **Безопасное соединение**.  
Используемый порт автоматически меняется на порт RCPP.



#### **Замечание!**

После обновления до новой версии рекомендуется изменить включить безопасное соединение.

См.

– *Добавление Video Streaming Gateway вручную, Страница 209*

## 12.29.3

### Добавление камеры в VSG



В VSG можно добавить следующие устройства.

- Кодеры Bosch
- Камеры ONVIF
- Камеры JPEG
- Кодеры RTSP

После добавления кодеров VSG в автономном режиме можно обновить их состояние.

**Порядок добавления:**

1. Щелкните правой кнопкой мыши , наведите указатель на **Добавить кодер/камеру** и нажмите требуемую команду.
2. Задайте необходимые параметры в диалоговом окне для добавления устройства.
3. Нажмите **ОК**.  
Устройство добавляется.

**Обновление:**

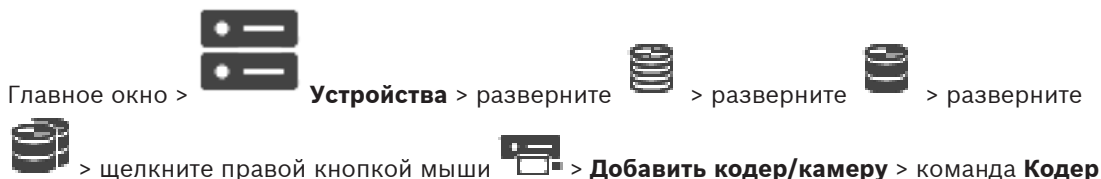
- ▶ Щелкните правой кнопкой необходимый кодер и выберите **Обновить состояние**. Извлекаются свойства устройства.

**См.**

- Диалоговое окно "Добавить кодер Bosch", Страница 212
- Диалоговое окно "Добавить кодер ONVIF", Страница 213
- Диалоговое окно "Добавить камеру JPEG", Страница 215
- Диалоговое окно "Добавить кодер RTSP", Страница 216

**12.29.4**

**Диалоговое окно "Добавить кодер Bosch"**



Можно добавить кодер Bosch для устройства VSG.

**Имя**

Введите необходимое отображаемое имя для устройства.

**Сетевой адрес**

Введите сетевой адрес устройства.

**Тип**

Отображает определенный тип устройства, если он поддерживается.

**Имя пользователя**

Введите имя пользователя, используемое для аутентификации на устройстве. Обычно: service

**Пароль**

Введите действующий пароль для аутентификации на устройстве.

**Show password**

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

**Тест**

Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

**Свойства**

Нажмите для включения необходимых функций, доступных для этого устройства.

<b>Аудио</b>	Выберите этот пункт, чтобы включить звук, если он доступен для этого устройства.
<b>PTZ</b>	Выберите этот пункт, чтобы включить режим PTZ, если он доступен для этого устройства.
<b>Протокол камеры</b>	TCP Используется для передачи в Интернете и (или) для передачи данных без потерь. Обеспечивает отсутствие потерь пакетов данных. Могут предъявляться высокие

	<p>требования к полосе пропускания. Используйте, если устройство защищено брандмауэром. Не поддерживает многопоточную передачу. UDP Используется при облегченной передаче данных без соединения в частных сетях. Пакеты данных могут теряться. Требования к пропускной способности могут быть низкими. Поддерживает многоадресную передачу.</p>
<p><b>Используйте видеовход 1 - Используйте видеовход 4</b></p>	<p>Нажмите для выбора видеовходов, если выполняется настройка многоканального устройства.</p>



См.

– *Добавление камеры в VSG, Страница 211*

### 12.29.5

#### Диалоговое окно "Добавить кодер ONVIF"


 Главное окно > **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > **Добавить кодер/камеру** > команда **Добавить кодер ONVIF** или


 Главное окно > **Устройства** > щелкните правой кнопкой мыши  > команда **Добавить кодер ONVIF**

Можно добавить кодер ONVIF к устройству VSG или как кодер, работающий только в режиме реального времени.  
Необходимо настроить используемый профиль для видеозаписи и видео в режиме реального времени в таблице камер.

Начиная с версии BVMS 10.0 события кодера ONVIF можно получить непосредственно от VSG или кодера ONVIF. При добавлении нового кодера ONVIF флажок **Извлекать события ONVIF из VSG (Profile S, T)** устанавливается по умолчанию, а Profile T поддерживается. Следующие возможности поддерживаются, только если кодер ONVIF добавлен в систему через устройство VSG:

- Если события кодера ONVIF извлекаются из VSG, настроенные по умолчанию события ONVIF уже сопоставлены.
- Оператор может включать и выключать реле в Operator Client.



**Замечание!**

Получение событий ONVIF из VSG доступно только начиная с VSG версии 7.0. При переходе на BVMS версии 10.0 существующие события кодера ONVIF извлекаются непосредственно из кодера ONVIF. Необходимо обновить VSG до версии 7.0.

**Имя**

Введите необходимое отображаемое имя для устройства.

**Сетевой адрес / порт**

Введите сетевой адрес устройства. При необходимости измените номер порта.

**Имя пользователя**

Введите имя пользователя, используемое для аутентификации на устройстве. Обычно: service

**Пароль**

Введите действующий пароль для аутентификации на устройстве.

**Show password**

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

**Тест**

Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

**Безопасное соединение**

Можно активировать безопасное подключение для видео в режиме реального времени, передаваемого кодером ONVIF на ваше устройство VSG.

**Примечание.**

Если эта функция включена, пользователь Operator Client не может переключить поток на протокол UDP или многоадресный протокол UDP.

Когда эта функция включена, ANR не работает на подверженных устройствах.

При активации этой функции воспроизведение с помощью кодера в кодерах с микропрограммой до версии 6.30 не поддерживается.

**Замечание!**

Порт 443 выбран по умолчанию. Вы можете изменить номер порта в соответствии с настроенным портом HTTPS кодера.

Настроенный номер порта не будет сохранен.

**Свойства**

<b>Тип устройства</b>	Отображает полученный тип устройства.
<b>Производитель</b>	Отображает полученное название производителя.
<b>Модель</b>	Отображает полученное название модели.
<b>Версия микропрограммы</b>	Отображает полученную версию микропрограммного обеспечения.
<b>Дополнительные команды</b>	Если флажок установлен, вспомогательные команды поддерживаются.
<b>Число входных видеоканалов</b>	Введите необходимое количество видеовходов.
<b>Число входных аудиоканалов</b>	Введите необходимое количество аудиовходов.
<b>Число тревожных входов</b>	Введите необходимое количество тревожных входов.

<b>Число реле</b>	Введите необходимое количество реле.
<b>Назначенные каналы шлюза</b>	Введите необходимо количество каналов шлюза.
<b>Протокол камеры</b>	Выберите необходимый протокол камеры.
<b>Использовать видеовход {0}</b>	Установите флажок, чтобы использовать соответствующий видеовход.
<b>Профиль ONVIF</b>	Выберите профиль (если поддерживается), который нужно настроить.


**Замечание!**

Параметры **Настройки Video Streaming Gateway** недоступны для кодеров ONVIF, которые добавлены в качестве кодеров, работающих только в режиме реального времени.

См.

– *Добавление камеры в VSG, Страница 211*

**12.29.6****Диалоговое окно "Добавить камеру JPEG"**

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > **Добавить кодер/камеру** > команда

**Камера JPEG**

Можно добавить камеру JPEG для устройства VSG.

**Имя**

Введите необходимое отображаемое имя для устройства.

**URL**

Введите URL-адрес камеры JPEG или камеры RTSP.

Для камеры JPEG производства Bosch введите следующую строку:

```
http://<ip-address>/snap.jpg?jpegCam=<channel_no.>
```

Для камеры RTSP производства Bosch введите следующую строку:

```
rtsp://<ip-address>/rtsp_tunnel
```

**Имя пользователя**

Введите имя пользователя, используемое для аутентификации на устройстве. Обычно: service

**Пароль**

Введите действующий пароль для аутентификации на устройстве.

**Show password**

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

**Тест**

Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.





**Свойства**

<b>Число входных видеоканалов</b>	Введите количество доступных видеовходов (если они есть).
<b>Частота кадров [кадр/с]</b>	Введите необходимую частоту кадров.

**См.**

– *Добавление камеры в VSG, Страница 211*

**12.29.7****Диалоговое окно "Добавить кодер RTSP"**

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > **Добавить кодер/камеру** > команда

**Камера RTSP**

Можно добавить кодер RTSP для устройства VSG.

**Имя**

Введите необходимое отображаемое имя для устройства.

**URL**

Введите URL-адрес камеры JPEG или камеры RTSP.

Для камеры JPEG производства Bosch введите следующую строку:

```
http://<ip-address>/snap.jpg?jpegCam=<channel_no.>
```

Для камеры RTSP производства Bosch введите следующую строку:

```
rtsp://<ip-address>/rtsp_tunnel
```

**Имя пользователя**

Введите имя пользователя, используемое для аутентификации на устройстве. Обычно: service

**Пароль**

Введите действующий пароль для аутентификации на устройстве.

**Show password**

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

**Тест**

Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

**Свойства**

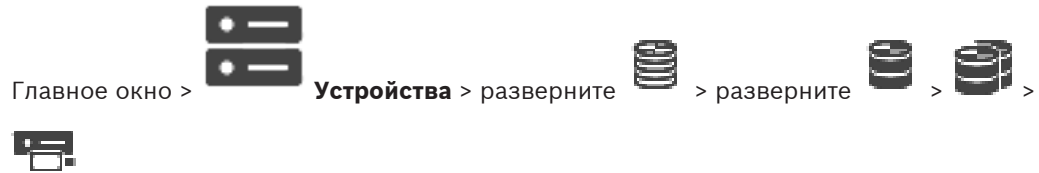
<b>Число входных видеоканалов</b>	Введите количество доступных видеовходов (если они есть).
-----------------------------------	---

**См.**

– *Добавление камеры в VSG, Страница 211*



## 12.29.8

**Перемещение VSG в другой пул («Изменение пула»)**

Устройство можно переместить из одного пула в другой в пределах одного устройства VRM без потерь записи.

**Для перемещения:**

- Щелкните правой кнопкой мыши / / и выберите команду **Изменить пул...**  
Откроется диалоговое окно **Изменить пул**.
- В списке **Новый пул:** выберите необходимый пул.
- Нажмите **ОК**.  
Устройство перейдет к выбранному пулу.

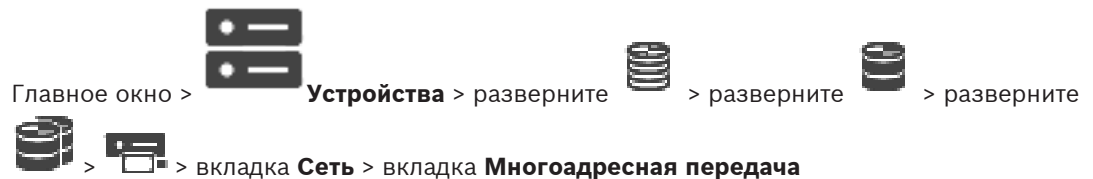
## 12.29.9

**Настройка многоадресной передачи (вкладка «Многоадресная передача»)**

Для каждой камеры, назначенной устройству Video Streaming Gateway, можно настроить адрес многоадресной передачи и порт.

**Порядок настройки многоадресной передачи:**

- Установите требуемый флажок для включения многоадресной передачи.
- Введите правильный адрес многоадресной передачи и номер порта.
- При необходимости настройте непрерывный поток многоадресной передачи.

**Вкладка Многоадресная передача**

Позволяет настроить многоадресную передачу для назначенных камер.

**Включить**

Нажмите, чтобы активировать многоадресную передачу для данной камеры.

**Адрес многопоточной передачи**

Вставьте допустимый адрес многоадресной передачи (в диапазоне от 224.0.0.0 до 239.255.255.255).

Введите *1.0.0.0*. Уникальный адрес многоадресной передачи вставляется автоматически в зависимости от MAC-адреса устройства.

**Порт**






Если используется брандмауэр, введите номер порта, который не блокируется в брандмауэре.

**Поток**

Нажмите, чтобы активировать непрерывную многоадресную потоковую передачу на коммутатор. Это означает, что многоадресному соединению не будет предшествовать регистрация RCP+. Кодер всегда будет передавать на коммутатор все данные. Коммутатор, в свою очередь (если не поддерживается или не настроена многоадресная фильтрация IGMP), будет передавать эти данные на все порты, то есть через коммутатор будет непрерывно проходить полный поток.

Потоковая передача необходима для получения многоадресного потока при использовании устройства другой компании (не Bosch).

**12.29.10****Настройка ведения журналов (вкладка «Дополнительно»)**

Главное окно >  **Устройства** > Разверните  > Разверните  > Разверните  >  > Вкладка **Обслуживание** > Вкладка **Дополнительно**

Позволяет активировать регистрацию для шлюза потокового видео.

Файлы журнала обычно хранятся в следующем каталоге:

```
C:\Program Files (x86)\Bosch\Video Streaming Gateway\log
```

Начиная с VSG версии 7.0 файлы журнала обычно хранятся в следующем каталоге:

```
C:\ProgramData\Bosch\VSG\log
```

**Примечание.** При обновлении до VSG 7.0 или более новой версии предыдущие файлы журнала автоматически перемещаются в этот каталог.

Файлы журнала старых версий VSG обычно хранятся в следующем каталоге:

```
C:\Program Files (x86)\Bosch\Video Streaming Gateway\log
```

**Вкладка Дополнительно****Регистрация RCP+**

Нажмите, чтобы включить функцию ведения журнала RCP+.

**Регистрация данных отладки**

Нажмите, чтобы включить функцию ведения журнала отладки.

**Регистрация RTP**

Нажмите, чтобы включить функцию ведения журнала RTP.

**Срок хранения (в днях)**

Выберите требуемое количество дней.

**Полный дамп-файл памяти**

Включайте этот параметр только в случае необходимости, например, если в службе технической поддержки потребуют полную сводку состояния основной памяти.

**Поддержка Telnet**

Включайте этот параметр, если требуется поддержка доступа по протоколу Telnet.

Включайте только в случае необходимости.

**Замечание!**

Для интенсивной регистрации в журналах необходимы значительные ресурсы центрального процессора и емкость жесткого диска.

Не пользуйтесь интенсивной регистрацией постоянно.

## 12.29.11 Запуск ONVIF Camera Event Driver Tool из Configuration Client



ONVIF Camera Event Driver Tool для выбранного VSG можно запустить непосредственно из Configuration Client.

**Примечание.** Данный инструмент также можно запустить из меню «Пуск» Windows. ONVIF Camera Event Driver Tool позволяет сопоставлять события ONVIF с событиями BVIP VSG. Можно подключаться к камерам ONVIF и извлекать события ONVIF для сопоставления.

### Для запуска ONVIF Camera Event Driver Tool из Configuration Client:

1. Щелкните правой кнопкой мыши соответствующий VSG.
2. Нажмите **Запустите ONVIF Camera Event Driver Tool**.  
Отобразится ONVIF Camera Event Driver Tool.



### Замечание!

ONVIF Camera Event Driver Tool поддерживает только безопасное подключение к VSG.

## 12.30 Страница Режим реального времени и локальное хранилище



Позволяет добавлять и настраивать кодеры, работающие только в режиме реального времени. Вы можете добавить кодеры Bosch и сетевые видеопередатчики ONVIF.

Сведения о добавлении, изменении и настройке кодеров ONVIF, работающих только в режиме реального времени, см. в разделе *Страница "ONVIF"*, *Страница 244*.

### См.


- *Добавление кодера, работающего только в режиме реального времени, Страница 228*
- *Поиск устройств, Страница 73*
- *Страница «Кодер/декодер/камера Bosch», Страница 226*
- *Страница "ONVIF", Страница 244*
- *Настройка многоадресной передачи, Страница 242*

### 12.30.1 Добавление устройств, работающих только в режиме реального времени, путем поиска

Для добавления устройств Bosch, работающих только в реальном времени, путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши и выберите команду **Поиск кодеров, работающих только в реальном времени**.  
Откроется диалоговое окно **BVMS Scan Wizard**.

2. Установите флажки для устройств, которые необходимо добавить.
3. Нажмите **Далее >>**.  
Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.  
Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.  
Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.  
Затем щелкните это поле правой кнопкой мыши и выберите **Копировать ячейку в столбец**.

В столбце **Состояние** успешные подключения обозначены значком .

Неудачные подключения обозначены значком .



, что означает, что для устройства требуется начальный пароль.

Для установки начального пароля введите его в поле **Пароль**.



Статус изменится на .

Повторите эти действия для всех устройств, которые требуют первоначальный пароль.

**Примечание:** пока вы не установили первоначальный пароль для всех устройств в списке, которые требуют начальный пароль, вы не сможете продолжить работу.

5. Нажмите **Готово**.  
Устройство добавлено в дерево устройств.

## 12.30.2






### Добавление кодера и декодера вручную


Позволяет добавить кодер или декодер вручную. Это особенно полезно, если необходимо добавить какое-либо IP-видеоустройство производства Bosch (только для VRM).

#### Внимание.

Если добавляется IP-видеокодер или декодер Bosch с выбранным параметром **<Автоопределение>**, это устройство должно быть доступно в сети.

#### Добавление IP-видеоустройства производства Bosch:

1. Разверните , разверните , щелкните правой кнопкой мыши .  
Или  
щелкните правой кнопкой мыши .  
Или  
щелкните правой кнопкой мыши .
2. Нажмите **Добавить кодер**.  
Откроется диалоговое окно **Добавить кодер**.
3. Введите соответствующий IP-адрес.
4. В списке выберите **<Автоопределение>**.
5. Нажмите **ОК**.  
Устройство будет добавлено в систему.

6. Если для устройства требуется начальный пароль, отображается . Чтобы установить начальный пароль, щелкните правой кнопкой мыши значок устройства и нажмите **Задать первоначальный пароль...**. Отобразится диалоговое окно



**Введите пароль.**



Введите пароль для пользователя service и нажмите **ОК**.








закроется; вы можете использовать устройство.

**Диалоговое окно Добавить кодер**

Главное окно >  **Устройства** > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Добавить кодер** > диалоговое окно **Добавить кодер** или

Главное окно >  **Устройства** > щелкните правой кнопкой мыши  > нажмите **Добавить кодер** > диалоговое окно **Добавить кодер** или

Главное окно >  **Устройства** > щелкните правой кнопкой мыши  > нажмите **Добавить кодер** > диалоговое окно **Добавить кодер** или

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Добавить декодер** > диалоговое окно **Добавить кодер**

**IP-адрес:**

Введите действительный IP-адрес.




**Тип кодера:/Тип декодера:**

Для устройства с известным типом выберите соответствующий элемент. Устройство не обязательно должно быть доступно в сети.

Если требуется добавить какое-либо IP-видеоустройство производства Bosch, выберите **<Автоопределение>**. Это устройство должно быть доступно в сети.

## 12.30.3

**Предоставление пароля пункта назначения декодеру («Проверка подлинности...»)**

Главное окно >  **Устройства** > разверните  > разверните  > щелкните

правой кнопкой мыши  > нажмите **Аутентификация...** > диалоговое окно **Введите пароль**

Для предоставления доступа к защищенному паролем кодеру для декодера необходимо ввести пароль уровня авторизации пользователя кодера в качестве пароля пункта назначения в декодере.

**Предоставление.**

1. В списке **Введите имя пользователя** выберите destination password.
  2. В поле **Введите пароль для пользователя** введите новый пароль.
  3. Нажмите **ОК**.
- ✓ Пароль на устройстве изменяется незамедлительно.

**См.**

- *Изменение пароля кодера и декодера («Изменить пароль»/«Введите пароль»)*,  
Страница 145

## 12.31


**Страница Локальное хранилище**

Главное окно >  **Устройства** > разверните  > 

Позволяет добавлять и настраивать кодеры с локальным хранилищем.

**Для добавления кодеров локального хранилища путем поиска выполните следующие действия.**

1. В дереве устройств щелкните  правой кнопкой мыши и выберите **Поиск кодеров локального хранилища**.  
Откроется диалоговое окно **BVMS Scan Wizard**.
2. Установите флажки для устройств, которые необходимо добавить.
3. Нажмите **Далее >>**.  
Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.  
Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.  
Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.  
Затем щелкните это поле правой кнопкой мыши и выберите **Копировать ячейку в столбец**.

В столбце **Состояние** успешные подключения обозначены значком  .

Неудачные подключения обозначены значком



, что означает, что для устройства требуется начальный пароль.

Для установки начального пароля введите его в поле **Пароль**.



Статус изменится на .

Повторите эти действия для всех устройств, которые требуют первоначальный пароль.

**Примечание:** пока вы не установили первоначальный пароль для всех устройств в списке, которые требуют начальный пароль, вы не сможете продолжить работу.

5. Нажмите **Готово**.

Устройство добавлено в дерево устройств.

#### См.

- *Настройка многоадресной передачи, Страница 242*
- *Добавление кодера локального хранилища, Страница 228*
- *Страница «Кодер/декодер/камера Bosch», Страница 226*
- *Поиск устройств, Страница 73*

## 12.32

### Страница Unmanaged Site



Главное окно >  **Устройства** > разверните  > 

Можно добавить сетевое видеорустройство в элемент **Unmanaged Sites** дерева устройств.

Предполагается, что все unmanaged сетевые устройства unmanaged site находятся в одном часовом поясе.

#### Имя объекта

Отображает имя объекта, введенное во время создания этого элемента.

#### Описание

Введите описание этого объекта site.

#### Часовой пояс

Выберите соответствующий часовой пояс для этого unmanaged site.

#### См.

- *Неуправляемый объект, Страница 23*
- *Добавление объекта unmanaged site вручную, Страница 223*
- *Импорт неуправляемых объектов, Страница 224*
- *Настройка часового пояса, Страница 225*

### 12.32.1


#### Добавление объекта unmanaged site вручную



Главное окно >  **Устройства** > 

#### Создание



1. Щелкните  правой кнопкой мыши и выберите пункт **Добавить Unmanaged Site**. Отображается диалоговое окно **Добавить Unmanaged Site**.
2. Введите имя и описание объекта.
3. В списке **Часовой пояс** выберите нужный элемент.
4. Нажмите **ОК**.  
В систему будет добавлен новый unmanaged site.

**См.**

- *Неуправляемый объект, Страница 23*
- *Страница Unmanaged Site, Страница 223*

**12.32.2****Импорт неуправляемых объектов**

Главное окно &gt;

Устройства &gt;

Вы можете импортировать файл CSV, содержащий конфигурацию видеорегистратора или другой системы BVMS, которую вы хотите импортировать в вашу систему BVMS как неуправляемый объект.

**Импорт:**

1. Щелкните правой кнопкой мыши, затем нажмите **Импорт Unmanaged Sites**.
2. Выберите нужный файл и нажмите кнопку **Открыть**.

В систему будет добавлен один или несколько новых неуправляемых объектов. Теперь можно добавить эти неуправляемые объекты в логическое дерево.

**Примечание.** Если возникает ошибка и файл импортировать невозможно, появится соответствующее сообщение об ошибке.

**12.32.3****Страница «Unmanaged Site»****Имя объекта**

Отображает имя объекта, введенное во время создания этого элемента.

**Описание**

Введите описание этого объекта site.

**Часовой пояс**

Выберите соответствующий часовой пояс для этого unmanaged site.

**12.32.4****Добавление unmanaged сетевого устройства**




Главное окно &gt;

Устройства &gt;

1. Щелкните правой кнопкой мыши этот элемент и выберите команду **Добавить неуправляемое сетевое устройство**.  
Откроется диалоговое окно **Добавить неуправляемое сетевое устройство**.
2. Выберите необходимый тип устройства.
3. Введите допустимый IP-адрес или имя узла и учетные данные для этого устройства.
4. Нажмите **ОК**.  
В систему будет добавлен новое **Unmanaged сетевое устройство**.  
Теперь можно добавить этот объект unmanaged site в логическое дерево. Обратите внимание, что в логическом дереве виден только объект, но не относящиеся к нему сетевые устройства.
5. Введите действующее имя пользователя для этого сетевого устройства при его наличии.
6. Введите действующий пароль, если есть.



### Диалоговое окно Добавить неуправляемое сетевое устройство

главное окно >  **Устройства** > развернуть  > щелкните правой кнопкой мыши  > нажмите **Добавить неуправляемое сетевое устройство**

#### Тип устройства:

Выберите запись, применимую для данного устройства.

Доступные записи:

- **DIVAR AN / DVR**
- **DIVAR IP (AiO), BVMS**
- **IP-камера/кодер Bosch**

#### Сетевой адрес:

Введите IP-адрес или имя узла. При необходимости измените номер порта.

**Примечание:** при использовании подключения SSH введите адрес в следующем формате:  
**ssh://IP или servername:5322**

#### Безопасность

Флажок **Безопасное соединение** установлен по умолчанию.



#### Замечание!

При добавлении цифрового видеорегистратора с установленным флажком **Безопасное соединение**, подключения команд и управления защищены. Поточковая передача видеоданных не защищена.

#### Имя пользователя:

Введите действующее имя пользователя для этого сетевого устройства при его наличии. Подробную информацию см. в разделе *Неуправляемый объект, Страница 23*.

#### Пароль:




Введите действующий пароль при наличии. Сведения об учетных данных пользователя см. в разделе *Неуправляемый объект, Страница 23*.

#### См.

- *Неуправляемый объект, Страница 23*

## 12.32.5

### Настройка часового пояса

Главное окно >  **Устройства** > разверните  > 

Вы можете настроить часовой пояс unmanaged site. Это полезно, когда пользователь Operator Client имеет намерение получить доступ к unmanaged site с помощью компьютера с Operator Client, расположенного в другом часовом поясе, чем этот unmanaged site.

#### Чтобы настроить часовой пояс:

- ▶ в списке **Часовой пояс** выберите нужный элемент.

#### См.

- *Страница Unmanaged Site, Страница 223*





## 13

## Страница «Кодер/декодер/камера Bosch»



В данном разделе содержится информация о настройке кодеров и декодеров в системе. Подробные сведения о параметрах кодера, декодера или камеры (например, Video Content Analysis (VCA)) или о параметрах сети см. в руководстве по соответствующему устройству.

Количество элементов под записью отображается в квадратных скобках.

## Для настройки кодера выполните следующие действия.

Главное окно >  **Устройства** > разверните  > разверните  >  >

или





Главное окно >  **Устройства** > развернуть  > развернуть  > развернуть  > 

или

Главное окно >  **Устройства** >  > 






Главное окно >  **Устройства** >  > 






## Для настройки декодера выполните следующие действия.


Главное окно >  **Устройства** > разверните  > разверните  > 

Дополнительные сведения о страницах  см. в интерактивной справке.

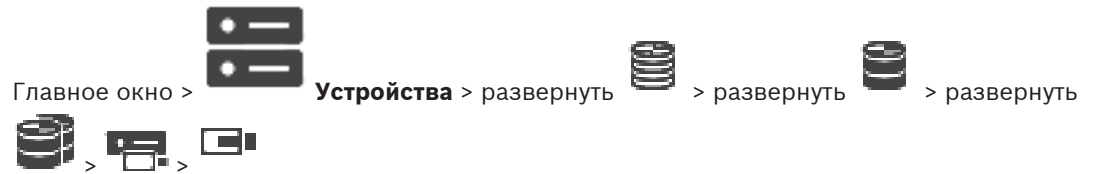
## Для настройки камеры:

Главное окно >  **Устройства** > развернуть  > развернуть  >  > 

Главное окно >  **Устройства** > развернуть  > развернуть  >  > 

> 

или





или




или





– Нажмите  для сохранения настроек.

– Нажмите  для отмены последней настройки.

– Нажмите  для активации конфигурации.

Большинство параметров на страницах кодера / декодера / камеры вступают в силу сразу

же после нажатия . При переходе на другую вкладку без нажатия  после внесения изменений отображаются два окна сообщений. Для сохранения изменений следует подтвердить изменения в обоих окнах.

Чтобы изменить пароли кодера, щелкните правой кнопкой мыши значок устройства и выберите команду **Изменить пароль...**

Чтобы открыть устройство в веб-браузере, щелкните значок устройства правой кнопкой мыши и выберите команду **Показать страницу в браузере**.

### Примечание.


В зависимости от выбранного кодера или камеры не все описанные здесь страницы будут доступны для каждого устройства. Используемые здесь формулировки, описывающие названия полей, зависят от используемого вами программного обеспечения.

- ▶ Щелкните вкладку для перехода к соответствующей странице свойств.

### Добавление кодеров путем поиска:

- Щелкните правой кнопкой мыши  и выберите команду **Поиск кодеров**. Откроется диалоговое окно **BVMS Scan Wizard**.
- Выберите необходимые кодеры, выберите необходимый пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.
- Нажмите **Далее >>**. Откроется диалоговое окно мастера **Проверки подлинности устройств**.
- Введите пароль для каждого устройства, защищенного паролем. Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля. Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**. Затем щелкните это поле правой кнопкой мыши и выберите **Копировать ячейку в**

**столбец.**

В столбце **Состояние** успешные подключения обозначены значком  .

Неудачные подключения обозначены значком  .



, что означает, что для устройства требуется начальный пароль.

Для установки начального пароля введите его в поле **Пароль**.

Статус изменится на  .

Повторите эти действия для всех устройств, которые требуют первоначальный пароль.

**Примечание:** пока вы не установили первоначальный пароль для всех устройств в списке, которые требуют начальный пароль, вы не сможете продолжить работу.

5. Нажмите **Готово**.  
Устройство добавлено в дерево устройств.

**См.**

- Поиск устройств, Страница 73

## 13.1 Добавление кодера в пул VRM

Сведения о добавлении кодеров в пул VRM см. в разделе *Добавление кодеров путем поиска, Страница 187*.

**См.**

- Добавление устройства, Страница 124

## 13.2 Добавление кодера, работающего только в режиме реального времени

Сведения о добавлении кодера, работающего только в режиме реального времени, путем поиска см. в разделе *Добавление устройств, работающих только в режиме реального времени, путем поиска, Страница 219*.

**См.**

- Добавление устройства, Страница 124
- Страница Режим реального времени и локальное хранилище, Страница 219

## 13.3 Добавление кодера локального хранилища






Сведения о добавлении кодеров локального хранилища путем поиска см. в разделе *Страница Локальное хранилище, Страница 222*.




**См.**




- Добавление устройства, Страница 124
- Страница Локальное хранилище, Страница 222

## 13.4 Редактирование кодера

### 13.4.1 Шифрование видео в режиме реального времени («Изменение кодера»)

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > нажмите  > диалоговое окно **Изменить кодер**

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > диалоговое окно **Изменить кодер**

Главное окно >  **Устройства** > разверните  > нажмите  > диалоговое окно **Изменить кодер**

Вы можете активировать защищенное подключенное для видео в реальном времени, передаваемого с кодера следующим устройствам, если на кодере настроен порт HTTPS 443:

- Компьютер с Operator Client
- Компьютер с Management Server
- Компьютер с Configuration Client
- Компьютер с VRM
- Декодер

#### Примечание.

Когда эта функция включена, ANR не работает на данных устройствах.

При активации этой функции воспроизведение с помощью кодера в кодерах с микропрограммой до версии 6.30 не поддерживается.

Защищенный протокол UDP поддерживаются только кодерами с версией микропрограммного обеспечения 7.0 или выше. Если в этом случае включено безопасное соединение, пользователь Operator Client может переключиться поток на UDP и на multicast UDP.




#### Для активации выполните следующие действия:




1. Установите флажок **Безопасное соединение**.
2. Нажмите **ОК**.  
Для этого кодера включено безопасное соединение.




#### См.

- *Настройка многоадресной передачи, Страница 242*
- *Диалоговое окно «Изменить кодер / Изменить декодер», Страница 230*

## 13.4.2 Обновление возможностей устройства («Изменение кодера»)

Главное окно  **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**  
или

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**  
или

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**  
или

Главное окно >  **Устройства** > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить декодер** > диалоговое окно **Изменить декодер**

После замены устройства можно обновить его функциональные возможности. Текст сообщения информирует о том, соответствуют ли полученные возможности устройства возможностям, сохраненным в BVMS.





### Для обновления:

1. Нажмите кнопку **ОК**.  
Отображается окно сообщения со следующим текстом:  
**Если применить данные возможности устройства, могут измениться настройки записи и событий для данного устройства. Проверьте эти настройки.**
2. Нажмите кнопку **ОК**.  
Выполняется обновление возможностей устройства.



### См.

– *Диалоговое окно «Изменить кодер / Изменить декодер», Страница 230*

## 13.4.3 Диалоговое окно «Изменить кодер / Изменить декодер»



Главное окно  **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**

или

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой




мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**

или

Главное окно >  **Устройства** > разверните  > щелкните правой кнопкой

мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**

или

Главное окно >  **Устройства** > разверните  > разверните  > щелкните

правой кнопкой мыши  > нажмите **Изменить декодер** > диалоговое окно **Изменить декодер**

Позволяет проверить и обновить возможности устройства. Устройство подключается при открытии этого диалогового окна. Запрашивается пароль, и возможности устройства сравниваются с возможностями устройства, сохраненными вBVMS.

#### **Имя**

Отображает имя устройства. При добавлении IP-видеоустройства производства Bosch имя устройства генерируется системой. При необходимости измените значение.

#### **Сетевой адрес / порт**

Введите сетевой адрес устройства. При необходимости измените номер порта.

#### **Имя пользователя**

Отображает имя пользователя, используемое для аутентификации на устройстве.

#### **Пароль**

Введите действующий пароль для аутентификации на устройстве.

#### **Отобразить пароль**

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

#### **Проверить подлинность**

Нажмите для аутентификации на устройстве с использованием введенных выше учетных данных.

#### **Безопасность**

Флажок **Безопасное соединение** установлен по умолчанию.

Если безопасное подключение невозможно, отображается соответствующее сообщение. Нажмите, чтобы снять флажок.

#### **Следующие декодеры поддерживают безопасное соединение:**

- VID 7000
- VID 8000
- VIP XD HD

**Замечание!**

Соединение между декодером и кодером безопасно, только если они настроены с использованием безопасного соединения.

**Возможности устройства**

Отображаемые возможности устройства можно упорядочивать по категориям или по алфавиту.

Текст сообщения информирует о том, соответствуют ли автоматически определенные возможности устройства возможностям данного устройства.

Нажмите **ОК** для применения изменений возможностей устройства после обновления устройства.

**См.**

- *Шифрование видео в режиме реального времени («Изменение кодера»)*, Страница 229
- *Обновление возможностей устройства («Изменение кодера»)*, Страница 230

## 13.5

### Управление проверкой подлинности

Для активации проверки подлинности на кодере необходимо выполнить следующие действия:

- настройте проверку подлинности на кодере.
- загрузить сертификат кодера.
- установить этот сертификат кодера на рабочую станцию, используемую для проверки подлинности.

**См.**

- *Проверка подлинности*, Страница 232

### 13.5.1

#### Проверка подлинности

Пользователь клиента Operator Client может проверить подлинность записей.

Подлинность экспортов проверяется автоматически.

Администратору следует выполнить следующие действия для обеспечения непрерывности цепочки сертификатов. Для крупных систем (> 30 камер) рекомендуется выполнить следующие действия:

- Разрешить сертифицирующему органу (CA) создать сертификат для каждого кодера.
- Загрузить созданный сертификат (включая закрытый ключ) надежным способом на каждом кодере.
- Установить сертификат на Operator Client рабочих станций, где требуется выполнить проверку подлинности.

Для небольших систем (< 30 камер) рекомендуется выполнить следующие действия:

- Загрузить сертификат *сервера HTTPS* от каждого кодера.
- Установить эти сертификаты на Operator Client рабочих станций, где требуется выполнить проверку подлинности.

За подробной информацией обратитесь в службу IT-поддержки вашей компании.

Для активации надежной проверки подлинности администратор должен выполнить следующие действия:

- Активировать проверку подлинности на каждой выбранной камере.
- Для крупных систем: загрузить и назначить соответствующий сертификат для каждой выбранной камеры.



- Для небольших систем: загрузить сертификат от каждого кодера. Установить сертификаты, позволяющие выполнять проверку на рабочей станции.

#### Ограничения

Требуется версия микропрограммного обеспечения 6.30 или более поздней версии. Не рекомендуется выполнять проверку подлинности более 4 камер одновременно. Пользователь Operator Client не может проверить подлинность видеоизображения в реальном времени.

**Примечание:** не следует осуществлять замену сертификата, когда выполняется запись. Если необходимо изменить сертификат, сначала остановите запись, затем измените сертификат и запустите запись еще раз.

Для проверки подлинности записи эта запись будет воспроизводиться в фоновом режиме с максимальной скоростью. В сетях с низкой пропускной способностью воспроизведение может быть замедленным. В этом случае продолжительность проверки может быть равна продолжительности выбранного отрезка записи. Пример: выбран период времени, равный 1 часу. Процесс проверки может длиться до 1 часа.

Пользователь может проверить лишь факт подлинности записи. Если процесс проверки подлинности завершился неудачей, это не всегда означает, что видео было изменено. Неудача может быть вызвана множеством причин, например, удалением вручную. Пользователь Operator Client не может отличить намеренное изменение видео от мошеннического изменения.

Проверка подлинности связана только с методами проверки подлинности видео.

Проверка подлинности видео никаким образом не связана с передачей видео или данных.

Функция водяного знака для проверки подлинности в более ранних версиях BVMS заменена. Новая проверка подлинности автоматически становится доступной после обновления до самой последней версии BVMS. Проверки подлинности, успешно проведенные в прошлом, теперь не могут быть подтверждены, так как эти записи не содержат необходимой расширенной информации.

Проверка подлинности не поддерживается в следующих случаях:

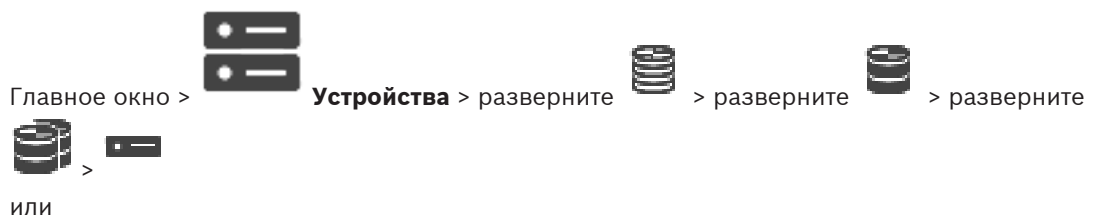
- Транскодирование
- Локальная запись
- VSG
- Цифровой видеорегистратор
- Bosch Recording Station
- ANR


#### См.

- *Настройка проверки подлинности, Страница 233*
- *Отправка сертификата, Страница 234*
- *Загрузка сертификата, Страница 234*
- *Установка сертификатов на рабочей станции, Страница 235*

## 13.5.2


### Настройка проверки подлинности



Главное окно >  **Устройства** > разверните  >  >

Вы можете активировать проверку подлинности для кодера.

#### Настройка

1. Нажмите **Камера**, затем нажмите **Видеовход**.
2. В списке **Проверка подлинности видео** выберите пункт **SHA-256**.
3. В списке **интервалы подписи** выберите необходимое значение.  
Небольшое значение повышает степень защиты, большое значение снижает нагрузку кодера.
4. Нажмите  .

### 13.5.3

#### Отправка сертификата


Главное окно >  **Устройства** > разверните  > разверните  > разверните  >  >

или

Главное окно >  **Устройства** > разверните  >  >

Вы можете отправить производный сертификат на кодер.

#### Для отправки:



1. нажмите **Обслуживание**, затем **Сертификаты**.
2. Нажмите **Отправка сертификата**.
3. Выберите соответствующий файл с сертификатом для данного кодера. Этот файл должен содержать закрытый ключ, например, \*.pem.  
Убедитесь, что передача данных защищена.
4. Нажмите **Открыть**.
5. В списке **Использование** выберите **HTTPS-сервер**, чтобы назначить отправленный сертификат элементу **HTTPS-сервера**.
6. Нажмите  .

### 13.5.4

#### Загрузка сертификата

Главное окно >  **Устройства** > разверните  > разверните  > разверните  >  >

или

Главное окно >  **Устройства** > разверните  >  >

Вы можете загрузить сертификат с кодера.

**Для загрузки:**

1. нажмите **Обслуживание**, затем **Сертификаты**.
2. Выберите требуемый сертификат и нажмите значок *Save*.
3. Выберите соответствующий каталог для сохранения файла сертификата.
4. Переименуйте расширение файла сертификата на \*.cer.





Теперь можно установить этот сертификат на рабочей станции, на которой необходимо проверить подлинность.

**13.5.5****Установка сертификатов на рабочей станции**

Можно установить сертификат, загруженный с кодера, на рабочую станцию, на которой требуется выполнить проверку подлинности.

1. Запустите *Microsoft Management Console* на рабочей станции.
2. Добавьте *Сертификаты* в отправку на данном компьютере с выбранным параметром *Учетная запись компьютера*.
3. Разверните *Сертификаты (локальный компьютер)*, разверните *Доверенный корневой орган сертификации*.
4. Щелкните правой кнопкой мыши *Сертификаты*, поместите указатель мыши на *Все задачи* и нажмите *Импорт...*  
Отобразится *Мастер импорта сертификатов*.  
Параметр *локального компьютера* является выбранным заранее, и его нельзя изменить.
5. Нажмите *Далее*.
6. Выберите файл сертификата, который вы загрузили с кодера.
7. Нажмите *Далее*.
8. Оставьте параметры без изменений и нажмите кнопку *Далее*.
9. Оставьте параметры без изменений и нажмите кнопку *Завершить*.

**13.6****Предоставление пароля пункта назначения декодеру («Проверка подлинности...»)**

Главное окно >  **Устройства** > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Аутентификация...** > диалоговое окно **Введите пароль**

Для предоставления доступа к защищенному паролем кодеру для декодера необходимо ввести пароль уровня авторизации пользователя кодера в качестве пароля пункта назначения в декодере.

**Предоставление.**





1. В списке **Введите имя пользователя** выберите *destination password*.
  2. В поле **Введите пароль для пользователя** введите новый пароль.
  3. Нажмите **ОК**.
- ✓ Пароль на устройстве изменяется незамедлительно.

**См.**

- *Изменение пароля кодера и декодера («Изменить пароль»/«Введите пароль»»), Страница 236*

## 13.7

**Изменение пароля кодера и декодера («Изменить пароль»)/«Введите пароль»)**

Главное окно >  **Устройства** > разверните  > разверните  >  >







или

Главное окно >  **Устройства** >  > 

или


Главное окно >  **Устройства** >  > 

или

Главное окно >  **Устройства** > разверните  > разверните  > 

Определите или измените отдельный пароль для каждого уровня. Введите пароль (не более 19 символов; без специальных символов) для выбранного уровня.

**Для изменения пароля выполните следующие действия.**

1. щелкните правой кнопкой мыши  и нажмите **Изменить пароль...**  
Откроется диалоговое окно **Введите пароль**.
  2. Из списка **Введите имя пользователя** выберите пользователя, для которого необходимо изменить пароль.
  3. В поле **Введите пароль для пользователя** введите новый пароль.
  4. Нажмите **ОК**.
- ✓ Пароль на устройстве изменится незамедлительно.

Пароль препятствует несанкционированному доступу к устройству. Для ограничения доступа могут быть использованы различные уровни авторизации.

Надлежащая защита паролем обеспечивается только в тех случаях, когда все более высокие уровни авторизации также защищены паролем. Таким образом, всегда следует начинать с самого высокого уровня авторизации при назначении паролей.

Можно задать и изменить пароль для каждого уровня авторизации, если вы вошли в учетную запись пользователя «service».

Устройство имеет три уровня авторизации: service, user и live.

- service представляет собой высший уровень авторизации. Ввод правильного пароля дает доступ ко всем функциям и позволяет изменять все параметры конфигурации.
- user представляет собой средний уровень авторизации. На этом уровне можно эксплуатировать устройство, воспроизводить записи и управлять камерой, однако невозможно изменять конфигурацию.
- live представляет собой низший уровень авторизации. На этом уровне можно только просматривать видеоизображения в реальном времени и переключаться между различными экранами изображений в реальном времени.

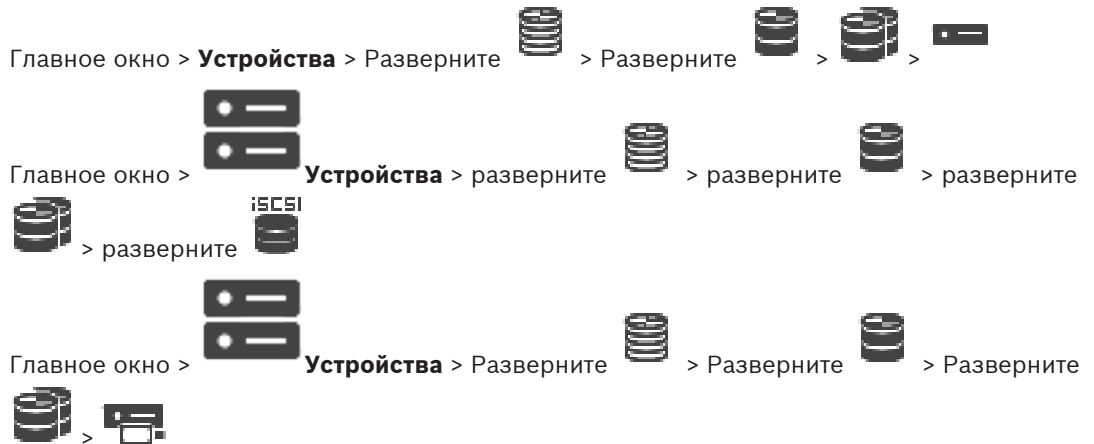
Для декодера уровень авторизации live заменяется следующим уровнем авторизации:

- destination password (доступно только для декодеров)  
Используется для доступа к кодеру.

**См.**




- *Предоставление пароля пункта назначения декодеру («Проверка подлинности...»),  
Страница 235*

## 13.8 Перемещение кодера в другой пул («Изменение пула»)



Устройство можно переместить из одного пула в другой в пределах одного устройства VRM без потерь записи.

**Для перемещения:**

1. Щелкните правой кнопкой мыши  /  /  iSCSI и выберите команду **Изменить пул...**  
Откроется диалоговое окно **Изменить пул**.
2. В списке **Новый пул:** выберите необходимый пул.
3. Нажмите **ОК**.  
Устройство перейдет к выбранному пулу.

**Диалоговое окно Изменить пул**

Позволяет изменить назначенный устройству пул.

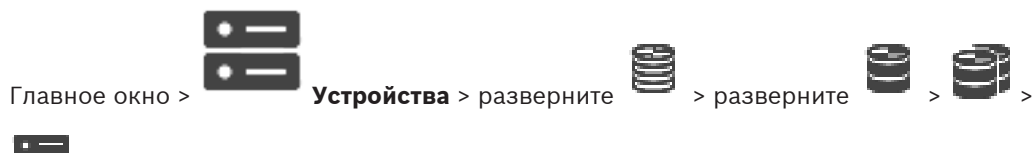
**Текущий пул:**

Отображает номер пула, к которому в данный момент соотносится выбранное устройство.

**Новый пул:**

Выберите требуемый номер пула.

## 13.9 Восстановление записей с замененного кодера (диалоговое окно «Связать с записями предшествующего устройства»)






В случае замены неисправного кодера записи замененного кодера будут доступны на новом кодере при выборе нового кодера в Operator Client.

**Замечание!**

Кодер может быть заменен только на кодер с тем же количеством каналов.

**Для восстановления записей с замененного кодера****Замечание!**

Не используйте команду **Изменить кодер**.

1. Щелкните правой кнопкой мыши по  > команде **Связать с записями предшественника...**
2. Отображается диалоговое окно **Связать с записями предшественника...**
3. Введите сетевой адрес и действительный пароль для нового устройства.
4. Нажмите **ОК**.
5. Нажмите , чтобы сохранить настройки.
6. Нажмите  для активации конфигурации.

**Диалоговое окно Связать с записями предшественника...**

Позволяет восстановить записи с замененного кодера. После настройки параметров в диалоговом окне записи замененного кодера доступны для нового кодера при выборе нового кодера в Operator Client.

**Сетевой адрес / порт**

Введите сетевой адрес устройства.

**Имя пользователя**

Отображает имя пользователя, используемое для аутентификации на устройстве.

**Пароль**

Введите действующий пароль для аутентификации на устройстве.

**Проверить подлинность**





Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

## 13.10

## Настройка кодеров/декодеров

### 13.10.1

### Настройка носителей данных кодера

Главное окно >  **Устройства** > разверните  > разверните  >  >



> **Дополнительные параметры** > **Управление записями**

**Примечание.** Убедитесь, что требуемые камеры этого кодера добавлены в Логическое дерево.

Для использования функции ANR необходимо настроить носитель данных кодера.

**Примечание.** Если необходимо настроить носитель данных кодера, который уже добавлен в систему и записан с помощью VRM, убедитесь, что остановлена вторичная запись:

Функция ANR работает только на кодерах с версией микропрограммного обеспечения 5.90 и выше. Не все типы кодеров поддерживают ANR, даже если установлена верная версия микропрограммного обеспечения.

#### Настройка носителя данных кодера

1. В разделе **Вторичная запись** в списке **Предпочитаемый тип целевого хранилища** выберите носитель данных. В зависимости от типа устройства будут доступны разные носители.
2. При необходимости нажмите кнопку ..., чтобы отформатировать носитель данных. После успешного форматирования носитель данных будет готов к использованию с функцией ANR.
3. Настройте функцию ANR для этого кодера на странице **Камеры и запись**.

#### См.

- Страница "Управление записью", Страница 242
- Настройка функции ANR, Страница 311

## 13.10.2

### Настройка нескольких кодеров / декодеров

Главное окно

Вы можете одновременно изменить следующие свойства нескольких кодеров и декодеров:

- Пароли устройств
- IP-адреса
- Краткие имена
- Маска подсети
- Идентификатор шлюза
- Версии микропрограмм

#### Чтобы выбрать несколько устройств:

- ▶ Выберите нужные устройства, нажав клавишу CTRL или SHIFT.

#### Чтобы выбрать все доступные устройства:

- ▶ Нажмите команду  **Выделить все.**

**Чтобы изменить пароль для нескольких устройств:**

1. В главном окне **Устройства** выберите команду  **Изменить пароли устройств**.  
Или  
в меню **Аппаратное обеспечение** нажмите **Изменить пароли устройств...**  
Откроется диалоговое окно **Изменить пароли устройств**.
2. Выберите требуемые устройства.
3. Щелкните правой кнопкой мыши выбранные устройства.
4. Нажмите **Изменить пароль...** Откроется диалоговое окно **Изменение паролей**.
5. Установите необходимые параметры.

**Замечание!**

Вы можете выбрать только те типы паролей, которые доступны для всех выбранных устройств.

**Чтобы настроить несколько кратких имен:**

1. В меню **Аппаратное обеспечение** выберите пункт **Изменить IP-адрес устройства и сетевые параметры...**  
Отображается диалоговое окно **Изменить IP-адрес и сетевые параметры устройства**.
2. Выберите требуемые устройства.
3. Щелкните правой кнопкой мыши выбранные устройства.
4. Нажмите **Задать краткие имена...**  
Отображается диалоговое окно **Задать краткие имена**.
5. Установите необходимые параметры.

**Чтобы настроить несколько IP-адресов:****Замечание!**

Изменение IP-адреса может сделать IP-устройство недоступным.

1. В меню **Аппаратное обеспечение** выберите пункт **Изменить IP-адрес устройства и сетевые параметры...**  
Отображается диалоговое окно **Изменить IP-адрес и сетевые параметры устройства**.
2. Выберите требуемые устройства.
3. Щелкните правой кнопкой мыши выбранные устройства.
4. Нажмите **Задать IP-адреса...**  
Откроется диалоговое окно **Установить IP-адреса**.
5. Установите необходимые параметры.

**Чтобы изменить маску подсети/идентификатор шлюза для нескольких устройств:**

1. Нажмите нужную поле одного из устройств, значение которого требуется изменить.
2. Введите соответствующее значение.



3. Выберите все требуемые устройства.
4. Щелкните правой кнопкой мыши нужное поле устройства, значение которого вы уже изменили.
5. Выберите команду и команду **Копировать ячейку в** и команду **Выделение в столбце** . Или нажмите команду **Заполнить столбец**, если это необходимо.



#### Замечание!

Вы можете также скопировать полные строки для изменения IP-адресов, кратких имен, масок подсети и идентификаторов шлюза для нескольких устройств.

#### Чтобы обновить микропрограммы для нескольких устройств:

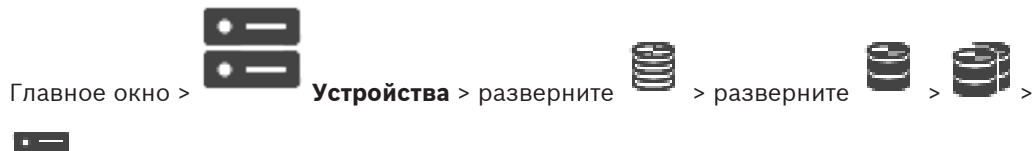
1. В меню **Аппаратное обеспечение** выберите пункт **Обновить микропрограмму устройства...**  
Отображается диалоговое окно **Обновить микропрограмму устройства**.
2. Выберите требуемые устройства.
3. Нажмите команду **Обновить микропрограмму**.
4. Выберите файл с обновлением.
5. Нажмите **ОК**.

#### Результат операции

Отображает соответствующее состояние затрагиваемых устройств.

### 13.10.3

#### Настройка резервного режима записи на кодере



**требования:** на странице **Пул** в списке **Режим настроек записи** выберите **При отказе**. Если выбран **Автоматически** режим, параметры настраиваются автоматически, и изменить их нельзя.

Если вы хотите использовать вторичный целевой объект как для автоматического, так и для резервного режима: на странице **Пул** в списке **Использование вторичной цели** выберите **Вкл.**

Рекомендуется настроить хотя бы два устройства iSCSI для резервного режима.

#### Для настройки:

1. Нажмите **Дополнительные параметры**.
2. Нажмите **Очередность записи**.
3. В разделе **Главная цель** выберите запись для нужного объекта. Все системы хранения, введенные на вкладке **Хранение**, будут перечислены в списке.
4. В разделе **Второстепенная цель** выберите запись для нужного объекта. Все системы хранения, указанные в разделе **Хранение**, отображаются в списке.  
Изменения вступают в силу немедленно. Активация не требуется.

#### Дополнительная информация

- *Настройка автоматического режима записи в пуле, Страница 190*

## 13.10.4 Страница "Управление записью"



Активные записи обозначаются значком .

Наведите курсор на значок. Откроется окно с подробной информацией об активных записях.

### Записи, управляемые вручную

Управление записями на данном кодере осуществляется локально. Все необходимые параметры настраиваются вручную. Кодер или IP-камера действует как устройство только в режиме реального времени. Его нельзя удалять из VRM автоматически.

### Запись 1 управляется диспетчером VRM

Управление записями кодера осуществляется системой VRM.

### Двойной VRM

Запись 2 данного кодера управляется вторичным VRM.

### Вкладка Носитель iSCSI

Нажмите, чтобы отобразить доступные хранилища iSCSI, подключенные к данному кодере.

### Вкладка Локальный носитель

Нажмите, чтобы отобразить доступное локальное хранилище на данном кодере.

### Добавить

Нажмите, чтобы добавить устройство хранения в список управляемых носителей данных.

### Удалить

Нажмите, чтобы удалить устройство хранения из данного списка управляемых носителей данных.

### См.

– *Настройка носителей данных кодера, Страница 238*

## 13.10.5 Страница "Параметры записи"

Страница **Параметры записи** отображается для каждого кодера. Эта страница появляется только в том случае, если устройство добавлено в систему VRM.

### Главная цель

Отображается, только если список **Режим настроек записи** на странице **Пул** настроен как

### При отказе.

Выберите запись для необходимого целевого объекта.

### Второстепенная цель

Отображается, только если список **Режим настроек записи** на странице **Пул** настроен как

**При отказе** и если список **Использование второстепенной цели** настроен как **Вкл.**

Выберите запись для необходимого целевого объекта для настройки резервного режима.

### См.

– *Страница "Пул", Страница 188*

## 13.11 Настройка многоадресной передачи

Для каждой назначенной камеры можно настроить адрес многоадресной передачи и порт.

### Порядок настройки многоадресной передачи:

1. Установите требуемый флажок для включения многоадресной передачи.
2. Введите правильный адрес многоадресной передачи и номер порта.
3. При необходимости настройте непрерывный поток многоадресной передачи.






### Вкладка Многоадресная передача

Главное окно >  **Устройства** >  > 

или

Главное окно >  **Устройства** >  > 

или

Главное окно >  **Устройства** > разверните  > разверните  >  > 

> вкладка **Сеть** > вкладка **Многоадресная передача**

Позволяет настроить многоадресную передачу для назначенных камер.

#### Включить

Нажмите, чтобы активировать многоадресную передачу для данной камеры.

#### Адрес многопоточковой передачи

Вставьте допустимый адрес многоадресной передачи (в диапазоне от 224.0.0.0 до 239.255.255.255).

Введите *1.0.0.0*. Уникальный адрес многоадресной передачи вставляется автоматически в зависимости от MAC-адреса устройства.

#### Порт

Если используется брандмауэр, введите номер порта, который не блокируется в брандмауэре.

#### Поток

Нажмите, чтобы активировать непрерывную многоадресную потоковую передачу на коммутатор. Это означает, что многоадресному соединению не будет предшествовать регистрация RCP+. Кодер всегда будет передавать на коммутатор все данные. Коммутатор, в свою очередь (если не поддерживается или не настроена многоадресная фильтрация IGMP), будет передавать эти данные на все порты, то есть через коммутатор будет непрерывно проходить полный поток.

Потоковая передача необходима для получения многоадресного потока при использовании устройства другой компании (не Bosch).



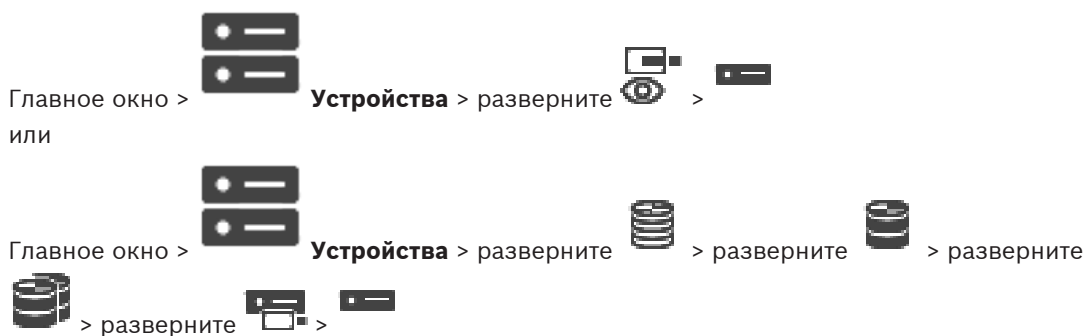
#### Замечание!

Многоадресные потоки могут быть защищены, только если в кодере установлена микропрограмма версии 7.0 или более поздней и установлен флажок **Безопасное соединение**.

#### См.

– *Шифрование видео в режиме реального времени («Изменение кодера»), Страница 229*

## 14 Страница "ONVIF"



См.

- Страница устройства Video Streaming Gateway, Страница 208
- Страница Режим реального времени и локальное хранилище, Страница 219

### 14.1 Добавление устройства ONVIF, работающего только в режиме реального времени, путем сканирования

Для добавления устройств ONVIF, работающих только в реальном времени:

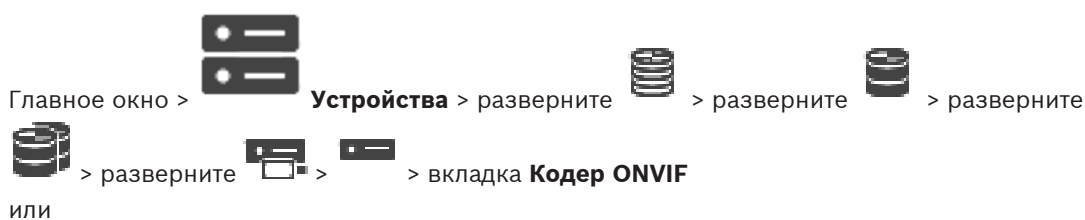
- Щелкните  правой кнопкой мыши, затем щелкните **Поиск кодеров ONVIF, работающих только в реальном времени.**  
Отображается диалоговое окно **BVMS Scan Wizard**.
- Установите флажки для устройств, которые необходимо добавить.
- Нажмите **Далее >>**.  
Откроется диалоговое окно мастера **Проверки подлинности устройств.**
- Введите пароль для каждого устройства, защищенного паролем.  
Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.  
Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.  
Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.




В столбце **Состояние** успешные входы в систему обозначены значком .

Неудачные попытки входа обозначены значком .

- Нажмите **Готово**.  
Устройство добавлено в дерево устройств.

### 14.2 Страница "Кодер ONVIF"



Главное окно >  **Устройства** > разверните  >  > вкладка **Кодер ONVIF**  
 Отображает сведения о кодере ONVIF, работающем только в режиме реального времени, добавленном к BVMS.

**Имя**

Отображает имя устройства ONVIF. Его можно переименовать непосредственно в дереве устройств.

**Сетевой адрес**

Отображает IP-адрес устройства.

**Производитель**

Отображает название производителя.

**Модель**

Отображает название модели.

**Видеовходы**

Введите количество камер, подключенных к этому кодери.

**Аудиовходы**

Введите количество аудиовходов, подключенных к этому кодери.

**Тревожные входы**

Введите количество тревожных входов, подключенных к этому кодери.

**Реле**

Введите количество реле, подключенных к этому кодери.

**См.**

- *Страница "События кодери ONVIF", Страница 245*
- *Добавление кодери, работающего только в режиме реального времени, Страница 228*
- *Настройка таблицы сопоставления ONVIF, Страница 249*

**14.3****Страница "События кодери ONVIF"**







Начиная с версии BVMS 10.0 события кодери ONVIF можно получить непосредственно от VSG или кодери ONVIF. При добавлении нового кодери ONVIF флажок **Извлекать события ONVIF из VSG (Profile S, T)** устанавливается по умолчанию, а Profile T поддерживается.

Следующие возможности поддерживаются, только если кодери ONVIF добавлен в систему через устройство VSG:

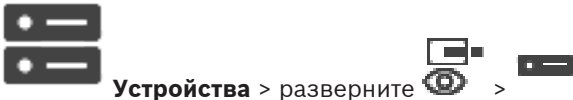


- Если события кодери ONVIF извлекаются из VSG, настроенные по умолчанию события ONVIF уже сопоставлены.
- Оператор может включать и выключать реле в Operator Client.

**Замечание!**

Получение событий ONVIF из VSG доступно только начиная с VSG версии 7.0. При переходе на BVMS версии 10.0 существующие события кодери ONVIF извлекаются непосредственно из кодери ONVIF. Необходимо обновить VSG до версии 7.0.

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **События кодери ONVIF**

или


 Главное окно > **Устройства** > разверните  >  > вкладка **События кодера ONVIF**

Если события кодера ONVIF извлекаются непосредственно из кодера ONVIF, вам необходимо сопоставить события ONVIF с событиями BVMS. За счет этого в дальнейшем можно настраивать события ONVIF как тревоги BVMS.




#### Замечание!


Если события кодера ONVIF извлекаются из VSG, события ONVIF по умолчанию уже сопоставлены.

#### Таблица сопоставлений

Можно создать или изменить таблицу сопоставления.



Нажмите , чтобы открыть диалоговое окно **Добавление таблицы сопоставлений**.

Нажмите , для отображения диалогового окна **Изменение имени таблицы сопоставлений**.

Нажмите , чтобы удалить таблицу сопоставления и все входящие в нее строки.

Нажмите  или , чтобы импортировать или экспортировать таблицу сопоставления ONVIF.

#### События и тревоги

Выберите событие BVMS для сопоставления с событием ONVIF.

#### Добавить строку

Нажмите , чтобы добавить строку в таблицу сопоставления.

Если доступно несколько строк, событие происходит, когда верно условие в одной строке.

#### Удалить строку

Нажмите , чтобы удалить выбранную строку из таблицы сопоставления.

#### Тема ONVIF

Введите или выберите текстовую строку, например:

*tns1:VideoAnalytics/tnsaxis:MotionDetection*

#### Имя данных ONVIF

Введите или выберите текстовую строку.

#### Тип данных ONVIF

Введите или выберите текстовую строку.

#### Значение данных ONVIF

Введите или выберите текстовую строку или число.

Если события ONVIF извлекаются из VSG, по умолчанию сопоставлены следующие события с VSG:

– **Глобальное изменение — обнаружено**







- **Глобальное изменение** — не обнаружено
- **Обнаружение движения** - Обнаружено движение
- **Обнаружение движения** - Движение остановлено
- **Проверка контрольного изображения** - Настройки отменены
- **Проверка контрольного изображения** - Настроено
- **Потеря видеоизображения** - Видеосигнал утерян
- **Потеря видеоизображения** - Видеосигнал в порядке
- **Потеря видеоизображения** - Состояние видеосигнала неизвестно
- **Видеосигнал слишком размытый** — Видеосигнал в порядке
- **Видеосигнал слишком размытый** — Видеосигнал не в порядке
- **Видеосигнал слишком яркий** - Видеосигнал в порядке
- **Видеосигнал слишком яркий** - Видеосигнал не в порядке
- **Видеосигнал слишком темный** - Видеосигнал в порядке
- **Видеосигнал слишком темный** - Видеосигнал не в порядке
- **Видеосигнал с большими помехами** - Видеосигнал в порядке Видеосигнал не в порядке
- **Состояние реле** - Реле открыто
- **Состояние реле** - Реле закрыто
- **Состояние реле** - Ошибка реле
- **Состояние входа** - Вход открыт
- **Состояние входа** - Вход закрыт
- **Состояние входа** - Ошибка ввода

См.




- *Сопоставление событий ONVIF, Страница 37*
- *Настройка таблицы сопоставления ONVIF, Страница 249*

### 14.3.1

#### Добавление и удаление профиля ONVIF

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **События кодера ONVIF**

или

Главное окно >  **Устройства** > разверните  >  > вкладка **События кодера ONVIF**

Можно добавить, удалить или изменить профили ONVIF для выбранного кодера.

##### Добавление:

1. Нажмите кнопку **Добавить...**
  2. В диалоговом окне **Добавить профиль** введите название нового профиля.
  3. Нажмите кнопку **Далее >**.
  4. В следующем диалоговом окне выберите нужную камеру.
  5. Нажмите кнопку **Далее >**.
  6. В следующем диалоговом окне выберите нужный профиль кодера не для записи.
  7. Нажмите кнопку **Сохранить**.
- Новый профиль будет сохранен.

Параметры этого профиля заполняются значениями из выбранного профиля кодера. При необходимости можно изменить эти значения.

#### Удаление:






- ▶ Выберите профиль в списке и нажмите кнопку **Удалить**.




#### Изменение:

1. Выберите профиль в списке.
2. Измените необходимые параметры.

### 14.3.2


#### Экспорт файла таблицы сопоставления ONVIF

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  > вкладка **События кодера ONVIF**  
или

Главное окно >  **Устройства** > разверните  >  > вкладка **События кодера ONVIF**

Можно экспортировать таблицу сопоставления ONVIF в виде файла (файл-OMF). Таблица сопоставления сохраняется для выбранной модели кодера.

#### Экспорт:






1. Нажмите  .
2. Введите имя файла и нажмите кнопку **Сохранить**.  
Таблица сопоставления ONVIF экспортируется как OMF-файл для выбранной модели кодера.




#### См.

– Страница "События кодера ONVIF", Страница 245

### 14.3.3

#### Импорт файла таблицы сопоставления ONVIF

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  > вкладка **События кодера ONVIF**  
или

Главное окно >  **Устройства** > разверните  >  > вкладка **События кодера ONVIF**

Можно импортировать таблицу сопоставления ONVIF в виде файла (OMF-файл). Выпущенные файлы сопоставления ONVIF хранятся в следующем каталоге Configuration Client:


– `%programdata%\Bosch\VMS\ONVIF`

Если уже импортирована таблица сопоставления с таким же именем, выводится сообщение об ошибке.










Если импортирована более новая версия этого файла, выводится предупреждение. Нажмите кнопку **ОК**, если нужно импортировать этот файл. В противном случае нажмите кнопку **Отмена**.





#### Импорт:

1. Нажмите .
2. Выберите нужный файл и нажмите кнопку **Открыть**.  
Откроется диалоговое окно **Импорт таблицы сопоставлений**.
3. Настройте необходимые параметры.
4. Нажмите **ОК**.

#### Диалоговое окно Импорт таблицы сопоставлений

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **События кодера ONVIF** > 

или

Главное окно >  **Устройства** > разверните  >  > вкладка **События кодера ONVIF** > 

#### Производитель

Отображает имя производителя, для которого действует эта таблица сопоставления.

#### Модель

Отображает имя модели, для которой действует эта таблица сопоставления.

#### Описание

Отображает дополнительные сведения: например, протестированные модели камер.

#### Имя таблицы сопоставления

Отображает имя таблицы сопоставления. Измените это имя, если оно уже используется в BVMS.

Можно выбрать один из следующих параметров, чтобы указать, к каким кодерам ONVIF следует применить таблицу сопоставления.

#### Применить только к выбранному кодеру ONVIF







#### Применить ко всем кодерам ONVIF перечисленных моделей

#### Применить ко всем кодерам ONVIF данного производителя

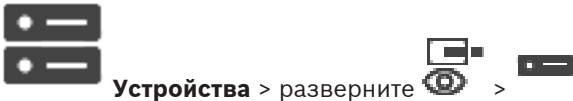

Существующее сопоставление событий ONVIF продолжает действовать. Нельзя импортировать OMT-файлы из более ранних версий BVMS.

### 14.3.4

#### Настройка таблицы сопоставления ONVIF


Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **События кодера ONVIF**

или


 Главное окно > **Устройства** > разверните  > > вкладка **События кодера ONVIF**


Таблицы сопоставления настраиваются для сопоставления событий ONVIF с событиями BVMS.

Таблица сопоставления настраивается для всех кодеров ONVIF одной модели или всех кодеров ONVIF одного производителя.


Нажмите , чтобы обновить кодеры ONVIF, добавленные в автономном режиме, и настроить для них сопоставление событий уже добавленного кодера ONVIF того же производителя или с тем же названием модели.

Для многоканальных кодеров можно настроить источники событий, например определенную камеру или реле.

#### Создание таблицы сопоставления:

1. Нажмите  .  
Отображается диалоговое окно **Добавление таблицы сопоставлений**.
2. Введите имя для таблицы сопоставления.
3. При необходимости в списках **Производитель** и **Модель** выберите записи.  
Если вы выбрали **<нет>** в обоих списках, сопоставление событий действительно только для данного устройства.  
Если вы выбрали **<нет>** в списке **Модель** и название производителя в списке **Производитель**, сопоставление событий действительно для всех устройств одного и того же производителя.  
Если вы выбрали доступные записи в обоих списках, сопоставление событий действительно для всех устройств одного и того же производителя и одной и той же модели.
4. Нажмите кнопку **ОК**.  
Теперь можно отредактировать таблицу сопоставления, например добавить строку к событию **Обнаружено движение**.

#### Изменение таблицы сопоставления:

1. Нажмите  .  
Отображается диалоговое окно **Изменение имени таблицы сопоставлений**.
2. Измените необходимые записи.

#### Добавление и удаление сопоставлений событий:





1. В списке **Таблица сопоставлений** выберите необходимое имя.
2. Добавление строки: нажмите **Добавить строку**.
3. В строке выберите необходимые записи.  
Если доступно несколько строк, событие создается, когда верно условие только в одной строке.
4. Удаление строки: нажмите **Удалить строку**.

#### Удаление таблицы сопоставления:








1. В списке **Таблица сопоставлений** нажмите имя сопоставлений событий, которые необходимо удалить.

2. Нажмите .






#### Настройка источника событий:

1. Разверните  и нажмите ,  или .
2. Перейдите на вкладку **Источник событий ONVIF**.
3. В столбце **Активирующее событие** включите событие, настроенное в данной строке.
4. Выберите необходимые определения события.

#### Диалоговое окно «Добавить/переименовать таблицу сопоставления ONVIF»

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  > вкладка **События кодера ONVIF** >  или 

или

Главное окно >  **Устройства** > разверните  >  > вкладка **События кодера ONVIF** >  или 

Позволяет добавить таблицу сопоставления. Если эта таблица сопоставления будет использоваться как шаблон для следующих кодеров ONVIF того же производителя и такой же модели, выберите соответствующие записи.

#### Имя таблицы сопоставления

Введите удобное имя.

#### Производитель

При необходимости выберите запись.

#### Модель




При необходимости выберите запись.

#### См.




- Включение журнала для событий ONVIF, Страница 391
- Сопоставление событий ONVIF, Страница 37
- Страница "События кодера ONVIF", Страница 245
- Страница "Источник событий ONVIF", Страница 266

## 14.4

### Страница конфигурации ONVIF

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  > вкладка **Конфигурация ONVIF**

или

Главное окно >  **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF**

Можно выбрать несколько кодеров ONVIF и изменить настройки на странице **Профиль видеокодера**. Измененные настройки действуют для всех выбранных устройств. Эта страница доступна только для кодеров ONVIF.









#### Замечание!




Ограничения для конфигурации ONVIF

Параметры, настраиваемые на этих страницах, могут не реализовываться правильно, так как они не поддерживаются вашей камерой. Поддерживаемые камеры ONVIF были протестированы только с параметрами по умолчанию.

### 14.4.1

#### Доступ к устройству

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Доступ к устройству**  
или

Главное окно >  **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Доступ к устройству**

#### Производитель

Отображает название производителя выбранного кодера.

#### Модель

Отображает название модели выбранного кодера.

**Примечание.** Если вы хотите экспортировать какие-либо сопоставления событий в файл сопоставления ONVIF, выберите имя этой модели как имя файла.

#### ID аппаратного обеспечения

Отображает идентификатор оборудования выбранного кодера.

#### Версия ПО

Отображает версию микропрограммного обеспечения выбранного кодера.

**Примечание.** По списку совместимости с BVMS убедитесь, что используется правильная версия микропрограммы.

#### Серийный номер

Отображает серийный номер выбранного кодера.

#### MAC-адрес

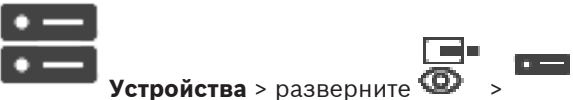


Отображает MAC-адрес выбранного кодера.

#### Версия ONVIF

Отображает версию ONVIF выбранного кодера.  
Для BVMS требуется версия ONVIF 2.0.

## 14.4.2 Дата / время


 Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Дата/Время**  
или


 Главное окно > **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Дата/Время**

### Часовой пояс

Выберите часовой пояс, в котором находится система.


Если в вашей системе или сети функционируют несколько устройств, необходимо осуществить их внутреннюю синхронизацию. Например, идентификация и правильная оценка одновременных записей возможна только в том случае, если часы всех устройств синхронизированы.

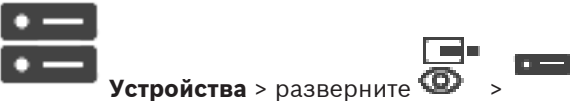


1. Введите текущую дату. Поскольку время устройства управляется внутренними часами, нет необходимости вводить день недели — он будет добавлен автоматически.
2. Введите текущее время или нажмите **Синхр. ПК**, чтобы применить системное время вашего компьютера к устройству.

### Примечание

Важно, чтобы дата и время при записи были выставлены правильно. Неверная установка параметров даты и времени может привести к неправильному функционированию записи.

## 14.4.3 Управление пользователями


 Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Управление пользователями**  
или


 Главное окно > **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Управление пользователями**

Эти пользовательские параметры используются для сторонних приложений, таких как прямой доступ к кодерам через веб-клиент.

Для доступа через сторонние приложения поддерживаются следующие роли пользователей:

- **Анонимный:** у этой роли есть неограниченный доступ только к устройствам, на которых не зарегистрированы пользователи с другими ролями (**Пользователь, Оператор, Администратор**). Если на устройстве есть хотя бы один из указанных выше пользователей, анонимный пользователь имеет право только смотреть параметры времени.
- **Администратор** (не поддерживается клиентом Configuration Client): у этой роли есть доступ ко всем разделам и функциям приложения, права для перезагрузки устройства, сброса настроек и обновления микропрограммы, а также полномочия создавать других пользователей с различными правами доступа.

Первый созданный на устройстве пользователь должен быть **Администратор**.

Различия в правах доступа оператора и пользователя по умолчанию (роли **Оператор** и **Пользователь**) см. в следующей таблице.

Раздел конфигурации или функция ONVIF	Оператор	Пользователь
Идентификация	ПРОСМОТР	СКРЫТО
Параметры времени	ПРОСМОТР	ПРОСМОТР
Параметры сети	ПРОСМОТР	ПРОСМОТР
Пользователи	СКРЫТО	СКРЫТО
Параметры реле	ИЗМЕНЕНИЕ	ПРОСМОТР
Видеоизображение в реальном времени (включая связь RTSP)	ИЗМЕНЕНИЕ	ИЗМЕНЕНИЕ
Потоковая передача видео	ИЗМЕНЕНИЕ	ПРОСМОТР
Профили	ИЗМЕНЕНИЕ	ПРОСМОТР

ИЗМЕНЕНИЕ: изменение текущих и создание новых параметров.

ПРОСМОТР: параметры не скрыты, но изменять и создавать их нельзя.

СКРЫТО: некоторые параметры или даже целые разделы скрыты.

#### Пользователи

Список доступных пользователей устройства.

#### Пароль

Введите действующий пароль.

#### Подтверждение пароля




Подтвердите введенный пароль.

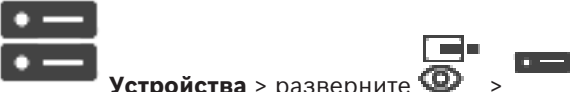

#### Роль

Выберите требуемую роль для выбранного пользователя. Права доступа изменяются соответствующим образом.

## 14.4.4

### Страница "Профиль видеокодера"

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Камера** > вкладка **Профиль видеокодера**  
или


 Главное окно > **Устройства** > разверните  > > вкладка **Конфигурация ONVIF** > вкладка **Камера** > вкладка **Профиль видеокодера**

Профили достаточно сложны и включают ряд взаимодействующих друг с другом параметров, поэтому, как правило, рекомендуется использовать предустановленные профили. Изменение профиля допускается только в том случае, если вы полностью ознакомились со всеми параметрами конфигурации.




### Профили

Выберите нужное имя.

### Замечание!

Настроенные здесь профили можно выбирать в клиенте Configuration Client.




 В главном окне последовательно нажмите **Камеры и запись** и  или  .  
 Параметр по умолчанию <Automatic> можно изменить на один из перечисленных и настроенных профилей

**Примечание.** Обратите внимание, что при активном использовании нескольких профилей на одном устройстве применяются некоторые ограничения производительности; при перегрузке камера может автоматически ограничить качество потока.

### Имя

Здесь можно ввести новое имя для профиля. Это имя будет отображаться в списке доступных профилей в поле «Активный профиль».

### Кодирование

Выберите необходимый кодек.

### Разрешение

Здесь можно выбрать необходимое разрешение для видеоизображения.

### Качество

Этот параметр позволяет уменьшить нагрузку на канал, снизив разрешение изображения. Этот параметр задается с помощью ползунка: самое левое положение соответствует максимальному разрешению, самое правое — минимальной нагрузке на видеоканал.

### Ограничение по частоте кадров

Частота кадров (кадров в секунду) указывает, какое количество кадров в секунду записывается видеочамерой, подключенной к устройству. Этот параметр отображается только для информации.

Если указан интервал кодирования, итоговая частота кадров после кодирования уменьшается на заданный коэффициент.

### Ограничение скорости передачи

Чем меньше скорость передачи данных, тем меньше конечный размер видеофайла. При значительном снижении скорости передачи данных программе придется использовать более сильные алгоритмы сжатия, из-за чего снижается качество видеоизображения. Выберите максимальную выходную скорость передачи данных в кбит/сек. Эта максимальная скорость передачи не превышает ни при каких обстоятельствах. В зависимости от настроек качества видеоизображения для I-кадров и P-кадров это может привести к пропуску отдельных изображений.

Введенное здесь значение должно быть по крайней мере на 10 % больше, чем стандартная целевая скорость передачи данных.

**Интервал кодировки**

Интервал кодирования (количество кадров) обозначает частоту, с которой кодируются кадры, поступающие из камеры. Например, если интервал кодирования составляет 25, это означает, что 1 кадр из 25, записанных в секунду, кодируется и передается пользователю. Максимальное значение снижает нагрузку на канал, но может привести к пропуску информации от некодированных кадров. Уменьшение интервала кодирования увеличивает частоту обновлений изображения, а также нагрузку на канал.

**Длина группы видеокадров**

Длину группы видеокадров можно изменить, только если используется кодек H.264 или H.265. Этот параметр обозначает длину группы изображений между двумя ключевыми кадрами. Чем выше это значение, тем меньше нагрузка на сеть, но тем ниже и качество видео.

Значение 1 означает, что I-кадры генерируются непрерывно. Значение 2 означает, что каждое второе изображение является I-кадром, 3 — что только каждое третье и т. д. Кадры между ними кодируются как P-кадры или B-кадры.

**Истекло время таймаута**

Истекло время ожидания сеанса RTSP для соответствующего потока видеоданных. Время ожидания сеанса предоставляется как подсказка для поддержания сеанса RTSP устройством.

**Многоадресная передача - IP-адрес**

Для работы в режиме многоадресной передачи (дублирование потоков данных в сети) введите правильный адрес многоадресной передачи.

При установке параметра в значение 0.0.0.0 кодек соответствующего потока работает в режиме много-/одноадресной передачи (копирование потоков данных в устройстве). Камера поддерживает много-/одноадресные соединения для пяти одновременно подключенных приемников.

Копирование данных существенно загружает ЦП и при определенных условиях может приводить к ухудшению качества изображения.

**Многоадресная передача - Порт**

Выберите порт назначения многоадресной передачи RTP. Устройство может поддерживать RTCP. В этом случае значение порта должно быть четным, чтобы обеспечить сопоставление соответствующего потока RTCP со следующим более высоким номером порта назначения (нечетным), как указано в спецификации RTSP.

**Многоадресная передача — TTL**

Вы можете ввести значение для указания того, в течение какого времени пакеты для многоадресной передачи будут активны в сети. Если многоадресная передача осуществляется через маршрутизатор, это значение должно быть больше единицы.

**Замечание!**




Многоадресная передача возможна только при использовании протокола UDP. Протокол TCP не поддерживает многоадресные соединения.

Если устройство защищено брандмауэром, то в качестве протокола передачи выберите протокол TCP (порт HTTP). Для работы в локальной сети выберите UDP.



## 14.4.5 Профиль аудиокодера

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Камера** > вкладка **Профиль аудиокодера**  
или

Главное окно >  **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Камера** > вкладка **Профиль аудиокодера**

Профили достаточно сложны и включают ряд взаимодействующих друг с другом параметров, поэтому, как правило, рекомендуется использовать предустановленные профили. Изменение профиля допускается только в том случае, если вы полностью ознакомились со всеми параметрами конфигурации.

### Кодирование

Выберите необходимое кодирование для аудиоисточника при наличии:

- **G.711 [ITU-T G.711]**
- **G.726 [ITU-T G.726]**
- **AAC [ISO 14493-3]**

### Скорость передачи данных

Выберите необходимую скорость передачи данных звуковых сигналов, например 64 кбит/сек.

### Частота дискретизации

Введите частоту дискретизации на выходе в кГц, например 8 кбит/сек.




### Истекло время таймаута

Истекло время ожидания сеанса RTSP для соответствующего потока аудиоданных.

Время ожидания сеанса предоставляется как подсказка для поддержания сеанса RTSP устройством.

## 14.4.6 Обработка изображений, общие данные

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Камера** > вкладка **Обработка изображений, общие данные**  
или

Главное окно >  **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Камера** > вкладка **Обработка изображений, общие данные**

### Яркость

Настройте яркость изображения в соответствии с условиями эксплуатации.

**Насыщенность цвета**

Откорректируйте насыщенность цвета, чтобы обеспечить максимально реалистичную цветопередачу на мониторе.

**Контраст**

Можно настроить контрастность видеоизображения в соответствии с вашими условиями эксплуатации.

**Резкость**

Откорректируйте резкость изображения.






При низком значении изображение становится менее резким. При повышении резкости отображается больше деталей. Повышение резкости может улучшить детализацию номерных знаков, черт лица и краев некоторых поверхностей, но это может увеличить требования к полосе пропускания.



**Отключение ИК-фильтра**

Выберите состояние ИК-фильтра.

Состояние АВТО позволяет алгоритму экспозиции принимать решение о моменте переключения ИК-фильтра.

**14.4.7****Компенсация фоновой засветки**

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Компенс. фоновой засветки**  
или

Главное окно >  **Устройства** > разверните  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Компенс. фоновой засветки**  
В зависимости от модели устройства здесь можно настроить параметры компенсации фоновой засветки.

**Режим**






Выберите пункт **Выключено**, чтобы выключить компенсацию фоновой засветки.




Выберите пункт **Включено**, чтобы обеспечить детализацию в условиях высокого контраста и очень большой разницы между яркими и темными участками.

**Уровень**

Введите или выберите необходимое значение.

**14.4.8****Экспозиция**

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Экспозиция**  
или

Главное окно >  **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Экспозиция**

В зависимости от модели устройства здесь можно настроить параметры экспозиции.

#### Режим

Выберите **Авто**, чтобы включить алгоритм экспозиции на устройстве. Алгоритм использует значения в следующих полях:

- **Приоритет**
- **Окно**
- **Мин. время экспозиции**
- **Макс. время экспозиции**
- **Мин. усиление**
- **Макс. усиление**
- **Мин. диафрагма**

Выберите **Вручную**, чтобы отключить алгоритм экспозиции на устройстве. Алгоритм использует значения в следующих полях:

- **Время экспозиции**
- **Усиление**
- **Диафрагма**

#### Приоритет

Настройте режим приоритета экспозиции (низкое отношение шум/частота кадров).

#### Окно

Определите прямоугольную маску экспозиции.

#### Мин. время экспозиции

Настройте минимальную продолжительность экспозиции [мкс].

#### Макс. время экспозиции

Настройте максимальную продолжительность экспозиции [мкс].

#### Мин. усиление

Настройте минимальный диапазон усиления датчика [дБ].

#### Макс. усиление

Настройте максимальный диапазон усиления датчика [дБ].

#### Мин. диафрагма

Настройте минимальное затухание падающего света за счет диафрагмы [дБ]. 0 дБ соответствует полностью открытой диафрагме.

#### Макс. диафрагма

Настройте максимальное затухание падающего света за счет диафрагмы [дБ]. 0 дБ соответствует полностью открытой диафрагме.

#### Время экспозиции

Задайте время фиксированной экспозиции [мкс].

#### Усиление







Настройте фиксированное усиление [дБ].




#### Диафрагма

Настройте фиксированное затухание падающего света за счет диафрагмы [дБ]. 0 дБ соответствует полностью открытой диафрагме.

## 14.4.9

**Фокусировка**

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Фокус**  
или

Главное окно >  **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Фокус**

В зависимости от модели устройства здесь можно настроить параметры фокусировки. На этой странице можно перемещать объектив в абсолютных и относительных координатах, а также непрерывно. Корректировка фокусного расстояния с помощью этой функции отключает автофокус. Устройство с поддержкой удаленного управления фокусировкой обычно поддерживает управление через эту операцию перемещения. Положение фокуса отображается определенным числовым значением. Возможны следующие состояния фокуса:

**ПЕРЕМЕЩЕНИЕ****ОК****НЕИЗВЕСТНО**

Кроме того, могут отображаться сведения об ошибке, например ошибка позиционирования, о которой сообщает оборудование.

**Режим**

Выберите **Авто**, чтобы включить автоматическую фокусировку объектива в любой момент в соответствии с объектами в сцене. Алгоритм использует значения в следующих полях:

- **Ближний предел**
- **Дальний предел**

Выберите **Вручную**, чтобы вручную регулировать фокусировку. Алгоритм использует значения в следующих полях:

- **Скорость по умолчанию**

**Скорость по умолчанию**

Настройте скорость перемещения фокуса по умолчанию (если нет параметра скорости).

**Дальний предел**







Настройте ближний предел фокусировки объектива [м].




**Дальний предел**

Настройте дальний предел фокусировки объектива [м].

## 14.4.10

**Широкий динамический диапазон**

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Широкий динамический диапазон**  
или

Главное окно >  **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Широкий динамический диапазон**

В зависимости от модели устройства здесь можно настроить параметры широкого динамического диапазона.

#### Режим

Введите или выберите необходимое значение.

#### Уровень




Введите или выберите необходимое значение.

### 14.4.11

#### Баланс белого

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Баланс белого**

или

Главное окно >  **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Баланс белого**

В зависимости от модели устройства здесь можно настроить параметры баланса белого.

#### Режим

Автоматический режим позволяет камере постоянно выполнять корректировки, чтобы обеспечить оптимальную цветопередачу с использованием метода средней отражательной способности или в условиях с естественными источниками света.

В режиме «Вручную» усиление красного, зеленого и синего можно установить в желаемое положение вручную.

Смещение белой точки необходимо изменять только в особых условиях:

- источники света в помещениях и цветная светодиодная подсветка;
- источник света с натриевыми лампами (уличное освещение);
- любой доминирующий в изображении цвет, например зеленый на футбольном поле или на игровом столе.

#### Усиление красного







В режиме баланса белого «Вручную» отрегулируйте ползунок усиления красного, чтобы сместить стандартную установку белой точки (уменьшение красного приводит к увеличению голубого).




#### Усиление синего

В режиме баланса белого «Вручную» отрегулируйте ползунок усиления синего, чтобы сместить стандартную установку белой точки (уменьшение синего приводит к увеличению желтого).

## 14.4.12

### Доступ к сети

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Сеть** > вкладка **Доступ к сети**  
или

Главное окно >  **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Сеть** > вкладка **Доступ к сети**  
Здесь можно настроить различные сетевые параметры.

#### Ethernet IPv4

##### ДНСР

Если для динамического назначения IP-адресов в сети используется DHCP-сервер, можно активировать принятие IP-адресов, автоматически назначенных кодеру. BVMS использует IP-адрес для уникального назначения кодера. DHCP-сервер должен поддерживать привязку IP-адреса к MAC-адресу, а также должен быть правильно настроен, чтобы после назначения IP-адреса он сохранялся при каждой перезагрузке компьютера.

##### Маска подсети

Введите соответствующую маску подсети для установленного IP-адреса. Если включен DHCP-сервер, маска подсети назначается автоматически.

##### Шлюз по умолчанию

Если вы хотите, чтобы модуль установил соединение с удаленным пунктом в другой подсети, введите IP-адрес шлюза. В противном случае оставьте это поле пустым (0.0.0.0).

#### Ethernet IPv6

##### ДНСР

Введите или выберите необходимое значение.

##### IP-адрес

Отображает адрес IPv6 устройства, предоставленный DHCP-сервером.

##### Длина префикса

Отображает длину префикса устройства, предоставляемого DHCP-сервером.

##### Шлюз по умолчанию

Отображает шлюз устройства по умолчанию, предоставленный DHCP-сервером.

##### Имя сервера

Введите или выберите необходимое значение.

##### DNS

DNS-сервер позволяет устройству найти адрес, указанный как имя. Введите здесь IP-адрес DNS-сервера.

##### NTP-серверы

Введите IP-адрес необходимого сервера времени или предоставьте это DHCP-серверу.

Кодер может принимать сигнал времени с сервера времени с использованием различных протоколов сервера времени, а затем использовать его для установки внутренних часов. Модуль запрашивает сигнал времени автоматически каждую минуту. Введите IP-адрес сервера времени. Он поддерживает высокий уровень точности и необходим для работы специальных приложений.

#### **Порты HTTP**

При необходимости выберите другой порт HTTP-браузера. Порт HTTP по умолчанию — 80. Чтобы разрешить безопасные соединения по протоколу HTTPS, необходимо отключить порт HTTP.

**Примечание.** Не поддерживается системой BVMS.

#### **Порты HTTPS**

**Примечание.** Не поддерживается системой BVMS.

Если вы хотите предоставить доступ в сеть через безопасное соединение, при необходимости выберите порт HTTPS. Порт HTTPS по умолчанию — 443. Выберите параметр **Выкл**, чтобы отключить порты HTTPS; будут возможны только небезопасные соединения.

#### **Шлюз по умолчанию**

Введите или выберите необходимое значение.

#### **Порты RTSP**

При необходимости выберите другой порт для обмена данными RTSP. Стандартный порт RTSP — 554. Выберите **Выкл**, чтобы отключить функцию RTSP.

#### **Адрес нулевой конфигурации**

Включите или отключите обнаружение нулевой конфигурации выбранной камеры. Нулевая конфигурация — это альтернативный способ назначения IP-адресов камер, не использующий DHCP и DNS-серверов. Он автоматически создает работающий сетевой IP-адрес без конфигурации или специальных серверов.

**Примечание.** В стандарте ONVIF используется только обнаружение службы нулевой конфигурации.

Если нулевая конфигурация не используется, сеть должны предоставить службы, такие как DHCP или DNS.

В противном случае необходимо вручную настроить сетевые параметры всех IP-камер.

#### **Режим обнаружения ONVIF**

Если функция включена, можно отсканировать камеру в сети. Это включает ее возможности.

Если эта функция отключена, камера не отправляет сообщения обнаружения, чтобы избежать атак отказа в обслуживании.

Рекомендуется отключить обнаружение после добавления камеры в конфигурацию.

Введите или выберите необходимое значение.

#### **Включить DynDNS**

Позволяет включить DynDNS.

Динамическая служба доменных имен (DNS) позволяет выбрать устройство через Интернет по имени хоста, не указывая текущий IP-адрес устройства. Для этого необходимо иметь учетную запись у одного из поставщиков услуг динамического DNS и зарегистрировать требуемое имя узла для устройства на этом сайте.

#### **Примечание.**

Информацию об этой службе, процессе регистрации и доступных именах узлов см. на сайте поставщика услуг DynDNS по адресу [dyndns.org](http://dyndns.org).

**Тип**

Введите или выберите необходимое значение.






**Имя**




Введите имя учетной записи пользователя DynDNS.

**TTL**

Введите или выберите необходимое значение.

**14.4.13****Области**

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  > вкладка **Конфигурация ONVIF** > вкладка **Сеть** > вкладка **Области**  
или

Главное окно >  **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Сеть** > вкладка **Области**

Вы можете добавлять характеристики устройства ONVIF или удалить их с использованием URI, имеющих следующий формат:

```
onvif://www.onvif.org/<path>
```

В следующем примере показано использование значения характеристики. Это просто пример, а не полное описание параметров характеристики, входящих в конфигурацию кодера. В данном примере предполагается, что на кодере настроены следующие характеристики:

```
onvif://www.onvif.org/location/country/china
onvif://www.onvif.org/location/city/beijing
onvif://www.onvif.org/location/building/headquarter
onvif://www.onvif.org/location/floor/R5
onvif://www.onvif.org/name/ARV-453
```

Можно присвоить устройству подробное местоположение и имя устройства, чтобы идентифицировать его в списке устройств.

В таблице показаны основные возможности и другие свойства устройства, которые являются стандартными:

Категория	Определенные значения	Описание
тип	video_encoder	Устройство является устройством сетевого видеокодера.
	PTZ	Устройство является устройством PTZ.
	audio_encoder	Устройство поддерживает аудиокодер.
	video_analytics	Устройство поддерживает видеоаналитику.
	Network_Video_Transmitter	Устройство является сетевым видеопередатчиком.
	Network_Video_Decoder	Устройство является сетевым видеodeкодером.










Категория	Определенные значения	Описание
	Network_Video_Storage	Устройство является сетевым устройством хранения видео.
	Network_Video_Analytic	Устройство является сетевым устройством видеоаналитики.
местонахождение	Любая строка символов или значение пути.	Не поддерживается системой BVMS.
оборудование	Любая строка символов или значение пути.	Строка или значение пути, описывающие оборудование устройства. В список характеристик устройства должна входить как минимум одна запись оборудования.
имя	Любая строка символов или значение пути.	Доступное для поиска имя устройства. Это имя отображается в дереве устройств и в логическом дереве.

Имя характеристики, модель, производитель влияют на то, как устройство отображается в дереве устройств и на идентификацию кодера ONVIF и основные параметры.

## 14.4.14

### Реле

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  > вкладка **Конфигурация ONVIF** > вкладка **Интерфейсы** > вкладка **Реле**

Главное окно >  **Устройства** > разверните  > вкладка **Конфигурация ONVIF** > вкладка **Интерфейсы** > вкладка **Реле**

Состояние физического бездействия релейного выхода можно настроить, задав состояние бездействия **разомкнуто** или **замкнуто** (инверсия поведения реле).

Доступные цифровые выходы устройства отображаются вместе с именем, например:

- **AlarmOut\_0**
- **AlarmOut\_1**

Для любого сопоставления событий реле в пределах системы BVMS следует использовать указанные здесь имена.

#### Режим

Реле может работать в двух режимах:

- **Бистабильный.** После изменения состояния реле остается в этом состоянии.
- **Моностабильный.** После изменения состояния реле возвращается в состояние бездействия после заданного времени задержки.

#### Свободное состояние

Выберите **Разомкнуто**, если хотите, чтобы реле работало как нормально разомкнутый контакт, или **Замкнуто**, если реле должно работать как нормально замкнутый контакт.

#### Время задержки

Установите время задержки. После этого периода времени реле переключается обратно в состояние бездействия, если это настроено в **Моностабильном** режиме.

Если вы хотите проверить конфигурации, связанные с изменением состояния реле, нажмите **Активировать** или **Отключить** для переключения реле. Можно проверить правильную работу настроенных событий реле камеры: отображение состояния значка реле в логическом дереве, события в списке тревожных сигналов и журнале событий.

#### Активировать

Нажмите для переключения реле в настроенное состояние бездействия.





#### Отключить







Нажмите для переключения реле в настроенное активное состояние.





## 14.5


### Страница "Источник событий ONVIF"





Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  > разверните  >  > вкладка **Источник событий ONVIF**  
или

Главное окно >  **Устройства** > разверните  > разверните  >  > вкладка **Источник событий ONVIF**  
или

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  > разверните  > вкладка **Источник событий ONVIF**  
или

Главное окно >  **Устройства** > разверните  > разверните  >  > вкладка **Источник событий ONVIF**  
или

Главное окно >  **Устройства** > разверните  > разверните  > разверните  > разверните  > разверните  > вкладка **Источник событий ONVIF**  
или

Главное окно >  **Устройства** > разверните  > разверните  >  > вкладка **Источник событий ONVIF**

Можно настроить события ONVIF источника (видеоканал, вход или реле). Определение активированного события добавляется в таблицу сопоставления кодера.

Например, для многоканального кодера выполняется выбор камеры, для которой создается событие **Обнаружено движение**.

**Активирующее событие**

Активировать это событие.

**Тема ONVIF**

Введите или выберите текстовую строку.

**Имя источника ONVIF**

Введите или выберите текстовую строку.

**Тип источника ONVIF**

Введите или выберите текстовую строку.

**Значение источника ONVIF**

Введите или выберите текстовую строку.

**См.**

- *Сопоставление событий ONVIF, Страница 37*
- *Настройка таблицы сопоставления ONVIF, Страница 249*

**14.6****Назначение профиля ONVIF**

Главное окно >

Камеры и запись >

Можно назначить ключ медиапрофиля ONVIF камере ONVIF.

Ключ можно назначить либо для видео в реальном времени, либо для записи.

**Назначение ключа для видео в реальном времени.**

- ▶ В столбце **Видеоизображение в реальном времени – Профиль** выберите необходимый элемент.

**Назначение ключа для записи.**

- ▶ В столбце **Запись – Профиль** выберите необходимый элемент.

**См.**

- *Страница Камеры, Страница 292*

## 15 Вкладка Карты и структура

Количество элементов под записью отображается в квадратных скобках.



главное окно > **Карты и структура**

Разрешения могут быть утрачены. При перемещении группы устройств они утрачивают свои параметры разрешений. Необходимо снова установить разрешения на странице **Группы пользователей**.

Отображает дерево устройств, логическое дерево и окно карт.

Позволяет создать структуру всех устройств системы BVMS. Структура отображается в логическом дереве.

Позволяет выполнять следующие задачи:

- Настройка полного логического дерева
- Управлять файлами ресурсов, назначая их узлам дерева
- Создание активных точек на карте
- Создание реле сигнализации о неисправностях

Файлами ресурсов могут быть:



- Файлы карт объектов
- Файлы документов
- Веб-файлы
- Аудиофайлы
- Командные сценарии
- Файлы последовательностей камер

Активными точками могут быть:


- Камеры
- Входы
- Реле
- Командные сценарии
- Последовательности
- Ссылки на другие карты
- Считыватели системы контроля и управления доступом



### Значки

	Отображает диалоговое окно управления файлами ресурсов.
	Отображает диалоговое окно для добавления командного сценария в логическое дерево или управления им.
	Отображает диалоговое окно для добавления или изменения файла последовательности камер.
	Создает папку в логическом дереве.
	Отображает диалоговое окно для добавления файлов ресурсов карт.
	Отображает диалоговое окно для добавления файла документов (HTML, HTM, TXT, URL-адрес, MHT).

	Отображает диалоговое окно для добавления ссылки на внешнее приложение.
	Отображает диалоговое окно для добавления реле сигнализации о неисправностях.

### Символы

	Устройство добавлено в логическое дерево.
---	---

Введите строку и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы. Отображаются только элементы, содержащие введенную строку, и их соответствующие родительские элементы (только в деревьях). Указывается число отфильтрованных элементов и совокупное число элементов. На активный фильтр указывает значок . Для поиска точных фраз строки следует заключать в кавычки, например, в случае строки "Самега 1" отфильтровываются только камеры с таким именем, но не самега 201 .  
Чтобы отменить фильтрацию, нажмите .




## 16 Настройка логического дерева

В данном разделе содержится информация о настройке логического дерева и управлении файлами ресурсов, например, картами.



### Замечание!

При перемещении группы устройств в логическом дереве, устройства утрачивают параметры разрешений. Необходимо снова установить разрешения на странице **Группы пользователей**.

- Нажмите  для сохранения настроек.
- Нажмите  для отмены последней настройки.
- Нажмите  для активации конфигурации.

### См.

- *Диалоговое окно Диспетчер ресурсов, Страница 272*
- *Диалоговое окно Выбрать ресурс, Страница 273*
- *Диалоговое окно Конструктор последовательностей, Страница 276*
- *Диалоговое окно Добавить последовательность, Страница 278*
- *Диалоговое окно Добавить шаг последовательности, Страница 278*
- *Диалоговое окно Добавить URL-адрес, Страница 274*
- *Диалоговое окно Выбрать карту для ссылки, Страница 280*
- *Диалоговое окно "Реле сигнализации о неисправностях", Страница 282*
- *Диалоговое окно Ссылка на внешнее приложение, Страница 274*

### 16.1 Настройка логического дерева

#### См.

- *Вкладка Карты и структура, Страница 268*

### 16.2 Добавление устройства в логическое дерево



Главное окно > **Карты и структура**

#### Для добавления устройства выполните следующие действия.

- ▶ Перетащите элемент из дерева устройств в нужное место логического дерева. Можно перетащить весь узел с подчиненными элементами из дерева устройств в логическое дерево. Можно выбрать несколько устройств, нажав клавишу CTRL или SHIFT.

#### См.

- *Вкладка Карты и структура, Страница 268*

### 16.3 Удаление элемента дерева



Главное окно > **Карты и структура**

**Чтобы удалить элемент из логического дерева:**

- ▶ Щелкните элемент в логическом дереве правой кнопкой мыши и выберите команду **Удалить**. Если выбранный элемент имеет подчиненные элементы, на экране появляется окно сообщения. Чтобы подтвердить выбор, нажмите кнопку **ОК**. Элемент будет удален из системы.  
При удалении элемента из папки карт логического дерева он одновременно удаляется с карты.

**См.**

– *Вкладка Карты и структура, Страница 268*

**16.4****Управление файлами ресурсов**

Главное окно >  **Карты и структура** >   
или

Главное окно >  **Тревожные сигналы** > 


Можно импортировать файлы ресурсов следующих форматов:

- Файлы DWF (двумерные файлы ресурсов карты)
- PDF
- JPG
- PNG
- Файлы HTML
- MP3 (аудиофайлы)
- Файлы TXT (командные сценарии или последовательности камер)
- Файлы MHT (веб-архивы)
- Файлы URL (ссылки на веб-страницы)
- Файлы URL-адресов HTTPS (ссылки на виджеты Intelligent Insights)
- WAV (аудиофайлы)


Импортируемые файлы ресурсов заносятся в базу данных. Они не связаны с исходными файлами.

**Замечание!**


По окончании каждого из следующих действий:

Нажмите  , чтобы сохранить настройки.


**Чтобы импортировать файл ресурса:**

1. Нажмите  .  
Откроется диалоговое окно **Импортировать ресурс**.
2. Выберите один или несколько файлов.
3. Нажмите **Открыть**.  
Выбранные файлы будут добавлены в список.  
Если файл уже был импортирован, на экране появляется окно сообщения.  
Если вы решили повторно импортировать уже импортированный файл, в список будет добавлена новая запись.


**Чтобы удалить файл ресурса:**

1. Выберите файл ресурса.
2. Нажмите  .  
Выбранный файл ресурса будет удален из списка.


**Чтобы переименовать файл ресурса:**

1. Выберите файл ресурса.
2. Нажмите  .
3. Введите новое имя.  
Исходное имя файла и дата создания сохраняются.

**Чтобы заменить содержимое файла ресурса:**

1. Выберите файл ресурса.
2. Нажмите  .  
Откроется диалоговое окно **Заменить ресурс**.
3. Выберите файл с подходящим содержимым и нажмите **Открыть**.  
Имя ресурса будет сохранено, а исходное имя файла будет заменено новым.



**Чтобы экспортировать файл ресурса:**

1. Выберите файл ресурса.
2. Нажмите  .  
Отображается диалоговое окно для выбора каталога.
3. Выберите нужный каталог и нажмите **ОК**.  
Исходный файл будет экспортирован.

**См.**

- *Диалоговое окно Выбрать ресурс, Страница 273*

**16.4.1****Диалоговое окно Диспетчер ресурсов**








Главное окно >  **Карты и структура** >  > диалоговое окно **Диспетчер ресурсов**

Позволяет осуществлять управление файлами ресурсов.

Вы можете осуществлять управление файлами следующих форматов:

- Файлы DWF (файлы ресурсов карты)  
Для использования в Operator Client эти файлы конвертируются в растровый формат.
- PDF
- JPG
- PNG
- Файлы HTML (документы HTML, например планы действий)
- MP3 (аудиофайлы)
- Файлы TXT (текстовые файлы)
- Файлы URL (содержат ссылки на веб-страницы или виджеты Intelligent Insights)
- Файлы MHT (веб-архивы)
- WAV (аудиофайлы)
- EXE



-  Нажмите для отображения диалогового окна импорта файла ресурса.
-  Нажмите для отображения диалогового окна **Добавить URL-адрес**.
-  Нажмите для отображения диалогового окна **Ссылка на внешнее приложение**.
-  Нажмите для удаления выбранного файла ресурсов.
-  Нажмите для переименования выбранного файла ресурсов.
-  Нажмите для отображения диалогового окна для замены выбранного файла ресурсов другим.
-  Нажмите для отображения диалогового окна для экспорта выбранного файла ресурсов.

## 16.4.2

### Диалоговое окно Выбрать ресурс

Главное окно >  **Карты и структура** > 

Позволяет добавлять файл карты в формате DWF, PDF, JPG или PNG в Логическое дерево.

#### Выберите файл ресурса:

Для выбора файла карты нажмите на имени файла. Содержимое выбранного файла отображается на панели предварительного просмотра.

#### Управление...

Нажмите для отображения диалогового окна **Диспетчер ресурсов**.

#### См.

- *Добавление карты, Страница 279*
- *Назначение карты папке., Страница 280*
- *Добавление документа, Страница 273*

## 16.5


### Добавление документа

Главное окно >  **Карты и структура**

В качестве документов можно добавить текстовые файлы, файлы HTML (в том числе MHT), файлы URL (содержащие интернет-адрес) или файлы URL HTTPS (например, содержащие виджет Intelligent Insights). Кроме того, можно добавить ссылку на другое приложение. Перед добавлением документа необходимо иметь импортированные файлы документов. Информация по импорту файлов документа содержится в *Управление файлами ресурсов, Страница 271*.

#### Чтобы добавить файл документа карты или виджет Intelligent Insights:

1. Убедитесь, что файл документа, который вы хотите добавить, уже импортирован.
2. Выберите папку, в которую нужно добавить новый документ.

3. Нажмите  . Отображается диалоговое окно **Выбрать ресурс**.

4. Выберите файл из списка. Если необходимые файлы отсутствуют в списке, нажмите **Управление...** для отображения диалогового окна **Диспетчер ресурсов** для импорта файлов.
5. Нажмите **ОК**. Новый документ будет добавлен в выбранную папку.

**См.**

- *Диалоговое окно Выбрать ресурс, Страница 273*
- *Управление файлами ресурсов, Страница 271*

**16.5.1****Диалоговое окно Добавить URL-адрес**

Позволяет добавить в систему Интернет-адрес HTTP (URL) или Интернет-адрес HTTPS, например виджеты Intelligent Insights. Вы можете добавить этот URL-адрес в логическое дерево в качестве документа. Пользователь может отобразить интернет-страницу или виджет Intelligent Insights в своем Operator Client.

**Имя**

Введите отображаемое имя для URL-адреса.

**URL-адрес**

Введите URL-адрес.

**Только для безопасного подключения****Пользователь**

Введите имя пользователя для URL-адреса HTTPS.

**Пароль:**

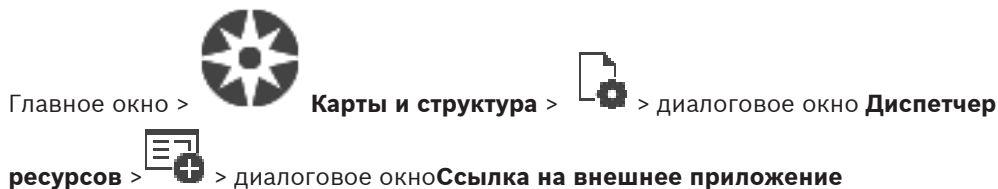
Введите пароль для URL-адреса HTTPS.

**Отобразить пароль**

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

**См.**

- *Добавление документа, Страница 273*

**16.6****Диалоговое окно Ссылка на внешнее приложение**

Позволяет добавить ссылку на внешнее приложение. Ссылка должна быть действительна на рабочей станции, на которой она используется.

**Замечание!**

Внешнее приложение, которое запускается с экрана с заставкой, будет работать неправильно.

Внешнее приложение, которое имеет совместные функции с Operator Client, не будет работать правильно, и в редких случаях его использование может привести к сбою клиента Operator Client.

**Имя**

Введите имя для ссылки, которая отображается в логическом дереве.

**Путь**

Введите имя внешнего приложения или выберите путь к нему. Путь к внешнему приложению должен быть действительным на рабочей станции, на которой пользователь клиента Operator Client использует эту ссылку.

**Аргументы**

При необходимости введите аргументы в команду, которая выполняет внешнее приложение.


**16.7****Добавление командного сценария**

Главное окно > **Карты и структура**

Чтобы можно было добавить командный сценарий, должны быть предварительно импортированы или созданы файлы командного сценария.

Более подробные сведения см. в *Настройка командных сценариев, Страница 93*.

**Чтобы добавить файл командного сценария:**

1. Выберите папку, в которую вы хотите добавить новый командный сценарий.
  2. Нажмите . Отображается диалоговое окно **Выбрать клиентский сценарий**.
  3. Выберите файл из списка.
  4. Нажмите **ОК**.
- Новый командный сценарий будет добавлен в выбранную папку.

**См.**



– *Диалоговое окно Выбрать ресурс, Страница 273*

**16.8****Добавление последовательности камер**

Главное окно > **Карты и структура**

Можно добавить последовательность камер в корневой каталог или папку логического дерева.

**Для добавления последовательности камер выполните следующие действия.**

1. В логическом дереве выберите папку, в которую вы хотите добавить новую последовательность камер.
2. Нажмите . Откроется диалоговое окно **Конструктор последовательностей**.
3. Выберите последовательность камер из списка.
4. Нажмите **Добавить в Логическое дерево**. Новая последовательность  будет добавлена в выбранную папку.

**См.**

– *Диалоговое окно Конструктор последовательностей, Страница 276*

## 16.8.1 Диалоговое окно Конструктор последовательностей






Главное окно >

Карты и структура >



Позволяет осуществлять управление последовательностями камер.

### Значки

	Нажмите для отображения диалогового окна <b>Добавить последовательность</b> .
	Нажмите для переименования последовательности камер.
	Нажмите для удаления выбранной последовательности камер.



### Замечание!

Если последовательность удалена в диалоговом окне **Конструктор последовательностей**, она автоматически удаляется из списка **Начальная последовательность** видеостены, если она задана в нем.

### Добавить шаг

Нажмите для отображения диалогового окна **Добавить шаг последовательности**.

### Удалить шаг

Нажмите, чтобы удалить выбранные шаги.

### Шаг

Отображает номер шага. Все камеры определенного шага имеют одинаковое время задержки.

### Переключение

Позволяет устанавливать время задержки (в секундах).

### Номер камеры

Щелкните ячейку для выбора камеры в соответствии с логическим номером.

### Камера

Щелкните ячейку для выбора камеры в соответствии с именем.

### Функция камеры

Щелкните ячейку для изменения функции камеры в данной строке.

### Данные

Введите время, в течение которого будет выполняться данная функция камеры. Чтобы настроить этот параметр, следует выбрать запись в столбце **Камера** и запись в столбце

### Функция камеры.

### Единица данных

Выберите единицу времени, например секунды. Чтобы настроить этот параметр, следует выбрать запись в столбце **Камера** и запись в столбце **Функция камеры**.

### Добавить в Логическое дерево

Нажмите для добавления выбранной последовательности камер в логическое дерево и для закрытия диалогового окна.

### См.

– *Страница Настенная панель мониторов, Страница 150*

- Управление предварительно настроенными последовательностями камер, Страница 277

## 16.9

### Управление предварительно настроенными последовательностями камер



Главное окно >

#### Карты и структура

При управлении последовательностью камер вы можете выполнять следующие действия:

- Создавать последовательность камер
- Добавлять к существующей последовательности камер шаг с новым периодом переключения
- Удалять шаг из последовательности камер
- Удалять последовательность камер

#### Замечание!

При изменении и активации конфигурации последовательность камеры (предварительно настроенная или автоматическая) обычно продолжается после перезапуска Operator Client.

Однако в следующих случаях последовательность не продолжается:

Монитор, на котором последовательность настроена на отображение, был удален.

Режим монитора (один экран/четыре экрана), на котором последовательность настроена на отображение, был изменен.

Логический номер монитора, на котором последовательность настроена на отображение, был изменен.



#### Замечание!

По окончании каждого из следующих действий:

Нажмите для сохранения настроек.



#### Чтобы создать последовательность камер:

1. В логическом дереве выберите папку, в которой вы хотите создать новую последовательность камер.

2. Нажмите .

Откроется диалоговое окно **Конструктор последовательностей**.

3. В диалоговом окне **Конструктор последовательностей** нажмите .

Откроется диалоговое окно **Добавить последовательность**.

4. Введите соответствующие значения.
5. Нажмите **ОК**.

Новая последовательность камер будет добавлена.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

#### Чтобы добавить к последовательности камер шаг с новым периодом переключения:

1. Выберите нужную последовательность камер.
2. Нажмите **Добавить шаг**.


Откроется диалоговое окно **Добавить шаг последовательности**.

3. Установите необходимые параметры.
4. Нажмите **ОК**.  
Новый шаг будет добавлен к последовательности камер.

**Чтобы удалить шаг из последовательности камер:**

- ▶ Щелкните правой кнопкой мыши нужную последовательность камер правой кнопкой мыши и нажмите **Удалить шаг**.  
Шаг с наибольшим номером будет удален.

**Чтобы удалить последовательность камер:**

1. Выберите нужную последовательность камер.
2. Нажмите . Выбранная последовательность камер будет удалена.

**См.**

– *Диалоговое окно Конструктор последовательностей, Страница 276*

## 16.9.1

### Диалоговое окно Добавить последовательность

Главное окно >  **Карты и структура** >  > диалоговое окно **Конструктор последовательностей** > 

Позволяет настроить параметры последовательности камер.

**Имя последовательности:**

Введите соответствующее имя новой последовательности камер.

**Логический номер:**

При использовании клавиатуры Bosch IntuiKey введите логический номер для последовательности.

**Период переключения:**

Введите соответствующий период переключения.

**Камер на шаг:**



Введите количество камер на каждый шаг.

**Шаги:**

Введите соответствующее количество шагов.

## 16.9.2

### Диалоговое окно Добавить шаг последовательности

Главное окно >  **Карты и структура** >  > кнопка **Добавить шаг**  
Позволяет добавить к существующей последовательности камер шаг с новым периодом переключения.

**Период переключения:**



Введите соответствующий период переключения.

## 16.10

### Добавление папки

Главное окно >  **Карты и структура**

**Для добавления папки выполните следующие действия.**

1. Выберите папку, в которую нужно добавить новую папку.
2. Нажмите . Новая папка будет добавлена в выбранную папку.
3. Нажмите , чтобы переименовать папку.
4. Введите новое имя и нажмите клавишу ВВОД.

**См.**

– *Вкладка Карты и структура, Страница 268*

## 16.11

### Добавление карты



Главное окно >


**Карты и структура**

Чтобы можно было добавить карту, необходимо предварительно импортировать файлы ресурса карты.

Информация по импорту файла ресурса карты содержится в *Управление файлами ресурсов, Страница 271*.


**Чтобы добавить карту:**

1. Убедитесь, что файл ресурса карты, который вы хотите добавить, уже импортирован.
2. Выберите папку, в которую нужно добавить новую карту.

3. Нажмите . Отображается диалоговое окно **Выбрать ресурс**.
4. Выберите файл из списка.

Если необходимые файлы отсутствуют в списке, нажмите **Управление...** для отображения диалогового окна **Диспетчер ресурсов** для импорта файлов.

5. Нажмите **ОК**.

Новая карта  будет добавлена в выбранную папку.

Карта будет отображаться.

В верхнем левом углу карты будут отображаться все устройства, находящиеся в данной папке.

**См.**

– *Диалоговое окно Выбрать ресурс, Страница 273*

## 16.12

### Добавление ссылки на другую карту





Главное окно >

**Карты и структура**

После добавления двух и более карт вы можете создать ссылку для перехода с одной карты на другую, чтобы пользователь мог переходить с одной карты на другую одним щелчком мыши.

**Чтобы добавить ссылку:**


1. Щелкните на папке карт  в логическом дереве.
2. Щелкните карту правой кнопкой мыши и нажмите **Создать ссылку**. Отображается диалоговое окно **Выбрать карту для ссылки**.

3. В диалоговом окне выберите карту .
4. Нажмите **Выбрать**.
5. Перетащите элемент в нужное место на карте.

### 16.12.1

#### Диалоговое окно Выбрать карту для ссылки



Главное окно > **Карты и структура** > Выберите папку карты  в логическом дереве > На карте щелкните правой кнопкой мыши и выберите **Создать ссылку**.  
Позволяет выбрать карту для создания ссылки на другую карту.



Щелкните другую карту, чтобы выбрать.

#### Выбрать

Нажмите для вставки ссылки в выбранную карту.

### 16.13

#### Назначение карты папке.




Главное окно > **Карты и структура**

Чтобы можно было назначить карты, необходимо предварительно импортировать файлы ресурса карты.

Более подробные сведения см. в *Управление файлами ресурсов, Страница 271*.

#### Чтобы назначить файл ресурса карты:

1. Щелкните правой кнопкой мыши папку и нажмите **Назначить карту**.  
Отображается диалоговое окно **Выбрать ресурс**.
2. Выберите файл ресурса карты из списка.
3. Нажмите **ОК**. Выбранная папка будет отображаться как .  
Карта будет отображаться в окне карт.  
В верхнем левом углу карты будут отображаться все элементы, находящиеся в данной папке.

#### См.

- *Вкладка Карты и структура, Страница 268*
- *Диалоговое окно Выбрать ресурс, Страница 273*

### 16.14

#### Управление устройствами на карте



Главное окно > **Карты и структура**

Перед тем, как начать управление устройствами на карте, необходимо добавить карту или назначить карту папке и добавить устройства в данную папку.



#### Замечание!

По окончании каждого из следующих действий:

Нажмите  для сохранения настроек.



**Чтобы поместить элемент на карту:**

1. Выберите папку карт.
2. Перетащите устройства из дерева устройств в папку карт.  
Устройства папки карт расположены в левом верхнем углу карты.
3. Перетащите элементы в нужные места на карте.

**Чтобы удалить элемент логического дерева только с карты:**

1. Щелкните элемент на карте правой кнопкой мыши и выберите пункт **Невидимый**.  
Элемент будет удален с карты.  
Элемент останется в логическом дереве.
2. Чтобы элемент снова отображался на карте, щелкните устройство правой кнопкой мыши в логическом дереве и выберите пункт **Видимый на карте**.

**Чтобы удалить элемент с карты и из полного логического дерева:**

- ▶ Щелкните элемент в логическом дереве правой кнопкой мыши и выберите пункт **Удалить**.  
Элемент будет удален с карты и из логического дерева.

**Чтобы сменить значок ориентации камеры:**

- ▶ Щелкните элемент правой кнопкой мыши, выберите команду **Изменить изображение** и нажмите необходимый значок.  
Значок изменяется.

**Чтобы изменить цвет элемента:**

- ▶ Щелкните элемент правой кнопкой мыши и выберите команду **Изменить цвет**.  
Выберите необходимый цвет.  
Значок изменится.

**Для активации / деактивации режима обхода устройства на карте:**

1. Щелкните правой кнопкой мыши по определенному устройству на карте.
2. Нажмите **Обход / Отменить обход**.

**Замечание!**

Имеется возможность фильтрации устройств в режиме обхода в текстовом поле поиска.

**См.**

- *Настройка обхода устройств, Страница 283*
- *Вкладка Карты и структура, Страница 268*

**16.15****Добавление реле сигнализации о неисправностях**

Главное окно >

**Карты и структура** >



> диалоговое окно **Реле сигнализации о неисправностях**

**Назначение**

Реле сигнализации неисправности переключается в случае какой-либо серьезной системной ошибки, приводя в действие внешнее сигнальное устройство (стробоскоп, сирену и т. п.).

Пользователь должен вручную сбросить реле.

Функцию реле сигнализации неисправности может выполнять одно из следующих устройств:

- реле кодера или декодера BVIP;
- реле ADAM;
- выход охранной панели.

### Пример

В случае какого-либо события, серьезно влияющего на работу системы (например, сбой жесткого диска), или происшествия, которое представляет угрозу для объекта (например, сбой при проверке контрольного изображения), срабатывает реле сигнализации неисправности. Оно может, например, активировать звуковую сигнализацию или автоматически закрыть двери.

### Описание принципа действия

Можно настроить одно реле для выполнения функции реле сигнализации неисправности. Реле сигнализации неисправности автоматически активируется, когда происходит событие из заданного пользователем набора событий. Активация реле означает, что на реле подается команда замыкания контакта. Последующее событие «Реле замкнуто» не привязано к команде. Оно происходит и регистрируется, только если состояние реле изменяется физически! Например, ранее замкнутое реле не создает это событие. За исключением того факта, что реле сигнализации неисправности автоматически срабатывает по событию из заданного пользователем набора событий, во всем остальном оно работает так же, как и все остальные реле. В частности, пользователь может отключить реле сигнализации неисправности в Operator Client. Веб-клиент также позволяет отключить реле сигнализации неисправности. Поскольку на реле сигнализации неисправности также распространяются разрешения регулярного доступа, всем клиентам требуется учитывать разрешения, имеющиеся у вошедшего в систему пользователя.

### Порядок добавления:

1. В списке **Реле сигнализации о неисправностях** выберите нужное реле.
2. Нажмите **События...**  
Отображается диалоговое окно **Выбор событий для реле сигнализации о неисправностях**.
3. Выберите необходимые события, которые могут вызвать срабатывание реле сигнализации о неисправностях.
4. Нажмите **ОК**.  
Реле сигнализации о неисправностях добавляется в систему.

## 16.15.1

### Диалоговое окно "Реле сигнализации о неисправностях"



Главное окно >

Карты и структура >



> диалоговое окно **Реле**

**сигнализации о неисправностях**

Можно добавить в систему реле сигнализации о неисправностях. Вы определяете, какое реле будет использоваться в качестве реле сигнализации о неисправностях, и настраиваете события, которые могут привести к срабатыванию реле сигнализации о неисправностях.

Это реле уже должно быть настроено в Логическом дереве.

#### Реле сигнализации о неисправностях

В списке выберите требуемое реле.

#### События...

Нажмите, чтобы открыть диалоговое окно **Выбор событий для реле сигнализации о неисправностях**.

## 16.16 Настройка обхода устройств



Главное окно >

### Карты и структура

Вы можете настроить обход определенных кодеров, камер, входов и реле, например, во время строительных работ. При настроенном обходе кодера, камеры, входа или реле запись остановлена, BVMSOperator Client не отображает никакие события или тревоги, при этом последние не регистрируются в журнале.

Камеры в режиме обхода по-прежнему отображают видео в режиме реального времени в Operator Client и оператор по-прежнему имеет доступ к старым записям.



#### Замечание!

Если кодер находится в режиме обхода, никакие тревоги и события не создаются для всех камер, реле и входов этого кодера. Если определенные отдельные камера, реле или вход находятся в режиме обхода и определенное устройство будет отключено от кодера, такие тревоги по-прежнему создаются.

#### Для активации / деактивации режима обхода устройства в логическом дереве или дереве устройств:

1. в логическом дереве или дереве устройств правой кнопкой мыши щелкните по определенному устройству.
2. Нажмите **Обход** / **Отменить обход**.

#### Для активации / деактивации режима обхода устройства на карте:

см. *Управление устройствами на карте, Страница 280*



#### Замечание!

Имеется возможность фильтрации устройств в режиме обхода в текстовом поле поиска.

#### См.

– *Управление устройствами на карте, Страница 280*

## 17 Страница Расписания



Главное окно >

Позволяет настроить расписания записей и расписания задач.



Нажмите для переименования выбранного расписания записей или задач.

### Расписания записей

Отображает дерево расписаний записей. Выберите элемент для настройки.

### Расписания задач

Отображает дерево расписаний задач. Выберите элемент для настройки.

### Добавить

Нажмите для добавления нового расписания задач.

### Удалить

Нажмите для удаления выбранного расписания задач.

### См.

– *Настройка расписаний, Страница 287*

## 17.1 Страница Расписания записей



Главное окно >

> Выбрать элемент в дереве расписания записей

Позволяет настроить расписания записей.

### Рабочие дни

нажмите для отображения расписания для рабочих дней. Отображаются временные интервалы для всех настроенных расписаний записей.

Перетащите указатель для выделения периодов времени в выбранном расписании. Все выделенные ячейки будут отображаться тем же цветом, что и выбранное расписание.

24 часа в сутках отображаются по горизонтали. Каждый час разделен на 4 ячейки. Одна ячейка представляет собой 15 минут.

### Выходные дни

Нажмите для отображения расписания на выходные.

### Дни исключений

Нажмите для отображения расписания на дни исключений.

### Добавить

Нажмите, чтобы отобразить диалоговое окно для добавления выходных и дней исключений.

### Удалить

Нажмите, чтобы отобразить диалоговое окно для удаления выходных и дней исключений.

### См.

- *Настройка расписания записей, Страница 287*
- *Добавление выходных дней и дней исключений, Страница 289*
- *Удаление выходных дней и дней исключений, Страница 290*
- *Переименование расписания, Страница 291*

## 17.2 Страница Расписания задач



Главное окно > > Выбрать элемент в дереве расписания записей

Позволяет настроить доступные расписания задач. Вы можете настроить стандартную или повторяющуюся схему.

### Стандарт

Нажмите, чтобы отобразить таблицу для настройки стандартных расписаний задач. Если вы настраиваете стандартную схему, повторяющаяся схема недоступна для выбранного расписания.

### Повторение

Нажмите, чтобы отобразить таблицу настройки схемы повторения для выбранного расписания задач. Например, вы можете настроить расписание на каждый второй четверг каждого месяца или на 4 июля каждого года. Если вы настраиваете повторяющуюся схему, стандартная схема недоступна для выбранного расписания задач.

### Рабочие дни

нажмите для отображения расписания для рабочих дней.

Перетащите указатель для выделения периодов времени в выбранном расписании.

Выделенные ячейки будут отображаться тем же цветом, что и выбранное расписание.

24 часа в сутках отображаются по горизонтали. Каждый час разделен на 4 ячейки. Одна ячейка представляет собой 15 минут.

### Выходные дни

Нажмите для отображения расписания на выходные.

### Дни исключений

Нажмите для отображения расписания на дни исключений.

### Очистить все

Нажмите, чтобы очистить временные интервалы для всех доступных дней (рабочих, выходных, дней исключений).

### Выделить все

Нажмите, чтобы выделить временные интервалы для всех доступных дней (рабочих, выходных, дней исключений).

### Добавить...

Нажмите, чтобы отобразить диалоговое окно для добавления выходных и дней исключений.

### Удалить...

Нажмите, чтобы отобразить диалоговое окно для удаления выходных и дней исключений.

### Схема повторения

Выберите частоту, с которой должны повторяться задачи расписания (Ежедневно, Еженедельно, Ежемесячно, Ежегодно), после чего выберите соответствующие параметры.

### Схема дней

Перетащите указатель для выделения периодов времени в схеме повторения.

### См.

- *Добавление расписания задач, Страница 288*
- *Настройка стандартного расписания задач, Страница 288*
- *Настройка повторяющегося расписания задач, Страница 289*

- *Удаление расписания задач, Страница 289*
- *Добавление выходных дней и дней исключений, Страница 289*
- *Удаление выходных дней и дней исключений, Страница 290*
- *Переименование расписания, Страница 291*

## 18 Настройка расписаний



Главное окно > **Расписания**

Имеется два типа расписаний:

- Расписания записей
- Расписания задач




Вы можете настроить до 10 различных расписаний записей в таблице расписаний записей. В этих сегментах камеры могут функционировать по-разному. Например, они могут иметь разную частоту кадров и параметры разрешения (настраиваются на странице **Камеры и запись**). В каждый момент времени действует только одно расписание записей. В нем отсутствуют какие-либо пробелы или накладки.

Настраиваются расписания задач для планирования различных событий в системе (настройка производится на странице **События**).

Определения терминов "Расписание записей" и "Расписания задач" см. в глоссарии.

Расписания также используются на других страницах Configuration Client:

- Страница **Камеры и запись**  
Используется для настройки записи.
- Страница **События**  
Используется для определения времени, когда события заносятся в журнал, вызывают тревожные сигналы или выполнение командных сценариев.
- Страница **Группы пользователей**  
Используется для определения времени, когда члены пользовательской группы могут войти в систему.

- Нажмите  для сохранения настроек.
- Нажмите  для отмены последней настройки.
- Нажмите  для активации конфигурации.

**См.**

- *Страница Расписания записей, Страница 284*
- *Страница Расписания задач, Страница 285*

### 18.1 Настройка расписания записей



Главное окно > **Расписания**

В любое расписание записей можно добавить дни исключений. Данные установки корректируют обычные недельные параметры.

Последовательность уменьшения приоритета такова: дни исключений, выходные дни, будни.

Максимальное число расписаний записей составляет 10. Первые три записи настраиваются по умолчанию. Вы можете изменить эти настройки. Записи с серым

значком  не имеют настроенного периода времени.

Рабочие дни для всех расписаний записей одинаковы.

Для каждого стандартного расписания задач существуют собственные шаблоны рабочих дней.

**Чтобы настроить расписание записей:**

1. В дереве **Расписания записей** выберите расписание.
2. Перейдите на вкладку **Рабочие дни**.
3. В поле **Расписание** перетащите указатель для выделения периодов времени в выбранном расписании. Выделенные ячейки будут отображаться тем же цветом, что и выбранное расписание.

**Примечания:**

- Временной интервал рабочего дня в расписании записей может быть отмечен цветом из другого расписания записей.

**См.**

- *Страница Расписания записей, Страница 284*

## 18.2



### Добавление расписания задач



Главное окно > **Расписания**

**Чтобы добавить расписание задач:**

1. Нажмите **Добавить**.  
Будет добавлена новая запись.
2. Введите соответствующее имя.
3. Нажмите **Стандарт** для создания стандартного расписания задач или **Повторение** для создания повторяющегося расписания задач.  
При изменении настроек отображается окно сообщения. Нажмите **ОК**, если вы хотите изменить тип расписания.

Стандартное расписание задач отображается как , повторяющееся расписание задач отображается как .

4. Установите соответствующие параметры для выбранного расписания.

**См.**

- *Страница Расписания задач, Страница 285*

## 18.3

### Настройка стандартного расписания задач



Главное окно > **Расписания**

Для каждого стандартного расписания задач существуют собственные шаблоны рабочих дней.

**Чтобы настроить стандартное расписание задач:**

1. в дереве **Расписания задач** выберите стандартное расписание задач.
2. Перейдите на вкладку **Рабочие дни**.
3. В поле **Расписание** перетащите указатель для выделения периодов времени в выбранном расписании.

**См.**

- *Страница Расписания задач, Страница 285*




## 18.4 Настройка повторяющегося расписания задач



Главное окно > **Расписания**

Для каждого повторяющегося расписания задач существуют собственная схема дней.

**Чтобы настроить повторяющееся расписание задач:**

1. В дереве **Расписания задач** выберите повторяющееся расписание задач .
2. В поле **Схема повторения** выберите частоту, с которой должны повторяться задачи расписания (**Ежедневно**, **Еженедельно**, **Ежемесячно**, **Ежегодно**), после чего выберите соответствующие параметры.
3. Выберите подходящую начальную дату из списка **Начальная дата:**.
4. В поле **Схема дней** перетащите указатель для выбора соответствующего периода времени.

**См.**

– *Страница Расписания задач, Страница 285*

## 18.5 Удаление расписания задач



Главное окно > > Выбрать элемент в дереве **Расписания задач**

**Чтобы удалить расписание задач:**

1. В дереве **Расписания задач** выберите элемент.
2. Нажмите **Удалить**.  
Расписание задач будет удалено. Все задачи, имевшиеся в этом расписании, удаляются и не будут выполнены.

**См.**

– *Страница Расписания задач, Страница 285*

## 18.6 Добавление выходных дней и дней исключений



Главное окно > **Расписания**

### **Замечание!**

Список дней исключений и выходных можно оставить пустым. Дни исключений и выходных заменяют расписание для соответствующего дня недели.

Пример:

Старая конфигурация:

Расписание рабочего дня должно быть активно с 9:00 до 10:00

Расписание дня исключений должно быть активно с 10:00 до 11:00

Результат: активность с 10:00 до 11:00

То же самое работает и для выходных дней.



Вы можете добавлять выходные дни и дни исключений в расписание записей и в расписание задач.

Выходные дни и дни исключений одинаковы для всех расписаний записей.

Для каждого стандартного расписания задач существуют собственные шаблоны выходных дней и дней исключений.

**Чтобы добавить в расписание выходные дни и дни исключений:**

1. В дереве **Расписания записей** или **Расписания задач** выберите расписание.
2. Перейдите на вкладку **Выходные дни**.
3. Нажмите **Добавить**.  
Откроется диалоговое окно **Добавить выходные**.
4. Выберите один или несколько выходных дней и нажмите **ОК**.  
Выбранные выходные дни будут добавлены в расписание.
5. Перетащите указатель для выбора соответствующего периода времени (это невозможно осуществить для расписаний записей).  
Выделенные ячейки будут очищены и наоборот.
6. Перейдите на вкладку **Дни исключений**.
7. Нажмите **Добавить**.  
Откроется диалоговое окно **Добавить дни исключений**.
8. Выберите один или несколько специальных дней и нажмите **ОК**.  
Выбранные дни исключений будут добавлены в расписание.
9. Перетащите указатель для выбора соответствующего периода времени (это невозможно для расписаний записей).  
Выделенные ячейки будут очищены и наоборот.  
Сортировка добавленных выходных дней и дней исключений осуществляется в хронологическом порядке.

**Примечания:**

- Временной интервал выходного дня или дня исключений в расписании записей может быть отмечен цветом из другого расписания записей.

**См.**

- *Страница Расписания записей, Страница 284*
- *Страница Расписания задач, Страница 285*

## 18.7

### Удаление выходных дней и дней исключений



Главное окно > **Расписания**

Из расписания видеозаписи и расписания задач можно удалить выходные дни и дни исключений.

**Чтобы удалить выходные дни и дни исключений из расписания задач:**

1. В дереве **Расписания записей** или **Расписания задач** выберите расписание.
2. Перейдите на вкладку **Выходные дни**.
3. Нажмите **Удалить**.  
Откроется диалоговое окно **Выберите выходные для удаления**.
4. Выберите один или несколько выходных дней и нажмите **ОК**.  
Выбранные выходные дни будут удалены из расписания.
5. Перейдите на вкладку **Дни исключений**.
6. Нажмите **Удалить**.  
Откроется диалоговое окно **Выберите дни исключений для удаления**.
7. Выберите один или несколько дней исключений и нажмите **ОК**.  
Выбранные дни исключений будут удалены из расписания.

**См.**

- Страница Расписания записей, Страница 284
- Страница Расписания задач, Страница 285

**18.8****Переименование расписания**

Главное окно >

**Чтобы переименовать расписание:**

1. В дереве **Расписания записей** или **Расписания задач** выберите элемент.

2. Нажмите  .

3. Введите новое имя и нажмите клавишу ВВОД. Элемент будет переименован.

**См.**

- Страница Расписания записей, Страница 284
- Страница Расписания задач, Страница 285

## 19 Страница Камеры и запись



Главное окно >

### Камеры и запись

Отображает страницу с таблицей камер или страницу с таблицей записей.

Позволяет настроить различные свойства камеры и параметры записи.

Позволяет отфильтровать камеры, отображаемые в соответствии с их типом.

#### Значки

	Нажмите для копирования настроек записи из одного расписания записей в другое.
	Нажмите для отображения диалогового окна <b>Параметры качества потока</b> .
	Нажмите для отображения диалогового окна <b>Настройки записи по расписанию</b> .
	Нажмите, чтобы отобразить диалоговое окно настройки выбранной камеры PTZ.
	Отображает все доступные камеры, независимо от их устройства хранения.
	Нажмите для изменения Таблицы камер в соответствии с выбранным устройством хранения.
	Отображает соответствующую Таблицу камер. Настройки записи недоступны, поскольку запись с этих камер не осуществляется в BVMS.



Введите строку и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы. Отображаются только элементы, содержащие введенную строку, и их соответствующие родительские элементы (только в деревьях). Указывается число отфильтрованных элементов и совокупное число элементов. На

активный фильтр указывает значок . Для поиска точных фраз строки следует заключать в кавычки, например, в случае строки "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

Чтобы отменить фильтрацию, нажмите .

### 19.1 Страница Камеры



Главное окно >

**Камеры и запись** > нажмите значок, чтобы изменить страницу

"Камеры" в соответствии с требуемым устройством хранения, например

Отображает различную информацию о камерах, доступных в BVMS.

Позволяет изменять следующие свойства камеры:

- Название камеры
- Назначение источника аудиосигнала
- Логический номер
- управление PTZ
- Качество режима реального времени (VRM и Режим реального времени / Локальное хранилище)
- Профиль параметров записи
- Минимальное и максимальное время хранения
- Область интереса
- Automated Network Replenishment
- Двойная запись
- ▶ Щелкните заголовок столбца, чтобы отсортировать таблицу по этому столбцу.

**Камера - Кодер**

Отображает тип устройства.

**Камера - Камера**

Отображает название камеры.

**Камера - Сетевой адрес**

Отображает IP-адрес камеры.

**Камера - Местонахождение**

Отображает местонахождение камеры. Если камера еще не назначена логическому дереву, отображается надпись **Неназначенное местоположение**.

**Камера - Серия устройств**

Отображает название семейства устройств, к которому относится выбранная камера.

**Камера - Номер**

Щелкните ячейку для изменения логического номера, автоматически получаемого камерой при ее обнаружении. Если введен номер, который уже используется, появляется соответствующее сообщение об ошибке.

Логический номер "освобождается" после удаления камеры.

**Аудио**

Нажмите ячейку, чтобы назначить камере источник аудиосигнала.

Если срабатывает тревожное событие с низким приоритетом и камерой с настроенным аудиосигналом, этот аудиосигнал воспроизводится даже в том случае, когда на экране отображается тревожное событие с более высоким приоритетом. Это происходит только в том случае, если для тревожного события с более высоким приоритетом не настроен аудиосигнал.

**Поток 1 - Кодек / Поток 2 - Кодек (только VRM и локальное хранилище)**

Щелкните на ячейку для выбора необходимого кодека для кодирования потока.

**Поток 1 - Качество / Поток 2 - Качество**

Выберите требуемое качество потока, используемое при записи или трансляции в реальном времени. Настройка параметров качества осуществляется в диалоговом окне **Параметры качества потока**.

**Поток 1 - Активная платформа / Поток 2 - Активная платформа**

Отображает название параметров платформы в диалоговом окне **Параметры качества потока**. Этот столбец доступен только для чтения и указывает, какие параметры профиля будут записываться на кодер.

**Замечание!**

Это возможно только в том случае, если выбраны профили качества потока «тихий», «стандартный» или «оживленный».

Значение **Активная платформа** изменяется при изменении кодека выбранной камеры. Целевая скорость передачи данных регулируется автоматически, и отображается название параметров платформы.

**Видеоизображение в реальном времени - Поток (только VRM и режим реального времени, и локальное хранилище)**

Нажмите ячейку для выбора потока для VRM или кодера, работающего только в режиме реального времени или локального хранилища.

**Видеоизображение в реальном времени - Профиль (доступно только для камер ONVIF)**

Нажмите ячейку для выбора доступных ключей профиля реального режима этой камеры ONVIF.

Если выбирается элемент **<Автоматически>**, автоматически используется поток наивысшего качества.

**Видеоизображение в реальном времени - Область интереса ""**

Нажмите, чтобы включить Region of Interest (ROI). Это возможно, только если в столбце **Качество** выбран элемент H.264 MP SD ROI или H.265 MP SD ROI для потока 2, а поток 2 назначен режиму реального времени.

**Примечание.** Если поток 1 используется для режима реального времени для конкретной рабочей станции, клиент оператора, запущенный на этой рабочей станции, не может включить функцию ROI этой камеры.



автоматически включается в таблице .

**Запись - Параметр**

Нажмите ячейку для выбора требуемых параметров записи. Доступные параметры качества можно настроить в диалоговом окне **Настройки записи по расписанию**.

**Запись - Профиль (доступно только для камер ONVIF)**

Нажмите ячейку для выбора доступных ключей профиля записи этой камеры ONVIF. Выберите требуемый элемент.

**Запись - ANR**

Установите флажок для включения функции ANR. Эту функцию можно включить, только если кодер имеет соответствующую версию микропрограммного обеспечения и соответствующий тип устройства.

**Запись - Максимальная длительность до тревожного сигнала**

Отображает расчетную максимальную длительность записи до включения тревожного сигнала для этой камеры. Это значение может помочь в вычислении необходимого пространства для хранения на локальном носителе данных.

**Замечание!**

Если зеркальный диспетчер VRM уже настроен для кодера, невозможно изменить какие-либо настройки для этого кодера в столбцах **Вторичная запись**.

**Вторичная запись — Параметр (доступно, только если настроен вторичный VRM)**


Нажмите ячейку для назначения параметров записи по расписанию двойной записи этого кодера.

В зависимости от конфигурации при некоторых обстоятельствах настроенное качество потока для вторичной записи может не быть действительным. В таком случае вместо него используется качество потока, настроенное для основной записи.

#### **Вторичная запись - Профиль (доступно только для камер ONVIF)**

Нажмите ячейку для выбора доступных ключей профиля записи этой камеры ONVIF.



(отображается только после нажатия  **Все**)

Установите флажок для активации управления панорамированием, наклоном и увеличением камеры.

#### **Примечание.**

Сведения о параметрах порта см. в . COM1.

**Порт** (отображается только после нажатия  **Все**)

Щелкните ячейку, чтобы выбрать нужный последовательный порт кодера для управления панорамированием/наклоном/увеличением камеры. Для камеры PTZ, подключенной к системе Bosch Allegiant, можно выбрать **Allegiant**. Для такой камеры магистральная линия не требуется.

**Протокол** (отображается только после нажатия  **Все**)

Щелкните ячейку, чтобы выбрать нужный протокол для управления панорамированием/наклоном/увеличением камеры.

**Адрес PTZ** (отображается только после нажатия  **Все**)

Введите адрес для управления панорамированием/наклоном/увеличением камеры.

#### **Запись — Мин. время хранения [дни]**

##### **Вторичная запись — Мин. время хранения [дни] (только VRM и локальное хранилище)**

Щелкните ячейку и введите минимальное количество дней, в течение которых будут сохраняться видеоданные с этой камеры. Видеоизображения, записанные в течение этого периода времени, не будут автоматически удаляться.

#### **Запись — Макс. время хранения [дни]**

##### **Вторичная запись — Макс. время хранения [дни] (только VRM и локальное хранилище)**




Щелкните ячейку и введите максимальное количество дней, в течение которых будут сохраняться видеоданные с этой камеры. Автоматически будут удаляться только те видеоизображения, которые записаны ранее этого указанного периода времени. 0 = без ограничений.

#### **См.**

- *Настройка двойного режима записи в Таблице камер, Страница 311*
- *Настройка предустановленных положений и дополнительных команд, Страница 307*
- *Настройка параметров портов PTZ, Страница 307*
- *Настройка параметров качества потока, Страница 299*
- *Копирование и вставка в таблицы, Страница 297*
- *Настройка функции ANR, Страница 311*
- *Экспорт таблицы камер, Страница 298*
- *Назначение профиля ONVIF, Страница 312*
- *Настройка функции ROI, Страница 309*

## 19.2

**Страницы параметров записи (только сетевой видеорегистратор)**

Главное окно >  **Камеры и запись** >  > Перейдите на вкладку "Расписание записей" (например, )

Позволяет настраивать параметры записи для всех кодеров, назначенных сетевому видеорегистратору системы.

Настройка отображаемых расписаний записей производится на странице **Расписания**.

Описаны только те столбцы, которые не являются частью Таблицы камер.

- ▶ Щелкните заголовок столбца, чтобы отсортировать таблицу по этому столбцу.

**Непрерывная запись**

Щелкните ячейку в столбце **Качество** для отключения записи или выбора качества потока для потока 1.

В столбце  установите флажок для активации аудиосигнала.

**Запись в реальном времени/перед событием**

Щелкните ячейку в столбце **Качество**, чтобы выбрать качество потока для просмотра в реальном времени (требуется для немедленного воспроизведения) и для режима записи перед событием (необходимого для записи по тревоге и записи движущихся объектов) для потока 2. Если двухпоточковая передача данных активна на данном кодере, вы можете выбрать поток 1 для использования для записи в реальном времени или для записи перед событием.

В столбце  установите флажок для активации аудиосигнала.

**Запись движения**

Щелкните ячейку в столбце **Качество** для отключения записи или выбора качества потока для потока 1.

В столбце  щелкните ячейку для активации аудиосигнала.

Щелкните ячейку в столбце **Перед событием [с]** для выбора времени записи перед движением в секундах.

Щелкните ячейку в столбце **После события [с]** для выбора времени записи после движения в секундах.

**Запись по тревоге**

В столбце **Качество** нажмите на ячейку для выбора качества записи потока 1.

Для активации записи по тревоге нужно настроить соответствующий тревожный сигнал.

В столбце  установите флажок для активации аудиосигнала.

Щелкните ячейку в столбце **Перед событием [с]** для выбора времени перед тревожным сигналом в секундах.

Щелкните ячейку в столбце **После события [с]** для выбора времени после тревожного сигнала в секундах.

**См.**

- *Копирование и вставка в таблицы, Страница 297*
- *Настройка параметров записи (только Сетевой видеорегистратор), Страница 303*
- *Копирование параметров записи (только Сетевой видеорегистратор), Страница 310*



## 20




# Настройка камер и параметров записи



Главное окно > **Камеры и запись**

В данном разделе содержится информация о конфигурировании устройств в BVMS.

Вы можете настроить различные свойства камеры и параметры записи.

- Нажмите  для сохранения настроек.
- Нажмите  для отмены последней настройки.
- Нажмите  для активации конфигурации.

**См.**

- Страница Камеры, Страница 292
- Диалоговое окно Настройки записи по расписанию (только VRM и локальное хранилище), Страница 304
- Диалоговое окно Параметры качества потока, Страница 299
- Диалоговое окно «Предустановленные положения и дополнительные команды», Страница 309
- Диалоговое окно Копировать настройки записи (только сетевой видеорегистратор), Страница 310

### 20.1

## Копирование и вставка в таблицы

Можно одновременно настраивать многие объекты в таблице камер, таблице настройки событий или таблице настройки тревог.

Вы можете скопировать настраиваемые значения из табличной строки в другие строки:

- Копировать все значения из строки в другие строки.
- Копировать только одно значение из строки в другую строку.
- Копировать значение из одной ячейки в целый столбец.

Вы можете копировать значения двумя способами:

- Копирование значения в буфер обмена с последующей вставкой из него.
- Непосредственное копирование и вставка.

Вы можете выбрать, в какие строки вставлять скопированные значения:

- Вставка во все строки.
- Вставка в выделенные строки.

**Чтобы скопировать все настраиваемые значения из одной строки в другую:**

1. Щелкните правой кнопкой мыши нужные значения и выберите **Копировать строку**.
2. Щелкните заголовок строки, которую вы хотите изменить.  
Для выбора нескольких строк нажмите и удерживайте клавишу CTRL.
3. Щелкните таблицу правой кнопкой мыши и нажмите **Вставить**.  
Значения будут скопированы.

**Чтобы скопировать одно значение из одной строки в другую:**

1. Щелкните правой кнопкой мыши нужные значения и выберите **Копировать строку**.
2. Щелкните правой кнопкой мыши ячейку, которую вы хотите изменить, выберите **Вставить ячейку в** и нажмите **Текущая ячейка**.  
Значение будет скопировано.

**Чтобы скопировать все настраиваемые значения непосредственно:**

1. Щелкните заголовок строки, которую вы хотите изменить.  
Для выбора нескольких строк нажмите и удерживайте клавишу CTRL.
2. Щелкните правой кнопкой мыши нужные значения и выберите **Копировать строку в** и нажмите **Выбранные строки**.  
Значения будут скопированы.

**Чтобы скопировать одно значение непосредственно:**

1. Щелкните заголовок строки, которую вы хотите изменить.  
Для выбора нескольких строк нажмите и удерживайте клавишу CTRL.
2. Щелкните правой кнопкой мыши ячейку с нужным значением, выберите **Копировать ячейку в** и нажмите **Выделение в столбце**.  
Значение будет скопировано.

**Чтобы скопировать значение из одной ячейки во все остальные ячейки в данном столбце:**

- ▶ Щелкните правой кнопкой мыши ячейку с нужным значением, выберите **Копировать ячейку в** и нажмите **Заполнить столбец**.  
Значение будет скопировано.

**Чтобы скопировать строку:**

- ▶ Щелкните строку правой кнопкой мыши и нажмите **Добавить повторяющуюся строку**.  
Строка будет добавлена ниже под новым именем.

**См.**

- *Страница Камеры, Страница 292*
- *Диалоговое окно Настройки записи по расписанию (только VRM и локальное хранилище), Страница 304*
- *Страница События, Страница 313*
- *Страница Тревожные сигналы, Страница 319*

## 20.2

### Экспорт таблицы камер




Главное окно > **Камеры и запись**  
или



Главное окно > **Камеры и запись** > нажмите значок, чтобы изменить страницу




"Камеры" в соответствии с требуемым устройством хранения, например  Отображает различную информацию о камерах, доступных в BVMS. Таблицу камер можно экспортировать в файл CSV.

**Порядок выполнения экспорта:**


1. Щелкните в любом месте Таблицы камер правой кнопкой мыши и нажмите **Экспортировать таблицу...**
2. В диалоговом окне введите соответствующее имя файла.
3. Нажмите **Сохранить**.  
Выбранная Таблица камер экспортируется в файл CSV.

## 20.3 Настройка параметров качества потока

**Чтобы добавить элемент с параметрами качества потока:**

1. Нажмите  для добавления нового элемента в список.
2. Введите имя.

**Чтобы удалить элемент с параметрами качества потока:**

- ▶ Выберите элемент из списка и нажмите  для его удаления.  
Вы не можете удалить стандартные элементы.

**Чтобы переименовать элемент с параметрами качества потока:**

1. Выберите элемент из списка.
2. Введите новое имя в поле **Имя**.  
Вы не можете переименовать стандартные элементы.
3. Нажмите **ОК**.

**Чтобы настроить параметры качества потока:**

1. Выберите элемент из списка.
2. Установите необходимые параметры.



### 20.3.1 Диалоговое окно Параметры качества потока





Позволяет настраивать профили качества потока, которые затем можно назначить камерам на странице **Камеры и запись** или в диалоговом окне **Настройки записи по расписанию**.

Качество потока включает в себя разрешение видео, частоту кадров, максимальную полосу пропускания и видеосжатие.

**Качество потока**

 Выберите предварительно заданное качество потока и нажмите , чтобы добавить новое качество потока на основании предварительно заданного качества. При

выборе одного потока и нажатии  настройка качества этого потока копируется как узел верхнего уровня без дочерних элементов.

 Нажмите для удаления выбранного качества потока. Невозможно удалить параметры качества потока.

В этом списке приводятся все доступные предварительно заданные параметры качества потока. Рекомендуется назначать качество потока с таким же именем, что и у платформы камеры.

Для различных настроек качества потока доступны следующие профили:

**Image optimized:** параметры оптимизируются для обеспечения качества изображения. Это может увеличить нагрузку на сеть.

**Bit rate optimized:** параметры оптимизируются согласно низкой пропускной способности сети. Это может снизить качество изображения.

**Balanced:** эти параметры представляют собой компромисс между оптимальным качеством потока и оптимальной нагрузкой на сеть.

Доступны следующие профили для различных настроек качества потока, начиная с BVMS 9.0 для поддержки функции Intelligent Streaming камер Bosch:

Cloud optimized 1/8 FR: параметры оптимизируются для низкой полосы пропускания одинаково для всех типов камер.

PTZ optimized: параметры оптимизируются для камер PTZ.

Image optimized quiet / standard / busy

Bit rate optimized quiet / standard / busy

Balanced quiet / standard / busy

Категории типов сцен:

quiet: параметры оптимизируются для изображений с низкой активностью. 89 % — статичная сцена, 10 % — обычная сцена, 1 % — оживленная сцена.

standard: параметры оптимизируются для изображений со средней активностью. 54 % — статичная сцена, 35 % — обычная сцена, 11 % — оживленная сцена.

busy: параметры оптимизируются для изображения с высокой активностью. 30% статичная сцена, 55% оживленная сцена, 15% сцена со скоплением людей.

Значения в процентах указывают на распределение в течение дня.

По умолчанию назначен профиль Balanced standard.

**Замечание!**

Для каждой комбинации платформы камеры (CPP3-CPP7.3) и для каждого доступного разрешения существует отдельный параметр, позволяющий установить необходимую скорость передачи данных для камер.

Профиль и соответствующий тип сцены необходимо выбрать вручную для каждой камеры.

**Замечание!**

При обновлении установки новые профили необходимо выбрать вручную для их активации. Прежние профили сохраняются.

**Имя**

Отображает имя качества потока. При добавлении нового качества потока можно изменить имя.

**Разрешение SD-видео**

Выберите нужное видеоразрешение. Для качества HD задается качество SD для потока 2.

**Интервал кодирования изображений**

Переместите ползунок или введите соответствующее значение.

Система помогает вычислить соответствующее значение кадров/сек.

При помощи значения для интервала кодирования изображений вы настраиваете интервал, с которым изображения кодируются и передаются. Если введено значение 1, кодируются все изображения. Значение 4 означает, что кодируется только каждое четвертое изображение, а следующие три пропускаются — это может оказаться особенно полезным при низкой пропускной способности. Чем ниже пропускная способность, тем выше должно быть это значение для обеспечения видеоизображений наилучшего качества.

### Структура группы видеок кадров (GOP)

Выберите требуемую структуру для группы изображений (GOP). В зависимости от того, чему отдается больший приоритет — минимально возможной задержке (только для I-кадров) или использованию минимально возможной пропускной способности, — можно выбрать IP, IBP или IBBP. (Выбор GOP недоступен на некоторых камерах.)

#### Примечание.

V-кадры поддерживаются только камерами с разрешением от 1080 p и микропрограммой версии от 6.40.

### Объектная скорость передачи [кбит/с]

Переместите ползунок или введите соответствующее значение.

Можно ограничить скорость передачи данных для encoder, чтобы оптимизировать использование пропускной способности сети. Необходимая скорость передачи данных должна устанавливаться в соответствии с требуемым качеством изображения для стандартных сцен без излишнего движения.

Для сложных изображений или частых смен изображения в результате частого движения этот предел может быть временно увеличен до значения, которое можно ввести в поле

### Максимальная скорость передачи [кбит/с].

#### Максимальная скорость передачи [кбит/с]

Переместите ползунок или введите соответствующее значение.

Посредством данного значения вы устанавливаете максимальную скорость передачи, которая не может быть превышена.

Ограничение скорости устанавливается для того, чтобы иметь возможность надежного определения необходимого дискового пространства для хранения видеоданных.

В зависимости от настроек качества изображения для I-кадра и P-кадра это может привести к пропуску отдельных изображений.

Введенное здесь значение должно быть по крайней мере на 10% выше значения, указанного в поле **Объектная скорость передачи [кбит/с]**. Слишком низкое значение, введенное для этого параметра, будет автоматически изменено на допустимое.

### Расстояние между I-кадрами

Данный параметр позволяет установить интервалы, с которыми будут кодироваться I-кадры. Нажмите **Авто**, чтобы вставить I-кадры в случае необходимости. Значение 1 означает, что I-кадры генерируются непрерывно. Значение 2 означает, что только каждое второе изображение является I-кадром, значение 3 означает, что только каждое третье изображение является I-кадром и т.д. Все изображения, находящиеся между ними, кодируются как P-кадры.

### Уровень качества кадра

Здесь можно установить значение между 0 и 100 для I-кадров и P-кадров. Самое низкое значение приводит к наивысшему качеству и самой низкой частоте обновления кадров. Самое высокое значение приводит к самому низкому качеству изображения и наивысшей частоте обновления кадров.

Чем ниже пропускная способность, тем выше должен быть уровень качества для сохранения высокого качества видеоизображений.

#### Примечание.

Уровень качества настраивается в зависимости от движения и уровня детализации видеоизображения. Если установлены флажки **Авто**, оптимальное соотношение между движением и резкостью изображения настраивается автоматически.

### Параметры VIP X1600 XFM4

Позволяет настраивать следующие параметры H.264 для модуля кодера VIP X 1600 XFM4.

**Разблокирующий фильтр H.264** — выберите для повышения качества видеоизображения и эффективности прогнозирования путем сглаживания резких границ.

**Кодирование САВАС** — выберите для активации высокоэффективного сжатия. Использует большой объем вычислительной мощности.

См.

– *Настройка параметров качества потока, Страница 299*

## 20.4 Настройка свойств камеры

Главное окно >  **Камеры и запись** > 

**Чтобы изменить свойства камеры:**

1. Выберите ячейку в столбце **Камера** и введите новое имя камеры. Это имя будет отображаться в других местах, в которых упоминается эта камера.
2. Установите соответствующие параметры в других столбцах.

Для получения подробной информации о различных полях щелкните ссылку на соответствующее окно приложения ниже.

См.



– *Страница Камеры, Страница 292*

## 20.5 Настройка параметров записи (только VRM и Локальное хранилище)

Главное окно > >  **Камеры и запись** 


Можно настроить параметры записи для всех устройств, которые добавлены к VRM в дереве устройств.

**Примечание:** при записи убедитесь, что соответствующий VRM или локальное хранилище настроены правильно.


VRM: **Устройства** > Разверните  > 

Локальное хранилище: **Устройства** > Разверните  > 

**Добавление элемента, содержащего параметры записи.**

1. Нажмите  для добавления нового элемента в список.
2. Введите имя.

**Удаление элемента, содержащего параметры записи.**

- ▶ Выберите элемент из списка и нажмите  для его удаления. Вы не можете удалить стандартные элементы.

**Переименование элемента, содержащего параметры записи.**

1. Выберите элемент из списка.
2. Введите новое имя в поле **Имя:**. Вы не можете переименовать стандартные элементы.
3. Нажмите **ОК**.

**Чтобы настроить параметры записи:**

1. Выберите элемент из списка.
2. Установите подходящие параметры и нажмите **ОК**.



3. Нажмите  или .


4. В столбце **Запись** выберите необходимые параметры записи для каждого кодера. Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

**См.**

- Диалоговое окно Настройки записи по расписанию (только VRM и локальное хранилище), Страница 304



**20.6****Настройка параметров записи (только Сетевой видеорегистратор)**

Главное окно >  **Камеры и запись** > Нажмите  > Перейдите на вкладку

Расписание записей (например, )

Прежде чем настраивать параметры записи, настройте уровни качества потока.

**Примечание.** Перед началом записи следует настроить соответствующий сетевой

видеорегистратор (**Устройства** > Разверните вкладку  >  > **Запоминающее устройство на диске**).



**Замечание!**

Все кодеры используют параметры режима реального времени для записи перед событием.



Для кодеров, использующих двухпоточный режим, параметры записи в реальном времени / записи перед событием, записи по движению и записи по тревоге настраиваются индивидуально.

В кодерах, поддерживающих только однопоточный режим (напр., VideoJet 8004), при воспроизведении и записи в реальном времени используется один и тот же поток. В этом случае приоритет имеют параметры записи, поэтому при просмотре в реальном времени используются параметры качества потока для непрерывной записи, записи по движению и записи по тревоге. Параметры режима реального времени/записи перед событием могут быть изменены только в том случае, если отключена непрерывная запись.







Поток реального времени можно переключить с потока 2 (по умолчанию) на поток 1 для

рабочей станции (**Устройства** > разверните  >  > вкладка **Настройки** > **Переопределить настройки со страницы "Камеры и запись"**) или для кодера. Этот параметр не оказывает влияния на запись перед событием.

**Чтобы настроить параметры записи:**

1. В столбце  **Непрерывная запись** выберите нужное качество потока или отключите непрерывную запись.
2. В столбце  установите флажок для активации аудиосигнала.



3. В столбце  **Запись в реальном времени/перед событием** выберите нужное качество потока или выберите поток 1.
4. В столбце  установите флажок для активации аудиосигнала.
5. В столбце  **Запись движения** выберите нужное качество потока или отключите запись по движению.
6. В столбце  установите флажок для активации аудиосигнала.
7. Нажмите ячейку в столбце **Перед событием [с]** и введите соответствующий интервал времени.
8. Нажмите ячейку в столбце **После события [с]** и введите соответствующий интервал времени.
9. В столбце  **Запись по тревоге** выберите нужное качество потока или отключите запись по тревоге.
10. В столбце  установите флажок для активации аудио.
11. Нажмите ячейку в столбце **Перед событием [с]** и введите соответствующий интервал времени.
12. Нажмите ячейку в столбце **После события [с]** и введите соответствующий интервал времени.

**Замечание!**

Если время перед событием для записи по движению отличается от времени перед событием для записи по тревоге, для обоих параметров используется большее значение. Если установленное время перед событием накладывается на предшествующую запись по движению или запись по тревоге, запись перед событием начинается по завершении предшествующей записи.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

**См.**

– *Страница Камеры, Страница 292*

**20.7****Диалоговое окно Настройки записи по расписанию (только VRM и локальное хранилище)**

Главное окно >

**Камеры и запись** >

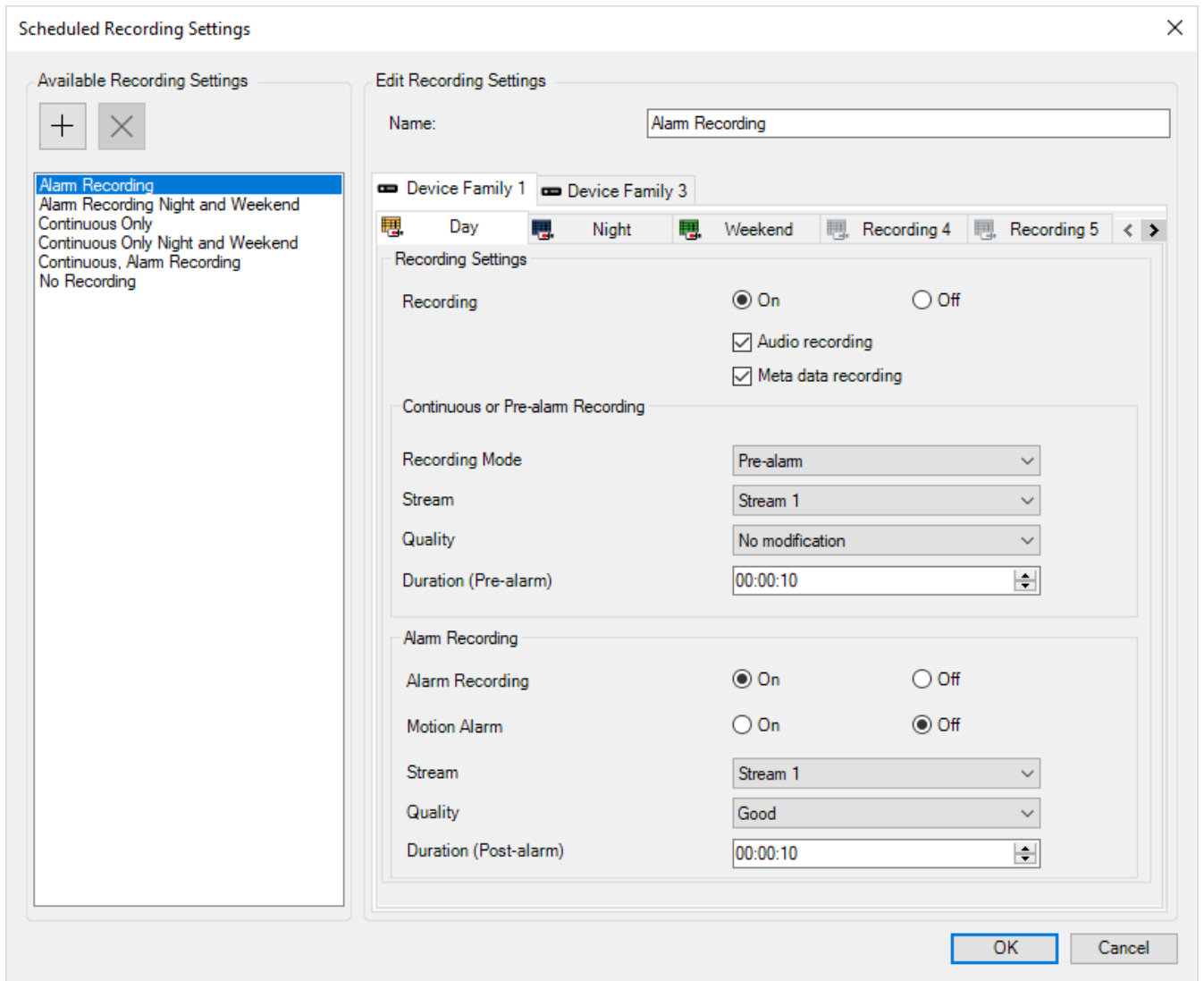


Позволяет настроить зависящие от расписания параметры записи для каждой доступной серии устройств. Серия устройств доступна, если в Дерево устройств добавлен хотя бы один кодер данной серии устройств. В таблице **Камеры** такие параметры записи назначаются каждой камере.

Используются Расписания записей, настроенные на странице **Расписания**.

**Примечание.** Включение или отключение обычной записи действительно для всех серий устройств.





### Доступные настройки записи

Выберите предварительно заданную настройку записи для изменения ее параметров. Можно добавлять и удалять заданные пользователем настройки.

### Имя:

Введите имя файла для новой настройки записи.



Выберите требуемое семейство устройств для настройки параметров записи, действительных для этого семейства устройств.



Для выбранного семейства устройств выберите расписание записи для настройки параметров записи.

### Запись

Включите или отключите стандартную запись (непрерывную или до сигнала тревоги).

### Запись аудио

Выберите, нужно ли записывать звук.

### Запись метаданных

Выберите, нужно ли записывать метаданные.

**Режим записи**

Выберите требуемый режим записи.

Доступны следующие параметры:

- **Непрерывно**
- **До тревоги**

**Поток**

Выберите требуемый поток, используемый для стандартной записи.

**Примечание.** Доступность потоков зависит от серии устройства.

**Качество**

Выберите требуемое качество потока, используемое для стандартной записи. Параметры качества доступны для настройки в диалоговом окне **Параметры качества потока**.

**Длительность (до тревоги)**

Введите необходимое время записи до тревожного сигнала. Введите время в формате чч:мм:сс.

**Примечание.** Включено, только если выбран пункт **До тревоги**.

**Замечание!**

Для значений времени перед тревожным сигналом от 1 до 10 с данные до тревожного сигнала хранятся в ОЗУ кодера, если в ОЗУ достаточно места, в противном случае они передаются в хранилище.

Для значений времени перед тревожным сигналом более 10 с данные до тревожного сигнала передаются в хранилище.

Хранение данных до тревожного сигнала в ОЗУ кодера доступно только для версий микропрограммного обеспечения 5.0 и выше.

**Запись по тревоге**

Позволяет включать и отключать запись по тревоге для этой камеры.

**Тревожный сигнал движения**

Позволяет включать и отключать запись по тревоге, запускаемую датчиком движения.

**Поток**

Выберите поток, который будет использоваться для записи по тревоге.

**Примечание.** Доступность потоков зависит от серии устройства.

**Качество**

Выберите требуемое качество потока, используемое для записи по тревоге. Параметры качества доступны для настройки в диалоговом окне **Параметры качества потока**.

Только для устройств, относящихся к семейству устройств 2 или 3: если выбран элемент **Без изменения**, для записи по тревоге используется такое же качество, как и для записи до срабатывания тревоги или непрерывной записи. Рекомендуется использовать значение **Без изменения**. При выборе качества потока для записи по тревоге изменяются только интервал кодирования изображений и скорость передачи в соответствии с параметрами качества данного потока. Используются другие параметры качества, которые настроены для профиля качества, назначенного непрерывной записи или записи до тревожного сигнала.

**Длительность (после тревоги)**





Введите необходимое время записи по тревоге. Введите время в формате чч:мм:сс.




**См.**

- *Копирование и вставка в таблицы, Страница 297*

– *Настройка параметров записи (только VRM и Локальное хранилище), Страница 302*

## 20.8 Настройка параметров портов PTZ

Главное окно >  **Устройства** > Разверните  > Разверните  >  >  
 Вкладка **Интерфейсы** > Вкладка **Периферия**

Главное окно >  **Устройства** >  >  > Вкладка **Интерфейсы** > Вкладка **Периферия**

Вы можете настраивать параметры порта только для кодера, на котором активировано управление камерой.

При замене кодера или камеры PTZ настройки порта не сохраняются. Их необходимо настроить снова.

После обновления микропрограммы проверьте настройки порта.

### Чтобы настроить параметры порта кодера:

- ▶ Внесите необходимые изменения в настройки.  
Изменения в настройках вступают в силу сразу после их сохранения. Активировать конфигурацию нет необходимости.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

## 20.9 Настройка предустановленных положений и дополнительных команд

Главное окно >  **Камеры и запись** > 

Для PTZ-камер, камер с функцией ROI и панорамных камер можно заранее определять и сохранять положения камеры. Для PTZ-камер также можно определять дополнительные команды.

**Примечание.** Для настройки параметров PTZ-камеры сначала необходимо настроить параметры ее порта. В противном случае управление PTZ в данном диалоговом окне работать не будет.

### Для настройки предустановленного положения:

1. В таблице **Камеры** выберите нужный кодер.
2. Только для PTZ-камер: чтобы активировать управление PTZ-камерой, установите

флажок в столбце .

3. Нажмите кнопку .
- Отобразится диалоговое окно **Препозиции и вспомогательные команды**.

4. Можно определить требуемое количество предустановленных положений.


5. Выберите положение, которое нужно задать.

6. В окне предварительного просмотра с помощью мыши перейдите к положению, которое нужно настроить.

Изображение можно увеличивать или уменьшать с помощью колесика мыши и можно перемещать путем перетаскивания.

7. При необходимости введите имя для настроенного положения.


8. Нажмите , чтобы сохранить предустановленное положение.


**Примечание.** Значок  нужно нажимать для каждого предустановленного положения. Иначе положение не сохранится.

9. Нажмите **ОК**.

**Чтобы отобразить уже настроенные предустановленные положения:**

1. В таблице **Камеры** выберите нужный кодек.

2. Нажмите кнопку .  
Отобразится диалоговое окно **Препоозиции и вспомогательные команды**.
3. Выберите соответствующее положение.

4. Нажмите .  
В окне предварительного просмотра отобразится предустановленное положение камеры.

**Примечание.**

В случае PTZ-камер и камер с функцией ROI предустановленные положения хранятся непосредственно в самой камере. Что касается панорамных камер, то предустановленные положения хранятся в системе BVMS.

PTZ-камеры физически перемещаются в предустановленное положение. Панорамные камеры и камеры с функцией ROI не перемещаются, а лишь отображают некоторый фрагмент полного изображения с камеры.


**Для настройки дополнительных команд для PTZ-камер:**

1. В таблице **Камеры** выберите нужный кодек.

2. Нажмите кнопку .  
Отобразится диалоговое окно **Препоозиции и вспомогательные команды**.

3. Откройте вкладку **Aux Commands**.




4. Задайте необходимые настройки.

5. Для сохранения предустановленных команд нажмите .  
Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

**См.**

- Диалоговое окно «Предустановленные положения и дополнительные команды», Страница 309
- Настройка параметров портов PTZ, Страница 307
- Настройка тревоги, Страница 333
- Диалоговое окно Выбрать содержимое Области изображений, Страница 321
- Диалоговое окно Параметры тревог, Страница 323
- Диалоговое окно «Выбрать содержимое области изображений» (MG), Страница 322



## 20.10 Диалоговое окно «Предустановленные положения и дополнительные команды»

Главное окно >  **Камеры и запись** >  > выберите PTZ-камеру, камеру с функцией ROI или панорамную камеру > 

Позволяет настроить PTZ-камеру, камеру с функцией ROI или панорамную камеру. Для камер с функцией ROI и панорамных камер дополнительные команды недоступны.

**Примечание.** Для настройки параметров PTZ-камеры сначала необходимо настроить параметры ее порта. В противном случае управление PTZ в данном диалоговом окне работать не будет.

### Значки

	Нажмите для перемещения камеры в предустановленное положение или для выполнения команды.
	Нажмите для сохранения предустановленного положения или команды.

### Вкладка Препозиции

Нажмите для отображения таблицы predetermined positions.

### Номер

Отображает номер predetermined position.

### Имя

Щелкните ячейку для изменения имени predetermined position.

### Вкладка Aux Commands (только для камер PTZ)

Нажмите для отображения таблицы вспомогательных команд.

**Примечание.** Если кодек ONVIF поддерживает вспомогательные команды, они предоставляются непосредственно из кодера ONVIF.

### Номер

Отображает номер вспомогательной команды.

### Имя

Щелкните ячейку для изменения имени вспомогательной команды.




### Код

Щелкните ячейку для редактирования кода команды.

### См.

- *Настройка параметров портов PTZ, Страница 307*
- *Настройка предустановленных положений и дополнительных команд, Страница 307*

## 20.11 Настройка функции ROI

Главное окно >  **Камеры и запись** >  >   
 Можно включить функцию ROI для фиксированной камеры HD.

Необходимо настроить поток 2 для видео в реальном времени и необходимо настроить кодек H.264 MP SD ROI или H.265 MP SD ROI для потока 2.  
Убедитесь, что поток 2 используется для видео в реальном времени на всех рабочих станциях, где будет использоваться ROI.

#### Включение функции ROI.

1. В столбце **Поток 2 - Кодек** выберите необходимый кодек H.264 MP SD ROI или H.265 MP SD ROI.
2. В столбце **Видеоизображение в реальном времени - Поток** выберите **Поток 2**.
3. Установите флажок в столбце **Видеоизображение в реальном времени - Область интереса ""**.

#### Отключение функции ROI.

1. Снимите установленный флажок в столбце **Видеоизображение в реальном времени - Область интереса ""**.
2. В столбце **Поток 2 – Кодек** выберите необходимый кодек.

См.

– *Страница Камеры, Страница 292*

## 20.12

### Копирование параметров записи (только Сетевой видеорегистратор)



Главное окно > **Камеры и запись** > Нажмите значок записывающего устройства



(например, ) > Перейдите на вкладку "Расписание записей" (например, )



Вы можете скопировать параметры записи из одного расписания записей в другое.

#### Чтобы скопировать параметры записи из выделенной строки таблицы:

1. Выберите строку таблицы с нужными параметрами записи.
2. Нажмите . Отображается диалоговое окно **Копировать настройки записи** .
3. Выберите из списка расписание записей, в которое вы хотите скопировать параметры.
4. Нажмите **Копировать текущее выделение**.
5. Нажмите **ОК**. Параметры записи выделенной строки таблицы будут скопированы.

#### Чтобы скопировать все параметры записи из расписания записей:

1. Нажмите . Отображается диалоговое окно **Копировать настройки записи** .
2. Выберите из списка расписание записей, в которое вы хотите скопировать параметры.
3. Нажмите **Копировать все**.
4. Нажмите **ОК**. Параметры записи всех строк таблицы будут скопированы.

### 20.12.1

#### Диалоговое окно Копировать настройки записи (только сетевой видеорегистратор)



Главное окно > **Камеры и запись** > Нажмите значок записывающего устройства



(например, ) > Перейдите на вкладку "Расписание записей" (например, ) >



Позволяет копировать параметры записи из одного расписания записей в другое.

**Копировать все**

Нажмите для копирования всех параметров записи из выбранного расписания в другое расписание.

**Копировать текущее выделение**

Нажмите для копирования параметров записи, содержащихся в выделенных строках таблицы, в другое расписание.

## 20.13 Настройка функции ANR



Главное окно > **Камеры и запись** >

Перед включением функции ANR необходимо добавить носитель данных кодера требуемому кодеру и настроить этот носитель данных.

Для настройки функции ANR необходимо отключить двойную запись кодера.

Функция ANR работает только на кодерах с версией микропрограммного обеспечения 5.90 и выше. Не все типы кодеров поддерживают ANR, даже если установлена верная версия микропрограммного обеспечения.

**Для включения:**

- ▶ Установите флажок в строке требуемой камеры в столбце **ANR**.

**См.**

- *Настройка двойного режима записи в Таблице камер, Страница 311*
- *Страница Камеры, Страница 292*
- *Настройка носителей данных кодера, Страница 238*

## 20.14 Настройка двойного режима записи в Таблице камер



Главное окно > **Камеры и запись** >

Для настройки двойной записи функцию ANR необходимо отключить.

Если выполняется настройка двойной записи для одной камеры многоканального кодера, система следит за тем, чтобы все камеры этого кодера были настроены на один и тот же получатель записи.

**Для настройки:**

1. В столбце **Вторичная запись - Целевой объект** выберите ячейку требуемого кодера, а затем нажмите требуемый пул вторичного VRM.  
Все камеры соответствующего кодера автоматически настраиваются на запись в выбранный вторичный VRM.
2. В столбце **Параметр** выберите параметр записи по расписанию.

**См.**

- *Настройка двойного режима записи в Дереве устройств, Страница 197*
- *Настройка функции ANR, Страница 311*
- *Двойная / резервная запись, Страница 26*
- *Страница Камеры, Страница 292*

## 20.15 Управление шлюзом Video Streaming Gateway

**См.**

- Страница устройства Video Streaming Gateway, Страница 208
- Диалоговое окно "Добавить кодер Bosch", Страница 212
- Диалоговое окно "Добавить кодер ONVIF", Страница 213
- Диалоговое окно "Добавить камеру JPEG", Страница 215
- Диалоговое окно "Добавить кодер RTSP", Страница 216

### 20.15.1 Назначение профиля ONVIF



Главное окно > **Камеры и запись** >

Можно назначить ключ медиапрофиля ONVIF камере ONVIF.

Ключ можно назначить либо для видео в реальном времени, либо для записи.

**Назначение ключа для видео в реальном времени.**

- ▶ В столбце **Видеоизображение в реальном времени – Профиль** выберите необходимый элемент.

**Назначение ключа для записи.**

- ▶ В столбце **Запись – Профиль** выберите необходимый элемент.

**См.**

- Страница Камеры, Страница 292



## 21

## Страница События



Главное окно > **События**

Отображает дерево событий со всеми доступными событиями и таблицей настройки событий для каждого события. События сгруппированы по типу, например все события записи с камер, такие как непрерывная запись или запись по тревоге, сгруппированы по режиму записи.


Доступные события сгруппированы по соответствующим устройствам. Изменение

состояния устройства отображается под значком  в виде . Все другие события

отображаются в зависимых от устройства группах в виде .

Для каждого события могут быть настроены:

- Включение тревоги в соответствии с расписанием (доступно не для всех событий).
- Регистрация события в журнале в соответствии с расписанием. Если событие зарегистрировано в журнале, оно отображается в списке событий Operator Client.
- Выполнение командного сценария в соответствии с расписанием (доступно не для всех событий).

– Для событий типа : добавление текстовых данных к записи.

Если событие происходит, ваши настройки выполняются.

При помощи логических выражений вы можете создать сложное событие, объединяющее несколько событий.

- ▶ Щелкните элемент дерева для отображения соответствующей таблицы настройки событий.



Нажмите для дублирования события. Используйте это для генерирования нескольких тревожных сигналов для определенного события.



Нажмите для удаления дублированного или сложного события.



Нажмите для переименования выбранного сложного события.



Нажмите, чтобы отобразить диалоговое окно для создания при помощи логических выражений сложного события, состоящего из других событий (максимум 10).

Сложные события добавляются в таблицу настройки события.




Нажмите для редактирования выбранного сложного события.



Нажмите, чтобы отобразить диалоговое окно для создания и редактирования командных сценариев.



Введите строку и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы. Отображаются только элементы, содержащие введенную строку, и их соответствующие родительские элементы (только в деревьях). Указывается число отфильтрованных элементов и совокупное число элементов. На

активный фильтр указывает значок . Для поиска точных фраз строки следует заключать в кавычки, например, в случае строки "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

Чтобы отменить фильтрацию, нажмите .

**См.**

- *Настройка событий и тревог, Страница 328*
- *Настройка командных сценариев, Страница 93*
- *Диалоговое окно «Параметры» (меню «Настройки»), Страница 118*
- *Настройка мигающих активных точек, Страница 336*

## 21.1

### Вкладка "Настройки задержки"

**Примечание:** для некоторых событий вкладка "Параметры задержки" недоступна из-за технических ограничений.

Позволяет настроить параметры задержки для выбранного события.

#### Время задержки

В течение указанного периода времени все дальнейшие события игнорируются.

#### Приоритет состояния события

Состоянию события можно назначить настройку приоритета.

#### Изменить приоритеты

Нажмите, чтобы отобразить диалоговое окно для настройки параметров приоритета.

#### Добавить параметр

Нажмите для добавления строки для настройки времени задержки, которое отличается от времени задержки всех устройств.

#### Удалить параметр

Нажмите, чтобы удалить выделенную строку. Для выбора строки нажмите левый заголовок строки.


## 21.2

### Вкладка "Настройки" для расширенного отображения карты

Настройка цвета состояний на картах возможна, только если установлен флажок

**Включить расширенное отображение состояний (цвет активных точек на картах в зависимости от состояния)** или флажок **Включить расширенное отображение тревог (цвет активных точек на картах в зависимости от тревоги)** в диалоговом окне

#### Параметры.


Для каждого события или тревоги (  ) можно настроить цвет фона и поведение активных точек (мигает или не мигает). Например, можно настроить событие или тревогу

 устройства так, чтобы его значок устройства на карте начинал мигать при изменении состояния этого устройства.

Кроме того, можно настроить приоритет отображения для всех активных точек. Это необходимо, если для одного устройства возникают различные события. (1 = наивысший приоритет)

Настроенный цвет действует для всех активных точек с одинаковым приоритетом отображения. Можно изменить цвет, поведение и приоритет для любого события или

тревоги  : изменение цвета и поведения используется для всех активных точек всех

остальных событий или тревог  , имеющих такой же приоритет.

#### **Включить цвет состояний на картах**

Нажмите, чтобы активные точки устройств, принадлежащих этому событию, отображались с цветным фоном и могли мигать на картах.

#### **Приоритет отображения на карте:**

Щелкайте стрелки, чтобы изменять приоритет активных точек устройств, принадлежащих этому событию.

#### **Цвет фона на карте:**

Нажмите поле цвета, чтобы выбрать цвет фона, используемый для активных точек устройств, принадлежащих этому событию.

**Примечание.** Все события состояния всех устройств с одинаковым приоритетом имеют один и тот же цвет.

#### **Мигание**

Нажмите, чтобы включить мигание активных точек устройств, принадлежащих этому событию.

## 21.3

## **Вкладка "Настройки" для конфигурации событий**

### **Устройство**

Отображает имя устройства или расписания.

### **Сеть**

Отображает IP-адрес соответствующего IP-устройства.

### **Активировать тревогу**

Нажмите ячейку, чтобы выбрать расписание записей или задач для активации тревоги. Выберите **Всегда**, если нужно, чтобы тревога была активирована независимо от момента времени.

Выберите **Никогда**, если не нужно активировать тревогу.

### **Журнал**

Нажмите ячейку в столбце **Расписание**, чтобы выбрать расписание записей или задач для регистрации в журнале.

Выберите **Всегда**, если хотите, чтобы событие было зарегистрировано независимо от момента времени.

Выберите **Никогда**, если не нужно регистрировать событие.

### **Сценарий**

Нажмите ячейку в столбце **Сценарий**, чтобы выбрать командный сценарий.

Нажмите ячейку в столбце **Расписание**, чтобы выбрать расписание записей или задач для выполнения командного сценария.

Выберите **Всегда**, если нужно, чтобы командный сценарий был выполнен независимо от момента времени.

Выберите **Никогда**, если не нужно выполнять командный сценарий.

### **Запись текстовых данных**

Можно настроить добавление текстовых данных к непрерывной записи камеры.

**Примечание.** Этот столбец доступен только для событий, содержащих текстовые данные, например **Устройства ATM/POS > Вход банкомата > Ввод данных**

## 21.4 Диалоговое окно Редактор командных сценариев

Главное окно >  **События** > 

Позволяет создавать и редактировать командные сценарии.



Нажмите для сохранения измененных настроек.



Нажмите для восстановления сохраненных настроек.



Нажмите для проверки кода сценария.



Нажмите для создания файла команды.



Нажмите для удаления файла команды.



Нажмите, чтобы отобразить диалоговое окно для импорта файла сценария.



Нажмите, чтобы отобразить диалоговое окно для экспорта файла сценария.



Нажмите для преобразования существующего сценария в другой доступный язык сценария. Все существующие тексты сценариев удаляются.



Нажмите для отображения интерактивной справки BVMS Script API.



Нажмите для отображения интерактивной справки BVMS.



Нажмите для закрытия диалогового окна **Редактор командных сценариев**.

**См.**


– *Настройка командных сценариев, Страница 93*

## 21.5 Диалоговое окно Создать сложное событие / Редактировать сложное событие

Главное окно >  **События** > 

Позволяет создавать и изменять сложные события.



Введите строку и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы. Отображаются только элементы, содержащие введенную строку, и их соответствующие родительские элементы (только в деревьях). Указывается число отфильтрованных элементов и совокупное число элементов. На активный фильтр указывает значок . Для поиска точных фраз строки следует заключать в кавычки, например, в случае строки "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

Чтобы отменить фильтрацию, нажмите .

**Имя события:**

Введите нужное имя сложного события.

**Состояния событий:**

Выберите изменение состояния, которое должно стать частью сложного события.

**Объекты:**

Выберите один или несколько доступных объектов выбранного состояния события. Это состояние и выбранный объект отображаются в дереве сложных событий как непосредственный дочерний элемент корневого оператора.

**Сложное событие:**

Позволяет создавать сложные события в дереве сложных событий. Все непосредственные дочерние элементы логического оператора (AND, OR) объединяются этим оператором.

**См.**

- *Создание сложного события, Страница 332*
- *Редактирование сложного события, Страница 333*

## 21.6

### Диалоговое окно Выберите язык сценария



Главное окно > **События** >

Позволяет выбрать язык для вашего командного сценария.

Вы не можете изменить язык существующих командных сценариев.

**Язык сценария:**

Выберите нужный язык сценария.

**См.**

- *Настройка командных сценариев, Страница 93*

## 21.7

### Диалоговое окно Изменение приоритетов типа события



Главное окно > **События** > вкладка **Параметры задержки** > **Изменить приоритеты** кнопка

Можно настроить приоритеты разных изменений состояния типа событий (если применимо), например "Виртуальных вход закрыт" и "Виртуальный вход открыт".

Изменение состояния с более высоким приоритетом переопределяет время задержки другого изменения состояние с более низким приоритетом.

**Название приоритета:**

Введите название для данного параметра приоритета.

**Значение состояния**

Отображаются названия состояний выбранного события.

**Приоритет состояния:**

Введите требуемый приоритет. 1=наивысший приоритет, 10=самый низкий приоритет.



## 21.8 Диалоговое окно Выбор устройств

Главное окно >  **События** >  или  > вкладка **Настройки задержки** > кнопка **Добавить параметр**

### Выбрать

Установите данный флажок для требуемой записи и нажмите **ОК**, чтобы добавить строку в таблицу **Устройства со специальными параметрами задержки**.

## 21.9 Диалоговое окно "Запись текстовых данных"

Главное окно >  **События** > в дереве событий выберите  **Ввод данных** (текстовые данные должны быть доступны, например **Устройства чтения кредитных карточек** > **Устройство чтения кредитных карточек** > **Карта отклонена**) > столбец **Запись текстовых данных** > ...

Можно настроить камеры, для которых к непрерывной записи камеры будут добавляться текстовые данные.

### См.

- *Включение записи по тревоге с помощью текстовых данных, Страница 335*

## 22

## Страница Тревожные сигналы



Главное окно > **Тревожные сигналы**

Отображает дерево событий и таблицу настройки тревог для каждого события.

Отображаются только те события, которые настроены на странице **События**.

В таблицах вы можете настроить, каким образом будет отображаться тревожный сигнал, вызванный данным событием, а также, какие камеры будут вести запись и отображаться при срабатывании данного тревожного сигнала.

Некоторые события настроены как тревожные сигналы по умолчанию, например, системная ошибка.

Вы можете настроить тревожный сигнал для следующих событий:

- Изменение режима записи
- Изменение состояния тревожного сигнала
- Большинство пользовательских действий, например, действия по управлению камерами PTZ




Нажмите для отображения диалогового окна **Диспетчер ресурсов**.



Отображает диалоговое окно настройки параметров тревоги, действующих на этом сервере Management Server.



Введите строку и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы. Отображаются только элементы, содержащие введенную строку, и их соответствующие родительские элементы (только в деревьях). Указывается число отфильтрованных элементов и совокупное число элементов. На активный фильтр указывает значок . Для поиска точных фраз строки следует заключать в кавычки, например, в случае строки "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

Чтобы отменить фильтрацию, нажмите .

- ▶ Щелкните элемент дерева для отображения соответствующей таблицы настройки тревожного сигнала.

#### Устройство

Отображает устройство условия события, выбранного в дереве событий.

#### Сетевой адрес

Отображает IP-адрес соответствующего IP-устройства.

#### Устройство

Щелкните в ячейке в столбце **Приоритет** и введите приоритет тревожного сигнала для выбранной тревоги (**100** - низкий, **1** - высокий). Щелкните в ячейке в столбце **Название** и введите название тревожного сигнала, которое будет отображаться в BVMS, например в списке тревог. Щелкните в ячейке в столбце **Цвет**, чтобы отобразить диалоговое окно для выбора цвета, которым будет отображаться тревожный сигнал в Operator Client, например в списке тревог.

#### Идентификатор тревоги

Щелкните ... в ячейке в одном из столбцов **1-5** для отображения диалогового окна выбора камеры.

Можно выбрать только ту камеру, которая была добавлена в логическое дерево на странице **Карты и структура**.

Можно настроить количество доступных областей изображений тревог в диалоговом окне **Настройки тревог**.

Щелкните ... в ячейке в столбце **Аудиофайл**, чтобы отобразить диалоговое окно для выбора аудиофайла, воспроизводимого в случае тревоги.

#### Параметры тревог

Нажмите ... в ячейке для отображения диалогового окна **Параметры тревог**.

См.

– *Обработка сигналов тревоги, Страница 35*

## 22.1

### Диалоговое окно Настройки тревог

Главное окно >  Тревожные сигналы > 

#### Вкладка Настройки тревог

##### Макс. количество областей изображений на тревогу:

Введите максимальное количество Областей изображений тревог, которое будет отображаться в случае тревоги.

##### Время автоматического отключения:

Введите время в секундах, через которое тревожное событие будет автоматически отключено.

Это относится только к тревожным сигналам, для которых на странице **Тревожные сигналы** задано значение **Автоотключение тревоги по истечении определенного времени (диалоговое окно 'Настройки тревог')**.

##### Многострочное отображение тревоги в окне изображений тревог

Установите флажок, чтобы включить режим многострочных тревог окна тревожных изображений.



#### Замечание!

Для существующих конфигураций тревог режим многострочных тревог активирован; для новой конфигураций тревог он отключен по умолчанию, при этом активирован одноэкранный режим.

#### Настроить лимит продолжительности записи тревог, вызванных состояниями:

Установите флажок, чтобы включить ограничение длительности записей по тревоге. Введите длительность записи по тревоге в минутах. Запись по тревоге останавливается автоматически по истечении установленного времени.

Пользователь может ввести длительность от 1 до 1440 минут.

Когда тревожное событие инициирует запись с настроенным ограничением длительности:

- если тревожное событие повторно активируется до истечения времени ожидания, запись продолжается, а время ожидания начинается с 0;
- если тревогу отменяют до истечения времени ожидания, запись продолжается в течение настроенного времени ожидания после тревоги.



### Вкладка Группы мониторов

#### Порядок отображения в случае одинакового приоритета тревог

Выберите нужное значение для сортировки сигналов тревоги с одним приоритетом в соответствии с их меткой времени.

#### Отображать пустой экран

Нажмите, чтобы на мониторе, не используемом в качестве экрана тревожных сигналов, не отображалось ничего.

#### Продолжать отображение в режиме реального времени




Нажмите, чтобы на мониторе, не используемом в качестве экрана тревожных сигналов, отображалось изображение в реальном времени.

См.

– *Настройка параметров для всех тревог, Страница 334*

## 22.2

### Диалоговое окно Выбрать содержимое Области изображений

Главное окно >  Тревожные сигналы >  или  > столбец **Области изображений тревог** > нажмите ... в одном из столбцов **1-5**

Позволяет выбирать элемент логического дерева, который отображается и записывается (если элементом является камера) в случае возникновения выбранного тревожного события.



#### Замечание!

Изображение карты в области тревожных изображений оптимизировано для отображения на экране и содержит только исходный вид оригинального файла карты.

#### Найти элемент

Введите текст для поиска элемента в логическом дереве.

#### Найти

Нажмите для поиска камеры по введенному тексту в ее описании.

#### Режим реального времени

Нажмите, чтобы указать, что в случае тревоги должно отображаться живое видео с камеры.

#### Немедленное воспроизведение

Нажмите, чтобы указать, что должно отображаться немедленное воспроизведение с камеры.

Время перемотки для тревоги при немедленном воспроизведении настраивается на странице **Функции оператора** (см. раздел *Страница Свойства оператора, Страница 351*).

#### Приостановить воспроизведение

Установите этот флажок для отображения приостановленного немедленного воспроизведения тревожного события с камеры. Пользователь при необходимости может запустить немедленное воспроизведение вручную.

#### Закольцованное воспроизведение

Установите этот флажок для отображения зацикленного немедленного воспроизведения тревожного события с камеры.

Продолжительность зацикленного немедленного воспроизведения в области тревожных изображений определяется как сумма: время перемотки + продолжительность состояния тревоги + плюс время перемотки.

#### **Записать с данной камеры**

Установите флажок, чтобы разрешить для данной камеры запись по тревоге. При срабатывании тревоги запись с этой камеры производится с качеством режима записи по тревоге. Продолжительность записи равна продолжительности состояния тревоги плюс время перед и после тревоги. Этот параметр непосредственно влияет на настройку записи по тревоге в диалоговом окне **Параметры тревог** и наоборот.

**Примечание.** Если для панорамной камеры выбрано предустановленное положение, сохраняется не только этот фрагмент изображения, но и полное круговое изображение.

#### **Панорамная препозиция**

В случае выбора панорамной камеры можно выбрать предустановленное положение камеры. После того как пользователь Operator Client подтверждает получение сигнала тревоги, отображается кадрированное тревожное изображение, соответствующее предустановленному положению.

В случае выбора **<нет>** тревожное изображение выводится в панорамном представлении.

**См.**



- *Страница Свойства оператора, Страница 351*
- *Настройка тревоги, Страница 333*

## 22.3

### **Диалоговое окно «Выбрать содержимое области изображений» (MG)**

Главное окно >



**Тревожные сигналы** >  или  > столбец **Параметры тревог** > нажмите ... > диалоговое окно **Параметры тревог** > вкладка **Группа мониторов** > нажмите ... в одном из столбцов 1–10

Позволяет выбрать камеру в логическом дереве. Изображение с этой камеры будет отображаться на назначенном мониторе в случае возникновения выбранной тревоги.

#### **Найти элемент**

Введите текст для поиска элемента в логическом дереве.

#### **Найти**

Нажмите для поиска камеры по введенному тексту в ее описании.

#### **Панорамная препозиция**

В случае выбора панорамной камеры можно выбрать предустановленное положение камеры. После того как пользователь Operator Client подтверждает получение сигнала тревоги, отображается кадрированное тревожное изображение, соответствующее предустановленному положению.

Если выбрать **<нет>**, декодер отображает тревожное изображение в виде круга.

#### **Камера не выбрана**

Нажмите, чтобы удалить камеру из столбца группы мониторов.

#### **Примечание.**

Поле обзора в предустановленном положении панорамной камеры у Operator Client или Configuration Client и у декодера разное.






#### Замечание!

Для использования предустановленных положений, настроенных для панорамных камер, параметр **Положение установки** панорамной камеры должен иметь значение **Стена** или **Потолок**.

## 22.4

### Диалоговое окно Параметры тревог

Главное окно >  Тревожные сигналы >  или  > столбец **Параметры тревог** > ...

Позволяет настроить следующие параметры тревог:

- Камеры, начинающие запись в случае тревоги.
- Включение защиты этих записей по тревоге.
- Включение и настройка отличающихся параметров длительности тревоги.
- Включение команд управления камерами PTZ в случае тревоги.
- Уведомления, отправляемые в случае тревоги.
- Поток заданий, выполняемый в случае тревоги.
- Назначение камер, отображаемых в группах мониторов в случае тревоги.

#### Вкладка Камеры

<b>Номер</b>	Отображает номер камеры в соответствии с настройками на странице <b>Камеры и запись</b> .
<b>Имя</b>	Отображает название камеры в соответствии с настройками на странице <b>Камеры и запись</b> .
<b>Местонахождение</b>	Отображает местонахождение в соответствии с настройками на странице <b>Карты и структура</b> .
<b>Запись</b>	Установите флажок, чтобы запись по тревоге с данной камеры включалась в случае тревоги. При срабатывании тревоги запись с этой камеры производится с качеством режима записи по тревоге. Продолжительность записи равна продолжительности состояния тревоги плюс время перед и после тревоги. Этот параметр непосредственно влияет на настройки записи по тревоге в диалоговом окне <b>Выбрать содержимое Области изображений</b> и наоборот.
<b>Защитить запись</b>	Установите флажок, чтобы обеспечить защиту записи по тревоге с данной камеры.
<b>Изменение настройки длительности тревоги</b>	Этот флажок устанавливается автоматически при установке флажка <b>Запись</b> , и если камера поддерживает ANR.

<b>Вспомогательная команда</b>	Щелкните ячейку для выбора вспомогательной команды, которая должна быть выполнена в случае тревоги. Записи в этом списке доступны только для камер PTZ.
<b>Препозиция</b>	Щелкните ячейку для выбора предопределенного положения, которое должно быть установлено в случае тревоги. Записи в этом списке доступны только для камер PTZ.

#### Вкладка Уведомления

<b>Электронная почта</b>	Установите флажок для отправки электронного сообщения в случае тревоги.
<b>Сервер:</b>	Выберите сервер электронной почты.
<b>Получатели:</b>	Введите адреса электронной почты получателей, разделяя их запятыми (пример: name@provider.com).
<b>SMS</b>	Установите флажок для отправки SMS-сообщения в случае тревоги.
<b>Устройство:</b>	Выберите SMS-устройство.
<b>Получатели:</b>	Введите номера мобильных телефонов получателей.
<b>Текст:</b>	Введите текст уведомления.
<b>Информация:</b>	Установите флажок для добавления соответствующей информации к тексту уведомления. <b>Примечание.</b> Для электронной почты используется дата часового пояса Management Server.

#### Вкладка Поток заданий

<b>Записывать только тревогу</b>	Установите флажок, для того чтобы в случае тревоги с данной камеры производилась запись, а изображение не отображалось. Этот флажок активен только в том случае, если установлен флажок <b>Запись</b> на вкладке <b>Камеры</b> .
<b>Автоотключение тревоги по истечении определенного времени (диалоговое окно 'Настройки тревог')</b>	Установите флажок, чтобы тревога автоматически отключалась.
<b>Автоотключение тревоги при возвращении события в нормальное состояние</b>	Установите этот флажок, чтобы тревога автоматически отключалась, когда событие, вызвавшее эту тревогу, изменяет свое состояние. Тревога не будет отключена автоматически, если она принята или не принята.
<b>Запретить удаление тревог при сохранении состояния срабатывания</b>	Установите флажок, чтобы предотвратить удаление тревоги до устранения причины тревоги.

<b>Подавлять дублирующиеся тревоги в списке тревог</b>	<p>Установите флажок, чтобы избежать дублирования тревог для одного типа события и устройства в списке тревог BVMS Operator Client.</p> <p>Пока тревога активна (в состоянии тревоги <b>Активно</b> или <b>Принято</b>), никакие последующие тревоги для того же типа события или устройства не отображаются в списке тревог.</p> <p><b>Примечание.</b></p> <ul style="list-style-type: none"> <li>– События по-прежнему регистрируются в журнале.</li> <li>– Обратите внимание, что все возможные действия по этой тревоге (например, отправке SMS-сообщения, запуск записи по тревоге и т.д.) не запускаются повторно.</li> </ul> <p>После очистки тревоги и возникновения новой тревоги того же типа для того же устройства, новая тревога снова появляется в списке тревог и снова возникают все возможные действия по этой тревоге.</p> <ul style="list-style-type: none"> <li>– Этот флажок заранее установлен для тревог Person Identification.</li> </ul>
<b>Показать план действий</b>	Установите флажок, чтобы обеспечить выполнение алгоритма реакции в случае тревоги.
<b>Ресурсы...</b>	Нажмите для отображения диалогового окна <b>Диспетчер ресурсов</b> . Выберите документ с описанием соответствующего потока заданий.
<b>Показать поле комментариев</b>	Установите флажок, чтобы обеспечить отображение поля комментариев в случае тревоги. В этом поле пользователь может ввести комментарии к тревоге.
<b>Форсировать обработку потока заданий оператором</b>	Установите флажок, чтобы форсировать обработку потока заданий пользователем. При установке данного флажка пользователь не может отключить тревогу, до тех пор пока не введет комментарий к тревоге.
<b>Выполнить следующий клиентский сценарий после принятия тревоги:</b>	выберите клиента Командный сценарий, который выполняется автоматически, когда пользователь принимает тревогу.


**Вкладка Группа мониторов**

<b>1...10</b>	<p>Нажмите ячейку в столбце под номером. Откроется диалоговое окно <b>Выбрать содержимое Области изображений</b>. Выберите камеру в логическом дереве. Изображение с этой камеры будет отображаться на назначенном мониторе в случае тревоги. Выберите предустановленные положения камеры, если они настроены. Дополнительные сведения см. в описании диалогового окна <b>Выбрать содержимое Области изображений (MG)</b> в онлайн-справке.</p>
---------------	---

<b>Очистить таблицу</b>	Нажмите для удаления всех назначений камер группам мониторов.
<b>Название тревожного сигнала</b>	Установите флажок, чтобы название тревоги отображалось на мониторах в виде экранного сообщения.
<b>Время тревожного сигнала</b>	Установите флажок, чтобы время тревоги отображалось на мониторах в виде экранного сообщения.
<b>Дата тревоги</b>	Установите флажок, чтобы дата тревоги отображалась на мониторах в виде экранного сообщения.
<b>Имя тревожной камеры</b>	Установите флажок, чтобы название тревожной камеры отображалось на мониторах в виде экранного сообщения.
<b>Номер тревожной камеры</b>	Установите флажок, чтобы номер тревожной камеры отображался на мониторах в виде экранного сообщения.
<b>Только на первом мониторе</b>	Установите флажок, чтобы время и название тревоги отображались в виде экранного сообщения только на первом мониторе группы мониторов.

#### Вкладка Изменение настройки длительности тревоги

Настройки на этой вкладке доступны, только если для этой камеры включена функция ANR.




<b>Использовать настройки профиля</b>	Нажмите, чтобы включить этот параметр. Для этой камеры используются параметры длительности до и после срабатывания тревоги, заданные в диалоговом окне <b>Настройки записи по расписанию</b> .
<b>Переопределить настройки</b>	Нажмите для включения следующих параметров длительности до и после срабатывания тревоги.
<b>Длительность (до тревоги)</b>	Доступно для всех событий.
<b>Длительность (после тревоги)</b>	Доступно только для событий  .

См.

- Диалоговое окно «Выбрать содержимое области изображений» (MG), Страница 322
- Включение записи по тревоге с помощью текстовых данных, Страница 335
- Настройка тревоги, Страница 333
- Настройка длительности до и после срабатывания тревожного сигнала, Страница 334

## 22.5

### Диалоговое окно Выбрать ресурс

Главное окно >  Тревожные сигналы >  или  > Столбец **Идентификатор тревоги** > Столбец **Аудиофайл** > Щелкнуть ...  
 Позволяет выбрать аудиофайл, воспроизводимый в случае тревоги.

**Воспроизведение**

Нажмите для воспроизведения выбранного аудиофайла.

**Пауза**

Нажмите для приостановки воспроизведения выбранного аудиофайла.

**Стоп**

Нажмите для остановки воспроизведения выбранного аудиофайла.

**Управление...**

Нажмите для отображения диалогового окна **Диспетчер ресурсов**.

**См.**

- *Настройка тревоги, Страница 333*
- *Управление файлами ресурсов, Страница 329*

## 23 Настройка событий и тревог

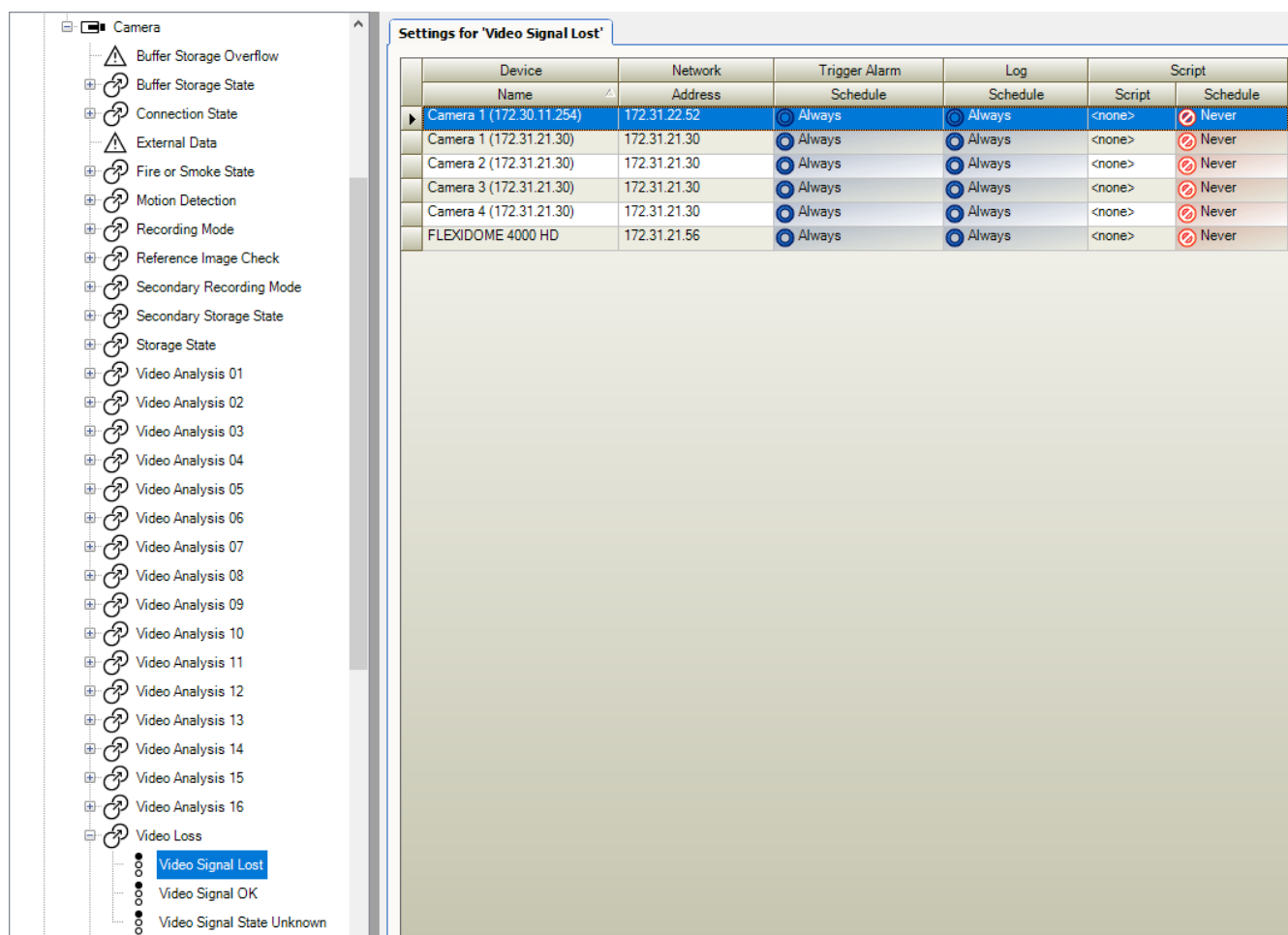
Главное окно >  **События**  
или

Главное окно >  **Тревожные сигналы**

В данном разделе содержится информация о настройке событий и тревог в системе. Доступные события сгруппированы по соответствующим устройствам.

На странице **События** можно настроить, в каких ситуациях событие в BVMS будет активировать тревогу, выполнять командный сценарий и регистрироваться в журнале.

Пример (часть таблицы настройки событий):



The screenshot shows the configuration interface for 'Video Signal Lost' events. On the left is a tree view of camera settings, with 'Video Signal Lost' selected. The main area displays a table with the following data:

Device Name	Network Address	Trigger Alarm Schedule	Log Schedule	Script	Script Schedule
Camera 1 (172.30.11.254)	172.31.22.52	Always	Always	<none>	Never
Camera 1 (172.31.21.30)	172.31.21.30	Always	Always	<none>	Never
Camera 2 (172.31.21.30)	172.31.21.30	Always	Always	<none>	Never
Camera 3 (172.31.21.30)	172.31.21.30	Always	Always	<none>	Never
Camera 4 (172.31.21.30)	172.31.21.30	Always	Always	<none>	Never
FLEXIDOME 4000 HD	172.31.21.56	Always	Always	<none>	Never

Данный пример означает следующее:



При потере видеосигнала с выбранной камеры активируется тревожный сигнал, событие регистрируется в журнале, а сценарии не выполняются.

На странице **Тревожные сигналы** можно настроить способ отображения тревоги, а также указать камеры, изображения с которых будут воспроизводиться и записываться в случае тревоги.

Некоторые системные события по умолчанию сконфигурированы как тревоги.

– Нажмите  для сохранения настроек.



- Нажмите  для отмены последней настройки.
- Нажмите  для активации конфигурации.

**См.**

- Вкладка "Настройки задержки", Страница 314
- Вкладка "Настройки" для расширенного отображения карты, Страница 314
- Вкладка "Настройки" для конфигурации событий, Страница 315
- Диалоговое окно Редактор командных сценариев, Страница 316
- Диалоговое окно Создать сложное событие / Редактировать сложное событие, Страница 316
- Диалоговое окно Выберите язык сценария, Страница 317
- Диалоговое окно Изменение приоритетов типа события, Страница 317
- Диалоговое окно Выбор устройств, Страница 318
- Диалоговое окно "Запись текстовых данных", Страница 318
- Диалоговое окно Настройки тревог, Страница 320
- Диалоговое окно Выбрать содержимое Области изображений, Страница 321
- Диалоговое окно Параметры тревог, Страница 323

## 23.1 Копирование и вставка в таблицы

Можно одновременно настраивать многие объекты в таблице камер, таблице настройки событий или таблице настройки тревог при помощи всего лишь нескольких щелчков мышью.

Подробные сведения см. в *Копирование и вставка в таблицы*, Страница 297.

## 23.2 Удаление строки из таблицы



Главное окно >  **Тревожные сигналы**

Вы можете удалять только те строки, которые были добавлены вами или другим пользователем, т.е. вы можете удалять дублированные или сложные события.

Сложные события находятся в дереве событий в разделе **Системные устройства** >

**Сложные события.**

**Чтобы удалить строку из таблицы:**

1. Выделите строку

2. Нажмите  .

**См.**

- Страница События, Страница 313

## 23.3 Управление файлами ресурсов

Подробные сведения см. в:

- *Управление файлами ресурсов*, Страница 271.

## 23.4 Настройка события



Главное окно > **События**

### Настройка события:

1. Выберите в дереве событие или состояние события, например **Системные устройства > Идентификация > Аутентификация оператора отклонена**. Откроется соответствующая таблица настройки событий.
2. В столбце **Активировать тревогу - Расписание** нажмите ячейку и выберите соответствующее расписание. Расписание определяет, когда запускается тревожный сигнал. Выберите одно из расписаний записей или расписаний задач, настроенных на странице **Расписания**.
3. Выберите ячейку в столбце **Журнал - Расписание** и выберите соответствующее расписание. Расписание определяет время регистрации события.
4. Выберите ячейку в столбце **Сценарий - Сценарий** и выберите соответствующий командный сценарий.
5. В столбце **Сценарий - Расписание** нажмите ячейку и выберите соответствующее расписание. Расписание определяет, когда событие запускает командный сценарий.

**См.**

– *Страница События, Страница 313*


## 23.5 Дублирование события



Главное окно > **События**

Вы можете дублировать событие для активации нескольких тревожных сигналов для одного события.

### Чтобы дублировать событие:

1. Выберите в дереве условие события. Отображается соответствующая таблица настройки событий.
2. Выберите строку таблицы.
3. Нажмите значок . В таблицу будет добавлена новая строка. Она имеет параметры по умолчанию.

**См.**

– *Страница События, Страница 313*

## 23.6 Регистрация пользовательских событий



Главное окно > **События Системные устройства > разверните Действия пользователя**

Можно настроить способы регистрации в журнале некоторых действий пользователя отдельно для каждой доступной группы пользователей.

Пример:

**Регистрация пользовательских событий:**

1. Выберите пользовательское событие для настройки способа его регистрации, например **Вход оператора**.  
Откроется соответствующая таблица настройки событий.  
Каждая группа пользователей отображается в столбце **Устройство**.
2. В случае доступности: выберите ячейку в столбце **Активировать тревогу - Расписание** и выберите соответствующее расписание.  
Расписание определяет время активации уведомляющего пользователя тревожного сигнала.  
Можно выбрать одно из расписаний записей или расписаний задач, настроенных на странице **Расписания**.
3. Выберите ячейку в столбце **Журнал - Расписание** и выберите соответствующее расписание.  
Расписание определяет время регистрации события.  
В данном примере вход оператора группы администраторов и группы опытных пользователей не будет зарегистрирован, а вход оператора группы пользователей "Live" будет зарегистрирован по расписанию **День**.

См.

– *Страница События, Страница 313*

## 23.7

### Настройка кнопок пользовательских событий



Главное окно > **События**

Вы можете настроить кнопки пользовательских событий Operator Client. Вы можете настроить Operator Client таким образом, чтобы одна или несколько кнопок пользовательских событий не отображались.

На странице **Группы пользователей** можно настроить систему таким образом, чтобы кнопки пользовательских событий отображались только в Operator Client соответствующей пользовательской группы.

**Чтобы настроить кнопки пользовательских событий:**

1. В дереве выберите **Системные устройства > Кнопки событий модуля Operator Client > Кнопка события нажата**.  
Отображается соответствующая таблица настройки событий.
2. Выберите кнопку пользовательского события для настройки режима ее работы.
3. Выберите ячейку в столбце **Активировать тревогу - Расписание** и выберите соответствующее расписание.  
Расписание определяет время активации тревожного сигнала, уведомляющего пользователя о событии.
4. Выберите ячейку в столбце **Журнал - Расписание** и выберите соответствующее расписание.  
Расписание определяет время регистрации события.  
При выборе **Никогда** кнопка пользовательского события становится недоступной в Operator Client для всех пользовательских групп, имеющих разрешение на кнопку пользовательского события.

5. Выберите ячейку в столбце **Сценарий - Сценарий** и выберите соответствующий командный сценарий.
6. Выберите ячейку в столбце **Сценарий - Расписание** и выберите соответствующее расписание.

Расписание определяет время исполнения командного сценария.

**См.**

– *Страница События, Страница 313*

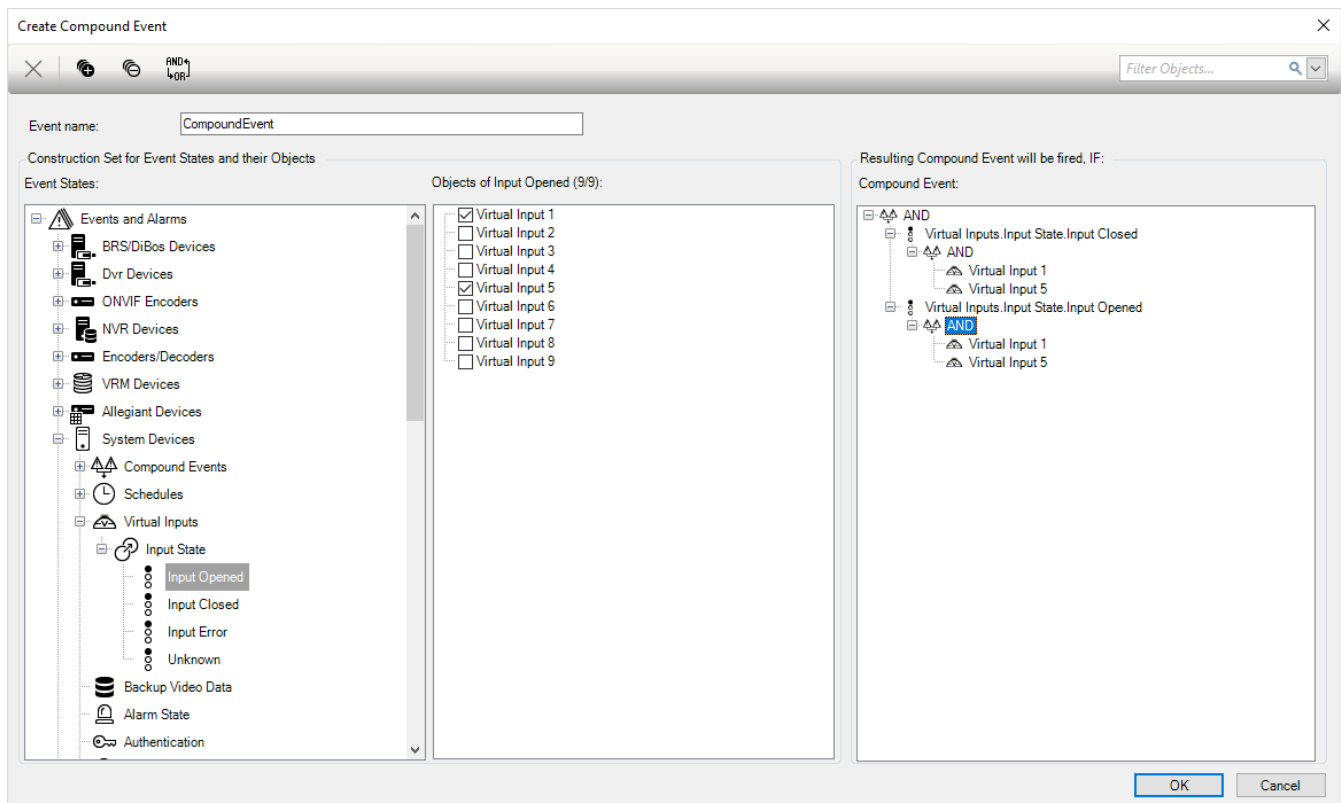
## 23.8

### Создание сложного события

Главное окно >  **События** > 

Необходимо создать Сложное событие. Вы можете объединять только изменения состояний и их объекты. Объектами могут быть, например, расписания или устройства. Вы можете объединять как изменения состояний, так и их объекты при помощи логических выражений AND и OR.

Пример: Вы объединяете состояния подключения IP-камеры и декодера. Сложное событие будет иметь место только в том случае, если оба устройства теряют подключение. В этом случае вы используете оператор AND для двух объектов (IP-камеры и декодера) и для двух состояний подключения **Видеосигнал утерян** и **Отключено**.



#### Создание сложного события.

1. В поле **Имя события:** введите имя для сложного события.
2. В поле **Состояния событий:** выберите состояние события.

Доступные объекты отображаются в поле **Объекты:**.

3. В поле **Объекты:** выберите нужное устройство.  
Соответствующее событие и выбранные устройства добавляются в область "Составное событие".
4. В поле **Сложное событие:** щелкните правой кнопкой мыши логическую операцию и внесите необходимые изменения.  
Логическая операция определяет сочетание своих непосредственных дочерних элементов.
5. Нажмите **ОК**.  
Новое сложное событие будет добавлено в таблицу настройки событий. Его можно будет найти в дереве событий в разделе **Системные устройства**.

См.

– *Страница События, Страница 313*

## 23.9

### Редактирование сложного события



Главное окно > **События**

Вы можете изменить ранее созданное сложное событие.

**Чтобы изменить сложное событие:**

1. В дереве событий разверните **Системные устройства > Состояние сложного события > Сложное событие верно**.
2. В столбце **Устройство** таблицы настройки событий щелкните правой кнопкой мыши нужное сложное событие и нажмите **Правка**.  
Отобразится диалоговое окно **Редактировать сложное событие**.
3. Внесите необходимые изменения.
4. Нажмите **ОК**.  
Сложное событие будет изменено.

См.

– *Страница События, Страница 313*

## 23.10

### Настройка тревоги



Главное окно > **Тревожные сигналы**

Перед настройкой тревоги нужно настроить активирующее ее событие в разделе **События**.

**Для настройки сигнала тревоги:**

1. Выберите тревогу в дереве, например **Системные устройства > Идентификация > Аутентификация оператора отклонена**.  
Отобразится соответствующая таблица настройки тревог.
2. В столбце **Приоритет** нажмите ... в ячейке и введите приоритет тревоги для выбранной тревоги (100 — низкий, 1 — высокий).  
В столбце **Название** нажмите ... в ячейке и введите название тревожного сигнала, которое будет отображаться в системе BVMS (например, в списке тревог).  
В столбце **Цвет** нажмите ... в ячейке, чтобы отобразить диалоговое окно для выбора цвета, которым будет отображаться тревожный сигнал в Operator Client (например, в списке тревог).

3. В столбцах 1-5 нажмите ... в ячейке для отображения диалогового окна **Выбрать содержимое Области изображений**.  
Задайте требуемые параметры.
  4. В столбце **Аудиофайл** нажмите ... в ячейке, чтобы отобразить диалоговое окно для выбора аудиофайла, который должен воспроизводиться в случае тревоги.
  5. В столбце **Параметры тревог** нажмите ... в ячейке для отображения диалогового окна **Параметры тревог**.
  6. Задайте требуемые параметры.
- Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

**См.**

- *Настройка события, Страница 330*
- *Страница Тревожные сигналы, Страница 319*
- *Диалоговое окно Выбрать содержимое Области изображений, Страница 321*
- *Диалоговое окно Параметры тревог, Страница 323*


**23.11****Настройка параметров для всех тревог**

Главное окно > **Тревожные сигналы**

Вы можете настроить следующие параметры тревоги, которые будут действительны для этого Management Server:

- Количество областей изображений на тревогу
- Время автоматического отключения
- Время записи по тревоге вручную
- Отображение тревог в нескольких строках в окне тревожных изображений
- Ограничение длительности записей по тревоге, активируемых в определенном состоянии
- Поведение всех групп мониторов

**Для настройки всех тревог выполните следующие действия.**

1. Нажмите .  
Откроется диалоговое окно **Настройки тревог**.
2. Настройте необходимые параметры.
  - ▶ Нажмите **ОК**.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

**См.**

- *Диалоговое окно Настройки тревог, Страница 320*

**23.12****Настройка длительности до и после срабатывания тревожного сигнала**

Для настройки параметров длительности до и после срабатывания тревожного сигнала требуется камера, поддерживающая функцию ANR с установленным микропрограммным обеспечением версии 5.90 или выше.



Главное окно >  **Камеры и запись** > 

- ▶ Для требуемой камеры включите функцию **ANR**.

Главное окно >  **События**

- ▶ Настройте требуемое событие для камеры с включенной функцией ANR.

Главное окно >  **Тревожные сигналы**

1. Настройте тревожный сигнал для этого события.
2. Выберите  или .
3. В столбце **Параметры тревог** нажмите ....  
Отображается диалоговое окно **Параметры тревог**.
4. Для включения записи по тревоге в столбце **Запись** установите флажок для камеры с включенной функцией ANR.  
Флажок в столбце **Изменение настройки длительности тревоги** устанавливается автоматически.
5. Перейдите на вкладку **Изменение настройки длительности тревоги**.
6. Настройте параметр длительности тревоги согласно необходимости.

См.

– *Диалоговое окно Параметры тревог, Страница 323*



## 23.13

### Включение записи по тревоге с помощью текстовых данных

Главное окно >  **Тревожные сигналы**

Можно включать запись по тревоге с помощью текстовых данных.

Перед настройкой тревоги необходимо настроить событие, содержащее текстовые данные.

Пример:  **События** > выберите в дереве событий  (текстовые данные должны быть доступны, например, **Устройства чтения кредитных карточек** > **Устройство чтения кредитных карточек** > **Карта отклонена**)



#### Замечание!

Задайте для выбранного события время задержки 0.  
Это необходимо, чтобы избежать потерь текстовых данных.

#### Настройка записи по тревоге:



1. Выберите тревогу в дереве, например **Устройства ATM/POS** > **Вход банкомата** > **Ввод данных**.

- Отображается соответствующая таблица настройки тревог.
2. Установите требуемые параметры.
  3. В столбце **Параметры тревог** щелкните ... в ячейке для отображения диалогового окна **Параметры тревог**.
  4. Нажмите вкладку **Камеры** и установите флажок **Запись**.

**См.**


- *Диалоговое окно Параметры тревог, Страница 323*
- *Диалоговое окно "Запись текстовых данных", Страница 318*

## 23.14 Добавление текстовых данных к непрерывной записи

Главное окно >  **События** > в дереве событий выберите  **Ввод данных** (текстовые данные должны быть доступны, например **Устройства чтения кредитных карточек** > **Устройство чтения кредитных карточек** > **Карта отклонена**) > столбец **Запись текстовых данных** > ...

Можно добавлять текстовые данные к непрерывной записи.

## 23.15 Защита записи по тревоге

Главное окно >  **Тревожные сигналы**

Перед настройкой тревоги необходимо настроить событие на странице **События**.

**Настройка записи по тревоге:**

1. Выберите тревогу в дереве, например **Устройства ATM/POS** > **Вход банкомата** > **Ввод данных**.  
Отображается соответствующая таблица настройки тревог.
2. Установите требуемые параметры.
3. В столбце **Параметры тревог** щелкните ... в ячейке для отображения диалогового окна **Параметры тревог**.
4. Нажмите вкладку **Камеры** и установите флажок **Запись**.
1. Установите флажок **Защитить запись**.

**См.**

- *Диалоговое окно Параметры тревог, Страница 323*

## 23.16 Настройка мигающих активных точек



**Замечание!**


Мигающие активные точки можно настроить только для события или тревоги.

Главное окно >  **События**  
или





Главное окно > **Тревожные сигналы**

Для каждого события или тревоги (  ) можно настроить цвет фона и поведение активных точек (мигает или не мигает). Например, можно настроить событие или тревогу




устройства так, чтобы его значок устройства на карте начинал мигать при изменении состояния этого устройства.

Кроме того, можно настроить приоритет отображения для всех активных точек. Это необходимо, если для одного устройства возникают различные события. (1 = наивысший приоритет)

Настроенный цвет действует для всех активных точек с одинаковым приоритетом отображения. Можно изменить цвет, поведение и приоритет для любого события или




тревоги  : изменение цвета и поведения используется для всех активных точек всех

остальных событий или тревог , имеющих такой же приоритет.

Настройка цвета состояний на картах возможна, только если установлен флажок

**Включить расширенное отображение состояний (цвет активных точек на картах в зависимости от состояния)** или флажок **Включить расширенное отображение тревог (цвет активных точек на картах в зависимости от тревоги)** в диалоговом окне **Параметры**.

**Для настройки мигающей активной точки для события:**

1. выберите в дереве состояние события (  ), например **Кодеры/Декодеры > Реле кодера > Состояние реле > Реле открыто**.  
Откроется соответствующая таблица настройки событий.
2. Нажмите **Включить цвет состояний на картах**.
3. Введите необходимый приоритет в поле **Приоритет отображения на карте:**.
4. Нажмите поле **Цвет фона на карте:**, чтобы выбрать необходимый цвет.
5. При необходимости щелчком включите функцию **Мигание**.

**Для настройки мигающей активной точки для тревоги:**

См. раздел *Устройство*, *Страница 319* на *Страница Тревожные сигналы*, *Страница 319*.



#### **Замечание!**

Активная точка мигает только в том случае, когда тревога содержится в списке тревог.

Значки устройств на карте мигают цветом, настроенным для тревоги или события.

**См.**

- *Страница События*, *Страница 313*
- *Диалоговое окно «Параметры» (меню «Настройки»)*, *Страница 118*

## **23.17**

### **События и тревоги для систем контроля и управления доступом**

Дополнительная информация о событиях и тревогах для систем контроля и управления доступом.

**Событие запроса доступа**

Это событие позволяет оператору BVMS вручную предоставить доступ или отказать в доступе человеку с помощью системы контроля и управления доступом. Можно настроить запись по тревоге, запись текстовых данных или дополнительную информацию для данного события.

События запроса доступа передаются в систему BVMS, только если на каждом считывающем устройстве системы контроля и управления доступом включен параметр

**Дополнительная проверка.** В конфигурации событий BVMS события **Доступ запрошен,** передаваемые считывающими устройствами, всегда активируют тревогу в BVMS.

**Замечание!**

Рекомендуется установить наивысший приоритет (1) для тревожных сигналов **Доступ запрошен.** В этом случае тревожные сигналы будут автоматически отображаться, привлекая внимание оператора.

## 24

## Страница Пользовательские группы



Главное окно >

### Группы пользователей

Позволяет настроить группы пользователей, Enterprise User Groups и доступ Enterprise.

По умолчанию доступна следующая группа пользователей:

- Группа администраторов (с одним пользователем Admin).

#### Вкладка Пользовательские группы

Нажмите, чтобы открыть страницы, доступные для настройки прав стандартной пользовательской группы.

#### Вкладка Enterprise User Groups (доступна только с действующей лицензией Enterprise)

Нажмите, чтобы открыть страницы, доступные для настройки разрешений Enterprise User Group.

#### Вкладка Доступ Enterprise (доступна только с действующей лицензией Enterprise)

Нажмите, чтобы открыть страницы, доступные для добавления и настройки Enterprise Access.

#### Параметры пользователей/пользовательских групп

Значок	Описание
	Нажмите, чтобы удалить выбранную запись.
	Нажмите, чтобы добавить новую группу или учетную запись.
	Нажмите, чтобы добавить нового пользователя к выбранной группе пользователей. При необходимости можно изменить имя пользователя по умолчанию.
	Нажмите, чтобы добавить новую группу с двойной авторизацией.
	Нажмите, чтобы добавить новую комбинацию для входа в систему при двойной авторизации.
	Открывает диалоговое окно для копирования разрешений из выбранной группы пользователей в другую группу пользователей.
	Нажмите, чтобы открыть страницы, доступные для настройки разрешений этой группы.
	Нажмите, чтобы открыть страницу, доступную для настройки свойств данного пользователя.
	Нажмите, чтобы открыть страницу, доступную для настройки свойств данной комбинации для входа в систему.
	Нажмите, чтобы открыть страницы, доступные для настройки разрешений данной пользовательской группы с двойной авторизацией.

**Активация изменений имени пользователя и пароля**

Нажмите, чтобы активировать изменение пароля.



Нажмите, чтобы активировать изменение имени пользователя.

**Замечание!**

Изменения имени пользователя и изменения пароля будут отменены и возвращены в исходное состояние после отката конфигурации.

**Разрешения Enterprise System**

Для Enterprise System можно настроить следующие права:

- Рабочие разрешения Operator Client, определяющие пользовательский интерфейс для работы в Enterprise System, например пользовательский интерфейс монитора тревожных сигналов.  
Воспользуйтесь Enterprise User Group. Настройте группу на Enterprise Management Server.
- Разрешения устройства, которые должны функционировать для работы в Enterprise Management Server, определяются на каждом Management Server.  
Используйте Enterprise Accounts. Настройте его на каждом Management Server.



**Права на один Management Server**

Для управления доступом к одному из Management Servers используйте стандартную группу пользователей. Все разрешения на этот Management Server можно настроить в этой группе пользователей.

Двойную авторизацию можно настроить для стандартных групп пользователей и Enterprise User Groups.

Тип	Содержит	Доступные параметры конфигурации	Где задается конфигурация?
Пользовательская группа	Пользователи	– Рабочие разрешения и использование устройств	– Management Server
Enterprise User Group	Пользователи	– Рабочие разрешения – На Management Server: имена соответствующих учетных записей доступа Enterprise с учетными данными	– Enterprise Management Server
Enterprise Account	-	– Разрешения на использование устройств – Пароль учетной записи	– Management Server


Тип	Содержит	Доступные параметры конфигурации	Где задается конфигурация?
Группа пользователей с двойной авторизацией	Группы пользователей	– См. группы пользователей	– См. группы пользователей
Enterprise двойная авторизация	Enterprise User Groups	– См. Enterprise User Groups	– См. Enterprise User Groups

Введите строку и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы. Отображаются только элементы, содержащие введенную строку, и их соответствующие родительские элементы (только в деревьях). Указывается число отфильтрованных элементов и совокупное число элементов. На активный фильтр указывает значок . Для поиска точных фраз строки следует заключать в кавычки, например, в случае строки "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201. Чтобы отменить фильтрацию, нажмите .

## 24.1

### Страница Свойства пользовательской группы



Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >  > вкладка **Рабочие разрешения** > вкладка **Свойства пользовательской группы** или



Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Рабочие разрешения** > вкладка **Свойства пользовательской группы**

Позволяет настроить следующие параметры выбранной группы пользователей:

- Расписание входа в систему
- Связывание группы пользователей LDAP

#### Свойства группы пользователей

##### Описание:

Введите информативное описание пользовательской группы.

##### Язык

Выберите язык клиента Operator Client.

##### Расписание входа в систему

Выберите расписание записей или задач. Пользователи выбранной группы могут входить в систему только в то время, которое определено расписанием.

##### Свойства LDAP

##### Связанная группа LDAP

Введите имя пользовательской группы LDAP, которое вы хотите использовать в системе. Вы также можете дважды щелкнуть элемент списка **Группы LDAP**.

**Группы LDAP**

Отображает доступные пользовательские группы LDAP. Настройка групп LDAP осуществляется в диалоговом окне **Настройки сервера LDAP**.

**Искать группы**

Нажмите для отображения доступных пользовательских групп LDAP в списке **Группы LDAP**. Чтобы найти пользовательские группы, следует установить необходимые параметры в диалоговом окне **Настройки сервера LDAP**.

**Настройки**

Нажмите для отображения диалогового окна **Настройки сервера LDAP**.

**Связать группу**

Нажмите, чтобы связать выбранную группу LDAP с данной пользовательской группой.

**Очистить группу**

Нажмите для очистки поля **Связанная группа LDAP**. Связь группы LDAP с пользовательской группой BVMS будет удалена.

**Изменить порядок...**

Нажмите для отображения списка **Изменить порядок групп пользователей LDAP**. В списке отображаются группы пользователей LDAP, а также связанные с ними группы пользователей BVMS и Enterprise User Groups. Порядок расположения групп можно изменять перетаскиванием или с помощью кнопок со стрелками вверх и вниз.


**Замечание!**



Пользователь LDAP может быть связан с несколькими группами пользователей LDAP, которые, в свою очередь, связаны с определенной группой пользователей BVMS. Пользователь LDAP получает права группы пользователей BVMS, которая расположена выше других групп пользователей LDAP, связанных с этим пользователем LDAP.

**См.**

- *Настройка параметров LDAP, Страница 370*
- *Связывание группы LDAP, Страница 371*
- *Составление расписания разрешений на вход пользователей в систему, Страница 372*

**24.2****Страница Свойства пользователей**

 **Группы пользователей** > вкладка **Пользовательские группы**

 > 

или

 **Группы пользователей** > вкладка **Enterprise User Groups** > 

> 

Позволяет настроить нового пользователя в стандартной группе пользователей или в Enterprise User Group.

Если изменить пароль пользователя или удалить пользователя, пока он зарегистрирован в системе, пользователь может продолжить работу с Operator Client и после изменения или удаления пароля. Если после изменения или удаления пароля соединение с Management

Server прерывается (например, после активации конфигурации), пользователь не может автоматически повторно подключиться к Management Server без выхода/входа в Operator Client.

#### Учетная запись включена

Установите флажок для активации учетной записи пользователя.

#### Имя

Введите полное имя пользователя.

#### Описание

Введите информативное описание пользователя.

#### Пользователь должен изменить пароль при следующем входе в систему

Установите флажок, чтобы обязать пользователя задать новый пароль при следующем входе.

#### Введите новый пароль

Введите пароль для нового пользователя.

#### Подтвердить пароль

Введите новый пароль еще раз.



#### Замечание!

Мы настоятельно рекомендуем назначить конкретный пароль для всех новых пользователей и обязать пользователя изменить пароль при входе.



#### Замечание!

Клиенты Mobile Video Service, Web Client, приложения Bosch iOS и клиенты SDK не могут изменить пароль при входе.

#### Применить

Нажмите для применения настроек.



Нажмите  для активации пароля.

#### Дополнительная информация

После обновления до BVMS 9.0.0.x установятся следующие настройки **Свойства пользователей**:

- **Учетная запись включена** установлен.
- **Пользователь должен изменить пароль при следующем входе в систему** не установлен.

## 24.3

### Страница Свойства комбинации для входа в систему



Главное окно >

Группы пользователей > вкладка Пользовательские группы >



Создать группу с двойной авторизацией >



или

Главное окно >  **Группы пользователей** > вкладка **Enterprise User Groups** > 

### **Создать группу Enterprise с двойной авторизацией** >

Позволяет изменить пару пользовательских групп к группе с двойной авторизацией. Пользователи первой пользовательской группы вводят свои данные в первом диалоговом окне входа в систему, пользователи второй пользовательской группы только подтверждают вход в систему.

### **Выбрать комбинацию для входа в систему**

Выберите из каждого списка группу пользователей.

### **Форсировать двойную авторизацию**



Установите флажок, чтобы каждый пользователь мог войти в систему только вместе с пользователем другой группы.



### **См.**

- *Добавление комбинации для входа в систему к группе с двойной авторизацией, Страница 369*

## 24.4

### **Страница Разрешения камеры**

Главное окно >  **Группы пользователей** > Вкладка **Пользовательские группы** >  > Вкладка **Разрешения для устройств** > Вкладка **Разрешения камеры**  
или

Главное окно >  **Группы пользователей** > Вкладка **Доступ Enterprise** >  > Вкладка **Разрешения для устройств** > Вкладка **Разрешения камеры**

Позволяет устанавливать права доступа к функциям выбранной камеры или группы камер для выбранной пользовательской группы.

После добавления новых компонентов разрешения камеры должны быть сконфигурированы заново.

Можно отменить доступ к камере на странице **Камера**.

### **Камера**

Отображает название камеры в соответствии с настройками на странице **Камеры и запись**.

### **Местоположение**

Отображает местонахождение камеры, заданное на странице **Карты и структура**.

### **Доступ**

Установите флажок для обеспечения доступа к камере.

### **Видео в реальном времени**

Установите флажок, чтобы обеспечить просмотр изображений в реальном времени.

### **Аудио в реальном времени**

Установите флажок, чтобы обеспечить прослушивание аудио в реальном времени.



**Запись вручную**

Установите флажок, чтобы разрешить запись вручную (запись по тревоге).

Можно установить или снять этот флажок только в том случае, если запись тревоги вручную активирована на странице **Функции оператора**.

**Воспроизвести видео**

Установите флажок для обеспечения возможности использования воспроизведения видеосигнала.

Можно установить или снять этот флажок только в том случае, если воспроизведение активировано на странице **Функции оператора**.

**Воспроизвести аудио**

Установите флажок для обеспечения возможности использования воспроизведения аудиосигнала.

Можно установить или снять этот флажок только в том случае, если воспроизведение активировано на странице **Функции оператора**.

**Текстовые данные**

Установите флажок для обеспечения отображения метаданных.

Можно установить или снять этот флажок только в том случае, если отображение метаданных активировано на странице **Функции оператора**.

**Экспорт**

Установите флажок для обеспечения экспорта видеоданных.

Можно установить или снять этот флажок только в том случае, если экспорт видеоданных активирован на странице **Функции оператора**.

**PTZ/область интереса**

Установите флажок, чтобы разрешить использование средств управления PTZ или функции ROI данной камеры.

Этот флажок можно установить или снять только в том случае, если управление PTZ или функция ROI этой камеры включена на странице **Функции оператора**. Кроме того необходимо настроить PTZ или ROI в Таблице камер.

**Аиx**

Установите флажок, чтобы обеспечить возможность исполнения вспомогательных команд.

Можно установить или снять этот флажок только в том случае, если управление камерой PTZ активировано на странице **Функции оператора**.

**Задать препозиции**

Установите флажок, чтобы разрешить пользователю устанавливать предустановки данной камеры PTZ.



Также можно задать предварительные положения для функции области интереса, если она включена и разрешена.



Можно установить или снять этот флажок только в том случае, если управление камерой PTZ активировано на странице **Функции оператора**.

**Контрольное изображение**

Установите флажок для обеспечения возможности обновления контрольного изображения данной камеры.

## 24.5 Страница Приоритеты управления


 Главное окно > **Группы пользователей** > Вкладка **Пользовательские группы** >  > Вкладка **Разрешения для устройств** > Вкладка **Приоритеты управления** или


 Главное окно > **Группы пользователей** > Вкладка **Доступ Enterprise** >  > Вкладка **Разрешения для устройств** > Вкладка **Приоритеты управления**

### Приоритеты управления

Переместите соответствующий ползунок вправо для уменьшения приоритета получения доступа к управлению камерами PTZ магистральным линиям Bosch Allegiant. Пользователь с более высоким приоритетом может заблокировать управление PTZ или управление магистральными линиями для пользователей с более низким приоритетом. Время, по истечении которого блокировка PTZ прекращается, устанавливается в поле **Время ожидания в мин..** По умолчанию используется значение 1 минута.




### Время ожидания в мин.

Введите время в минутах.

### См.

– *Настройка различных приоритетов, Страница 373*

## 24.6 Диалоговое окно Копировать разрешения пользовательской группы


 Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >  >  или


 Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > 

Позволяет выбрать разрешения группы пользователей для копирования в выбранные группы пользователей.

### Копировать из:

Отображает выбранную пользовательскую группу. Ее разрешения копируются в другую пользовательскую группу.

### Настройки для копирования

Установите флажок для выбора разрешений пользовательской группы, которые нужно скопировать.

**Копировать в:**

Установите флажок, чтобы указать пользовательскую группу, в которую следует скопировать разрешения.

**См.**

– *Копирование разрешений пользовательской группы, Страница 374*

**24.7****Страница Разрешения декодера**

Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** вкладка >



> **Разрешения для устройств** вкладка > **Разрешения декодера**

или



Главное окно >

**Группы пользователей** >

вкладка **Доступ Enterprise** >



>

вкладка **Разрешения для устройств** > вкладка **Разрешения декодера**

Позволяет настроить декодеры, к которым имеют доступ пользователи данной группы.

**Декодер**

Отображает доступные декодеры.

Установить флажок для предоставления пользовательской группе доступа к данному декодеру.

**Группа мониторов**

Установите флажок для предоставления пользователям выбранной пользовательской группы доступа к данной группе мониторов.

**24.8****Страница События и тревоги**

Главное окно >

**Группы пользователей** >

Вкладка **Пользовательские группы** >



> Вкладка **Разрешения для устройств** > Вкладка **События и тревоги**

или



Главное окно >

**Группы пользователей** >

Вкладка **Доступ Enterprise** >



>

Вкладка **Разрешения для устройств** > Вкладка **События и тревоги**

Позволяет настроить разрешения для дерева событий, например, вы настраиваете события, которые группа пользователей может или не может использовать.

Вы не можете изменить эти настройки для пользовательской группы по умолчанию.

Для каждого события имеется по крайней мере одно устройство. Например, для события

**Потеря видеозображения** устройствами являются доступные камеры. Для события

**Резервное копирование закончено** соответствующим устройством является **Резервное**



**копирование по времени**. Таким образом, устройством может быть программный процесс.



1. Разверните элемент дерева и установите нужные флажки для активации событий. Установите флажок в столбце **Доступ** устройства, чтобы включить события этого устройства. Параметры доступа к устройствам настраиваются на странице **Камера** и на странице **Разрешения камеры**.

2. Для включения или выключения всех событий сразу установите или снимите флажок **События и тревоги**.

## 24.9

### Диалоговое окно Настройки сервера LDAP

 Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >  > вкладка **Рабочие разрешения** > вкладка **Свойства пользовательской группы** > кнопка **Настройки** или

 Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Рабочие разрешения** > вкладка **Свойства пользовательской группы** > кнопка **Настройки**

Здесь вы вводите параметры сервера LDAP, которые настраиваются вне BVMS. Вам понадобится помощь администратора, настраивавшего сервер LDAP.

Все поля являются обязательными, за исключением полей в области **Тестовый пользователь / Пользовательская группа**.

#### Настройки сервера LDAP

##### Сервер LDAP

Введите имя сервера LDAP.

##### Порт

Введите номер порта LDAP-сервера (по умолчанию HTTP: 389, HTTPS: 636)

##### Безопасное соединение

Установите флажок, чтобы включить защиту передачи данных.

##### Механизм аутентификации

Параметр «Согласовать» позволяет выбрать соответствующий протокол проверки подлинности.

Параметр «Простой» позволяет передавать учетные данные для входа в систему в незашифрованном открытом тексте.

##### Анонимный

Используется для входа в систему в качестве гостя. Выберите этот параметр, если LDAP-сервер поддерживает его и вы не можете настроить конкретного пользователя прокси-сервера.

##### Используйте следующие учетные данные

##### Имя пользователя

Введите уникальное имя пользователя прокси-сервера. Этот пользователь необходим для того, чтобы пользователи группы BVMS имели доступ к серверу LDAP.

##### Пароль:

Введите пароль пользователя прокси-сервера.

##### Тест

Нажмите, чтобы проверить, имеет ли пользователь прокси-сервера доступ к серверу LDAP.

**Основание LDAP для пользователя**

Введите уникальное имя (DN = распознаваемое имя) пути LDAP, где вы хотите осуществить поиск пользователя. Пример для DN основания LDAP:CN=Users,DC=Security,DC=MyCompany,DC=com

**Фильтр для пользователя**

Выберите фильтр, используемый для поиска уникального имени пользователя. Примеры определены заранее. Замените %username% действительным именем пользователя.

**Основание LDAP для группы**

Введите уникальное имя пути LDAP, где вы хотите осуществить поиск групп. Пример для DN основания LDAP: CN=Users,DC=Security,DC=MyCompany,DC=com

**Фильтр для поиска членов групп**

Выберите фильтр, используемый для поиска члена группы. Примеры определены заранее. Замените %usernameDN% фактическим именем пользователя и его DN.

**Фильтр поиска группы**

Не оставляйте это поле пустым. Если запись отсутствует, вы не можете назначить группу LDAP пользовательской группе BVMS. Выберите фильтр для поиска пользовательской группы. Примеры определены заранее.

**Тестовый пользователь / Пользовательская группа**

Записи в этой области не сохраняются после нажатия на **ОК**. Они служат только для тестирования.

**Имя пользователя:**

Введите имя тестового пользователя. Пропустите DN.

**Пароль:**

Введите пароль тестового пользователя.

**Тестовый пользователь**

Нажмите, чтобы проверить, правильна ли комбинация имени пользователя и пароля.

**Группа (DN)**

Введите уникальное имя группы, с которой связан пользователь.

**Тестовая группа**


Нажмите для проверки связи пользователя с группой.

**См.**

– *Настройка параметров LDAP, Страница 370*

## 24.10

### Страница Учетные данные

Главное окно > **Группы пользователей** > Вкладка **Доступ Enterprise** >  > Вкладка **Разрешения для устройств** > Вкладка **Учетные данные**

Настройте учетные данные Enterprise Account на Management Server.

Вы можете настроить доступ Enterprise на каждом Management Server, входящем в Enterprise System. Enterprise Management Server использует эти учетные данные для предоставления доступа к устройствам этого Management Server Operator Client, выполняющему вход в систему как пользователь из Enterprise User Group.

**Описание:**

Введите описание требуемой учетной записи Enterprise Account.

### Strong password policy

Флажок **Strong password policy** предварительно установлен для всех вновь созданных пользовательских групп.

Мы настоятельно рекомендуем сохранить этот параметр в целях обеспечения защиты вашего компьютера от несанкционированного доступа.

Применяются следующие правила:

- Минимальная длина пароля соответствует указанной на странице **Политики учетных записей** для соответствующих групп пользователей.
- Не используйте один из предыдущих паролей.
- Используйте по крайней мере одну букву в верхнем регистре (A–Z).
- Используйте по крайней мере одну цифру (0–9).
- Используйте по крайней мере один специальный символ (например, ! \$ # %).

### Введите новый пароль: / Подтвердить пароль

Введите пароль для этого Management Server и подтвердите его.

#### См.

- *Строгая политика паролей, Страница 364*
- *Создание Enterprise Account, Страница 366*

## 24.11

### Страница Логическое дерево




Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >



> вкладка **Разрешения для устройств** > вкладка **Логическое дерево**  
или



Главное окно > **Группы пользователей** > вкладка **Доступ Enterprise** >  >  
вкладка **Разрешения для устройств** > вкладка **Логическое дерево**

Позволяет настроить логическое дерево для каждой группы пользователей.

#### Чтобы настроить разрешения:

- ▶ По необходимости установите или снимите флажки.
  - Выбор дочернего элемента узла автоматически выбирает узел.
  - Выбор узла автоматически выбирает все дочерние элементы.

#### Камера

Установите флажок для предоставления пользователям выбранной пользовательской группы доступа к соответствующим устройствам.

Можно отменить доступ к камере на странице **Разрешения камеры**.



#### Группа мониторов



Установите флажок для предоставления пользователям выбранной пользовательской группы доступа к данной группе мониторов.

#### См.

- *Настройка разрешений устройств, Страница 373*

## 24.12 Страница Свойства оператора

 Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >  > вкладка **Рабочие разрешения** > вкладка **Функции оператора** или

 Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Рабочие разрешения** > вкладка **Функции оператора**

Позволяет настроить различные разрешения для выбранной пользовательской группы.

### **Управление купольными камерами PTZ**

Установите флажок для активации управления камерой.

**Приоритеты управления** В поле **Приоритеты управления** можно установить приоритет для получения доступа к управлению камерой.

### **Магистральные линии Allegiant**

Установите этот флажок для обеспечения доступа к магистральным линиям Bosch Allegiant.

**Приоритеты управления** В поле **Приоритеты управления** можно установить приоритет для получения магистралей Bosch Allegiant.

### **Печать и сохранение**

Установите флажок для активации печати и сохранения видеоданных, карт и документов.

### **Обработка тревожных сигналов**

Установите флажок для включения обработки тревожных сигналов.

### **Прервать отображение заставки Windows при поступлении тревожного сигнала**

Установите этот флажок, чтобы входящий тревожный сигнал отображался даже в том случае, когда активна экранная заставка. Если для выхода из экранной заставки требуется ввод имени пользователя и пароля, этот параметр не используется.

### **Экран тревожных сигналов**

Установите флажок для включения отображения тревожных сигналов. При выборе данного параметра одновременно отключается параметр **Обработка тревожных сигналов**.

### **Воспроизведение**

Установите флажок, чтобы разрешить различные функции воспроизведения.

### **Экспортировать видео**

Установите флажок, чтобы разрешить экспорт видеоданных.

### **Экспорт в другие форматы**

Установите флажок, чтобы разрешить экспорт видеоданных в формате, отличном от собственного формата.

### **Защита видео**

Установите флажок для обеспечения защиты видеоданных.

### **Отменить защиту видео**

Установите флажок для активации и деактивации защиты видеоданных.

**Замечание!**

Настройте разрешения для введения и снятия ограничений с учетной записи пользователя на вашем устройстве DIVAR AN по необходимости. Создайте пользователя в системе BVMS с теми же учетными данными и настройте разрешения для введения и снятия ограничений соответствующим образом.

Это не влияет на отображение видео с ограниченным доступом, его необходимо настраивать отдельно.

**Ограничить видео**

Установите флажок, чтобы разрешить ограничение доступа к видеоданным.

**Отменить ограничение видео**

Установите флажок для введения и снятия ограничения доступа к видеоданным.

**Удалить видео**

Установите флажок для обеспечения возможности удаления видеоданных.

**Доступ к видео, записанному в то время, когда вход в систему для группы пользователей был запрещен**

Установите флажок для обеспечения доступа к описанным видеоданным.

**Доступ к журналу**

Установите флажок для обеспечения доступа к журналу.

**Удалить текстовые данные из записей журнала (для удаления данных, связанных с людьми)**

Установите этот флажок, чтобы разрешить удаление текстовых данных из записей журнала.

**Кнопки событий оператора**

Установите флажок для активации кнопок пользовательских событий в Operator Client.

**Закрыть модуль Operator Client**

Установите флажок для обеспечения возможности закрытия Operator Client.

**Свернуть Operator Client**

Установите флажок для обеспечения возможности свертывания Operator Client.

**Внутренняя аудиосвязь**

Установите флажок, чтобы позволить пользователю говорить с использованием громкоговорителя кодера с функциями аудиовхода и аудиовыхода.

**Запись тревожного сигнала вручную**

Установите флажок, чтобы разрешить запись по тревоге вручную.

**Доступ к монитору VRM**

Установите этот флажок, чтобы разрешить доступ к программному обеспечению VRM Monitor.

**Установить контрольное изображение**

Установите этот флажок, чтобы разрешить обновление контрольного изображения в Operator Client.

**Установить область для контрольного изображения**

Установите флажок для обеспечения возможности выбора области в изображении с камеры для обновления контрольного изображения в Operator Client.

**Изменить пароль**

Установите этот флажок, чтобы разрешить пользователю использовать Operator Client для изменения пароля входа в систему.



**Постановка на охрану областей тревожной панели**

Установите флажок, чтобы пользователь Operator Client мог ставить на охрану области, настроенные на охранной панели, входящей в конфигурацию BVMS.

**Принудительная постановка на охрану областей тревожной панели**

Установите флажок, чтобы пользователь Operator Client мог принудительно ставить на охрану области, настроенные на охранной панели, входящей в конфигурацию BVMS.

**Снятие с охраны областей тревожной панели**

Установите флажок, чтобы пользователь Operator Client мог снимать с охраны области, настроенные на охранной панели, входящей в конфигурацию BVMS.

**Отключение sireны для областей тревожной панели**

Установите флажок, чтобы пользователь Operator Client мог отключать сигнальные sireны областей, настроенных на охранной панели, входящей в конфигурацию BVMS.

**Обход точек тревожной панели**

Установите флажок, чтобы пользователь Operator Client мог изменять состояние точки, настроенной на охранной панели, на **Выполнен обход точки**. Обойденная точка не может передавать тревожный сигнал. Когда состояние снова меняется на **Выполнен обход точки**, ожидающий тревожный сигнал, если он есть, отправляется.

**Открывание дверей тревожной панели**

Установите флажок, чтобы пользователь Operator Client мог открывать дверь, настроенную на охранной панели.

**Блокировка и разблокировка дверей тревожной панели**

Установите флажок, чтобы пользователь Operator Client мог блокировать и разблокировать дверь, настроенную на охранной панели.

**Активация рабочего цикла дверей тревожной панели**

Установите флажок, чтобы пользователь Operator Client мог включать рабочий цикл двери, настроенной на охранной панели.

**Управление точками прохода**

Установите флажок, чтобы разрешить пользователю Operator Client изменять состояние входной двери (заблокирована, заперта, не заперта).

**Управление людьми**

Установите этот флажок, чтобы позволить пользователю Operator Client управлять лицами, связанными с тревогами Person Identification.

**Порядок отображения в случае одинакового приоритета тревог**

Выберите соответствующее значение для настройки порядка областей изображений тревог на экране тревожных сигналов Operator Client.

**Время перемотки при немедленном воспроизведении:**

Введите количество секунд, в течение которых должно осуществляться немедленное воспроизведение тревоги.

**Повторять звук тревоги:**

Установите флажок и введите количество секунд, по истечении которого будет повторяться звуковой сигнал тревоги.

**Ограничить доступ к записанному видео до последних n минут:**

Установите флажок, чтобы ограничить доступ к записанным видеоизображением. Введите в списке количество минут.

### **Принудительный автоматический выход оператора из системы после бездействия в течение:**

Установите этот флажок для включения автоматического выхода из системы Operator Client по истечении заданного времени.

#### **См.**

– *Отключение при бездействии, Страница 38*

## **24.13**

### **Страница Приоритеты**



Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >



> вкладка **Рабочие разрешения** > вкладка **Приоритеты**

или



Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Рабочие разрешения** > вкладка **Приоритеты**

Позволяет настраивать время ожидания для явной блокировки PTZ. Можно установить приоритеты управления PTZ и отображения входящих тревожных сигналов.

#### **Поведение автоматически всплывающих окон**

Переместите ползунок для установки приоритетного значения для окна изображений в реальном времени и для окна воспроизведения. Это значение необходимо для определения того, будет ли входящий тревожный сигнал автоматически отображаться в окне тревожных сигналов.

Например: Если вы переместите ползунок для изображения в реальном времени на значение 50, а для окна воспроизведения на 70, а тревожный сигнал будет иметь приоритет 60, он будет автоматически отображен на экране только в том случае, если активным окном будет окно воспроизведения. Тревожный сигнал не будет автоматически отображаться, если активным окном будет окно изображения в реальном времени.

#### **См.**

– *Настройка различных приоритетов, Страница 373*

## **24.14**

### **Страница Интерфейс пользователя**




Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >



> вкладка **Рабочие разрешения** > вкладка **Интерфейс пользователя**

или



Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Рабочие разрешения** > вкладка **Интерфейс пользователя**

Позволяет настроить пользовательский интерфейс четырех мониторов, используемых Operator Client.

Вы можете настроить многомониторный режим с максимум 4 мониторами. Для каждого монитора можно определить, что будет на нем отображаться; например, что монитор 2 отображает только изображения в реальном времени или что монитор 1 и монитор 2 используют соотношение сторон 16:9 для камер HD.

#### **Контрольный монитор**

Выберите монитор, который будет использоваться в качестве монитора управления.

#### **Макс. число строк областей изображений при воспроизведении**

Выберите максимальное число строк областей изображений для отображения в окне воспроизведения изображений на мониторе управления.

#### **Тревожный монитор**

Выберите тревожный монитор, который может отображать режим реального времени и режим тревоги либо только режим тревоги.

#### **Монитор 1–4**

Выберите нужный элемент из соответствующего списка каждого монитора.

- Для монитора управления запись **Управление** выбрана заранее и не может быть изменена.
- Для тревожного монитора можно выбрать одну из следующих записей:
  - **Видео в реальном времени и содержимое тревог**
  - **Только содержимое тревог**
- Для оставшихся мониторов можно выбрать одну из следующих записей:
  - **Только видео в реальном времени**
  - **Карта и документ**
  - **Две карты и документ**
  - **Видео в реальном времени на полный экран**
  - **Видео в реальном времени в квадрированном режиме**

#### **Макс. число строк областей изображений**

Выберите максимальное число строк областей изображений для отображения в окне изображений на соответствующем мониторе.

**Примечание:** этот параметр доступен только для следующих режимов просмотра.

- **Управление**
- **Только содержимое тревог**
- **Видео в реальном времени и содержимое тревог**
- **Только видео в реальном времени**

Остальные режимы просмотра имеют фиксированные схемы с фиксированным количеством строк окна изображений и не могут быть изменены.

#### **Соотношение сторон областей изображений**

Выберите необходимое соотношение сторон для каждого монитора для первоначального запуска Operator Client. Для камер HD используйте соотношение 16:9.

#### **Сохранить установки при выключении**

Установите флажок, чтобы система запоминала последнее состояние пользовательского интерфейса при отключении пользователя от Operator Client. Если этот флажок не установлен, Operator Client всегда запускается с настроенным интерфейсом пользователя.

#### **Восстановить значения по умолчанию**

Нажмите для восстановления на этой странице стандартных настроек. Все записи в списке восстанавливают свои исходные параметры.

## 24.15 Страница Доступ к серверу



Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  
> вкладка **Доступ к серверу**



Доступ к серверу настраивается на Enterprise Management Server. Необходимо ввести имя Enterprise Account и соответствующий пароль для каждого Management Server вашей системы Enterprise System. Эта учетная запись настраивается на каждом Management Server.

### Management Server

Отображает имя Management Server, настроенного на этом Enterprise Management Server.

### Сетевой адрес

Отображает частный IP-адрес или DNS-имя Management Server.

### Номер сервера

Отображает номер Management Server. Этот номер используется клавиатурой Bosch IntuiKey для выбора нужного Management Server.

### Доступ

Нажмите, чтобы выбрать, когда предоставлять доступ к серверу Management Server. Этот Management Server теперь является Enterprise Management Server.

### Access

Введите имя учетной записи Enterprise, настроенной на Management Server.

### Пароль учетной записи предприятия Enterprise Account

Нажмите, чтобы открыть диалоговое окно для ввода пароля учетной записи Enterprise, настроенной на сервере Management Server.

### Пароль учетной записи предприятия Enterprise Account

Отображает текст описания данного сервера.

Дополнительные столбцы отображаются, если они добавлены в список серверов.

### См.

- *Создание группы или учетной записи, Страница 365*
- *Создание системы Enterprise, Страница 89*
- *Настройка списка серверов для корпоративной системы, Страница 89*

## 24.16 Страница Разрешения конфигурации



Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >



**Рабочие разрешения** > вкладка **Разрешения конфигурирования**

или



Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  
> вкладка **Рабочие разрешения** > вкладка **Разрешения конфигурирования**



Позволяет настроить различные разрешения пользователей для Configuration Client. Разрешение для запуска Configuration Client подразумевает доступ только для чтения.

**Разрешения на вход**

Установите флажок для разрешения входа в приложение Configuration Client.

**Дерево устройств**

В этом разделе можно указать разрешения на стр. **Устройства**. Установите флажок для предоставления соответствующего разрешения.

**Карты и структура**

В этом разделе можно указать разрешения на стр. **Карты и структура**. Установите флажок соответствующего разрешения.

**Расписания**

В этом разделе можно указать разрешения на стр. **Расписания**. Установите флажок соответствующего разрешения.

**Камеры и запись**

В этом разделе можно указать разрешения на стр. **Камеры и запись**. Установите флажок соответствующего разрешения.

**События**

В этом разделе можно указать разрешения на стр. **События**. Установите флажок соответствующего разрешения.

**Тревожные сигналы**

В этом разделе можно указать разрешения на стр. **Тревожные сигналы**. Установите флажок соответствующего разрешения.

**Группы пользователей**

В этом разделе можно указать разрешения для настройки групп пользователей. Установите флажок соответствующего разрешения.

**Замечание!**

Флажок **Настройка групп пользователей** и флажок **Настроить пользователей** представляют собой взаимоисключающие параметры в целях безопасности.

**Команды меню**

В этом разделе можно указать разрешения для настройки команд меню. Установите флажок соответствующего разрешения.

**Отчеты**

В этом разделе можно указать разрешения для настройки отчетов. Установите флажок соответствующего разрешения.

**24.17****Страница Разрешения групп пользователей**

Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >



> вкладка **Рабочие разрешения** > вкладка **Разрешения группы пользователей**

или



Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >



> вкладка **Рабочие разрешения** > вкладка **Разрешения группы пользователей**

Позволяет установить, в какие группы пользователей пользователи определенной группы пользователей могут добавлять новых пользователей.



#### Замечание!

Вы можете назначать разрешения только для той группы пользователей, которой вы уже предоставили разрешение настраивать параметры пользователей. Вы можете назначить разрешение на странице **Разрешения конфигурирования** .



#### Замечание!



Пользователи из стандартной группы пользователей не имеют права добавлять новых пользователей в группу Admin. Этот флажок неактивен.



См.

– *Страница Разрешения конфигурации, Страница 356*

## 24.18

### Страница политик учетной записи


 Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >  > вкладка **Безопасность** > вкладка **Политики учетных записей** или


 Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Безопасность** > вкладка **Политики учетных записей**

Позволяет настроить параметры для пользователей и пароли.

#### Строгая политика паролей

Установите флажок, чтобы активировать политику требований к паролям.

Дополнительные сведения см. в разделе *Настройка пользователей, разрешений и корпоративного доступа, Страница 364*



#### Замечание!

Настройка **Строгая политика паролей** применяется только для пользователей, для группы которых установлен соответствующий флажок. Мы настоятельно рекомендуем сохранить этот параметр в целях обеспечения защиты вашего компьютера от несанкционированного доступа.

#### Минимальная длина пароля

Этот параметр определяет минимальное количество символов, которые может содержать пароль к учетной записи пользователя.

Установите флажок, чтобы активировать параметр, и введите минимальное количество символов.

#### Максимальный срок использования пароля в днях

Этот параметр определяет период времени (в днях), в течение которого пароль может использоваться, прежде чем система потребует от пользователя изменить его.

Установите флажок, чтобы активировать параметр, и введите максимальное количество дней.

**Число использованных паролей в журнале**

Этот параметр определяет количество уникальных новых паролей, которые должны быть использованы для учетной записи, прежде чем пользователь сможет повторно использовать старый пароль.

Установите флажок, чтобы активировать параметр, и введите минимальное количество паролей.

**Максимальное количество неудачных попыток входа**

Этот параметр позволяет задать отключение учетной записи после определенного числа неудачных попыток входа.

Установите флажок, чтобы активировать параметр, и введите максимальное количество попыток.

Если флажок **Максимальное количество неудачных попыток входа** установлен, можно задать два следующих параметра:

**Длительность блокировки учетной записи**

Этот параметр определяет время (в минутах), по истечении которого отключенная учетная запись автоматически включается.

Установите флажок, чтобы активировать параметр, и введите количество минут.

**Сброс счетчика блокировки учетной записи через**

Этот параметр определяет время (в минутах), которое должно пройти после того, как пользователю не удалось выполнить вход, чтобы счетчик неудачных попыток входа был обнулен.

Установите флажок, чтобы активировать параметр, и введите количество минут.

**Замечание!**

Если максимальное число неудачных попыток входа будет превышено, учетная запись будет отключена.

Если флажок **Длительность блокировки учетной записи** не установлен, учетную запись нужно будет включить вручную.

Если флажок **Длительность блокировки учетной записи** установлен, учетная запись будет включена автоматически по истечении заданного периода времени.

**Замечание!**

Счетчик неудачных попыток входа обнуляется:

после успешного входа

или по истечении заданного времени, если установлен флажок **Сброс счетчика блокировки учетной записи через**.

**Отключить автономный клиент**

Установите флажок, чтобы отключить вход в клиент в автономном режиме.

**Дополнительная информация**

В случае версий BVMS 9.0 и выше по умолчанию применяются следующие параметры

**Политики учетных записей.**

- Флажок **Строгая политика паролей** предварительно установлен.
- Флажок **Минимальная длина пароля** предварительно установлен. Значение по умолчанию — 10.
- Флажок **Максимальный срок использования пароля в днях** предварительно не установлен. Значение по умолчанию — 90.

- Флажок **Число использованных паролей в журнале** предварительно не установлен. Значение по умолчанию — 10.
  - Флажок **Максимальное количество неудачных попыток входа** предварительно не установлен. Значение по умолчанию — 1.
  - Флажок **Отключить автономный клиент** предварительно не установлен.
- Начиная с версии BVMS 10.0.1, указанные ниже параметры **Политики учетных записей** выбираются по умолчанию для всех групп пользователей:
- **Максимальное количество неудачных попыток входа**
  - **Длительность блокировки учетной записи**
  - **Сброс счетчика блокировки учетной записи через**

### 24.18.1

#### Operator Client в автономном режиме

Функция Operator Client в автономном режиме обеспечивает следующие варианты использования:

- Operator Client продолжает работу в режиме трансляции, воспроизведения и экспорта без подключения к компьютеру Management Server.
- Если рабочая станция однажды была подключена к компьютеру Management Server, она может в любой момент войти в систему в автономном режиме для любого пользователя.

Для использования автономного режима необходима версия BVMS 3.0 или выше.

Если рабочая станция Operator Client отключена от компьютера Management Server, можно продолжать работу. Доступны некоторые основные функции, например трансляция и воспроизведение видео.

В версии BVMS V5.5 рабочая станция Operator Client может работать автономно с конфигурацией BVMS V5.0.5.

#### Замечание!

Если смена пароля на Management Server происходит в то время, когда Operator Client находится в автономном режиме, смена пароля не распространяется на данный Operator Client.

Если Operator Client находится в режиме онлайн, пользователю следует войти в систему с использованием нового пароля.

Если Operator Client находится в автономном режиме, пользователю следует воспользоваться старым паролем для входа в систему. Пароль останется прежним до активации и переноса новой конфигурации на рабочую станцию Operator Client.



#### Замечание!

Если изображение с камеры выводится на дисплеи группы мониторов с помощью подключенной к рабочей станции клавиатуры Bosch Intuikey, а рабочая станция находится в автономном режиме, клавиатура не издает сигналов об ошибке.



#### 24.18.1.1

##### Работа в автономном режиме

Если клиент Operator Client отключен от сервера Management Server, соответствующий значок накладывается на отключенный Management Server в логическом дереве. Можно продолжать работать с клиентом Operator Client, даже если отключение продолжается долго, однако некоторые функции недоступны.

После восстановления соединения с сервером Management Server отображается соответствующий значок.



Если включена новая конфигурация Management Server, соответствующий значок отображается в логическом дереве поверх значка сервера Management Server, на который влияет изменение, и на несколько секунд открывается диалоговое окно. Примите новую конфигурацию или отклоните ее.

Если ваш экземпляр Operator Client должен выйти из системы в определенное время, выход выполняется, даже если соединение с сервером Management Server в этот момент не восстановлено.

Когда пользователь Operator Client входит в систему с использованием Поиска сервера в автономном режиме, отображается список серверов при последнем успешном входе в систему. Автономный режим в данном случае означает, что у рабочей станции Operator Client нет сетевого подключения к серверу, содержащему список серверов.

#### **Функции, недоступные при отключении**

При отсутствии подключения к серверу Management Server в клиенте Operator Client недоступны следующие функции.





- Список тревожных сигналов.  
Список включает обработку тревожных сигналов. Список тревожных сигналов пуст; он заполняется автоматически при восстановлении соединения.
- Allegiant.  
Недоступно управление магистральной линией. В предыдущих версиях камеры Allegiant автоматически закрывались с выводом сообщения при отсутствии доступа к управлению магистральной линией. С версии BVMS V3.0 отображается более удобная область изображений, информирующая пользователя о том, что отобразить данные с этой камеры сейчас невозможно.
- Группа мониторов.  
Невозможно перетаскивать камеры на элемент управления MG. Элемент управления отключен и включается автоматически при восстановлении соединения.
- Приоритеты PTZ.  
При отсутствии подключения к Management Server клиент Operator Client в автономном режиме может подключаться к камере PTZ, если сама камера PTZ не заблокирована. Приоритеты купольных камер обновляются автоматически при восстановлении соединения.
- Вход.  
Невозможно переключить вход.
- Журнал.  
Журнал недоступен, открыть его невозможно. Открытое окно поиска в журнале не закрывается автоматически. Можно использовать и экспортировать существующие результаты поиска.
- Комплект разработчика ПО Operator Client.  
Функции комплекта разработчика ПО Operator Client с IServerApi не обрабатываются. Невозможно создать RemoteClientApi.  
Не работают некоторые методы, доступные только через API клиента, например ApplicationManager (попробуйте GetUserName()).
- Изменение пароля.  
Оператор не может сменить свой пароль.
- Реле.  
Невозможно переключать реле.
- Серверный сценарий.  
Серверные методы интерфейса IServerApi обрабатываются, но не отправляются на клиент. К ним относятся следующие методы:

- AlarmManager
- AnalogMonitorManager
- CameraManager
- CompoundEventManager
- DecoderManager
- DeviceManager
- DomeCameraManager
- EventManager
- InputManager
- LicenseManager
- Журнал
- MatrixManager
- RecorderManager
- RelayManager
- ScheduleManager
- SendManager
- SequenceManager
- VirtualInputManager
- Наложения состояний.  
Недоступны наложения состояний камер, входов и реле.

### Состояния Operator Client


Клиент BVMS Operator Client предоставляет визуальную и текстовую информацию о своем состоянии.

Возможны следующие состояния Operator Client.

-  Клиент Operator Client подключен к серверу Management Server.
-  Клиент Operator Client не подключен к серверу Management Server. Возможная причина — физическое отключение от сети сервера Management Server.
-  Это состояние отображается только после восстановления подключения к серверу Management Server. Все соответствующие функции снова можно использовать, но конфигурация клиента Operator Client оказывается устаревшей, так как в сети доступна более новая конфигурация. Войдите в систему снова, чтобы обновить конфигурацию.
-  Этот значок состояния отображается, если на сервере Management Server установлена более ранняя версия BVMS, чем на рабочей станции Operator Client.

### Наложение состояний устройства

Состояния устройства (точка записи, слишком много помех, слишком темно и т. д.) обрабатываются сервером Management Server. При потере соединения между клиентом и сервером состояния клиента не обновляются. О недоступности всех состояний устройства оператора уведомляет новое графическое наложение состояний. Если клиент восстановил подключение к серверу, наложения состояний обновляются автоматически.

-  Состояние неизвестно  
Наложение состояний устройства в логическом дереве или на карте в ситуации, когда клиент отключен от компьютера Management Server.

**Причины отключения**

Возможные причины потери соединения между клиентом Operator Client и сервером Management Server:

- нарушено физическое соединение;
- в автономном режиме изменился пароль пользователя, выполнившего вход в систему;
- сервер Management Server передал свободную лицензию рабочей станции другому клиенту Operator Client, подключившемуся, пока текущий клиент Operator Client был в автономном режиме;
- разные версии Operator Client и Management Server (версия Management Server ниже 5.5).

## 25

## Настройка пользователей, разрешений и корпоративного доступа






Главное окно > **Группы пользователей**

В этой главе описано, как настраивать группы пользователей, групп Enterprise User Group и доступ Enterprise.

Вы можете настроить все разрешения на использование устройств и рабочие разрешения для группы пользователей, а не для отдельного пользователя.

Применяются следующие правила:

- Пользователь BVMS может быть членом только одной группы пользователей BVMS или Enterprise User Group. Пользователь LDAP может быть членом нескольких групп пользователей LDAP.
- Настройки пользовательской группы по умолчанию изменять нельзя.
- Эта группа пользователей имеет доступ ко всем устройствам полного логического дерева, и ей назначено расписание **Всегда**.
- Для доступа к пользовательским группам домена Windows используются пользовательские группы LDAP.

- Нажмите  для сохранения настроек.
- Нажмите  для отмены последней настройки.
- Нажмите  для активации конфигурации.

### Строгая политика паролей

Для повышения эффективности защиты компьютера от несанкционированного доступа рекомендуется использовать надежные пароли учетных записей пользователей.

В этих целях для всех вновь созданных групп пользователей по умолчанию активирована политика строгих требований к паролям. Это относится как к пользовательской группе Admin, так и стандартным пользовательским группам, группам Enterprise User Group и доступу Enterprise.

Применяются следующие правила:

- Минимальная длина пароля соответствует указанной на странице **Политики учетных записей** для соответствующих групп пользователей.
- Не используйте один из предыдущих паролей.
- Используйте по крайней мере одну букву в верхнем регистре (A–Z).
- Используйте по крайней мере одну цифру (0–9).
- Используйте по крайней мере один специальный символ (например, ! \$ # %).

При первом запуске пользователем Admin Configuration Client отображается диалоговое окно **Нарушена политика паролей** с предложением установить пароль для учетной записи администратора. Мы настоятельно рекомендуем сохранить этот параметр и задать надежный пароль для учетной записи Admin в соответствии с требованиями политики паролей.

При создании новой группы пользователей в Configuration Client политика строгих требований к паролям применяется по умолчанию. Если не задать пароли для новых учетных записей пользователей соответствующих пользовательских групп, вы не сможете активировать конфигурацию. Отобразится диалоговое окно **Нарушена политика паролей**, содержащее список всех пользователей, для которых пароль еще не задан. Для активации конфигурации необходимо задать недостающие пароли.

**См.**

- *Страница политик учетной записи, Страница 358*
- *Страница Свойства пользовательской группы, Страница 341*
- *Страница Свойства пользователей, Страница 342*
- *Страница Свойства комбинации для входа в систему, Страница 343*
- *Страница Разрешения камеры, Страница 344*
- *Страница Приоритеты управления, Страница 346*
- *Диалоговое окно Копировать разрешения пользовательской группы, Страница 346*
- *Страница Разрешения декодера, Страница 347*
- *Страница События и тревоги, Страница 347*
- *Диалоговое окно Настройки сервера LDAP, Страница 348*
- *Страница Учетные данные, Страница 349*
- *Страница Логическое дерево, Страница 350*
- *Страница Свойства оператора, Страница 351*
- *Страница Приоритеты, Страница 354*
- *Страница Интерфейс пользователя, Страница 354*
- *Страница Доступ к серверу, Страница 356*

## 25.1

### Создание группы или учетной записи



Главное окно > **Группы пользователей**

Вы можете создать стандартную группу пользователей, группу Enterprise User Group или Enterprise Account.

Чтобы разрешения группы пользователей соответствовали вашим требованиям, создайте новую группу и измените ее настройки.

#### 25.1.1

#### Создание стандартной группы пользователей



Главное окно > **Группы пользователей**

**Чтобы создать стандартную группу пользователей:**

1. перейдите на вкладку **Пользовательские группы**.



2. Нажмите . Откроется диалоговое окно **Создать группу пользователей**.

3. Введите имя и описание.

4. Нажмите кнопку **ОК**.

Новая группа добавляется в соответствующее дерево.

5. Щелкните по новой пользовательской группе правой кнопкой мыши и выберите **Переименовать**.

6. Введите нужное имя и нажмите клавишу ВВОД.

**См.**

- Страница Свойства пользовательской группы, Страница 341
- Страница Свойства оператора, Страница 351
- Страница Приоритеты, Страница 354
- Страница Интерфейс пользователя, Страница 354

## 25.1.2 Создание Enterprise User Group



Главное окно > **Группы пользователей**

Вы выполняете задачу создания Enterprise User Group для Enterprise System на Enterprise Management Server.

Вы создаете Enterprise User Group с пользователями для настройки их рабочих разрешений. Эти рабочие разрешения отображаются в Operator Client, подключенном к Enterprise Management Server. Примером рабочего разрешения является пользовательский интерфейс тревожного монитора.

### Чтобы создать Enterprise User Group:

1. Нажмите вкладку **Enterprise User Groups**.

**Примечание.** Вкладка **Enterprise User Groups** доступна только при наличии соответствующей лицензии и при условии, что один или несколько компьютеров



Management Server настроены в **Устройства > Система Enterprise > Список серверов / адресная книга**.

2. Нажмите . Откроется диалоговое окно **Создать группу пользователей Enterprise User Group**.
3. Введите имя и описание.
4. Нажмите кнопку **ОК**. Enterprise User Group добавлена в соответствующее дерево.
5. Щелкните правой кнопкой по новой группе Enterprise и выберите **Переименовать**.
6. Введите нужное имя и нажмите клавишу ВВОД.
7. На странице **Рабочие разрешения** требуемым образом настройте рабочие разрешения и доступ к серверу для настроенных компьютеров Management Server.

**См.**

- Страница Свойства пользовательской группы, Страница 341
- Страница Свойства оператора, Страница 351
- Страница Приоритеты, Страница 354
- Страница Интерфейс пользователя, Страница 354
- Страница Доступ к серверу, Страница 356

## 25.1.3 Создание Enterprise Account



Главное окно > **Группы пользователей**

**Замечание!**

Прежде чем вы сможете добавить Enterprise Account, необходимо задать конфигурацию по меньшей мере одного устройства в дереве устройств.

Вы выполняете задачу создания Enterprise Account на Management Server. Повторите те же действия на каждом Management Server, являющемся элементом вашей Enterprise System. Вы создаете Enterprise Account для настройки разрешений для устройств Operator Client с помощью Enterprise System.

**Чтобы создать Enterprise Account:**

1. Перейдите на вкладку **Доступ Enterprise**.
2. Нажмите .  
Откроется диалоговое окно **Создать учетную запись Enterprise Account**.
3. Введите имя и описание.
4. Флажок **Пользователь должен изменить пароль при следующем входе в систему** предварительно установлен для всех вновь созданных учетных записей.  
Введите пароль в соответствии с требованиями к паролям и подтвердите его.
5. Нажмите кнопку **ОК**.  
Новая учетная запись Enterprise Account добавлена в соответствующее дерево.
6. Щелкните правой кнопкой по новой Enterprise Account и выберите **Переименовать**.
7. Введите нужное имя и нажмите клавишу ВВОД.
8. На странице **Разрешения для устройств** настройте, если требуется, учетные данные, а также разрешения устройств.

**См.**

- *Строгая политика паролей*, Страница 364
- *Страница Учетные данные*, Страница 349
- *Страница Логическое дерево*, Страница 350
- *Страница События и тревоги*, Страница 347
- *Страница Приоритеты управления*, Страница 346
- *Страница Разрешения камеры*, Страница 344
- *Страница Разрешения декодера*, Страница 347

## 25.2

### Создание пользователя



Главное окно >  
или

**Группы пользователей** > вкладка **Пользовательские группы**



Главное окно >



**Группы пользователей** > вкладка **Enterprise User Groups**

Пользователь создается как новый член существующей стандартной группы пользователей или группы Enterprise User Group.

**Замечание!**

Имя и пароль пользователя, желающего работать с клавиатурой Bosch IntuiKey, подключенной к декодеру, должны состоять исключительно из цифр. Имя пользователя должно содержать не менее 3 цифр, а пароль — не менее 6 цифр.

**Чтобы создать пользователя:**

1. выберите группу и нажмите  или щелкните правой кнопкой по необходимой группе и выберите **Новый пользователь**.  
Новый пользователь будет добавлен в дерево **Группы пользователей**.
2. щелкните правой кнопкой мыши по новому пользователю и выберите **Переименовать**.
3. Введите нужное имя и нажмите клавишу ВВОД.
4. На странице **Свойства пользователей** введите имя пользователя и описание.
5. Флажок **Пользователь должен изменить пароль при следующем входе в систему** предварительно установлен для всех вновь созданных учетных записей пользователей.  
Введите пароль в соответствии с требованиями политики и подтвердите его.
6. нажмите **Применить** для применения настроек.
7. Нажмите  для активации пароля.

**См.**

- *Страница Свойства пользователей, Страница 342*
- *Строгая политика паролей , Страница 364*
- *Страница Пользовательские группы, Страница 339*

**25.3****Создание группы с двойной авторизацией**

Главное окно > **Группы пользователей** > вкладка **Пользовательские группы**  
или



Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups**

Вы можете создать двойную авторизацию для стандартной группы пользователей или для Enterprise User Group.

Для доступа Enterprise двойная авторизация недоступна.

Вы выбираете две пользовательских группы. Члены этих групп пользователей становятся членами новой группы с двойной авторизацией.

**Чтобы создать группу с двойной авторизацией:**



1. Нажмите кнопку .  
Откроется диалоговое окно **Создать группу с двойной авторизацией** или диалоговое окно **Создать группу Enterprise с двойной авторизацией** соответственно.
2. Введите имя и описание.
3. Нажмите **ОК**.  
Новая группа с двойной авторизацией будет добавлена в соответствующее дерево.
4. Щелкните правой кнопкой мыши новую группу с двойной авторизацией и нажмите **Переименовать**.
5. Введите нужное имя и нажмите клавишу ВВОД.





**См.**


- *Добавление комбинации для входа в систему к группе с двойной авторизацией, Страница 369*
- *Страница Свойства пользовательской группы, Страница 341*
- *Страница Свойства оператора, Страница 351*
- *Страница Приоритеты, Страница 354*
- *Страница Интерфейс пользователя, Страница 354*

**25.4****Добавление комбинации для входа в систему к группе с двойной авторизацией**


 Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >
   

**Создать группу с двойной авторизацией**


 Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >
 
  
**Создать группу Enterprise с двойной авторизацией**

**Чтобы добавить комбинацию для входа в систему к группе с двойной авторизацией:**

1. выберите требуемую группу с двойной авторизацией и нажмите кнопку  или щелкните правой кнопкой по группе и выберите **Новая комбинация для входа в систему**.  
Отображается соответствующее диалоговое окно.
2. Выберите группу пользователей из каждого списка.  
Пользователи первой группы пользователей вводят свои данные в первом диалоговом окне входа в систему, а пользователи второй группы пользователей подтверждают вход в систему.  
Вы можете выбрать одну и ту же группу в обоих списках.
3. Для каждой группы выберите **Форсировать двойную авторизацию** при необходимости.  
Когда этот флажок установлен, каждый пользователь из первой группы может входить в систему только вместе с пользователем из второй группы.  
Когда этот флажок не установлен, каждый пользователь из первой группы может войти систему отдельно, при этом пользуясь только правами доступа своей группы.
4. Нажмите кнопку **ОК**.  
Новая комбинация для входа в систему будет добавлена в соответствующую группу с двойной авторизацией.
5. Щелкните правой кнопкой мыши по новой комбинации для входа в систему и нажмите кнопку **Переименовать**.
6. Введите нужное имя и нажмите клавишу ВВОД

**См.**

- *Создание группы с двойной авторизацией, Страница 368*
- *Страница Свойства комбинации для входа в систему, Страница 343*

## 25.5 Настройка группы администраторов




Главное окно > **Группы пользователей** > вкладка **Пользовательские группы**




группа администраторов

Позволяет добавлять новых пользователей, переименовывать существующих пользователей и удалять их из группы администраторов.

### Чтобы добавить нового пользователя в группу администраторов:

1. Нажмите кнопку  или нажмите правой кнопкой мыши на группу администраторов и нажмите **Добавить нового пользователя**.  
В группу администраторов будет добавлен новый пользователь.
2. На странице **Свойства пользователей** введите имя пользователя и описание.
3. Флажок **Пользователь должен изменить пароль при следующем входе в систему** предварительно установлен для всех вновь созданных учетных записей.  
Введите пароль в соответствии с требованиями к паролям и подтвердите его.
4. нажмите **Применить** для применения настроек.



5. Нажмите  для активации пароля.

### Чтобы переименовать пользователя-администратора:

1. Щелкните правой кнопкой мыши нужного пользователя-администратора и нажмите кнопку **Переименовать**.
2. Введите нужное имя и нажмите клавишу ВВОД.



3. Нажмите , чтобы активировать изменение имени пользователя.

### Чтобы удалить пользователя из группы администраторов:

- ▶ Щелкните правой кнопкой мыши нужного пользователя и нажмите кнопку **Удалить**.  
Пользователь будет удален из группы администраторов.

### Примечание.

Вы можете удалить пользователя из группы администраторов только в том случае, если существуют другие пользователи-администраторы.

Если в группе администраторов всего один пользователь, его невозможно удалить.

### См.

- *Страница Пользовательские группы, Страница 339*
- *Страница Свойства пользователей, Страница 342*
- *Строгая политика паролей, Страница 364*

## 25.6 Настройка параметров LDAP



Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >



> вкладка **Рабочие разрешения**

или



Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  
> вкладка **Рабочие разрешения**



#### Замечание!

Внимательно вводите пути для поиска. Неверно указанные пути могут существенно замедлить поиск на сервере LDAP.



#### Замечание!

Пользователь LDAP может быть связан с несколькими группами пользователей LDAP, которые, в свою очередь, связаны с определенной группой пользователей BVMS. Пользователь LDAP получает права группы пользователей BVMS, которая расположена выше других групп пользователей LDAP, связанных с этим пользователем LDAP.

Настройка групп LDAP осуществляется в стандартных группах пользователей или в Enterprise User Groups.

#### Чтобы настроить параметры LDAP:

1. Щелкните вкладку **Свойства пользовательской группы**.
  2. В поле **Свойства LDAP** введите соответствующие параметры.
- Для получения подробной информации о различных полях щелкните ссылку на соответствующее окно приложения ниже.

#### См.

- *Диалоговое окно Настройки сервера LDAP, Страница 348*
- *Страница Свойства пользовательской группы, Страница 341*

## 25.7

### Связывание группы LDAP



Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >



> вкладка **Рабочие разрешения**  
или



Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  
> вкладка **Рабочие разрешения**



Группу LDAP можно связать с группой пользователей BVMS, чтобы пользователи этой группы LDAP имели доступ к Operator Client. Пользователи группы LDAP имеют права доступа группы пользователей в соответствии с настройками группы LDAP. Возможно, потребуется помощь ИТ-администратора, ответственного за сервер LDAP. Группы LDAP настраиваются в стандартных группах пользователей или в Enterprise User Groups.



#### Замечание!

Если группа LDAP связана с группой пользователей BVMS, пользователи этой группы LDAP могут запускать Operator Client с использованием единого входа.

**Чтобы связать группу LDAP:**

1. Перейдите на вкладку **Свойства пользовательской группы**.
2. В поле **Свойства LDAP** нажмите **Настройки**.  
Отображается диалоговое окно **Настройки сервера LDAP**.
3. Введите параметры вашего сервера LDAP и нажмите **ОК**.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.



Для получения подробной информации о различных полях щелкните ссылку на соответствующее окно приложения ниже.



- ▶ В списке **Группы LDAP** дважды щелкните мышью группу LDAP.  
Эта группа LDAP будет введена в поле **Связанная группа LDAP**.

**См.**

- *Диалоговое окно Настройки сервера LDAP, Страница 348*
- *Страница Свойства пользовательской группы, Страница 341*

**25.8****Составление расписания разрешений на вход пользователей в систему**



 Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >  > вкладка **Рабочие разрешения**  
или



 Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Рабочие разрешения**  
Вы можете запретить членам определенной пользовательской группы или Enterprise User Group входить в систему с их компьютеров в определенные периоды времени. Вы не можете изменить эти настройки для пользовательской группы по умолчанию.

**Составление расписания входа в систему**

1. Перейдите на вкладку **Свойства пользовательской группы**.
2. В списке **Расписание входа в систему** выберите расписание.

**25.9****Настройка рабочих привилегий**

 Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** >  > вкладка **Рабочие разрешения**  
или

 Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Рабочие разрешения**

- Вы можете настроить рабочие разрешения, такие как доступ к журналу событий Logbook и параметры пользовательского интерфейса.
- Вы не можете изменить эти параметры для группы пользователей по умолчанию.

- Рабочие разрешения настраиваются в стандартных группах пользователей или группах Enterprise User Group.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

Для получения подробной информации о различных полях щелкните ссылку на соответствующее окно приложения ниже.

**См.**

- *Страница Свойства пользовательской группы, Страница 341*
- *Страница Свойства оператора, Страница 351*
- *Страница Приоритеты, Страница 354*
- *Страница Интерфейс пользователя, Страница 354*
- *Страница Доступ к серверу, Страница 356*

## 25.10

### Настройка разрешений устройств



Главное окно > **Группы пользователей** > вкладка **Пользовательские группы** > вкладка **Разрешения для устройств**  
или



Главное окно > **Группы пользователей** > вкладка **Доступ Enterprise** > вкладка **Разрешения для устройств**

Разрешения для всех устройств логического дерева можно задавать отдельно.

После перемещения разрешенных устройств в папку, не имеющую разрешений для данной группы пользователей, следует установить разрешения для этой папки, чтобы обеспечить доступ к устройствам.

- Вы не можете изменить эти параметры для группы пользователей по умолчанию.
- Разрешения устройств настраиваются в стандартных группах пользователей или корпоративных учетных записях.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

Для получения подробной информации о различных полях щелкните ссылку на соответствующее окно приложения ниже.

**См.**

- *Страница Логическое дерево, Страница 350*
- *Страница События и тревоги, Страница 347*
- *Страница Приоритеты управления, Страница 346*
- *Страница Разрешения камеры, Страница 344*
- *Страница Разрешения декодера, Страница 347*

## 25.11

### Настройка различных приоритетов



Главное окно > **Группы пользователей** > вкладка **Пользовательские группы**  
или



Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups**  
или



Главное окно > **Группы пользователей** > вкладка **Доступ Enterprise**

Можно настроить следующие приоритеты:

- Стандартные группы пользователей и **Enterprise User Groups**: можно настроить приоритеты тревожных сигналов для режимов живого просмотра и воспроизведения.
- Для стандартных групп пользователей и **Доступ Enterprise**: можно настроить приоритеты для получения управления PTZ и магистральных линий Bosch Allegiant. Можно задать период времени для блокировки PTZ, т. е. пользователь с более высоким приоритетом может забрать управление камерой у пользователя с более низким приоритетом и заблокировать доступ на это время.

**Настройка приоритетов для режима реального времени и воспроизведения:**

1. Выберите стандартную пользовательскую группу или Enterprise User Group.
2. Нажмите кнопку **Рабочие разрешения**.
3. Перейдите на вкладку **Приоритеты**.
4. В поле **Поведение автоматически всплывающих окон** переместите ползунок в нужное положение.

**Настройка приоритетов для PTZ и магистральных линий Bosch Allegiant:**

1. Выберите стандартную пользовательскую группу или Enterprise Account.
2. Перейдите на вкладку **Разрешения для устройств**.
3. Перейдите на вкладку **Приоритеты управления**.
4. В поле **Приоритеты управления** переместите ползунок в нужное положение.
5. Выберите нужный элемент из списка **Время ожидания в мин..**

**См.**

- *Страница Приоритеты управления, Страница 346*
- *Страница Приоритеты, Страница 354*

## 25.12

### Копирование разрешений пользовательской группы



Главное окно > **Группы пользователей** > вкладка **Пользовательские группы**  
или



Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups**  
или




Главное окно > **Группы пользователей** > вкладка **Доступ Enterprise**

Разрешения для одной группы или учетной записи можно копировать для другой. Необходимо настроить по крайней мере 2 группы или учетные записи.

**Копирование разрешений:**

1. Выберите в дереве пользовательских групп группу или учетную запись.

2. Нажмите  .  
Откроется диалоговое окно **Копировать разрешения пользовательской группы**.
3. Выберите соответствующие разрешения и соответствующую группу или учетную запись.
4. Нажмите **ОК**. Разрешения данной группы будут скопированы в другую группу или учетную запись. Диалоговое окно закроется.

## 26 Настройка обнаружения пожара с помощью видео

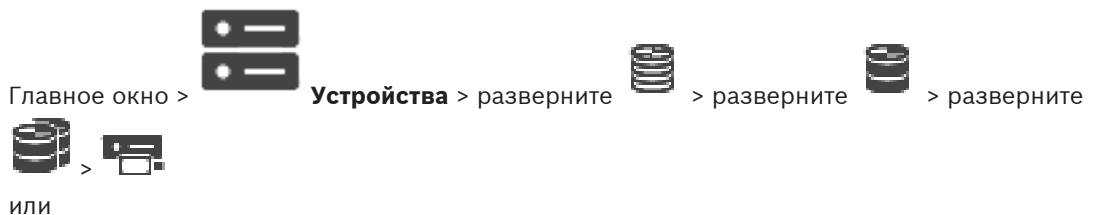
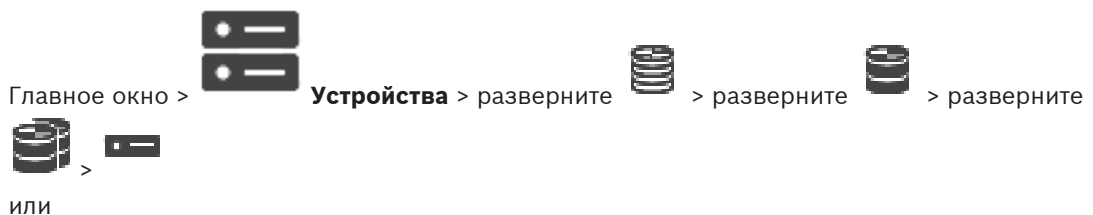
Чтобы настроить обнаружение пожара с помощью видео, необходимо выполнить следующие действия.

1. Настройте обнаружение пожара на камере, поддерживающей эту функцию.  
Это делается на веб-странице камеры.  
Подробную информацию о настройке камеры для обнаружения пожара см. в разделе – *Настройка камеры для обнаружения пожара, Страница 376*
2. Добавьте эту камеру для обнаружения пожара в систему. Можно добавить камеру для обнаружения пожара в пул VRM, как кодер, работающий только в режиме реального времени, или как кодер с локальным хранилищем.  
Подробную информацию о добавлении камеры см. в разделе – *Добавление кодера в пул VRM, Страница 228*  
– *Добавление кодера, работающего только в режиме реального времени, Страница 228*  
– *Добавление кодера локального хранилища, Страница 228*
3. Настройте событие пожара для этой камеры.  
– *Настройка события пожара, Страница 379*
4. Настройте тревожный сигнал для события пожара.  
– *Настройка тревожного сигнала пожара, Страница 379*

**См.**

- *Добавление кодера в пул VRM, Страница 377*
- *Добавление кодера, работающего только в режиме реального времени, Страница 228*
- *Добавление кодера локального хранилища, Страница 228*
- *Настройка события пожара, Страница 379*
- *Настройка тревожного сигнала пожара, Страница 379*

### 26.1 Настройка камеры для обнаружения пожара





Чтобы настроить обнаружение пожара с помощью видео, сначала необходимо настроить обнаружение пожара на соответствующей камере.  
 Подробные сведения см. в руководстве по эксплуатации камеры для обнаружения пожара.

#### Настройка

1. Щелкните правой кнопкой мыши значок устройства и выберите команду **Показать страницу в браузере**.
2. Нажмите **Конфигурация**.
3. На панели навигации разверните узел **Тревога** и выберите пункт **Обнаружение пожара**.
4. Введите требуемые параметры.

## 26.2 Добавление кодера в пул VRM

Сведения о добавлении кодеров в пул VRM см. в разделе *Добавление кодеров путем поиска, Страница 187*.

См.

– *Добавление устройства, Страница 124*

## 26.3 Добавление кодеров путем поиска

Для добавления кодеров путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск кодеров**. Откроется диалоговое окно **BVMS Scan Wizard**.
2. Выберите необходимые кодеры, выберите необходимый пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.
3. Нажмите **Далее >>**.  
Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.  
Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.  
Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**. Затем щелкните это поле правой кнопкой мыши и выберите **Копировать ячейку в столбец**.

В столбце **Состояние** успешные подключения обозначены значком .

Неудачные подключения обозначены значком .

, что означает, что для устройства требуется начальный пароль.

Для установки начального пароля введите его в поле **Пароль**.

Статус изменится на .

Повторите эти действия для всех устройств, которые требуют первоначальный пароль.


**Примечание:** пока вы не установили первоначальный пароль для всех устройств в списке, которые требуют начальный пароль, вы не сможете продолжить работу.


5. Нажмите **Готово**.  
Устройство добавлено в дерево устройств.

## 26.4

**Добавление устройств, работающих только в режиме реального времени, путем поиска**

Для добавления устройств Bosch, работающих только в реальном времени, путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск кодеров, работающих только в реальном времени**.  
Откроется диалоговое окно **BVMS Scan Wizard**.
2. Установите флажки для устройств, которые необходимо добавить.
3. Нажмите **Далее >>**.  
Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.  
Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.  
Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.  
Затем щелкните это поле правой кнопкой мыши и выберите **Копировать ячейку в столбец**.

В столбце **Состояние** успешные подключения обозначены значком .

Неудачные подключения обозначены значком .



, что означает, что для устройства требуется начальный пароль.

Для установки начального пароля введите его в поле **Пароль**.



Статус изменится на .




Повторите эти действия для всех устройств, которые требуют первоначальный пароль.

**Примечание:** пока вы не установили первоначальный пароль для всех устройств в списке, которые требуют начальный пароль, вы не сможете продолжить работу.


5. Нажмите **Готово**.  
Устройство добавлено в дерево устройств.

## 26.5


**Добавление кодеров локального хранилища путем поиска**

Главное окно >  **Устройства** > разверните  > .  
Позволяет добавлять и настраивать кодеры с локальным хранилищем.

Для добавления кодеров локального хранилища путем поиска выполните следующие действия.

1. В дереве устройств щелкните  правой кнопкой мыши и выберите **Поиск кодеров локального хранилища**.  
Откроется диалоговое окно **BVMS Scan Wizard**.
2. Установите флажки для устройств, которые необходимо добавить.
3. Нажмите **Далее >>**.  
Откроется диалоговое окно мастера **Проверки подлинности устройств**.

- Введите пароль для каждого устройства, защищенного паролем. Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля. Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**. Затем щелкните это поле правой кнопкой мыши и выберите **Копировать ячейку в столбец**.

В столбце **Состояние** успешные подключения обозначены значком .

Неудачные подключения обозначены значком .

, что означает, что для устройства требуется начальный пароль.

Для установки начального пароля введите его в поле **Пароль**.

Статус изменится на .

Повторите эти действия для всех устройств, которые требуют первоначальный пароль.

**Примечание:** пока вы не установили первоначальный пароль для всех устройств в списке, которые требуют начальный пароль, вы не сможете продолжить работу.

- Нажмите **Готово**. Устройство добавлено в дерево устройств.

## 26.6 Настройка события пожара



Главное окно >  **События**

### Настройка

- В дереве выберите **Кодеры/Декодеры > Камера > Состояние пожара или задымления > Пожар или задымление обнаружены**. Откроется соответствующая таблица настройки событий.
- В столбце **Активировать тревогу - Расписание** нажмите ячейку и выберите соответствующее расписание. Расписание определяет, когда запускается тревожный сигнал. Выберите одно из расписаний записей или расписаний задач, настроенных на странице **Расписания**.
- Установите требуемые параметры.

**Примечание.** Эту процедуру можно использовать для других доступных событий пожара.

## 26.7 Настройка тревожного сигнала пожара



Главное окно >  **Тревожные сигналы**

### Настройка

- В дереве выберите **Кодеры/Декодеры > Камера > Состояние пожара или задымления > Пожар или задымление обнаружены**. Отображается соответствующая таблица настройки тревог.
- Установите требуемые параметры.

## 27

## Настройка MIC IP 7000, подключенного к VIDEOJET 7000 connect

Для правильной работы камеры MIC IP 7000, подключенной к VIDEOJET 7000 connect, необходимо установить следующую конфигурацию.

Перед добавлением камеры MIC IP в систему BVMS выполните следующие действия:

1. Восстановите на камере MIC IP 7000 и устройстве VIDEOJET 7000 connect заводские параметры по умолчанию (это делается на веб-страницах устройств).
2. Установите для камеры MIC IP 7000 вариант использования **MIC IP Starlight 7000 HD-VJC-7000**.
3. Настройте камеру MIC IP 7000 и устройство VIDEOJET 7000 connect в соответствии с документацией, которая входит в комплект поставки устройств.
4. Если вы хотите использовать ANR, запустите сервисную программу установки ANR для устройства VIDEOJET 7000 connect.

Выполните эту задачу на компьютере, входящем в ту же сеть, что и устройство VIDEOJET 7000 connect.

Сервисную программу установки ANR можно найти на странице каталога продуктов для устройства VIDEOJET 7000 connect.

Выполните следующую процедуру, чтобы добавить камеру MIC IP 7000 в систему BVMS и настроить ее:

1. В дерево устройств добавьте только камеру MIC IP 7000.  
Устройство VIDEOJET 7000 connect нельзя добавить в систему BVMS.
2. Щелкните добавленную камеру правой кнопкой мыши и выберите команду **Изменить кодер**.  
Откроется диалоговое окно **Изменить кодер**.  
Возможности устройства загружаются автоматически в соответствии с выбранным выше вариантом.
3. При необходимости настройте ANR на странице **Камеры и запись**.

## 28 Устранение неполадок

В данном разделе содержится информация об устранении неполадок при использовании BVMS Configuration Client.

### Проблемы, возникающие после обновления Bosch Video Management System

Проблема	Причина	Решение
NVR не ведет запись после обновления системы Bosch Video Management System.	Соединение между сетевым видеорегистратором и сервером управления было прервано после обновления. После обновления, возможно, была изменена база данных BVMS на Management Server. Сетевой видеорегистратор должен «знать» об этих изменениях.	Восстановите соединение между сетевым видеорегистратором и сервером управления.

### Проблемы, возникающие при установке

Проблема	Причина	Решение
Программа установки отображает неверные символы.	Неверные языковые настройки Windows.	<i>Настройка языка в Windows, Страница 383</i>
Программа установки прерывается с сообщением о невозможности установить .	Файлы сервера OPC невозможно заменить.	Удалите OPC Core Components Redistributable и запустите программу установки BVMS еще раз.
Программное обеспечение не может быть удалено с помощью Настройки.		Запуск Control Panel > Add/Remove Programs и удаление BVMS.

### Проблемы, возникающие сразу после запуска приложения.

Проблема	Причина	Решение
BVMS отображается не на том языке.	В настройках Windows не установлен нужный язык	<i>Настройка языка Configuration Client, Страница 73</i> или <i>Настройка языка Operator Client, Страница 73</i>
Окно входа в систему Operator Client отображается не на том языке.	Несмотря на установку языка Operator Client в Configuration Client, язык окна входа в систему Operator Client зависит от языка Windows.	<i>Настройка языка в Windows, Страница 383</i>

**Проблемы с отображением языка**

Проблема	Причина	Решение
Отдельные тексты в Configuration Client или Operator Client отображаются на иностранном языке, чаще всего английском.	Язык операционной системы компьютера, на котором установлен Management Server, часто является английским. Поэтому когда на этом компьютере создается база данных BVMS, многие тексты также создаются на английском языке. Они остаются неизменными, независимо от языка Windows на компьютере с Operator Client. Чтобы избежать подобных языковых противоречий, установите программное обеспечение Management Server на компьютере с нужным языком интерфейса Windows.	Не изменяйте этого.

**Проблемы с клавиатурой Bosch IntuiKey**

Проблема	Причина	Решение
Клавиатура Bosch IntuiKey вызывает тревожный сигнал, а на дисплее отображается сообщение Off Line.	Прервано соединение с рабочей станцией. Поврежден или отключен кабель либо перезапущена рабочая станция.	<i>Повторная установка соединения с клавиатурой Bosch IntuiKey, Страница 384</i>

**Проблемы с настройкой панели управления звуковой картой**

Проблема	Причина	Решение
Обратная связь возникает при использовании микрофона в системе внутренней связи.	На панели управления звуковой картой должен быть выбран только микрофон, а не стереомикшер (или что-либо иное). Operator Client проверяет файл конфигурации при запуске и соответствующим образом изменяет настройки панели управления. В данном файле конфигурации имеется стандартный	Измените параметр в файле конфигурации Operator Client на микрофон.

Проблема	Причина	Решение
	параметр, который может не соответствовать данной системной конфигурации. Этот параметр восстанавливается при каждом запуске Operator Client.	

#### Аварийное завершение Configuration Client

Проблема	Причина	Решение
Configuration Client аварийно завершает работу.	При большом количестве камер, настроенных в файле Allegiant и не подключенных к Bosch Video Management System, следует сократить это количество. Это позволяет избежать дополнительной нагрузки на систему.	См. <i>Сокращение количества камер Allegiant</i> , Страница 384.



#### Поддержка

Наша **служба поддержки** доступна по адресу <https://www.boschsecurity.com/xc/en/support/>.

Bosch Security and Safety Systems предоставляет поддержку по следующим направлениям:

- [Приложения и инструменты](#)
- [Информационное моделирование здания](#)
- [Ввод в эксплуатацию](#)
- [Гарантия](#)
- [Устранение неисправностей](#)
- [Ремонт и замена](#)
- [Безопасность продуктов](#)



#### Bosch Building Technologies Academy

Посетите веб-сайт академии Bosch Building Technologies Academy и получите доступ к **учебным курсам, видеоучебникам и документам**: <https://www.boschsecurity.com/xc/en/support/training/>

## 28.1

### Настройка языка в Windows

Если нужно изменить язык отображения программы установки BVMS, нужно изменить язык в Windows. Для активации языковых настроек компьютер следует перезапустить после выполнения следующих действий.

**Чтобы настроить нужный язык.**

1. Нажмите кнопку **Пуск**, выберите **Панель управления** и дважды щелкните **Язык и региональные стандарты**.

2. Перейдите на вкладку **Дополнительно** и выберите нужный язык в поле **Язык программ, не поддерживающих Юникод**.
3. Нажмите **ОК**.
4. В каждом следующем окне сообщения нажмите **Да**.  
Компьютер будет перезагружен.

## 28.2 Повторная установка соединения с клавиатурой Bosch IntuiKey

1. Подключите кабель или дождитесь, пока рабочая станция войдет в оперативный режим.  
Отображается сообщение Off Line.
2. Нажмите программную клавишу Terminal для входа в BVMS.

## 28.3 Сокращение количества камер Allegiant

Для редактирования файла Allegiant требуется программное обеспечение Master Control Software.

### Для сокращения количества камер Allegiant:

1. Запустите Master Control Software.
2. Откройте файл Allegiant.
3. Перейдите на вкладку Camera.
4. Отметьте камеры, использование которых не является необходимым.
5. В меню Edit выберите пункт Delete.
6. Сохраните файл. Размер файла остается неизменным.
7. Повторите последнее действие для мониторов, использование которых не является необходимым. Перейдите на вкладку Monitors.
8. Импортируйте этот файл в Bosch Video Management System (см. *Добавление устройства, Страница 124*).

## 28.4 Используемые порты

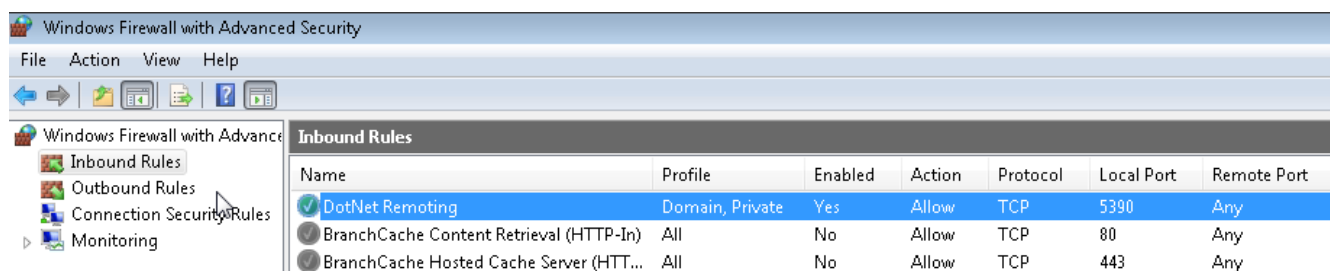
В этом разделе перечислены все компоненты портов BVMS, которые должны быть открыты в локальной сети. Не открывайте эти порты для доступа через Интернет! Для доступа через Интернет используйте безопасные соединения, такие как VPN или удаленный доступ.

В каждой таблице перечислены локальные порты, которые должны быть открыты на компьютере, где установлено серверное ПО, или на маршрутизаторе/коммутаторе уровня 3, подключенном к оборудованию.

В брандмауэре Windows настройте правило входящих подключений для каждого открытого порта.

Разрешите все исходящие подключения для всех приложений BVMS.

### Пример простого правила входящих подключений брандмауэра Windows 7





### Порты Management Server / Enterprise Management Server

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Management Server	UDP	123	Кодек	TimeServer NTP
Management Server	TCP	5322	Operator Client,	Подключение SSH
Management Server	TCP	5389	Устройство ONVIF	Прокси ONVIF, уведомления о событиях
Management Server	TCP	5390	Operator Client, Configuration Client,	Удаленная среда .NET
Management Server	TCP	5392	Operator Client, Configuration Client, Mobile Video Service, Приложение BVMS SDK	WCF, gateway.push.apple.com
Management Server	TCP	5393	Operator Client, VRM, MVS	Data-Access-Service
Management Server	TCP	5395	Configuration Client, Operator Client	Настройки пользователя, передача файлов
Management Server	UDP	12544	Клиент SNMP	Приемный (get) порт SNMP BVMS

### Порты Video Recording Manager

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
VRM	TCP	554	Клиент RTSP	Получить поток RTSP
VRM	TCP	1756	Management Server, Configuration Client	через RCP+
VRM	UDP	1757	Management Server, Operator Client	Сканировать целевой объект широковещательного вещания
VRM	UDP	1758	Management Server, Configuration Client	Отклик сканирования
VRM	UDP	1800	Management Server, Operator Client	Сканировать целевой объект многоадресной передачи
VRM	TCP	80	Operator Client	Воспроизведение основного VRM через http

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
VRM	TCP	443	Operator Client	Воспроизведение основного VRM через https
VRM	TCP	81	Operator Client	Воспроизведение вторичного VRM через http
VRM	TCP	444	Operator Client	Воспроизведение вторичного VRM через https

#### Порты Mobile Video Service

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Mobile Video Service	TCP	80	Management Server, Operator Client, Configuration Client, HTML-клиент, мобильные приложения	Доступ через http
Mobile Video Service	TCP	443	Management Server, Operator Client, Configuration Client, HTML-клиент, мобильные приложения	Доступ через https
Mobile Video Service	TCP	2195	Удаленное уведомление Apple	Mac iOS
Mobile Video Service	UDP	1064-65535	Кодер, VRM	
Транскодер Mobile Video Service	TCP	5382	Мобильный провайдер Mobile Video Service	Поток медиа
Транскодер Mobile Video Service	TCP	5385	Мобильный провайдер Mobile Video Service	Поток медиа
Провайдер Mobile Video Service BVMS	TCP	5383	Operator Client	Поток медиа
Мобильный провайдер Mobile Video Service	TCP	5384	HTML-клиент, мобильные приложения	Поток медиа
Транскодер Mobile Video Service	TCP	5385	Мобильный провайдер Mobile Video Service	Поток медиа

### Порты системы хранения iSCSI

Настройте перенаправление портов на подключенном маршрутизаторе для этого устройства.

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Система хранения iSCSI	TCP	3260	Кодек, VRM, Configuration Client	

### Порты Bosch Video Streaming Gateway

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Bosch Video Streaming Gateway	TCP	8756-8762	VRM, Management Server, Configuration Client	RCP +
Bosch Video Streaming Gateway	TCP	8080-8086	VRM, Management Server, Configuration Client, Operator Client	HTTP
Bosch Video Streaming Gateway	TCP	8443-8449	VRM, Management Server, Configuration Client, Operator Client	HTTPS
Bosch Video Streaming Gateway	TCP	1757	VRM Configuration Client	Сканировать целевой объект широкоэвещательной передачи
Bosch Video Streaming Gateway	TCP	1758	VRM Configuration Client	Отклик сканирования
Bosch Video Streaming Gateway	TCP	1800	VRM Configuration Client	Сканировать целевой объект многоадресной передачи
Bosch Video Streaming Gateway	UDP	1064-65535	Кодек, VRM	

### Порты камеры ONVIF

Настройте перенаправление портов на подключенном маршрутизаторе для этого устройства.

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Камера ONVIF	TCP	80	Management Server, VSG, Configuration Client, Operator Client	Доступ через http
Камера ONVIF	TCP	443	Management Server, VSG, Configuration Client, Operator Client	Доступ через https
Камера ONVIF	RTSP	554	Management Server, VSG, Configuration Client, Operator Client	

#### Порты BVMS Operator Client / Cameo SDK

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Operator Client	TCP	5394	Приложение BVMS SDK, BIS	WCF
Operator Client	UDP	1024-65535	Кодер, VRM	Поток в режиме реального времени
Operator Client	TCP	443	Кодер	Удаленный доступ, просмотр зашифрованного видео в режиме реального времени

#### Порты кодера

Настройте перенаправление портов на подключенном маршрутизаторе для этого устройства.

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Кодер	TCP	1756	Декодер, Management Server, VRM, Operator Client, Configuration Client, приложение BVMS SDK	через RCP+
Кодер	UDP	1757	Декодер, Management Server, Operator Client	Сканировать целевой объект
Кодер	UDP	1758	Декодер, Management Server, Operator Client	Отклик сканирования
Кодер	UDP	1800	Декодер, Management Server, Operator Client	Сканировать целевой объект многоадресной передачи
Кодер	TCP	80	Operator Client, приложение BVMS SDK, VSG	Доступ через http

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Кодер	TCP	443	Operator Client, приложение BVMS SDK, VSG	Доступ через https
Кодер	UDP	123	Management Server, VRM	SNTP
Кодер	UDP	161	Management Server, VRM	SNMP
Кодер	TCP	554	Operator Client, приложение BVMS SDK, VSG	Потоковая передача данных RTSP
Кодер	TCP	3260	Кодер (исходящий)	Запись iSCSI

#### Дополнительные порты кодера

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
FTP	TCP	21		
SSDP	UDP	1900		
UPNP	UDP	3702		
SRTSP	UDP	9554		
Отправить RTSP	UDP	15344, 15345		

#### Порты декодера BVMS

Настройте перенаправление портов на подключенном маршрутизаторе для этого устройства.

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Декодер	TCP	1756	Management Server, Operator Client, Configuration Client, приложение BVMS SDK	через RCP+
Декодер	UDP	1757	Management Server, Operator Client	Сканировать целевой объект
Декодер	UDP	1758	Management Server, Operator Client	Отклик сканирования
Декодер	UDP	1800	Management Server, Operator Client	Целевой объект сканирования сети многоадресной передачи
Декодер	TCP	80	Operator Client	Доступ через http
Декодер	TCP	443	Operator Client	Доступ через https
Декодер	UDP	1024-65535	Кодер	Порты потоковой передачи

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Декодер	UDP	123	Management Server, VRM	SNTP
Декодер	UDP	161	Management Server, VRM	SNMP

#### Порты BRS/DiBos

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
DiBos 8.7 / BRS 8.10	TCP	808	Management Server, Configuration Client	Веб-служба Для DiBos v. 8.7 необходимо исправление.
Альтернатива:				
BRS/DiBos	TCP	135	Operator Client, Management Server, Configuration Client	DCOM, используется, когда веб-служба не работает или используемая версия DiBos не поддерживает веб-службу Брандмауэр необходимо отключить
BRS/DiBos	UDP	135	Operator Client, Management Server, Configuration Client	DCOM, используется, когда веб-служба не работает или используемая версия DiBos не поддерживает веб-службу Брандмауэр необходимо отключить

#### Порты DVR

Настройте перенаправление портов на подключенном маршрутизаторе для этого устройства.

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Цифровой видеореги-стратор	TCP	80	Management Server, Configuration Client, Operator Client	Доступ через http

**Barco Monitor Wall**

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Barco Monitor Wall	TCP	1756	Management Server, Operator Client, Configuration Client, приложение BVMS SDK	через RCP+
Barco Monitor Wall	UDP	1757	Management Server, Operator Client	Сканировать целевой объект
Barco Monitor Wall	UDP	1758	Management Server, Operator Client	Отклик сканирования
Barco Monitor Wall	UDP	1800	Management Server, Operator Client	Целевой объект сканирования сети многоадресной передачи

**Порты PID, Person Identification**

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
PID	TCP	8443	Management Server	Доступ по протоколу HTTPS

**Порты адаптеров устройств LPR, BVMS**

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Адаптер устройства BVMS	TCP	32000	Камера Tattile	VRC

**Порты AMS, Access Management System**

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
AMS	TCP	62904	Management Server	Доступ по протоколу HTTPS

**28.5****Включение журнала для событий ONVIF**

Можно включить запись событий ONVIF в журнал, если, например, возникают проблемы с получением событий BVMS. Запись в журнал помогает найти проблему.

**Включение записи в журнал:**

1. Откройте файл `%programfiles(x86)%\Bosch\VMS\AppData\Server\CentralServer\BVMSLogCfg.xml` в подходящем редакторе, например Notepad. Запустите приложение Notepad в качестве администратора.

2. Перейдите к строке, содержащей следующий текст:  
*Add logging for onvif events of a device by network address*  
Строки, ограниченные символами комментариев, содержат краткое описание.
3. Введите имя средства записи журналов *OnvifEvents.<Networkaddress>*.  
Введите только *OnvifEvents*, чтобы записывать в журнал события для всех устройств ONVIF.
4. Введите значение переменной *DEBUG* для всех входящих и исходящих событий.  
Введите *INFO* для всех исходящих событий.  
Введите *WARN* или *ERROR* для отключения.

В строках кода ниже дан пример записи всех исходящих и входящих событий с устройства 172.11.122.22:

```
<logger name="OnvifEvents.172.11.122.22" additivity="false">  
<level value = "DEBUG"/>  
<appender-ref ref="OnvifRollingFileAppender"/>  
</logger>
```

**См.**

- *Настройка таблицы сопоставления ONVIF, Страница 249*
- *Сопоставление событий ONVIF, Страница 37*



# Глоссарий

## Allegiant

Семейство аналоговых матричных коммутаторов компании Bosch.

## ANR

Автоматическая компенсация сети. Интегрированный процесс, в ходе которого отсутствующие видеоданные копируются с видеопередатчика на сетевой видеорегистратор после сбоя сети. Скопированные видеоданные в точности заполняют пропуск, возникший в результате сбоя сети. По этой причине передатчику необходимо локальное устройство хранения любого типа. Объем этого локального хранилища рассчитывается по следующей формуле: (пропускная способность сети  $\times$  предполагаемое время простоя сети + запас надежности)  $\times$  (1 + 1/скорость резервного копирования). Получаемый объем требуется в связи с тем, что во время процесса копирования процесс непрерывной записи должен продолжаться.

## ATM

Банкомат

## BIS

Building Integration System

## BRS

Bosch Recording Station. Программное обеспечение для видеозаписи и управления.

## В-кадр

Двунаправленный кадр. Часть способа сжатия видео.

## DNS

Система доменных имен DNS-сервер конвертирует URL-адрес (например, www.myDevice.com) в IP-адрес в сетях, использующих протокол TCP/IP.

## DTP

Устройство DTP (процессор преобразования данных) преобразует последовательные данные устройств ATM в заданный формат данных и отправляет эти данные через соединение Ethernet системе BVMS. Необходимо проследить за тем, чтобы на устройстве DTP был настроен

фильтр трансформации. Эта задача выполняется отдельным ПО производителя устройства DTP.

## DWF

Design Web Format. Используется для отображения технических чертежей на мониторе компьютера.

## DynDNS

Динамическая система доменных имен Главный узел DNS, содержащий IP-адреса, готовые в базе данных. Динамическая система DNS позволяет подключаться к устройству через Интернет, используя имя главного узла устройства. См. DNS.

## GSM

Global System for Mobile Communication. Стандарт цифровой мобильной связи.

## H.264

Стандарт кодирования (сжатия) цифрового видео и аудио для мультимедийных приложений. Данный стандарт включает различные профили, которые могут зависеть от производителя. Доступны следующие профили: Baseline, Baseline+, Main Profile. Baseline (не используется в Bosch Video Management System) поддерживает 2 CIF. Baseline+ поддерживает 4 CIF и обеспечивает более высокое качество изображения, чем Baseline. Main Profile поддерживает 4 CIF и обеспечивает высокоэффективный алгоритм сжатия, называемый CABAC (Контекстно-адаптивное двоичное арифметическое кодирование). Он служит для высококачественного кодирования для хранения.

## H.265

H.265 — это стандарт сжатия видеосигнала, заданный ISO2 и ITU3 и принятый 29 октября 2014. Он рассматривается как преемник MPEG-4 AVC (Advanced Video Codec), также называемый H.264, и призван осуществлять сжатие разрешения от 4K и ultra HD до 36 МП.

## IQN

iSCSI Qualified Name (уточненное имя iSCSI). Имя инициатора в формате IQN используется для предоставления адресов как инициаторам,

так и получателям iSCSI. При сопоставлении IQN создается группа инициаторов, управляющая доступом к устройствам LUN на получателе iSCSI, а имена инициаторов каждого кодера и диспетчера видеозаписи записываются в данную группу инициаторов. Только тем устройствам, имена инициаторов которых добавлены в группу инициаторов, разрешен доступ к LUN. См. LUN и iSCSI.

## iSCSI

Internet Small Computer System Interface. Протокол, обеспечивающий хранение через сеть TCP/IP. iSCSI обеспечивает доступ к сохраненным данным из любого места сети. Особенно с появлением Gigabit Ethernet стало возможным подключение серверов хранения iSCSI как обычных удаленных жестких дисков к компьютерной сети. В терминологии iSCSI сервер, обеспечивающий ресурсы хранения, называется "получателем iSCSI", а клиент, подключающийся к серверу и пользующийся его ресурсами, называется "инициатором iSCSI".

## I-кадр

Ключевой кадр. Часть способа сжатия видео. Содержит информацию об изображении целиком, в отличие от P- или B-кадров, содержащих информацию об изменениях по отношению к предыдущему или последующему кадру.

## JPEG

Joint Photographic Expert Group (объединенная группа экспертов по фотографии)

## JPEG

Joint Photographic Expert Group (объединенная группа экспертов по фотографии). Процесс кодирования для фотографий.

## LDAP

Lightweight Directory Access Protocol; облегченный протокол службы каталогов. Сетевой протокол, работающий под управлением TCP / IP, обеспечивающий доступ к каталогам. Каталогом может быть, например, список пользовательских групп и их прав доступа. Bosch Video Management System использует этот протокол для получения доступа

к тем же группам, что и MS Windows или другая система управления пользователями для учреждений.

## LUN

Logical Unit Number (Логический номер устройства) Используется в окружении iSCSI для адресации отдельного диска или виртуального раздела (тома). Раздел является частью дискового массива RAID (получатель iSCSI).

## MHT

Другое название - веб-архивы. Формат файла, в котором могут сохраняться все файлы HTML и файлы изображений Интернет-сайта. Чтобы избежать проблем, рекомендуется создавать файлы MHT только при помощи Internet Explorer 7.0 или выше.

## OID

Object Identifier; идентификатор объекта. Термин в окружении SNMP. Определяет переменные MIB.

## ONVIF

Открытый форум по интерфейсу сетевого видео (Open Network Video Interface Forum). Глобальный стандарт для сетевых видеопродуктов. Устройства, соответствующие стандарту ONVIF, могут в режиме реального времени обмениваться видео- и аудиоданными, метаданными и информацией управления и обеспечивать автоматическое обнаружение и подключение к сетевым приложениям (например, к системам управления видео).

## Operator Client

Компонент Bosch Video Management System, который предоставляет пользовательский интерфейс для мониторинга и эксплуатации системы.

## PID

Person Identification Device. Оно извлекает характеристики человека из изображения, например его лица. Оно запускает специальные алгоритмы, способные идентифицировать человека в видеопотоке.

## POS

Point of sale; точка продажи.

**P-кадр**

Предикативный кадр. Часть способа сжатия видео.

**RAID**

Избыточный массив независимых дисков. Используется для организации двух или нескольких жестких дисков, как если бы они были одним диском. На таком диске данные используются совместно или дублируются. Это необходимо для достижения большей емкости, надежности и скорости.

**RCP**

Протокол дистанционного управления

**RTP**

Сокращение от "Real-Time Transport Protocol"; протокол для передачи видео и аудио в реальном времени

**RTSP**

Real Time Streaming Protocol. Сетевой протокол, позволяющий управлять непрерывной передачей аудио- и видеоданных или программного обеспечения по IP-сетям.

**SNMP**

Простой протокол сетевого управления. Протокол, основанный на IP, позволяющий получать информацию от сетевых устройств (GET), устанавливать параметры сетевых устройств (SET) и получать уведомления об определенных событиях (EVENT).

**TCP**

Transmission Control Protocol (протокол управления передачей)

**TCP/IP**

Transmission Control Protocol / Internet Protocol; протокол TCP/IP. Другое название – пакет интернет-протоколов. Набор протоколов связи, используемых для передачи данных по IP-сети.

**UDP**

User Datagram Protocol; Протокол без установления соединения, используемый для обмена данными по IP-сети. Протокол UDP более эффективен для передачи видеоданных, чем протокол TCP по причине более низких потерь.

**URI**

Универсальный идентификатор ресурса (Uniform Resource Identifier). Строка для определения сетевого ресурса. Каждый URI содержит схему, права, путь, запрос и фрагмент. Для Mobile Video Service обязательны только схема и фрагмент. Пример:  
http:<схема>//example.com<полномочия>/over/therepath?  
name=ferret<запрос>#nose<фрагмент>

**URL**

Сокращение от "Uniform Resource Locator"; URL-адрес, унифицированный указатель ресурсов

**VCA**

Анализ видеоданных: компьютерный анализ видеопотоков, позволяющий определить, что происходит в контролируемом кадре. См. также Intelligent Video Analytics

**VIDOS NVR**

Сетевой видеорегистратор VIDOS Программное обеспечение, сохраняющее аудио- и видеоданные с IP-кодеров на дисковый массив RAID 5 или другой носитель. VIDOS NVR обеспечивает функции воспроизведения и поиска записанного видео. Камеры могут быть интегрированы в систему Bosch Video Management System, которая подключена к компьютеру с VIDOS NVR.

**VRM**

Video Recording Manager (Диспетчер видеозаписи) Пакет программного обеспечения в Bosch Video Management System, который управляет сохранением видео (MPEG-4 SH++, H.264 и H.265) с аудиоданными и метаданными на устройства iSCSI в сети. VRM ведет базу данных, в которой содержится информация об источнике записи и список соответствующих устройств iSCSI. VRM реализуется как служба, запущенная на компьютере в сети Bosch Video Management System. Диспетчер видеозаписи не сохраняет видеоданные, а распределяет объем памяти на устройствах iSCSI по кодерам при одновременном распределении нагрузки между несколькими устройствами iSCSI. Диспетчер видеозаписи передает поток воспроизведения от iSCSI на модули Operator Client.

### Активная точка

Значок на карте, реагирующий на щелчок мышью. Активные точки настраиваются в ПО Configuration Client. Активными точками могут быть, например, камеры, реле, входы. Оператор использует их для локализации и выбора устройства в здании. При соответствующих настройках активные точки могут мигать цветом фона, когда возникает определенное событие состояния или тревога.

### Анализ видеоданных

Видеоаналитика — программный процесс, который сравнивает изображение с камеры с сохраненным изображением определенных людей или объектов. В случае соответствия программное обеспечение создает тревожный сигнал.

### Бесконтактное развертывание

Способ автоматической загрузки, установки и запуска приложений .NET без изменения реестра или совместно используемых компонентов системы. В системе Bosch Video Management System автоматическое развертывание используется для обновления клиентов Operator Client с сервера Management Server. Обновление происходит, если на сервере Management Server хранится новая версия, и при каждом входе пользователя в систему на клиенте Operator Client. Если вы работаете с одним клиентом Operator Client и несколькими компьютерами Management Server, автоматическое развертывание использует только версию программного обеспечения, хранящуюся на сервере Management Server, к которому клиент Operator Client в последний раз успешно подключился. При попытке подключения к другому серверу Management Server с другой версией приложения он отображает Management Server как отключенный, поскольку версии ПО не совпадают.

### Виртуальный вход

Используется для пересылки событий из внешних систем в систему Bosch Video Management System.

### время задержки

Временной период, который начинается с момента возникновения некоторого события. В течение этого временного периода обычно не принимаются никакие другие события того же типа. Например, это предотвращает создание датчиком переключения большого количества событий. Для событий с несколькими состояниями можно настроить разные приоритеты для каждого состояния. Приведенные ниже примеры поясняют концепцию времени задержки. В примере 1 рассматриваются события создания одного состояния: возникает событие "Информация о системе" и начинается отсчет настроенного времени задержки. В это время возникает другое событие "Информация о системе". Такое событие "Информация о системе" не принимается как новое событие. В примере 2 рассматриваются события создания разных состояний с одинаковым приоритетом: возникает событие "Обнаружено движение" и начинается отсчет настроенного времени задержки. В это время возникает событие "Движение остановлено" с таким же приоритетом. Такое событие "Движение остановлено" не принимается как новое событие. В примере 3 также рассматриваются события создания разных состояний с одинаковым приоритетом: активно состояние виртуального входа. Приоритеты состояний для обоих изменений состояний идентичны. В конкретный момент времени виртуальный вход выключается и начинается отсчет времени задержки. В течение этого времени задержки виртуальный вход включен. Это изменение состояния не принимается как новое событие, так как у него такой же приоритет. После истечения времени задержки виртуальный вход находится в другом состоянии. При включении задается метка времени завершения времени задержки, и новое время задержки не начинает отсчитываться. В примере 4 рассматриваются события с разными приоритетами создания разных состояний: возникает событие "Обнаружено движение" и начинается отсчет настроенного времени задержки. В это время возникает событие "Движение остановлено" с более высоким приоритетом. Событие

"Движение остановлено" принимается как новое событие, но новый отсчет времени задержки не начинается. В примере 5 также рассматриваются события с разными приоритетами создания разных состояний: состояние виртуального входа — выкл. Приоритет состояния "включено" — "5", для "выключено" — "2". В конкретный момент времени виртуальный вход включается (приоритет "5") и начинается отсчет времени задержки. В течение этого времени задержки виртуальный вход выключен (приоритет "2"). Это изменение состояния принимается как новое событие, так как у него более высокий приоритет. Продолжается отсчет времени задержки первого включения. В течение этого времени задержки дальнейшие изменения состояния не принимаются.

### Время перемотки

Количество секунд, через которые область изображений переключается на немедленное воспроизведение.

### Вторичный VRM

Программное обеспечение в среде BVMS. Обеспечивает выполнение записи, производимой одним или несколькими основными диспетчерами видеозаписи, дополнительно и одновременно на другой целевой объект iSCSI. Настройки записи могут отличаться от настроек основного диспетчера видеозаписи.

### группа мониторов

Несколько мониторов, подключенных к декодеру. Группа мониторов может быть использована для обработки тревожных сигналов в определенной физической области. Например, три изолированных друг от друга центра управления могут иметь три группы мониторов. Мониторы в группе мониторов логически объединены в строки и столбцы, их можно настроить на отображение с различной схемой расположения, например в квадрированном или полноэкранным режиме.

### Группа пользователей Enterprise

Enterprise User Group — пользовательская группа, настроенная на Enterprise Management Server. Enterprise User Group — это группа пользователей, которые могут получить доступ

одновременно к нескольким компьютерам Management Server. Определяет рабочие разрешения, доступные для этих пользователей.

### двойная авторизация

Политика безопасности, требующая входа в систему Operator Client двух отдельных пользователей. Оба пользователя должны быть членами обычной пользовательской группы Bosch Video Management System. Эта группа (или группы, если пользователи принадлежат к разным пользовательским группам) должна входить в группу с двойной авторизацией. Группа с двойной авторизацией имеет свои собственные права в системе Bosch Video Management System. Эта группа с двойной авторизацией должна иметь более широкие права доступа, чем обычная пользовательская группа, к которой принадлежат пользователи. Пример: Пользователь А является членом пользовательской группы с именем Группа А. Пользователь В является членом Группы В. Кроме того, создана группа с двойной авторизацией, в состав которой входят Группа А и Группа В. Для пользователей Группы А двойная авторизация факультативна, для пользователей Группы В она обязательна. При входе в систему пользователя А появляется второе диалоговое окно для подтверждения регистрационных данных. В этом диалоговом окне может зарегистрироваться второй пользователь, если он доступен. Если нет, пользователь А может продолжить и запустить Operator Client. В этом случае он имеет права доступа только группы А. После входа в систему пользователя В опять отображается второе диалоговое окно для регистрации. В этом диалоговом окне должен зарегистрироваться второй пользователь. В противном случае пользователь В не может запустить Operator Client.

### Двухпоточковая передача данных

Двухпоточковая передача обеспечивает одновременное кодирование потока входящих данных в соответствии с двумя различными, индивидуально настраиваемыми профилями. При этом создается два потока данных: один для записи в реальном времени и записи перед тревожным сигналом, второй для непрерывной записи, записи движения и записи по тревоге.

### декодер

Преобразует цифровой поток в аналоговый.

### Дерево устройств

Иерархический список всех доступных устройств системы.

### Доступ Enterprise

Доступ Enterprise — это компонент системы BVMS, который состоит из одного или нескольких учетных записей Enterprise Account. Каждая учетная запись Enterprise Account содержит разрешения устройств для определенного сервера Management Server.

### дуплекс

Этот термин используется для определения направления передачи данных между двумя сторонами. Полудуплекс обеспечивает передачу данных в двух направлениях, но не одновременно. Полный дуплекс обеспечивает одновременную передачу данных.

### Журнал

Хранилище записей обо всех событиях в системе Bosch Video Management System.

### Запрос

Термин в окружении SNMP для незапрошенного сообщения, отправляемого устройством (агент), мониторинг которого осуществляется системой мониторинга сети (диспетчер), о событии в этом устройстве.

### Зеркальный VRM

Программное обеспечение в среде BVMS. Особый случай вторичного диспетчера видеозаписи. Обеспечивает выполнение записи, производимым основным диспетчером видеозаписи, дополнительно и одновременно на другой целевой объект iSCSI с теми же параметрами записи.

### Кадр./сек

Количество кадров в секунду. Количество видеоизображений, передаваемых или записываемых за секунду.

### Камера PTZ

Камера с функциями панорамирования, наклона и увеличения.

### Ключ активации

Номер, который пользователю необходимо ввести для активации приобретенных лицензий. После ввода номера авторизации в менеджере лицензий ПО систем безопасности Bosch вы получите ключ активации.

### Кодировщик

Превращает аналоговый поток в цифровой, например, для интегрирования аналоговых камер в цифровую систему, например, Bosch Video Management System. Некоторые кодеры могут быть оснащены локальным устройством хранения данных, например, флэш-картой, жестким диском USB, или могут сохранять видеоданные на устройствах iSCSI. IP-камеры оснащены встроенным кодером.

### Командный сценарий

Макрос, который может создать администратор для автоматического выполнения определенных действий, например, установки положения камеры PTZ или отправки сообщений электронной почты. Bosch Video Management System предоставляет для этого специальный набор команд. Командные сценарии подразделяются на клиентские и серверные. Клиентские сценарии используются на клиентских рабочих станциях для выполнения определенных действий, которые могут быть осуществлены на клиентской рабочей станции. Серверные сценарии автоматически запускаются событием, происшедшим в системе. Они получают аргументы события, например, дату и время. Командный сценарий может состоять из нескольких команд. Вы можете создать командный сценарий при помощи следующих языков составления сценариев: C#, VB.Net. Командные сценарии выполняются в ответ на события или тревожные сигналы автоматически в соответствии с расписанием, вручную из логического дерева или вручную при помощи значков или карт.

### Контрольное изображение

Контрольное изображение постоянно сравнивается с текущим видеоизображением. Если текущее видеоизображение в отмеченных областях отличается от контрольного изображения, включается сигнал тревоги. Это позволяет обнаружить попытки

несанкционированного доступа, которые иначе не были бы обнаружены (например, при повороте камеры).

### Логический номер

Логический номер представляет собой уникальный идентификатор, присваиваемый каждому устройству системы для облегчения его идентификации. Логические номера уникальны только в пределах определенного типа устройств. Примером типичного использования логических номеров являются командные сценарии.

### Логическое дерево

Дерево с настроенной структурой всех устройств. Логическое дерево используется клиентом оператора для выбора камер и других устройств. Полное логическое дерево настраивается в клиенте настроек (на странице Карты и структура) и приспособляется для каждой группы пользователей (на странице Пользовательские группы).

### Магистральная линия

Аналоговые выходы или аналоговый матричный коммутатор, подключенный к устройству кодирования. Таким образом, матричные источники видеосигнала могут использоваться в системе Bosch Video Management System.

### многопутевой ввод-вывод

Метод хранения на компьютере, предполагающий указание множества физических путей, по которым сервер данных подключается к целевому объекту хранилища (с использованием различных контроллеров, шин, коммутаторов и т.п) в качестве решения для отработки отказа и распределения нагрузки (обеспечивает резервирование и эффективность).

### Многопутевой ввод-вывод

Использование метода многопутевого хранения на компьютере.

### Мониторинг сети

Измерение относящихся к сети значений и соотнесение этих значений с настраиваемыми пороговыми значениями.

### Мост ATM/POS Bosch

Получает строку через последовательный кабель / COM-интерфейс и передает эту строку через кабель Ethernet (TCP/IP). Строки обычно снимаются с данных ATM или POS.

### Немедленное воспроизведение

Воспроизведение записанного изображения с выбранной камеры в области изображений на экране реального времени. Можно настроить время начала воспроизведения (указать количество секунд в прошлом, или время обратной перемотки).

### неуправляемый объект

Элемент дерева устройств в системе BVMS, который может содержать сетевые видеоустройства, например цифровые видеорегистраторы. Эти устройства не управляются сервером Management Server вашей системы. Пользователь Operator Client может подключаться к устройствам объекта unmanaged site по требованию.

### Номер авторизации

Номер, который вы получаете от Bosch для лицензии на заказанное вами программное обеспечение. Необходимо ввести номер авторизации в менеджере лицензий ПО систем безопасности Bosch для получения ключа активации. Для активации приобретенных лицензий вам также понадобится цифровая подпись компьютера.

### области

Область — это термин, используемый при работе с камерами ONVIF. Это параметр используется для проверки устройства ONVIF. Обычно параметр содержит URI следующим образом: onvif: / / www.onvif.org/<path>. Параметр < путь > может быть, например, video\_encoder или audio\_encoder. Одно устройство ONVIF может иметь несколько областей. Этот URI обозначает область задач устройства.

### область

Группа устройств обнаружения, подключенных к системе безопасности.

### Область изображений

Используется для отображения видео в реальном времени и в записи, с одной камеры, с карты или файла HTML.

### Область интереса

Область интереса. Область интереса предназначена для сохранения пропускной способности сети при масштабировании участка изображения с камеры с помощью фиксированной камеры HD. Этот участок ведет себя, как камера PTZ.

### обход/отмена обхода

Режим обхода устройства означает, что все возможные тревоги будут проигнорированы, как правило, на время каких-либо смягчающих обстоятельств, таких как мероприятия по обслуживанию. Отмена обхода подразумевает прекращение игнорирования таких событий.

### Окно изображений

Контейнер для областей изображений, расположенных в соответствии с узором областей изображений.

### Окно тревожных сигналов

Окно изображений для отображения одной или нескольких областей тревожных сигналов.

### Основной VRM

Синоним для VRM.

### охранная панель управления

Универсальное имя для основного устройства в системе безопасности (системе защиты от взлома) производства Bosch. Клавиатуры, модули, детекторы и другие устройства подключаются к панели управления.

### Панель области изображений

Панель инструментов области изображений.

### Период переключения

Установленный промежуток времени, в течение которого камера отображается в окне изображений до отображения следующей камеры последовательности.

### ПО Master Control Software

Программное обеспечение, используемое в качестве интерфейса между Bosch Video Management System и устройством Allegiant. Используется версия 2.8 или выше.

### Пользовательская группа

Пользовательские группы используются для определения общих пользовательских атрибутов, например, разрешений, привилегий и приоритетов PTZ. Когда пользователь становится членом пользовательской группы, он автоматически наследует все атрибуты группы.

### Порт

1) На компьютерах и устройствах телекоммуникации порт обычно представляет собой определенное место для физического подключения к другому устройству, обычно посредством гнезда и вилки. Обычно персональный компьютер имеет один или несколько последовательных портов и один параллельный порт. 2) В программировании порт представляет собой "логическое место соединения" и в частности, при использовании Интернет-протокола TCP/IP, способ, который использует клиентская программа для указания на определенную серверную программу на компьютере или в сети. Приложения высокого уровня, использующие TCP/IP, как веб-протокол, протокол передачи гипертекста, имеют порты с заранее назначенными номерами. Они известны как "известные порты", которые были назначены Комитетом по цифровым адресам в Интернете (IANA). Другим приложениям номер порта присваивается динамически при каждом соединении. Когда происходит первоначальный запуск серверной программы, говорят, что она привязывается к назначенному номеру порта. Когда клиентская программа имеет намерение использовать этот сервер, она также должна привязываться к назначенному порту. Номера портов находятся в диапазоне от 0 до 65535. Порты от 1 до 1023 зарезервированы для привилегированных служб. Для службы HTTP порт 80 определен как стандартный и может не указываться в URL-адресе.

### Просмотр сервера

Способ доступа для пользователя Configuration Client или Operator Client, чтобы последовательно подключиться к нескольким



системным точкам доступа. Системными точками доступа могут быть Management Server или Enterprise Management Server.

### Рабочая станция

В среде BVMS: выделенный компьютер, на котором установлен модуль Operator Client. Этот компьютер настроен как рабочая станция в Configuration Client, чтобы включить определенные функции.

### Рабочая станция Operator Client

Компьютер в окружении Bosch Video Management System для просмотра изображений в реальном времени и записанных изображений, а также для выполнения конфигурационных действий. Приложение Operator Client установлено на этом компьютере.

### Развертка изображений

Использование программного обеспечения по конвертации круглого изображения из объектива типа «рыбий глаз» с радиальной дисторсией в прямоугольное изображение для нормального просмотра (устранение искажений является коррекцией дисторсии).

### Разрешение видеоканала

Количество пикселей по горизонтали и вертикали, передаваемых с видеосигналом.  
PAL: 1CIF = 352 x 288 2CIF = 704 x 288 4CIF = 704 x 576 QCIF = 176 x 144 NTSC 1CIF = 352 x 240 2CIF = 704 x 240 4CIF = 704 x 480 QCIF = 176 x 120 HD 720p = закодировано 1280 x 720 1080p = закодировано 1920 x 1080

### Расписание задач

Используется для планирования событий, которые могут произойти в системе Bosch Video Management System, например, выполнение командного сценария. На странице События вы можете назначить событиям расписание задач. Для планирования событий используется также расписание записей. В стандартном расписании задач вы настраиваете временные промежутки для каждого дня недели, для выходных дней и дней исключений. В повторяющемся расписании задач вы можете настроить повторяющиеся промежутки времени. Они могут повторяться каждый день, каждую неделю, каждый месяц или каждый год.

### Расписание записей

Используется для планирования записей и некоторых событий, например, запуска резервного копирования или ограничения входа в систему. В расписании записей не может быть пробелов или накладок. Это расписание определяет также качество записи видеоизображений.

### Режим реального времени

Функция Operator Client. Используется для просмотра видео в режиме реального времени.

### Резервный VRM

Программное обеспечение в среде BVMS. Берет на себя функцию назначенного основного диспетчера видеозаписи или вторичного диспетчера видеозаписи в случае выхода из строя.

### Сервер управления

Управление устройствами сервера BVMS.

### Сервер управления Enterprise

Enterprise Management Server — это сервер BVMS Management Server, на котором находится конфигурация групп Enterprise User Group. Необходима одна или несколько групп Enterprise User Group, относящихся к одному или нескольким компьютерам. Роли Enterprise Management Server и Management Server могут быть объединены в одной конфигурации.

### Серия устройств

Кодеры Bosch / IP-камеры могут принадлежать к одному из следующих семейств устройств. Семейство устройств 1, семейство устройств 2, семейство устройств 3. Устройства семейства 1 могут записывать только поток 1. Устройства семейства 2 могут записывать поток 1 или поток 2. Устройства семейства 3 могут записывать поток 1, поток 2 или только I-кадр.

### Сетевой видеорегиистратор

Сетевой видеорегиистратор Bosch; компьютер в окружении Bosch Video Management System, сохраняющий видео- и аудиоданные или выступающий в качестве резервного сетевого видеорегиистратора. Этот видеорегиистратор отличается от VIDOS NVR, который может быть интегрирован в Bosch Video Management System.

## Система Enterprise

Enterprise System — это компонент системы Bosch Video Management System, позволяющий пользователю Operator Client одновременно получать доступ к нескольким компьютерам Management Server.

## Скимминг

Взлом устройства чтения кредитных карточек. Скиммер считывает данные карточки, хранящиеся на магнитной полосе, когда владелец карточки не подозревает об этом.

## Сложное событие

Комбинация нескольких событий. Комбинация использует логические выражения, т.е., AND и OR. Вы можете комбинировать только изменения состояний, например, изменение состояния подключения на отключенное или активацию расписания.

## Событие

Обстоятельство или состояние, связанное с тревожным сигналом и/или действием. События могут генерироваться различными источниками, например, камерами, архивами, каталогами, цифровыми входами и т.п. Они могут включать в себя запускающие запись состояния, состояния потери сигнала, сообщения о переполнении дискового пространства, входы пользователя в систему, пусковые механизмы цифровых входов и т.п.

## Сопоставление портов

Сопоставление портов позволяет удаленным компьютерам подключаться к конкретному компьютеру или сервису в частной локальной сети (LAN).

## Список тревожных сигналов

Окно в системе Bosch Video Management System, которое используется для отображения списка активных тревожных сигналов.

## Текстовые данные

Данные POS или АТМ, например, дата и время или номер банковского счета, которые хранятся вместе с соответствующими видеоданными и предоставляют дополнительную информацию.

## Точка

Устройство обнаружения, подключенное к системе безопасности. Точки отображаются на клавиатуре по отдельности и с пользовательским текстом. Текст может описывать одну дверь, датчик движения, дымовой извещатель или защищенную область, например "Верхний этаж" или "Гараж".

## Тревога

Событие, сконфигурированное для создания тревожного сигнала. Это событие представляет собой определенную ситуацию (обнаружение движения, звонок в дверь, потеря сигнала и т.п.), которая требует немедленного реагирования. Тревожный сигнал может отображать видеоизображение в реальном времени, записанное видеоизображение, план действий, веб-страницу или карту.

## Удаленный доступ

Удаленный доступ позволяет подключать различные частные сети к общедоступным сетям. Компьютеры Operator Client могут получать доступ к нескольким сетям с частными (локальными) адресами одновременно или последовательно через открытые интерфейсы (маршрутизаторы). Задача маршрутизатора — перевести входящий общедоступный сетевой трафик на соответствующий частный сетевой адрес. Пользователи Operator Client могут получить доступ к Management Server или Enterprise Management Server и их устройствам с помощью удаленного доступа.

## Устранение искажений в камере

Устранение искажений, выполняемое в самой камере.

## Учетная запись Enterprise

Enterprise Account — это авторизация, позволяющая пользователю клиента Operator Client подключаться к устройствам Management Server, входящим в систему Enterprise. В Enterprise Account настраиваются все разрешения для устройств этого сервера Management Server. Клиент Operator Client может одновременно подключиться ко всем компьютерам Management Server, являющимся частью этой Enterprise System. Этот доступ управляется членством в Enterprise User Group

и разрешениями на использование устройств, настроенными в Enterprise Account для этого сервера Management Server.

### **Функция внутренней связи**

---

Используется для разговора через громкоговорители кодера. Кодер должен иметь аудиовход и аудиовыход. Функция внутренней связи предоставляется группам пользователей.

### **Цифровой видеореги́стратор**

---

Цифровой видеореги́стратор

### **Шлюз видеопотока (VSG)**

---

Виртуальное устройство, позволяющее выполнить интеграцию камер Bosch, камер ONVIF, камер JPEG, кодеров RTSP.

### **Эмуляция CCL**

---

Для управления матрицей Allegiant используется командный язык консоли. Можно использовать этот набор команд для переключения IP-камеры или кодера BVMS на IP-декодер BVMS.

Невозможно осуществлять прямое управление аналоговыми камерами или самой матрицей Allegiant.

## Указатель

### Символы

аварийное завершение		глобальный пароль по умолчанию	71, 96, 109
Клиент настроек	383	группа LDAP	371
автоматический вход	96	группа аналоговых мониторов	118, 124
автоматический выход из системы	119	группа мониторов	148, 149, 321, 326
автоматический перезапуск	96	камера запуска	149
автоматический режим записи	189	квадрированный режим	149
автоматическое отображение тревожных сигналов		один экран	149
37		первоначальная камера	149
автономная работа	342	экранное меню	149
автономный режим	360	группу мониторов	
активация	99	добавить	149
конфигурация	96	группы пользователей	339, 341
отложено	96, 108	Группы пользователей LDAP	341, 371
предыдущая конфигурация	97	данные конфигурации	
активация записи текстовых данных	335, 336	экспорт	98
активировать	96	данные конфигурации в OPC	
Bosch Video Management System	78	экспортировать	99
активные точки	268	датчики вибрации	333
Аналитический поиск	138	двойная авторизация	344
аналоговая матрица	135	двойная запись	26, 197, 311
База данных журнала	119	двойные IP-адреса	109
строка подключения	119	двухпоточковая передача данных	141
базовая конфигурация	202	декодер	
банкоматы и кассовые терминалы	124	Клавиатура Bosch IntuiKey	148
бездействие	119	Декодер BVIP	86, 230
блокировка PTZ	346, 354, 374	добавление	143, 190, 220
большие устройства LUN	189	декодер: пароль пункта назначения	222, 235
большое устройство LUN	189, 194, 200, 206	Дерево устройств	122, 181, 268
брандмауэр	212	дни исключений	289
Веб-клиент	168	добавить unmanaged site	223, 225
Ведение журнала	183, 333	добавить кодер BVIP	143, 144, 190, 220, 231
видеоаналитика	171	добавить мост ATM/POS Bosch	101
виртуальный вход	124	добавление VRM	179
Внутренняя аудиосвязь	352	добавление декодера BVIP	143, 190, 220
возможности устройства		добавление кодера	187, 196, 227, 377
обновить	86, 230	добавление кодера BVIP	143, 190, 220
время до тревожного сигнала	304	добавление неуправляемого объекта	223, 224
время перед событием	302, 304	добавление пула	
время перед событием	296	VRM	185
время после события	302, 304	добавление текстовых данных к непрерывной	
время после события	296	записи	318
время после тревожного сигнала	304	добавление тревожного входа Bosch Allegiant	102
вторичная запись	197, 311	добавление устройства видеоаналитики	172
Вторичный VRM	126, 180	дополнительный VRM	26
Вторичный резервный VRM	185	доступ к справке	14
выходные дни	289	дублирование события	330
глобальные настройки тревог	334	замена устройств	80
		замена устройства	82

заменить содержимое	271	кодеки	302
замечания к выпуску	18	кодер	
запись ONVIF в журнал	391	веб-страница	227
запись RAM	304	добавление	187, 196, 227, 377
запись вручную	39, 320, 335	кодер BVIP	86, 230
запись по тревоге	320, 335, 336	add	143, 190, 220
запись событий ONVIF в журнал	391	добавление	143, 190, 220
Запросы SNMP		Кодер BVIP: добавить	144, 231
get	117	Кодирование CABAC	301
отправить	117	кодирование на сетевых видеорегистраторах	122, 181
защита записи по тревоге	335, 336	командный сценарий	268, 275
избыточная запись	26	импорт	94
избыточный VRM	26, 126, 186	справка Bosch Script API	93
изменение пароля	184, 342	экспорт	95
изменить IP-адрес	110, 123, 142, 239	Команды CCL коммутатора Allegiant	60
изменить адрес сети	239	Команды CLL	167
изменить пароль	146, 227, 236, 342	Команды меню	105
изменить пул	237	Коммерческое название	115
изменить сетевой адрес	142	конфигурация по умолчанию	202
импорт		копировать и вставить	297
командный сценарий	94	Корпоративная система	89
файлы ресурсов	271	купольная камера	307, 309
имя инициатора сервера	182	лицензии	
интерактивная справка по приложению	14	Bosch Video Management System	78
использование пула	198	сервер Stratus	78
камера PTZ	307	лицензирование	
Allegiant	295	Мастер настройки конфигурации	71
камера для обнаружения пожара	376	Логическое дерево	270, 325
Камеры UHD	141	маршрутизируемый доступ	127
карта		Мастер конфигурации	
мигающие активные точки	314, 337	Mobile Video Service	63
карта тревог	321	Матричный коммутатор Allegiant	124, 135, 136
карты	268	мигающие значки устройств	314, 337
качество записи	299	многомониторный режим	355
квадрированный режим	149	многопоточная передача	213
Клавиатура Bosch IntuiKey	49, 50, 124, 138, 148, 163	множественный выбор	270
клавиатура CCTV	163	Мобильный видеосервис	168
разрыв соединения	382	модули ввода/вывода	124
Клавиатура DCZ	163	монитор устройств	99
клавиатура IntuiKey	163	настраиваемые события	313, 332
клавиатура KBD Universal XF	49, 50, 124, 138	настройка записи VRM	102
Клавиатуры Bosch IntuiKey	51, 54	Независимый Operator Client	360
Клиентский командный сценарий		ненадежная сеть	167
выполняется при запуске	94, 95, 140	Необходимая скорость передачи данных	301
тревога принята	325	новые устройства DiBos	131, 134, 135
кнопка пользовательских событий	331	область интереса	294, 345
кнопка пользовательского события	331	Область интереса ""	309
		Область интересов	309

область устройств	268	получение управления PTZ	374
обновить		пользователь	
возможности устройства	86, 230	удалить	342
обновление	381	пользователь LDAP	341
обновление микропрограммы		порядок сортировки	
Клавиатура Bosch IntuiKey	54	тревожные сигналы	321
обновление программного обеспечения	381	последовательность	278
обновление состояний	105	последовательность камер	268, 277, 278
обновление состояния	110, 111, 112	последовательность тревог	320
обход		последовательность тревожных сигналов	335
точка	353	поток	306
Основной VRM	26, 126, 180	поток по умолчанию	138, 294
Основной резервный диспетчер VRM	185	предыдущая конфигурация	97
отказано в доступе		примеры	101
Эмуляция Allegiant CCL	166	добавление моста ATM/POS Bosch	101
отключение сигнальных сирен	353	добавление тревожного входа Bosch Allegiant	
отключено	360	102	
отключить принудительную защиту паролем	109	настройка записи VRM	102
отложенная активация	96, 108	принудительная защита паролем	109
отсоединенный режим	360	приоритет тревоги	374
отсутствует пароль	96	проверить подлинность	234
охранная панель	169	Просмотр сервера	128
панорамная камера		профиль	299
режимы просмотра	40	пул	
Параметры SNMP	117	VRM	185, 237
Параметры записи	242	изменение	237
параметры интерфейса		перемещение устройства	205, 217, 237
VIP XD	148	Пул хранения iSCSI	178
пароль	146, 227, 236	Пул хранения VRM	178
пароль CHAP	182	пул хранилищ VRM	198
пароль iSCSI	182	пустой пароль	96
пароль не установлен	96	рабочая станция	118
пароль по умолчанию	96, 109	Разблокирующий фильтр H.264	301
пароль пункта назначения	222, 235	разрешения	268, 270
первоначальная камера	150	регистрация в журнале	331
перемещение устройства	205, 217, 237	режим записи	
перенаправление портов	75	автоматический	189
периферийное устройство	124	резервный	189
печать справки	15	режим записи кодера: резервный	241
поведение автоматически всплывающих окон	37	режим записи по тревоге	302, 304
подключение		Режим совместимости	39
Клавиатура Bosch IntuiKey и BVMS	51	режимы просмотра панорамной камеры	40
Матричный коммутатор Allegiant и BVMS	55	резервный VRM	26, 126, 185
поиск	103, 141	резервный режим записи	189
информация в справке	14	кодер	241
устройства	110, 111, 112, 122, 269, 292, 313, 316, 319, 341	реле	
поиск конфликтующих IP-адресов	109	неисправность	281
		реле сигнализации неисправности	281
		ручное включение	352

сервер OPC	381	тихие тревоги	353
сервер Stratus		точка	
лицензии	78	обход	353
сервер времени	87	тревожная панель	170
сервис транскодирования	168	тревожны сигналы	
сетевой адрес		порядок сортировки	321
изменить	142, 239	удаление препозиций	307
Сеть сервера	225	удаленный доступ	75, 89, 120, 128
Сеть серверов	223, 224, 225	удаленный экспорт	39
синхронизация	87	удалить пользователя	342
конфигурация VRM	188	управление PTZ	
синхронизация времени	87	блокировка	346, 354, 374
система «все в одном»	63	управление камерой	103, 302
система хранения iSCSI	198	устройства LUN	
системные требования	18	больше 2 ТБ	189
Системы контроля и управления доступом	170	устройства без защиты паролем	96
сканирование		устройство BVIP	
в подсетях	118	веб-страница	227
подсети	118	пароль	146, 227, 236
сканировать		устройство DiBos	124
VRM	126	устройство iSCSI	202
кодеры	125	устройство SMS	124
кодеры с локальными хранилищами	125	устройство мониторинга сети	124
кодеры, работающие только в реальном времени	125	устройство электронной почты	124
слишком много камер Allegiant	384	файл Allegiant	384
сложные события	313, 332	файлы HTML	268
служба транскодирования	167	файлы ресурсов	271
смена пароля	146, 227, 236	импорт	271
сменить пароль	184	фильтрация	110, 111, 112, 122, 269, 292, 313, 316, 319, 341
создание		Функция внутренней связи	352
командный сценарий	93	цикл камеры	268, 277, 278
создание пулов	178	цифровая клавиатура	163
соотношение сторон 16/9	355	Цифровой видеорегиистратор	124, 132
Сопоставление IQN	202	часовой пояс	223, 224
сопоставление портов	75, 120	экспорт	
состояние	99	ASF	351
состояния	105, 110, 111, 112	данные конфигурации	98
Список серверов		командный сценарий	95
добавить столбцы	90, 129	Таблица камер	298
удалить столбцы	90, 129	экспортировать	
справка	14, 15	данные конфигурации в OPC	99
справка Bosch Script API	93	Эмуляция Allegiant CCL	167
ссылка карты	279	отказано в доступе	166
ссылка на карту	279	Эмуляция CCL	167
Страница Эмуляция Allegiant CCL	166	язык	382
строка подключения	119	Configuration Client	118
Таблица записи	292	Operator Client	341
технические характеристики	18	язык графического интерфейса пользователя	382

<b>A</b>		
Allegiant		
версия микропрограммы	49, 51	
камера PTZ	295	
канал управления	58	
контрольный канал	59	
программа Network Host	58	
Сателлитная система	59	
слишком много камер	384	
Эмуляция CCL	124, 167	
ANR	88, 238, 294	
ASF	351	
<b>B</b>		
Bosch Video Management System	17	
активировать	78	
интерактивная справка	14	
лицензии	78	
обзор	17	
обновление	381	
язык графического интерфейса пользователя	382	
<b>D</b>		
DiBos		
версия	49, 51	
DSA E-Series	194, 195, 200, 201	
DTP3N	157	
DynDNS	75	
<b>E</b>		
Enterprise Management Server	356	
Enterprise System	21	
Enterprise User Groups	339	
<b>F</b>		
Forensic Search	140	
<b>H</b>		
H.264	301	
HD-камеры	355	
<b>I</b>		
iPad	167, 168	
iPhone	167, 168	
IP-адрес		
дубликаты	109	
изменить	110, 123, 142, 239	
IP-адреса по умолчанию	109	
<b>M</b>		
Management Server	18, 21, 360	
MIC IP 7000	380	
Mobile Video Service	63	
<b>N</b>		
NVR	18	
<b>O</b>		
ONVIF Media profile	294	
Operator Client	17, 270	
<b>P</b>		
Person Identification		
Person Identification Device	173	
Добавление Person Identification Device	173	
Добавление камер к Person Identification Device	175	
PTZ-камера	309	
<b>R</b>		
ROI	294, 345	
<b>S</b>		
Server ID	82	
stream	294	
<b>V</b>		
Video Streaming Gateway	124	
VIDEOJET 7000 connect	380	
VIP X1600 XFM4	301	
VIP XD	49	
квадрированный режим	149	
параметры интерфейса	148	
полудуплексный режим	148	
VPN	75	
VRM		
Вторичный	126, 180	
Вторичный резервный	185	
добавление	179	
добавление пула	185	
дополнительный	26	
избыточный	26, 126, 186	
Основной	26, 126, 180	
Основной резервный	185	
При отказе	126, 185	
пул	185, 237	
резервный	26	
VRM 3.50	188	
<b>W</b>		
WAN	75, 120	
WLAN	167, 168	











**Bosch Security Systems B.V.**

Torenallee 49

5617 BA Eindhoven

Netherlands

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Security Systems B.V., 2020