

2013

EDISON. Центр  
разработки  
программного  
обеспечения

[www.edsd.ru](http://www.edsd.ru)

[www.edsd.biz](http://www.edsd.biz)

[www.electrooffice.com](http://www.electrooffice.com)

Москва, Россия

# **[КРАТКОЕ ТЕХНИЧЕСКОЕ ЗАДАНИЕ ПО РАЗРАБОТКЕ И ВНЕДРЕНИЮ МОДУЛЬНОЙ СИСТЕМЫ КОНТРОЛЯ ДИСПЕТЧЕРИЗАЦИИ И УПРАВЛЕНИЯ УДАЛЕННЫМИ ОБЪЕКТАМИ PROTECTOR]**

Документ описывает требования к платформе предоставления услуг безопасности

## Оглавление

|       |   |    |
|-------|---|----|
| 1     | Список сокращений и обозначений .....                                       | 7  |
| 2     | Аннотация.....  | 9  |
| 3     | Общие положения.....  | 10 |
| 3.1   | Полное наименование работ .....   | 10 |
| 3.2   | Наименование Заказчика работ .....  | 10 |
| 3.3   | Наименование Исполнителя работ.....   | 10 |
| 3.4   | Назначение Системы .....  | 10 |
| 3.5   | Результаты работ.....   | 10 |
| 3.6   | Порядок контроля и приемки Системы .....                                    | 10 |
| 3.7   | Нормативная и техническая документация.....                                 | 11 |
| 4     | Введение .....  | 12 |
| 5     | Оконечное устройство (ОУ) .....   | 13 |
| 5.1   | Аппаратная спецификация.....  | 13 |
| 5.2   | Подключение устройств к ОУ .....  | 13 |
| 5.2.1 | Подключение USB-устройств .....   | 13 |
| 5.2.2 | Подключение устройств через Ethernet.....                                   | 14 |
| 5.2.3 | Подключение RS-устройств .....  | 14 |
| 5.3   | Доступ в Интернет .....   | 15 |
| 5.3.1 | Прямой доступ .....   | 15 |
| 5.3.2 | Доступ через аппаратный маршрутизатор .....                                 | 16 |
| 5.3.3 | Гибридный доступ.....   | 17 |
| 5.3.4 | Выбор основного и резервного провайдера.....                                | 17 |
| 5.3.5 | Дублирование подключений .....  | 18 |
| 5.3.6 | Фаервол.....  | 18 |
| 5.3.7 | Создание VLAN в случае нескольких Клиентов компании, обслуживаемых одним ОУ | 19 |
| 5.4   | Подключение к серверу ММ.....   | 19 |
| 5.4.1 | Холодный старт .....  | 19 |
| 5.4.2 | Безопасность подключения к серверу ММ .....                                 | 20 |
| 5.4.3 | Шифрование передаваемых данных .....  | 20 |
| 5.4.4 | Предупреждения об ошибках подключения.....                                  | 20 |
| 5.4.5 | Синхронизация времени .....   | 20 |
| 5.5   | Данные, передаваемые серверу ММ .....                                       | 21 |

|       |  |    |
|-------|--|----|
| 5.5.1 | Размер передаваемых данных .....                                 | 21 |
| 5.5.2 | Пакеты данных.....   | 21 |
| 5.5.3 | Типы пакетов данных.....   | 22 |
| 5.6   | Наблюдение за подконтрольными устройствами в локальной сети..... | 23 |
| 5.7   | Наблюдение за питанием .....                                     | 24 |
| 5.8   | Полный список функций ОУ .....                                   | 24 |
| 5.9   | Автоматическое обновление.....                                   | 24 |
| 6     | Модуль мониторинга (ММ).....                                     | 26 |
| 6.1   | Серверы ММ.....  | 26 |
| 6.1.1 | Программно-аппаратные требования к серверу ММ.....               | 26 |
| 6.1.2 | Способы размещения серверов ММ .....                             | 27 |
| 6.2   | Подход к репликации данных между серверами ММ.....               | 30 |
| 6.2.1 | Общие данные.....  | 30 |
| 6.2.2 | Сегментируемые данные.....                                       | 31 |
| 6.3   | Ввод в эксплуатацию нового сервера ММ .....                      | 31 |
| 6.4   | Передача команды на ОУ .....                                     | 32 |
| 6.4.1 | Оперативные команды .....  | 32 |
| 6.4.2 | Отложенные команды .....   | 32 |
| 6.5   | Отслеживание соединения с ОУ.....                                | 33 |
| 6.6   | Отслеживание состояний подконтрольных устройств ОУ.....          | 33 |
| 6.7   | Получение тревог от ОУ .....                                     | 33 |
| 6.8   | Синхронизация времени.....                                       | 33 |
| 6.9   | Безопасность.....  | 34 |
| 6.9.1 | Фаервол.....   | 34 |
| 6.9.2 | Безопасность соединений .....                                    | 34 |
| 6.10  | Полный список функций сервера ММ.....                            | 34 |
| 7     | Прибор приёмно-контрольный (ППК) .....                           | 36 |
| 7.1   | События ППК, передаваемые ОУ .....                               | 36 |
| 7.2   | Постановка ППК на охрану .....                                   | 37 |
| 8     | Модуль видеонаблюдения (МВ) .....                                | 38 |
| 8.1   | Камеры видеонаблюдения .....                                     | 38 |
| 8.1.1 | Контроль питания камер видеонаблюдения .....                     | 38 |
| 8.1.2 | Слежение за состоянием камер наблюдения .....                    | 38 |

|        |  |    |
|--------|--|----|
| 8.2    | DVR .....  | 38 |
| 8.2.1  | Ведение архива записей .....   | 39 |
| 8.2.2  | Просмотр видеозаписи с DVR Клиентом компании .....                   | 39 |
| 8.2.3  | Просмотр видеосигнала с DVR диспетчером .....                        | 39 |
| 8.3    | Плагин для работы с DVR, устанавливаемый на ОУ .....                 | 39 |
| 8.4    | Готовое ПО для просмотра видеоизображения с DVR .....                | 40 |
| 9      | АРМ диспетчера .....   | 41 |
| 9.1    | Программные требования .....   | 41 |
| 9.2    | Подключение к серверу ММ.....  | 41 |
| 9.2.1  | Безопасность подключения .....                                       | 41 |
| 9.2.2  | Проблемы подключения к серверу ММ .....                              | 42 |
| 9.3    | Схема подключения диспетчерских пунктов.....                         | 42 |
| 9.4    | Окно журнала событий.....  | 43 |
| 9.4.1  | Настраиваемое окно журнала событий .....                             | 44 |
| 9.5    | Окно тревог.....   | 45 |
| 9.6    | Захват тревоги в работу.....   | 46 |
| 9.7    | Отслеживание отключения АРМ диспетчера, вброс повторных тревог ..... | 46 |
| 9.8    | Отслеживание временного регламента .....                             | 46 |
| 9.9    | Протоколирование действий диспетчера .....                           | 47 |
| 9.10   | Окно карты.....  | 48 |
| 9.11   | Модуль оповещения клиентов.....                                      | 49 |
| 9.11.1 | Оповещения по электронной почте .....                                | 49 |
| 9.11.2 | Оповещения по SMS.....   | 49 |
| 9.12   | Поиск и просмотр информации о Клиенте компании .....                 | 50 |
| 9.13   | Просмотр топологии устройств охраняемого объекта.....                | 50 |
| 9.14   | Просмотр камер видеонаблюдения .....                                 | 51 |
| 9.15   | Синхронизация времени.....   | 51 |
| 9.16   | Просмотр хронологической последовательности событий объекта.....     | 51 |
| 9.17   | Полный список функций.....   | 52 |
| 10     | АРМ администратора .....   | 53 |
| 10.1   | Платформа .....  | 53 |
| 10.2   | Функциональные требования .....                                      | 53 |
| 10.3   | Требования к GUI.....  | 54 |

|        |  |    |
|--------|--|----|
| 10.4   | Справочная информация .....                              | 56 |
| 10.4.1 | Справочник организаций .....                             | 56 |
| 10.4.2 | Точки охраны .....                                       | 57 |
| 10.4.3 | Схема подключения устройств .....                        | 57 |
| 10.4.4 | Списки доступа .....                                     | 58 |
| 10.4.5 | Протоколирование изменений.....                          | 58 |
| 10.4.6 | Интеграция с 1С.....                                     | 58 |
| 11     | Модуль оповещения (МО).....                              | 59 |
| 12     | Модуль связи.....  | 60 |
| 12.1   | Голосовая связь .....                                    | 60 |
| 12.1.1 | Call-центр.....  | 60 |
| 12.1.2 | Мобильная радиосвязь .....                               | 60 |
| 13     | Мобильное приложение для смартфона.....                  | 61 |
| 13.1   | Платформа .....  | 61 |
| 13.2   | Внешний вид .....  | 61 |
| 13.3   | Активация приложения .....                               | 61 |
| 13.4   | Постановка на охрану и снятие с охраны.....              | 61 |
| 14     | Мессенджер.....  | 63 |
| 15     | Планшетный пульт управления.....                         | 64 |
| 15.1   | Платформа .....  | 64 |
| 15.2   | Активация программы.....                                 | 64 |
| 15.3   | Постановка на охрану и снятие с охраны.....              | 64 |
| 15.4   | Видеонаблюдение .....                                    | 64 |
| 15.5   | Связь с диспетчером .....                                | 64 |
| 16     | Протоколы обмена.....                                    | 65 |
| 16.1   | Протокол OpenDMTP .....                                  | 65 |
| 16.1.1 | Формат сообщений .....                                   | 65 |
| 16.1.2 | Пример пакета.....                                       | 65 |
| 16.1.3 | Двусторонняя связь .....                                 | 66 |
| 16.2   | Протокол обмена сообщениями между ОУ и сервером.....     | 66 |
| 16.2.1 | Процесс установления двусторонней связи .....            | 66 |
| 16.2.2 | Основные типы параметров задаваемых на ОУ .....          | 66 |
| 16.2.3 | Основные типы пакетов, передаваемых с ОУ на сервер ..... | 67 |

---

|        |   |    |
|--------|---|----|
| 16.2.4 | Основные типы пакетов, передаваемых с сервера на ОУ .....       | 67 |
| 16.3   | Протокол обмена между серверами .....                           | 68 |
| 16.3.1 | Типы пакетов, передаваемых между серверами.....                 | 68 |
| 16.4   | Протокол обмена между АРМ диспетчера и сервером.....            | 68 |
| 16.4.1 | Типы пакетов, передаваемых между АРМ диспетчера и сервером..... | 68 |
| 16.5   | Протокол обмена между пультом управления и ОУ .....             | 69 |
| 16.5.1 | Параметры ОУ .....  | 69 |
| 16.5.2 | Типы пакетов, передаваемых с ОУ на планшет .....                | 69 |
| 16.5.3 | Основные типы пакетов, передаваемых с планшета на ОУ .....      | 69 |
| 16.6   | Протокол обмена между мобильным приложением и ОУ.....           | 69 |
| 16.7   | Протокол обмена между мобильным приложением и сервером.....     | 69 |

## 1 Список сокращений и обозначений

| Термин                           | Наименование   |
|----------------------------------|--|
| Система                          | Разрабатываемое программное обеспечение и аппаратная часть, на которой работает данное программное обеспечение, целиком.   |
| АКБ                              | Аккумуляторная батарея.  |
| АРМ                              | Автоматизированное рабочее место.  |
| БД                               | База данных.   |
| БП                               | Блок питания.  |
| ППК                              | Прибор приёмно-контрольный. Функциональный аналог прибора Сигнал-10.   |
| RS-устройства                    | Все устройства, подключаемые к ОУ по шине RS-485. К ним относятся контроллеры исполнительных устройств и т.д.  |
| USB-устройства                   | 3G/4G донглы, GPS донглы, преобразователи USB-RS-485, считыватели, Ethernet-адаптеры, WiFi донглы.   |
| DVR                              | Видеорегистратор. Имеется в виду DVR, NVR и т.п.   |
| Тампер                           | Датчик вскрытия оборудования.  |
| ОУ                               | Оконечное устройство. Устройство на основе Raspberry PI, устанавливаемое на объекте, к которому подключаются ППК, RS-устройства, USB-устройства.   |
| ПО                               | Программное обеспечение.   |
| ГБР                              | Группа быстрого реагирования.  |
| Клиент компании                  | Физ. лицо, юр. лицо или его представитель, заключивший с компанией договор на оказание услуг в системе Protector.  |
| Сотрудник компании               | Диспетчер, член ГБР или иной сотрудник компании.   |
| ММ                               | Модуль мониторинга. Обеспечивает наблюдение за состоянием ППК и/или RS-устройств.  |
| МВ                               | Модуль видеонаблюдения.  |
| МС                               | Модуль связи. Сервер для осуществления текстовой, аудио- и видеоконференции. Построен на базе Asterisk. Позволяет общаться сотрудникам и клиентам компании между собой по Мессенджеру. Интегрирован с call-центром компании. |
| Мессенджер (Клиент модуля связи) | Клиентское ПО для ведения текстовых, аудио-, видеоконференций. Может быть установлено на ПК или мобильные устройства сотрудников компании, клиентов компании. Подключается к модулю связи.                                   |

|     |   |
|-----|---|
| МГП | Модуль геопозиции. Обеспечивает получение от объектов, оснащенных GPS, их текущих координат и отображает их положение на карте в АРМ диспетчера.<br>Также отображает объекты с фиксированной геопозицией (например, здания на карте, положение которых было предварительно задано). |
| МО  | Модуль оповещения клиентов компании. Обеспечивает рассылку электронной почты, SMS, текстовых сообщений по контактам Мессенджера.<br>Выполняет функции автоинформатора (например, сообщает о размере задолженности).   |



## 2 Аннотация

---

Настоящий документ включает в себя технические требования на создание и внедрение модульной системы контроля, диспетчеризации и управления удаленными объектами Protector.

Цели работы:

- Разработка ПО серверной части ММ.
- Разработка ПО оконечного устройства на основе ARM-микрокомпьютера.
- Разработка ПО микроконтроллера для ППК — функционального аналога «Сигнал 10».
- Разработка защищенного протокола передачи данных по шине RS-485.
- Разработка протоколов передачи данных между компонентами системы в локальной сети и сети Интернет.
- Разработка драйверов для USB-устройств в случае необходимости.
- Разработка структуры хранения данных.
- Разработка ПО АРМ диспетчера.
- Разработка ПО администратора.
- Разработка ПО для управления RS-устройствами (кроссплатформенное).
- Внедрение ПО для просмотра видео с сервера видеонаблюдения (кроссплатформенное).
- Разработка Мессенджера (кроссплатформенный).
- Разработка ПО для модуля оповещения.
- Разработка ПО для модуля геопозиции.
- Разработка ПО для модуля связи.
- Разработка проектной документации и инструкции пользователей.
- Опытная эксплуатация и внедрение в коммерческую эксплуатацию.

## **3 Общие положения**

---

### **3.1 Полное наименование работ**

Проектирование, разработка и внедрение программного обеспечения, создание и внедрение распределенной модульной системы контроля, диспетчеризации и управления удаленными объектами. Далее по тексту используется понятие «Система» или «Protector».

### **3.2 Наименование Заказчика работ**

Заказчиком работ является ООО «ВТИМБ».

### **3.3 Наименование Исполнителя работ**

Исполнителем работ является EDISON. Центр разработки программного обеспечения (<http://www.edsd.ru>).

### **3.4 Назначение Системы**

Контроль, диспетчеризация и управление удалёнными объектами.

### **3.5 Результаты работ**

По окончании работ по созданию Системы мониторинга должны быть получены следующие результаты:

- спроектировано, разработано, развернуто и настроено на оборудовании Заказчика необходимое программное обеспечение Системы мониторинга;
- разработана техническая и пользовательская документация, необходимая для эксплуатации Системы;
- после сдачи проекта исполнитель оказывает техническую поддержку на условиях дополнительного соглашения.

### **3.6 Порядок контроля и приемки Системы**

Подрядчик представляет Заказчику результаты работ в соответствии с перечнем и в сроки, определенные в Календарном плане работ.

Должны быть проведены внутренние испытания Системы на оборудовании Исполнителя, включающие в себя следующие работы:

- проведение внутренних испытаний всех Модулей Системы, кроме Модулей, требующих доступа к оборудованию, которое не было предоставлено заказчиком;
- исправление найденных дефектов;
- оформление акта завершения внутреннего испытания и готовности к комплексным испытаниям.

Должны быть проведены комплексные испытания Системы на оборудовании Заказчика, включающие в себя следующие работы:

- проведение испытаний всех Модулей Системы с подключением нескольких стендовых объектов;
- исправление найденных дефектов;
- оформление акта завершения комплексного испытания и готовности к опытной эксплуатации.

После завершения комплексных испытаний должна быть проведена опытная эксплуатация Системы в реальных условиях на оборудовании заказчика, включающая в себя следующие работы:

- проведение опытной эксплуатации Системы на нескольких объектах;
- исправление дефектов;
- постепенное подключение новых объектов;
- исправление дефектов;
- проведение полномасштабной опытной эксплуатации в течении двух недель;
- исправление дефектов;
- оформление акта завершения опытной эксплуатации и допуска к приемочным испытаниям.

После завершения опытной эксплуатации должны быть проведены приемочные испытания Системы, включающие в себя следующие работы:

- проведение приемочных испытаний;
- оформление акта готовности к вводу в промышленную эксплуатацию.

### **3.7 Нормативная и техническая документация**

При разработке Системы и создании документации должны быть использованы следующие нормативно-технические документы.

1. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
2. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
3. ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем.
4. ГОСТ 19. Единая система программной документации.
5. РД 50-34.698-90. Методические указания. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.

## 4 Введение

---

Система «Protector» (далее — Система) предназначена для контроля, диспетчеризации и управления удалёнными объектами.

Для осуществления этих функций в Систему включаются следующие компоненты.

- Оконечное устройство.
- ППК.
- Модуль видеонаблюдения.
- Модуль мониторинга.
- Модуль связи.
- Модуль оповещения.
- Модуль геопозиции.
- Мессенджер.
- АРМ диспетчера.
- АРМ администратора.
- ПО управления RS-устройствами.
- Планшетный пульт управления.
- И др. (список может расширяться по мере развития Системы и появления новых требований).

Все компоненты взаимосвязаны между собой и выполняют чётко определённую функцию в рамках всей Системы.

Функции каждого из компонентов Системы описываются далее по тексту.

Сначала описываются компоненты, связанные с удалёнными объектами, затем — серверные компоненты, специализированные приложения диспетчера, администратора и т.д.

## 5 Оконечное устройство (ОУ)

---

ОУ является главным звеном Системы на каждом конкретном охраняемом объекте.

Из описания станет ясно, за что отвечает ОУ и насколько важна его роль в рамках всей Системы.

ОУ представляет собой микрокомпьютер на основе Raspberry Pi model A.

Допускается использование старшей модели с большим количеством RAM и встроенным Ethernet контроллером — Raspberry Pi model B.

Программное обеспечение для ОУ должно быть написано на языке программирования Qt/C++. Хранение данных должно осуществляться в базе SQLite.

Для уникальной идентификации ОУ на серверах ММ каждому ОУ присваивается уникальный идентификатор во время прошивки.

### 5.1 Аппаратная спецификация

- SoC Broadcom BCM2835 (CPU, GPU, DSP, и SDRAM).
- Процессор: 700 МГц ARM1176JZF-S (семейства ARM11).
- GPU: Broadcom VideoCore IV, OpenGL ES 2.0, 1080p30 H.264/MPEG-4.
- Память (SDRAM): 256 МБ.
- Видео выходы: композитный RCA, HDMI.
- Аудио выходы: 3,5 мм разъем, HDMI.
- Встроенная память: SD, MMC, SDIO слот для карт памяти.
- Хранение с помощью SD / MMC / SDIO слот для карт памяти.
- General Purpose Input-Output (GPIO), включая SPI, I2C, serial UART.
- ОС Linux: Raspbian, Pidora, Fedora, Debian, Gentoo и др.

### 5.2 Подключение устройств к ОУ

#### 5.2.1 Подключение USB-устройств

Для увеличения числа подключаемых к ОУ USB-устройств применяется активный (с внешним питанием) USB-хаб.

К ОУ могут подключаться следующие USB-устройства.

- USB-Ethernet адаптеры для подключения к локальной сети и проводным Интернет-провайдерам. Если проводных Интернет-провайдеров несколько, то устанавливается необходимое количество USB-Ethernet адаптеров.
- GPS-адаптер для получения географических координат.

- USB-3G и (или) USB-4G донглы для подключения 3G и (или) 4G беспроводных Интернет-провайдеров. Допускается установка нескольких таких адаптеров.
- USB-WiFi адаптер для обеспечения WiFi-сети.
- И др. (список может расширяться новыми устройства, что может потребовать доработки ПО компонентов Системы).

### 5.2.2 Подключение устройств через Ethernet

Ethernet-устройства подключаются к ОУ через адаптер USB-Ethernet.

Примеры Ethernet-устройств:

- DVR;
- исполнительные устройства;
- и др. (список может расширяться новыми устройствами, что может потребовать доработки ПО компонентов Системы).

### 5.2.3 Подключение RS-устройств

RS-устройства, в частности ППК, контроллеры исполнительных устройств (см. устройства из «Болида»), подключаются к ОУ посредством интерфейса RS-485 через преобразователь интерфейсов USB-RS-485.

RS-устройства имеют адресацию. Допускается подключение до 127 RS-устройств на одну шину RS-485.

Подключение дополнительных RS-устройств, функционально совместимых с линейкой «Болид», может потребовать доработки ПО компонентов Системы.

#### *Подключение приёмно-контрольных приборов (ППК)*

ППК помимо подключения к ОУ через преобразователь USB-RS-485 может подключаться непосредственно к Serial UART GPIO через блок преобразования напряжений на микросхеме MAX485.

#### *Шифрование данных на шине RS-485*

Для защиты от неавторизованного подключения к шине RS-485 протокол обмена между RS-устройствами и ОУ должен быть уникален.

Все сообщения (пакеты) должны быть зашифрованы, чтобы их авторство могло быть проверено как передающей, так и принимающей стороной.

Пакеты сообщений нумеруются и шифруются криптоалгоритмом AES, поэтому записанные и отправленные повторно пакеты будут отброшены при проведении процедуры проверки сообщения.

Прописывание ключей AES в RS-устройства производится во время их прошивки. Все ключи хранятся на сервере.

В ОУ ключ AES может прописываться как при установке прошивки, так и задаваться сервером MM.

База данных ключей и RS-устройств ведётся на сервере администратором, который вносит данные при прошивке новых устройств. Контроль ключей не позволит переносить RS-устройства между объектами без обновления информации в БД администратором системы.

### 5.3 Доступ в Интернет

ОУ должно иметь стабильный доступ в Интернет для непрерывного взаимодействия с серверами Системы.

Доступ в Интернет может быть организован следующими способами:

- прямой доступ;
- доступ через аппаратный маршрутизатор;
- гибридный.

#### 5.3.1 Прямой доступ

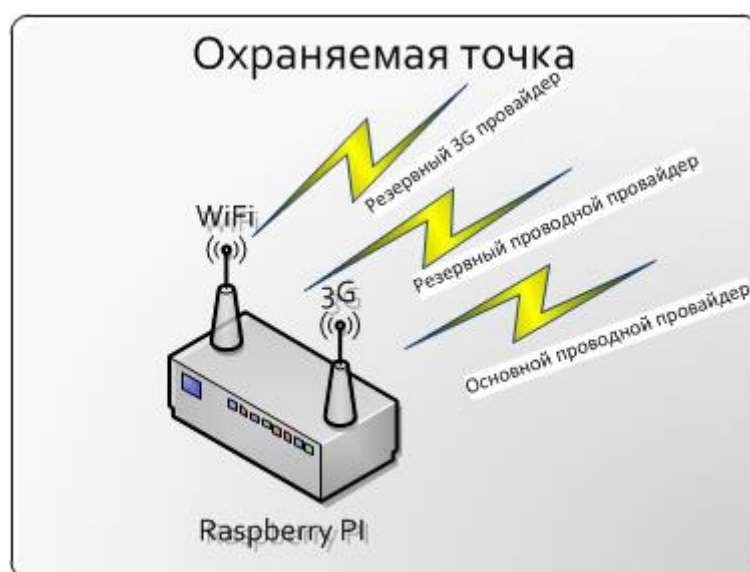


Рис.1. Прямое подключение ОУ к Интернету

В этом случае к ОУ могут напрямую подключаться различные USB-адаптеры (Ethernet, 3G, 4G) для доступа в Интернет (см. [рис. 1](#)).

При этом ОУ должно самостоятельно реализовывать функции по резервированию каналов доступа в Интернет.

Как достигается резервирование каналов:

- ОУ подключается сразу к нескольким Интернет-провайдерам (проводным и беспроводным);

- настраивается автоматическое переключение на резервного провайдера средствами установленной ОС Linux (Multi-WAN).

В итоге, в случае обрыва установленного соединения с серверами Системы ОУ автоматически переключается на резервный канал и заново устанавливает соединение с серверами.

При переключении между провайдерами ОУ формирует тревожное сообщение о причине переключения и отправляет его на сервер ММ.

### 5.3.2 Доступ через аппаратный маршрутизатор

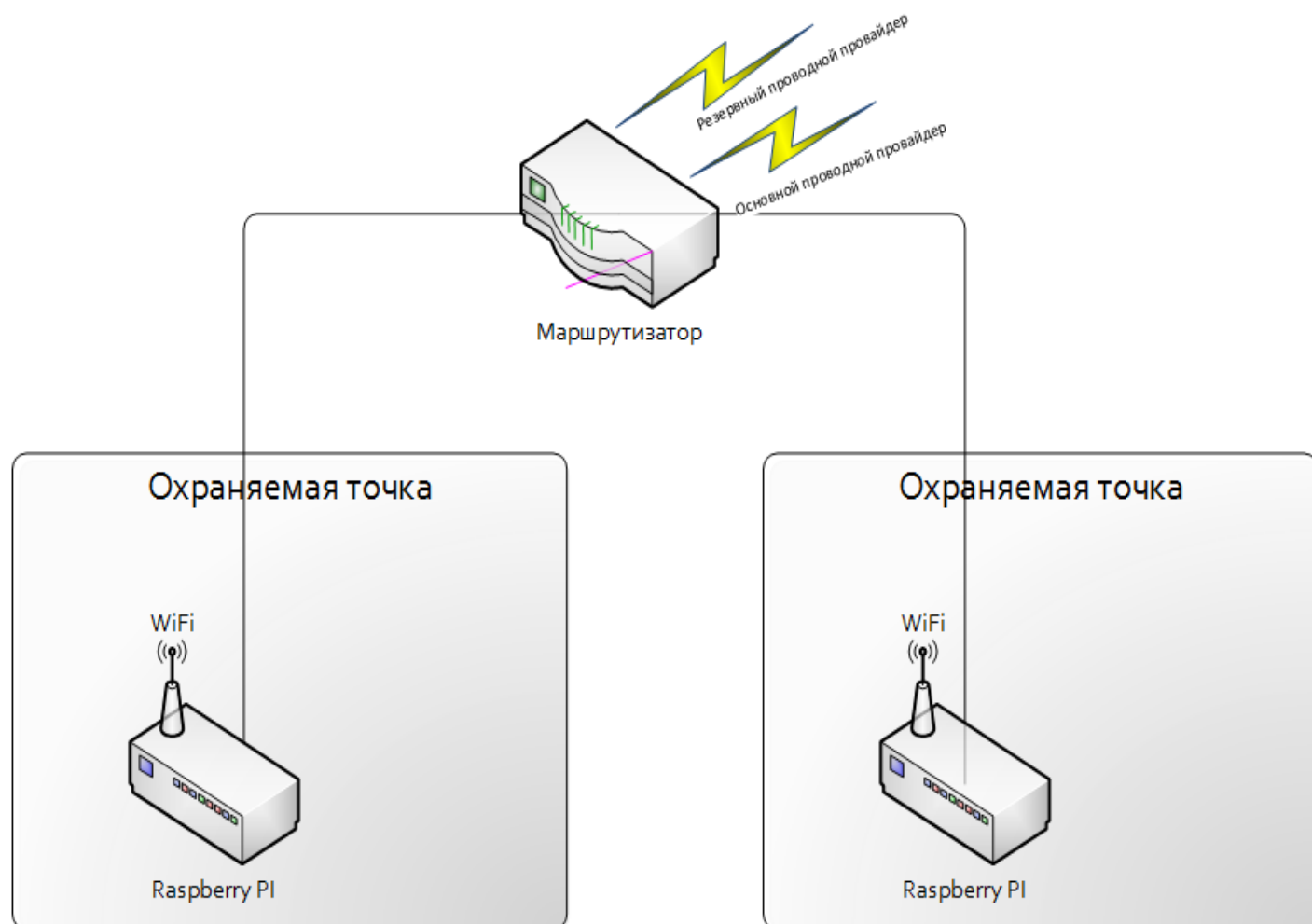


Рис.2. Подключение к Интернету нескольких ОУ через аппаратный маршрутизатор

К аппаратному маршрутизатору могут подключаться сразу несколько ОУ. Подключение к маршрутизатору происходит через Ethernet-адаптер (см. [рис. 2](#)).

Аппаратный маршрутизатор может быть подключен сразу к нескольким проводным Интернет-провайдерам. При этом он обеспечивает резервирование каналов встроенными средствами.



### Обеспечение надёжности работы аппаратного маршрутизатора

Во-первых, аппаратный маршрутизатор должен быть зарезервирован по питанию от БП. Контроль питания маршрутизатора осуществляется со стороны ОУ (см. ниже пункт «[Наблюдение за питанием](#)»).

Во-вторых, технология связи может быть выбрана по принципу надёжности при отключениях питания 220В. К примеру, модемы от «Ростелеком» при наличии резервного питания продолжают функционировать даже при отключении электроэнергии во всём здании. Это достигается с помощью технологии GPON.

### 5.3.3 Гибридный доступ

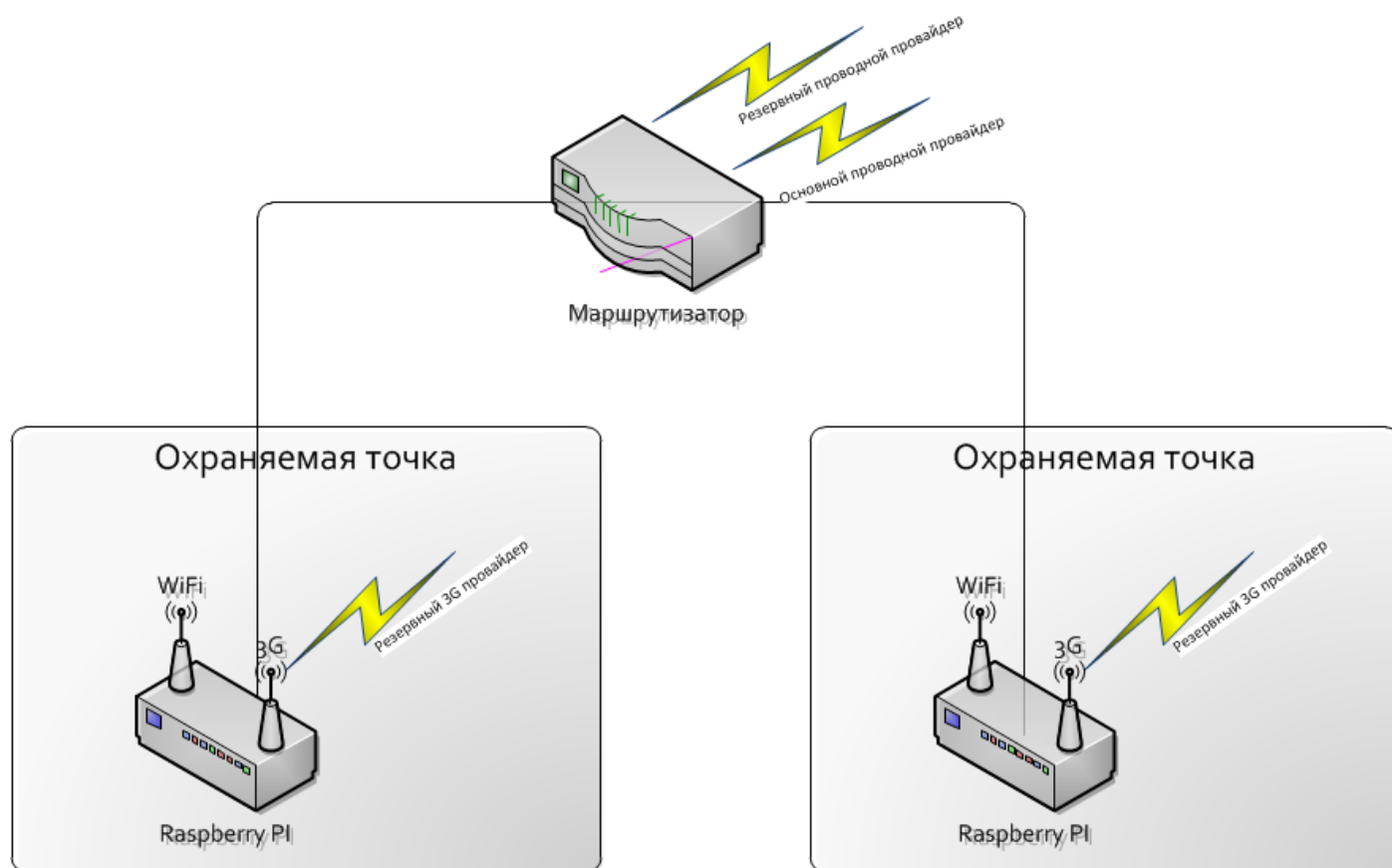


Рис.3. Гибридный доступ

При организации доступа в Интернет через аппаратный маршрутизатор можно дополнительно реализовать резервирование каналов и на самом ОУ (см. [рис. 3](#)). Такой вариант организации доступа в Интернет называется гибридным.

При гибридном доступе в случае потери доступа в Интернет через аппаратный маршрутизатор ОУ должно переключаться на резервного беспроводного Интернет-провайдера (3G/4G).

### 5.3.4 Выбор основного и резервного провайдера

Особое внимание должно быть уделено вопросу выбора основного и резервного провайдеров.

**Внимание!** Критерии выбора основного и резервного провайдеров могут быть уникальны для каждого конкретного охраняемого объекта. Зачастую этот вопрос решается уже на месте ответственным лицом. Здесь лишь приведены общие рекомендации!

По линии основного провайдера предполагается посылка данных в случае штатной работы.

Основной провайдер в большинстве случаев является проводным (имеется техническая возможность протянуть кабель и заключить договор с провайдером).

Резервный провайдер обычно нужен для нештатной работы — когда происходит обрыв связи по линии основного провайдера. Резервных провайдеров может быть несколько — как проводных, так и беспроводных.

### 5.3.5 Дублирование подключений

Для особо важных объектов администратором может настраиваться количество одновременных подключений к серверу Системы со стороны ОУ. При этом подключения устанавливаются через разных провайдеров в соответствии с приоритетом.

Например, если ОУ оборудовано двумя донглами 3G или 4G связи, а администратор настроил одновременное подключение по двум каналам, то будет установлено два TCP-подключения к одному и тому же серверу по двум каналам с наивысшим приоритетом. Пакеты будут передаваться одновременно по обоим каналам.

В случае обрыва связи по какому-либо одному каналу будет производиться несколько попыток установить соединение через этот же канал, а затем произойдет переключение на резервный. Нормально функционирующее подключение при этом не разрывается.

При получении двух или более одинаковых пакетов с разных TCP-подключений от одного ОУ сервер Системы должен использовать пакет, полученный первым, — все остальные отбрасываются. Подтверждение приема пакета в любом случае отправляется во все установленные соединения. Сервер также должен отправлять команды во все установленные с ОУ соединения.

### 5.3.6 Фаервол

На каждом ОУ должен быть настроен фаервол. Настройка обеспечивается встроенными средствами ОС Linux (iptables).

Функции фаервола:

- защита от DDoS-атак;
- ограничение доступа к ОУ из Интернета или LAN с посторонних адресов. ОУ может быть доступно только компонентам Системы.

### *Фаервол на аппаратном маршрутизаторе*

В случае подключения ОУ к Интернету через аппаратный маршрутизатор на самом маршрутизаторе также должен быть настроен фаервол для предотвращения DDoS-атак и попыток подключения с посторонних адресов (как из Интернета, так и внутри LAN).

#### **5.3.7 Создание VLAN в случае, когда несколько Клиентов компании обслуживаются одним ОУ**

Очень важным является вопрос обеспечения безопасности внутри LAN, когда одно ОУ обслуживает 2-х или более Клиентов компании.

Цель заключается в недопущении возможности доступа одного клиента к оборудованию другого клиента. Например, один клиент не должен иметь возможность подключаться к DVR другого клиента, или даже пинговать устройства другого клиента.

Для этого используется механизм создания VLAN, который является встроенным средством ОС Linux на ОУ.

### **5.4 Подключение к серверу ММ**

ОУ должно поддерживать постоянное подключение с одним из серверов ММ.

При первом запуске ОУ выполняет процедуру холодного старта для установления подключения к серверу ММ.

#### **5.4.1 Холодный старт**

Процедура начала работы ОУ после его запуска/перезапуска называется холодным стартом.

Холодный старт состоит из следующих шагов.

Шаг 1. Обнаружение всех серверов ММ в сети.

ОУ делает запрос к DNS-серверу. В ответе от DNS-сервера приходит список IP4- или IP6-адресов серверов ММ.

Если DNS-сервер недоступен, то используются заэкшированные IP-адреса, полученные при последнем обращении к DNS.

Шаг 2. Определение адреса сервера ММ для установления постоянного подключения.

Сначала делается запрос к любому серверу ММ. У него запрашивается список IP-адресов серверов ММ, с которыми ОУ может установить постоянное подключение.

Замечание: для каждого ОУ на серверах ММ формируется свой список IP-адресов. Приоритет каждого адреса в списке определяется степенью загрузки сервера ММ. Чем меньше загружен сервер ММ, тем выше его приоритет и тем выше он указан в списке IP-адресов, который получает ОУ.

Шаг 3. Установление постоянного подключения с сервером ММ.

ОУ подключается к первому серверу в списке, и, если TCP-подключение установлено, то работает с ним. Если сервер не отвечает, или происходят другие ошибки, то берётся следующий адрес из списка. Если ни с одним сервером не удалось установить подключение, то ОУ повторяет цикл холодного старта с шага 1.

#### **5.4.2 Безопасность подключения к серверу ММ**

В каждое ОУ во время прошивки записывается набор открытых ключей серверов ММ.

Таким образом, ОУ при попытке подключения к серверу ММ сможет проверять, является ли данный сервер доверенным. Если нет, то ОУ будет пытаться подключиться к другому серверу ММ из списка.

Позднее набор открытых ключей серверов ММ может быть изменён специальной командой сервера ММ, к которому подключено ОУ в данный момент.

#### **5.4.3 Шифрование передаваемых данных**

При установке прошивки каждому ОУ назначается собственный закрытый ключ для шифрования передаваемых данных. Открытый ключ фиксируется в базе данных серверов ММ.

Таким образом, только серверы ММ смогут осуществлять дешифровку данных, посылаемых ОУ.

#### **5.4.4 Предупреждения об ошибках подключения**

Если имела место ошибка подключения к серверу ММ, то о ней должно быть сформировано сообщение.

Однородные ошибки должны быть агрегированы так, чтобы передать сообщение вида: «ОУ XXX обнаружено N ошибок соединения с IP x.x.x.x к серверу IP x.x.x.x. с времени xx:xx до xx:xx».

В случае доступа в Интернет через аппаратный маршрутизатор IP внешнего адреса ОУ должно быть получено у маршрутизатора.

#### **5.4.5 Синхронизация времени**

Точное время является важной составляющей ОУ. Оно позволяет адекватно оценивать хронологию всех возникающих в Системе событий, тревог. Расхождения во времени недопустимы — для этого на ОУ используется механизм синхронизации времени.

Синхронизация времени на ОУ происходит при каждом подключении к серверу ММ.

Если время на ОУ расходилось с полученным временем от сервера ММ, то должно сгенерироваться предупреждение с последующей отправкой на сервер ММ. В предупреждении должно быть указано время на ОУ и время, полученное с сервера ММ.

## 5.5 Данные, передаваемые серверу ММ

### 5.5.1 Размер передаваемых данных

Желательно, чтобы за месяц работы ОУ не генерировало исходящего трафика более, чем предусматривает договор с основным провайдером. Для управления размером трафика возможна настройка интервала передачи пакетов данных.

Интервал передачи данных должен применяться на ОУ и на другие устройства, которые посылают на ОУ свои пакеты данных, к примеру, на DVR (которое может периодически посылать на ОУ пакеты состояний — см. ниже пункт «[Наблюдение за подконтрольными устройствами локальной сети](#)»).

Размер пакетов должен быть минимальным.

#### *Требование единого пакета для множества устройств*

Для достижения значительной экономии трафика вводится понятие единого пакета данных для множества устройств.

Пример: пусть к ОУ подключено два ППК. В этом случае ОУ при сборе данных с двух ППК может группировать все собранные данные в один единый пакет, а не создавать два. В результате ОУ отошлёт только один пакет, а не два.

Таким образом, достигается экономия трафика.

### 5.5.2 Пакеты данных

Пакет данных представляет собой одно сообщение, посылаемое с ОУ на сервер ММ.

Пакет должен быть минимального размера.

На каждый отправленный пакет от сервера ММ ожидается подтверждение. Если подтверждение не получено ко времени отправки следующего пакета, то происходит разрыв сессии и повторное подключение к тому же серверу — горячий старт. Если соединение установить не удаётся, то делается подключение к следующему серверу ММ по алгоритму холодного старта.

#### *Обязательные атрибуты всех пакетов данных*

Список обязательных атрибутов.

- Идентификатор ОУ.
- Номер пакета, сгенерированный ОУ.
- Время создания сообщения по часам ОУ.
- Время отправки сообщения по часам ОУ.

Все пакеты нумеруются последовательно. Счетчик нумерации пакетов 32-х битный. Нумерация начинается с 1.

Время указывается в формате UTC.

### *Хранение пакетов данных*

Перед отправкой пакет данных сохраняется в локальной БД ОУ. Сначала данный пакет имеет статус «не отправлено». После отправки и получения подтверждения от сервера ММ пакету выставляется статус «отправлено».

Если в результате обрыва подключения к серверу ММ на ОУ скопились неотправленные пакеты данных, то при последующем переподключении к серверу ММ происходит отправка сначала пакета с максимальным номером, а уже затем остальных, неотправленных, пакетов.

При превышении максимального размера локальной БД ОУ должна производиться автоматическая очистка БД от старых пакетов.

### *Корректировка счётчика пакетов данных*

В случае повреждения локальной БД ОУ может получиться так, что текущее значение счётчика окажется меньше, чем номер последнего пакета, хранящегося на сервере ММ. В этом случае счётчик должен быть исправлен, чтобы не возникло пересечений номеров пакетов, хранящихся на сервере ММ. При подключении к серверу ММ перед формированием первого нового сообщения ОУ должен согласовать с сервером ММ значение счётчика. Значение счётчика должно быть обязательно больше номера последнего принятого сообщения, которое хранится на сервере ММ. Если счётчик устройства оказывается меньше, то он корректируется, и об этом делается запись в БД сервера ММ и ОУ типа: «счётчик сообщений корректировался для ОУ со значения X на Y».

### **5.5.3 Типы пакетов данных**

ОУ может отправлять серверу ММ следующие типы пакетов данных.

- Пакет текущего состояния подконтрольного устройства (это устройство, с которого ОУ периодически снимает показания, считывает состояние или иные данные, подлежащие анализу).

Примеры:

- состояние RS-устройства;
- данные (координаты) GPS-адаптера;
- состояние БП;
- и пр.

Отсылка таких пакетов производится через настраиваемый интервал времени.

- Пакет с тревогой.

Примеры:

- срабатывания датчика, подключенного к ППК;
- тревожные события с DVR;
- смена провайдера;
- и т.д.

Данный пакет посылается немедленно и с наивысшим приоритетом, т.е. посылка всех остальных пакетов откладывается, пока не будет отослан пакет с тревогой.

- Пакет с ошибкой.

Примеры:

- переключение на другого провайдера;
- ошибка подключения к серверу Системы;
- разрыв подключения с сервером Системы;
- неверный ввод PIN-кода;
- корректировка счётчика сообщений;
- и т.д.

Данный пакет посылается так же, как пакет состояния подконтрольного устройства.

## **5.6 Наблюдение за подконтрольными устройствами в локальной сети**

ОУ периодически проверяет работу подконтрольных устройств локальной сети, таких как:

- DVR;
- планшетный пульт управления;
- и др. (список может быть расширен).

Информация о возникающих неполадках отправляется на сервер ММ в виде пакета с ошибкой или тревогой для дальнейшей обработки диспетчером.

Также ОУ периодически посылает пакеты текущего состояния устройств локальной сети.

### *Особенности наблюдения за DVR*

Возможны два варианта наблюдения за DVR:

- DVR сам посылает на ОУ пакеты состояний;
- ОУ ведёт опрос DVR с заданным интервалом.

## 5.7 Наблюдение за питанием

ОУ может отслеживать состояние сразу нескольких блоков питания. БП может быть подключен как к самому ОУ, так и к другим устройствам (например, к DVR, камерам видеонаблюдения и т.п.).

Для контроля отсутствия напряжения 220В и разряда батареи к одному из выходов специализированной платы, подключенной к GPIO, подсоединяется сигнальный провод, подключенный к реле БП (например, PSC-100 Mean Well).

При смене состояния БП ОУ генерирует событие изменения параметров питания (переход на АКБ, разряд батареи) и отправляет его на сервер ММ.

## 5.8 Полный список функций ОУ

- Поиск сервера и подключение к нему.
- Передача на сервер текущего состояния.
- Отслеживание состояния и управление приемно-контрольными и другими приборами, подключенными к устройству, и передача на сервер тревог при обнаружении нарушений.
- Мониторинг состояния устройств локальной сети.
- Мониторинг состояния подключения к Интернет-провайдерам.
- Отслеживание состояния питания: от сети, резервное, состояние батареи.
- Сохранение всех событий во внутреннюю память, чтобы в случае отсутствия связи имелась возможность отправить данные позднее.
- Параллельное подключение нескольких приемно-контрольных приборов для мониторинга объектов с большим количеством шлейфов.
- Прием и применение команд конфигурирования и управления от сервера по сети.
- Прием и установка обновлений ПО.
- Поддержка работы с пользователями.
- Постановка-снятие с охраны посредством планшетного пульта и PIN-кода, либо ключа Touch Memo, либо удаленно через приложение управления RS-устройствами.
- Управление устройствами, непосредственно подключенными к ОУ либо к локальной сети.
- Синхронизация времени с сервером мониторинга.

## 5.9 Автоматическое обновление

Разрешение на обновление ОУ конфигурируется администратором.

Если разрешение задано, то ОУ автоматически скачивает и помещает в отдельный каталог обновленные версии ПО со специального сервера обновлений.

Обновление ОУ происходит не сразу. ОУ запрещено обновляться, пока оно не снято с охраны.



После снятия с охраны через некоторое время основной модуль ПО выгружается, и запускается модуль обновления, который заменяет устаревшие файлы и затем перезапускает основной модуль ПО.

В модуле обновления должен быть предусмотрен аварийный режим, при котором в случае ошибок обновления или невозможности запуска новой версии ПО производится откат изменений и возврат ПО основного модуля к состоянию, в котором оно было до начала обновления.

Информация об успехе или ошибке обновления должна быть отправлена на сервер.

## 6 Модуль мониторинга (ММ)

### 6.1 Серверы ММ

Серверы ММ образуют распределенную децентрализованную систему.

Эта система должна быть организована таким образом, чтобы отключение или выход из строя любого из серверов ММ не приводило к потере функциональности всего ММ.

Серверы ММ реплицируют данные между собой для создания избыточности, что гарантирует доступность всей собранной информации.

#### 6.1.1 Программно-аппаратные требования к серверу ММ

Сервер ММ обычно состоит из Сервера приложений и Сервера БД.

На Сервере приложений работает ПО серверной части ММ. На Сервере БД расположена база данных, с которой напрямую взаимодействует Сервер приложений. Сервер приложений и Сервер БД должны быть соединены друг с другом по гигабитной сети.

С целью экономии и упрощения администрирования Сервер приложений и Сервер БД могут быть объединены в один физический сервер. В этом случае объём ОЗУ физического сервера должен быть удвоен по сравнению с объёмом ОЗУ Сервера приложений.

#### *Сервер приложений*

Программные требования.

**Платформа:** .NET Framework 4.5.

**Язык программирования:** C#.

**Операционная система:** Microsoft® Windows Server 2012 Foundation 64-bit, Rus.

Аппаратные требования.

Табл. 1. Рекомендуемая конфигурация сервера приложений в составе сервера ММ.

|                          |   |
|--------------------------|---|
| Чипсет                   | Intel® C204   |
| Процессор                | Intel Xeon Quad-Core Processor E3-1220v2 (8M Cache, 5 GT/s, 3.10 GHz, 22nm) |
| Оперативная память (ОЗУ) | 16GB DDR3-1600 SDRAM ECC  |
| Контроллеры              | Интегрированный SATA6 - 4x SATA2 RAID 0, 1, 5, 10; 2x SATA3 RAID 0,1        |
| Дисковый массив          | 500GB SATA hard drive (7200rpm)   |
| Сетевая карта            | Интегрированный Intel® Dual Gigabit Controller                              |

|  |                    |
|--|--------------------|
|  | (82574L + 82579LM) |
|--|--------------------|

### Сервер БД

Программные требования.

**Операционная система:** Microsoft® Windows Server 2012 Foundation 64-bit, Rus.

**СУБД:** Microsoft SQL Server 2012 Standard Edition.

Аппаратные требования.

Табл. 2. Рекомендуемая конфигурация сервера БД в составе сервера ММ.

|                          |   |
|--------------------------|---|
| Чипсет                   | Intel® C204   |
| Процессор                | Intel Xeon Quad-Core Processor E3-1220v2 (8M Cache, 5 GT/s, 3.10 GHz, 22nm) |
| Оперативная память (ОЗУ) | 16GB DDR3-1600 SDRAM ECC  |
| Контроллер               | Интегрированный SATA6 - 4x SATA2 RAID 0, 1, 5, 10; 2x SATA3 RAID 0,1        |
| Дисковый массив          | 2 x 1000GB SATA hard drive (7200rpm)  |
| Сетевая карта            | Интегрированный Intel® Dual Gigabit Controller (82574L + 82579LM)           |

### 6.1.2 Способы размещения серверов ММ

Серверы ММ программно организуются в кластер (кластер серверов ММ). Кластер позволяет выполнить требование сохранения функциональности при выходе из строя какого-либо из серверов кластера.

Кластеров серверов ММ может быть несколько. Обычно кластеры разносятся территориально плюс по разным дата-центрам.

Кроме того, возможно расположение кластера и в собственном офисе.

### Кластер серверов MM в дата-центре

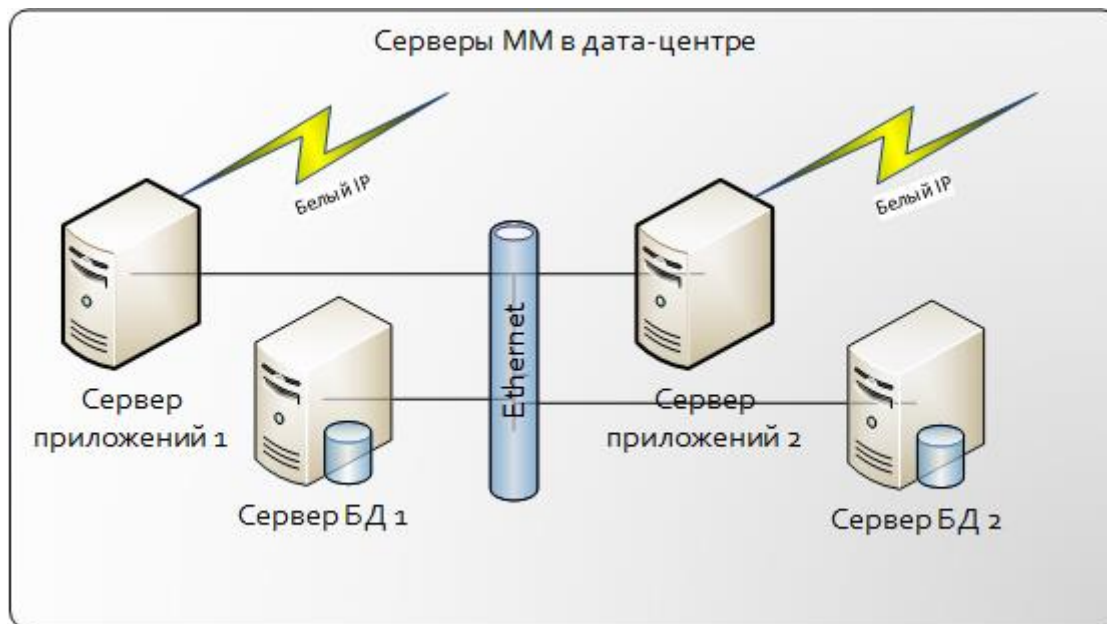


Рис. 4. Кластер серверов MM в дата-центре.

Для обеспечения высокой доступности серверы MM могут располагаться в дата-центрах, где гарантируется их доступность до 99,95% времени и выше.

При размещении в дата-центре, каждому серверу MM выдаётся статический глобальный IP-адрес (белый IP), который затем помещается в A или AAAA-запись DNS-сервера.

### Кластер серверов ММ в офисе



Рис. 5. Кластер серверов ММ в офисе.

При размещении в собственном офисе провайдер, по возможности, должен предоставить несколько статических глобальных IP-адресов (белых IP) по количеству серверов ММ.

Однако, возможен сценарий, когда имеется только один белый IP. Тогда сервера ММ оказываются за NAT маршрутизатора и обрабатывают подключения с разных портов (например, 82.112.65.12:3200, 82.112.65.12:3201 и т.д.).

В этом случае только один из серверов обрабатывает порт по умолчанию (82.112.65.12:3200).

В случае выхода из строя сервера, обрабатывающего порт по умолчанию, другой сервер должен быть переконфигурирован на этот порт.

В итоге каждый сервер ММ, расположенный в офисе, помимо IP-адреса привязывается к порту. Эта информация о привязке должна храниться в БД всех серверов ММ в общих настройках.

Когда ОУ получает список серверов ММ по алгоритму холодного старта, в данном списке должна будет фигурировать пара «IP-адрес и порт» для серверов ММ в офисе.

### Резервирование доступа в Интернет в офисе

В случае наличия аппаратного маршрутизатора, через который осуществляется доступ к серверам ММ в офисе, должно быть предусмотрено резервирование доступа в Интернет средствами самого

маршрутизатора. Маршрутизатор для этого должен быть подключен сразу к двум проводным Интернет-провайдерам (см. [рис. 4](#)).

При обрыве Интернет-соединения по линии основного провайдера маршрутизатор должен автоматически переключиться на другую линию (резервного провайдера соответственно).

Кроме того, в случае обрыва связи по линии основного провайдера и перехода на резервного, сервера ММ в офисе получают новые IP-адреса. Эти адреса должны быть сразу реплицированы на все другие сервера ММ после восстановления Интернет-соединения в офисе по линии резервного провайдера.

Если проблемы основного провайдера временные, администратор может не изменять в DNS-сервере IP-адрес сервера ММ, расположенного в офисе.

В этом случае для ОУ, работающего по алгоритму холодного старта, такой IP-адрес, указанный в DNS, будет недоступен. В результате ОУ придется запросить список серверов ММ для подключения с другого, доступного, IP-адреса. И, так как информация о новых IP-адресах серверов ММ, расположенных в офисе, реплицируется между всеми серверами ММ, то ОУ сможет соединиться с серверами ММ в офисе.

В итоге работоспособность всей Системы будет сохранена.

## **6.2 Подход к репликации данных между серверами ММ**

Как известно, каждый сервер ММ имеет собственный экземпляр БД.

Данные, хранимые в БД, можно условно поделить на 2 группы:

- общие;
- сегментируемые.

### **6.2.1 Общие данные**

Общие данные должны реплицироваться на все сервера ММ.

К общим данным относятся:

- данные о всех серверах ММ;
- данные о всех серверах МС;
- данные о всех МГП;
- данные о всех МО;
- данные о всех ОУ;
- данные о сотрудниках и клиентах компании;
- данные о тревогах и событиях;
- прочие (список будет дополняться по мере реализации Системы).

### 6.2.2 Сегментируемые данные

К сегментируемым данным относятся:

- все данные, посылаемые ОУ на серверы ММ.

Сегментируемые данные должны реплицироваться только на N серверов. Количество серверов для хранения копий сегментируемых данных определяется в настройках Системы администратором.

При сегментации выбираются сервера ММ, распределённые территориально.

Сегментация с одной стороны позволяет продублировать данные с целью обеспечения их доступности в случае выхода из строя какого-либо сервера ММ, а с другой — снижает среднюю пиковую нагрузку на кластер серверов ММ, т.к. данные дублируются не на все сервера, а только на N.

Например, если имеется 6 серверов ММ, то информацию можно продублировать только на 3 сервера. Так решается вопрос распределения нагрузки между серверами.

#### *Информационные группы*

Для сегментации данные делятся на информационные группы.

Информационная группа заводится администратором и позволяет логически группировать ОУ. Обычно информационные группы создаются либо по географическому признаку расположения ОУ, либо исходя из общего числа серверов ММ.

Изначально при вводе нового ОУ в Систему администратор задаёт его принадлежность той или иной информационной группе.

При вводе нового сервера ММ администратор определяет, какие информационные группы он обслуживает. Это означает, что данный сервер ММ будет принимать подключения и хранить данные со всех ОУ, принадлежащих указанным информационным группам.

### 6.3 Ввод в эксплуатацию нового сервера ММ

Введение в строй нового сервера ММ должно занимать как можно меньше времени.

На новом сервере ММ должно быть предварительно установлено разрабатываемое ПО серверной части ММ.

Должны быть сгенерированы уникальные закрытый и открытый ключи сервера ММ. Закрытый ключ должен быть установлен на новый сервер ММ и доступен только ему. Закрытым ключом сервер будет шифровать все свои данные.

По открытому ключу все остальные сервера ММ и ОУ смогут идентифицировать новый сервер в составе модуля мониторинга. Для этого администратору требуется внести этот открытый ключ в общие настройки ММ при добавлении нового сервера и задании его настроек. Далее этот ключ будет автоматически реплицирован на все остальные серверы ММ.

Замечание: До тех пор, пока открытый ключ нового сервера ММ не будет добавлен в общие настройки ММ, новый сервер не может быть добавлен в кластер серверов ММ.

После добавления администратором нового сервера ММ и определения его настроек (в том числе принадлежности к информационным группам) данный сервер становится способен принимать подключения от ОУ и данные по репликации от других серверов ММ.

В первую очередь реплицируется общая информация. Затем реплицируются самые последние (свежие) данные всех ОУ, входящих в назначенные этому серверу информационные группы.

И только после этого с самым низким приоритетом (в фоновом режиме) начинают реплицироваться все остальные данные в обратном хронологическом порядке (более свежие данные приходят раньше).

## 6.4 Передача команды на ОУ

Все серверы ММ могут управлять подключенными к ним ОУ. Для этого сервером ММ могут посылаться управляющие команды на ОУ.

Все команды делятся на 2 типа:

- оперативные;
- отложенные.

### 6.4.1 Оперативные команды

Оперативные команды могут выполняться только при наличии установленного соединения с ОУ. Выполнение такой команды нельзя откладывать.

К оперативным командам относятся:

- снятие с охраны;
- включение оповещения;
- постановка на охрану;
- и др. (список будет расширяться по мере добавления новых типов подключаемых к ОУ устройств и приборов).

Код ошибки или успеха выполнения команды должен передаваться немедленно и отображаться в АРМ диспетчера.

### 6.4.2 Отложенные команды

Отложенная команда имеет более низкий приоритет, чем оперативная. В случае отсутствия соединения с ОУ исполнение такой команды может быть отложено до восстановления связи.

Для отложенных команд можно задавать порог ожидания, по превышении которого попытки отправки команды будут приостановлены, после чего сервером ММ будет сгенерировано



предупреждение «Превышено время исполнения команды». Данное предупреждение должно быть обработано диспетчером.

## 6.5 Отслеживание соединения с ОУ

Сервер ММ отслеживает время передачи последнего пакета данных от всех ОУ, принадлежащих его информационным группам.

Если с момента получения последнего сообщения прошло более двух таймаутов на отправку сообщения ОУ (значение настраивается), то сервер ММ генерирует тревожное событие.

Так как состояние каждого ОУ одновременно отслеживается несколькими серверами ММ, то и тревожных событий, сгенерированных сервером ММ, возникнет несколько (по одному на каждом из серверов).

Каждый сервер ММ генерирует своё тревожное событие и помещает его в таблицу тревог с указанием ОУ и номера последнего полученного от него пакета данных. Данная таблица реплицируется между всеми серверами ММ.

Несмотря на наличие нескольких записей в таблице тревог на одно и то же ОУ, АРМ диспетчера при запросе тревожных событий получит только одну агрегированную запись. Агрегирование идёт по идентификатору ОУ и номеру последнего сообщения.

## 6.6 Отслеживание состояний подконтрольных устройств ОУ

Сервер ММ постоянно следит за сменой состояний подконтрольных устройств, посылаемых с ОУ (см. [пункт 5.5.3](#)).

В случае смены состояния сервер ММ генерирует событие или тревогу. Тревожные события заносятся сервером ММ в таблицу тревог и немедленно реплицируются на другие сервера ММ. Серверы ММ, получая новые записи в таблице тревог, немедленно генерируют тревожное событие.

## 6.7 Получение тревог от ОУ

Сообщения (пакеты данных) с тревогами, получаемые с ОУ, заносятся сервером ММ в таблицу тревог и немедленно реплицируются на другие сервера ММ. Серверы ММ, получая новые записи в таблице тревог, немедленно генерируют тревожное событие.

Таким образом достигается гарантированный сброс тревожного события в случае выхода из строя какого-либо сервера ММ.

АРМ диспетчера должно агрегировать все записи о тревоге в одну. Агрегирование идёт по идентификатору ОУ и номеру сообщения от ОУ с тревогой.

## 6.8 Синхронизация времени

Точное время является важной составляющей сервера ММ. Оно позволяет адекватно оценивать хронологию всех возникающих в Системе событий, тревог. Расхождения во времени недопустимы — для этого на сервере ММ используется механизм синхронизации времени.

Каждый сервер MM периодически синхронизирует внутренние часы с доверенными серверами времени по протоколу NTP. Синхронизация времени должна быть настроена на сервере MM администратором как периодическая задача.

Кроме того, каждый сервер MM является сервером времени для подключающихся к нему ОУ.

## 6.9 Безопасность

### 6.9.1 Фаервол

Для защиты от DDoS-атак и несанкционированных подключений используется аппаратный фаервол.

### 6.9.2 Безопасность соединений

Все соединения, устанавливаемые с сервером MM, шифруются. К таким соединениям относятся:

- соединение с ОУ;
- соединение с другим сервером MM;
- соединение с АРМ диспетчера, администратора;
- соединение с другими модулями Системы;
- соединение с ПО для управления RS-устройствами.

Шифрование соединения достигается туннелированием через протокол SSH-2. Протокол SSH-2 позволяет:

- проверять SSH-клиенту, является ли SSH-сервер, к которому устанавливается подключение, доверенным. Проверка идёт по открытому ключу сервера;
- проверять SSH-серверу, является ли подключающийся SSH-клиент доверенным. Проверка ведётся по открытому ключу SSH-клиента;
- шифровать все передаваемые по установленному соединению данные.

В итоге будут полностью исключены попытки установления несанкционированного подключения к серверам MM. Кроме того, будут исключены попытки несанкционированной подмены серверов MM и попытки перенаправления шифруемого трафика.

## 6.10 Полный список функций сервера MM

- Прием подключений ОУ.
- Прием подключений от ПО для управления RS-устройствами.
- Прием подключений АРМ диспетчеров.
- Прием подключений АРМ администраторов.
- Сохранение в БД данных от ОУ.
- Репликация БД между серверами MM.
- Отслеживание работы серверов MM.

- Отслеживание загрузки каждого сервера ММ по CPU, памяти, времени записи события в БД.
- Отслеживание количества подключений ОУ к каждому серверу ММ.
- Отслеживание наличия соединения с ОУ и получение от ОУ пакетов данных. Тревога в случае отсутствия связи с ОУ более чем XX секунд (время настраивается).
- Синхронизация времени с сервером времени по протоколу NTP.
- Предоставление сигналов точного времени для ОУ.
- Передача на ОУ команд управления диспетчера и команд настроек администратора.
- Передача на ОУ команд для управления RS-устройствами.
- Переадресация команд управления ОУ между серверами ММ, так как ОУ может быть подключено к одному серверу ММ, а приложение, передающее команду, к другому.
- Определение тревог и передача информации о них диспетчерам.
- Контроль временного регламента обработки тревоги со стороны диспетчера. В случае нарушения регламента повторная передача тревоги в общую очередь обработки тревог.
- Передача скриншотов с сервера видеонаблюдения на ПО для просмотра видео с серверов видеонаблюдения и на АРМ диспетчера.
- Передача обновлений на ОУ.
- Хранение истории событий, ошибок, предупреждений, тревог ОУ.
- Хранение истории действий диспетчеров.

## 7 Прибор приёмно-контрольный (ППК)

ППК — это устройство, предназначенное для приема сигналов от пожарных, охранных извещателей, обеспечения электропитанием активных (токопотребляющих) пожарных и охранных извещателей, выдачи информации на световые, звуковые оповещатели и пульты централизованного наблюдения, а также формирования стартового импульса запуска прибора пожарного управления. Основным элементом систем охранной, пожарной, охранно-пожарных сигнализаций.

ППК подключается к ОУ по шине RS-485.

### 7.1 События ППК, передаваемые ОУ

Все события, генерируемые ППК, отсылаются ОУ в виде пакета данных на сервер ММ.

ППК может генерировать следующие события (взято из «Болида» и дополнено).

- «ШС взята на охрану (взятие)» (ШС — сигнальная шина).
- «Неудачное взятие (невзятие)».
- «Сработка датчика».
- «Внимание! Опасность пожара».
- «Пожарная тревога».
- «Обрыв ШС».
- «Короткое замыкание ШС».
- «Взлом корпуса».
- «Восстановление корпуса».
- «Запуск теста».
- «Программирование».
- «Задержка взятия».
- «Снятие ШС с охраны».
- «Сброс прибора».
- «Неисправность источника питания».
- «Восстановление источника питания».
- «Доступ отклонён (неизвестный PIN-код)».
- «Идентификация хозоргана».
- «Восстановление технологической ШС».
- «Нарушение технологической ШС».

- «Тихая тревога».
- «Тревога входной зоны».
- «Восстановление снятой с охраны ШС».
- «Нарушение снятой с охраны ШС».
- «Тревога проникновения».

## 7.2 Постановка ППК на охрану

Команда постановки на охрану может формироваться с:

- считывателя, подключенного к ОУ;
- ПО для управления RS-устройствами.

Для постановки на охрану клиент убеждается, что все охраняемые входы перешли в дежурное состояние. Сигнальный светодиод при этом не должен гореть. В случае, если хотя бы один охраняемый шлейф находится в тревожном состоянии, постановка на охрану невозможна, и требуется перевести шлейф в дежурное состояние.

В интерфейсе ПО для управления RS-устройствами должен быть список шлейфов с расшифровкой и цветовой сигнализацией состояния, чтобы пользователь мог самостоятельно определить, какой из контуров охраны ему следует проверить.

Пример:

| Шлейф             | Состояние |
|-------------------|-----------|
| 1 Окно кабинет 1  | Дежурное  |
| 2 Окно кабинет 2  | Дежурное  |
| 3 Дверь кабинет 1 | Дежурное  |
| 4 Дверь кабинет 2 | Тревожное |

Допускается программирование одного шлейфа на задержку постановки. Например, выходная дверь должна вставать на охрану через 30 сек.

Далее пользователь вводит PIN-код либо подносит ключ к считывателю, устройство встает на охрану. Далее ОУ отправляет информацию о переходе в режим охраны на сервер.

В случае ввода неверного PIN-кода 5 раз подряд возникает состояние тревоги.

При постановке или снятии с охраны ОУ фиксирует, каким пользователем производились действия.

## 8 Модуль видеонаблюдения (МВ)

Модуль видеонаблюдения представляет собой программно-аппаратный комплекс, выполняющий функции по ведению видеонаблюдения за охраняемым объектом.

Из чего состоит МВ:

- камера видеонаблюдения;
- DVR, к которому подключены камеры;
- плагин для работы с DVR, устанавливаемый на ОУ;
- готовое ПО для просмотра видео с DVR.

### 8.1 Камеры видеонаблюдения

Камеры видеонаблюдения несут функцию по непосредственному видеонаблюдению заданной зоны охраняемого объекта (например, коридор или входная дверь на склад).

Камеры должны быть совместимы с DVR, к которому они подключены. Видео с камер отправляется напрямую на DVR.

#### 8.1.1 Контроль питания камер видеонаблюдения

Для контроля питания камер видеонаблюдения их БП дополнительно подключаются к выходу Alarm Input DVRa. Считается, что DVR имеет достаточное число выходов Alarm Input.

В случае нарушения питания DVR посылает сигнал тревоги на ОУ, которое затем ретранслирует его на сервер ММ.

#### 8.1.2 Слежение за состоянием камер наблюдения

DVR самостоятельно следит за состоянием камер. Эти состояния передаются ОУ для дальнейшей передачи на сервер ММ.

Примеры отслеживаемых состояний:

- подключена ли камера к DVR;
- есть ли питание на камере;
- ведётся ли трансляция сигнала с камеры.

### 8.2 DVR

DVR — это видеорегистратор, к которому подключаются все камеры на объекте.

Напомним, что DVR подключается к ОУ через переходник USB-Ethernet.

### 8.2.1 Ведение архива записей

DVR ведёт запись видеосигнала с камер наблюдения на дисковый носитель, установленный в DVR.

Архив записей может быть просмотрен в любое время диспетчером, клиентом компании.

Для просмотра архива используется готовое ПО для просмотра видеозаписи.

### 8.2.2 Просмотр видеозаписи с DVR Клиентом компании

Клиент компании использует готовое ПО для просмотра видеозаписи с DVR.

Подключение к DVR через Интернет.

**Внимание!** В случае, когда Клиент компании просматривает видеоизображение, подключаясь через Интернет, подключение к DVR должно вестись по отдельному каналу связи! Это исключает воздействие на работу Системы, так как не будут затронуты служебные каналы связи.

Возможно исключение, когда Клиенту компании предоставляют доступ через служебный канал связи для подключения к DVR.

Подключение к DVR через LAN.

Клиент компании может подключаться к DVR внутри LAN через планшетный пульт управления или со своего мобильного устройства с установленным ПО для просмотра видеосигнала с DVR. Подключение производится через WiFi.

### 8.2.3 Просмотр видеосигнала с DVR диспетчером

Диспетчер использует АРМ Диспетчера для просмотра видеосигнала с DVR. Для этого в АРМ диспетчера встраивается готовое ПО для просмотра видеозаписи с DVR.

Диспетчер подключается к DVR через Интернет.

## 8.3 Плагин для работы с DVR, устанавливаемый на ОУ

Специально для выбранной модели DVR должен быть разработан плагин, устанавливаемый на ОУ, для работы с DVR.

Для разработки плагина от производителя DVR требуется предоставить API контроля DVR, а ещё лучше, SDK для разработки плагина.

Цель плагина — это контроль состояний DVR и передача этих состояний серверу MM.

Примеры состояний:

- подключена ли камера к DVR;
- есть ли питание на камере;
- ведётся ли трансляция видеосигнала с камеры;

- есть ли питание на DVR;
- и т.д. (список будет расширяться).

#### **8.4 Готовое ПО для просмотра видеоизображения с DVR**

Производителем DVR должно быть предоставлено готовое ПО для просмотра видеоизображения с DVR (кроссплатформенное).

Это ПО будет устанавливаться на планшетный пульт управления, диспетчеру, клиенту компании.



## 9 АРМ диспетчера

---

Автоматизированное рабочее место диспетчера предназначено для наблюдения за состоянием ОУ и отработке тревог.

Программа имеет несколько окон, между которыми диспетчер может переключаться.

- Окно журнала событий.
- Окно тревог. В этом окне отображаются только тревожные ситуации, которые необходимо обрабатывать диспетчеру. Диспетчер берет в обработку тревогу из этого списка.
- Окно тревоги.
- Окно топологии устройств на охраняемом объекте.
- Окно информационной карточки о Клиенте компании.
- Окно карты.

### 9.1 Программные требования

**Платформа:** .NET Framework 4.5, WinForms.

**Язык программирования:** C#.

**СУБД:** Microsoft SQL Server Compact 4.0.

**Операционная система:** Windows.

GUI АРМ диспетчера должно работать асинхронно относительно запросов к серверам Системы.

Все запросы к серверам должны делаться в фоновом потоке. GUI, по возможности, не должно блокироваться, а должно показывать значок отправки запроса серверу и позволять пользователю производить другие действия.

### 9.2 Подключение к серверу ММ

При старте АРМ подключается к ближайшему наименее загруженному серверу ММ.

АРМ диспетчера не может работать без подключения к серверу ММ (режим offline недопустим).

#### 9.2.1 Безопасность подключения

АРМ диспетчера снабжается открытым и закрытым ключами. Открытый ключ АРМ диспетчера добавляется администратором в БД сервера ММ с последующей репликацией.

Таким образом, все серверы ММ позволят подключаться к ним только доверенным АРМ диспетчера, открытые ключи которых им известны.

Во время подключения АРМ диспетчера к серверу ММ устанавливается безопасное соединение с шифрованием всех передаваемых данных.

Подробности см. в разделе «[Безопасность](#)» модуля мониторинга.

### **9.2.2 Проблемы подключения к серверу ММ**

- При отсутствии ответов от сервера в течение заданного таймаута АРМ диспетчера следует подключиться к другому серверу.
- При явном разрыве соединения с сервером ММ должно автоматически происходить подключение к другому серверу ММ. На время соединения с сервером диспетчеру должно отображаться модальное окно с текстовым описанием текущего процесса. Диспетчер может скопировать текст из окна для отправки администратору (например, через Мессенджер или почтой), который должен будет отреагировать на сообщение и проверить работу сервера ММ, соединение с которым было потеряно.

### **9.3 Схема подключения диспетчерских пунктов**

Ниже приведена общая схема подключения диспетчерских пунктов.

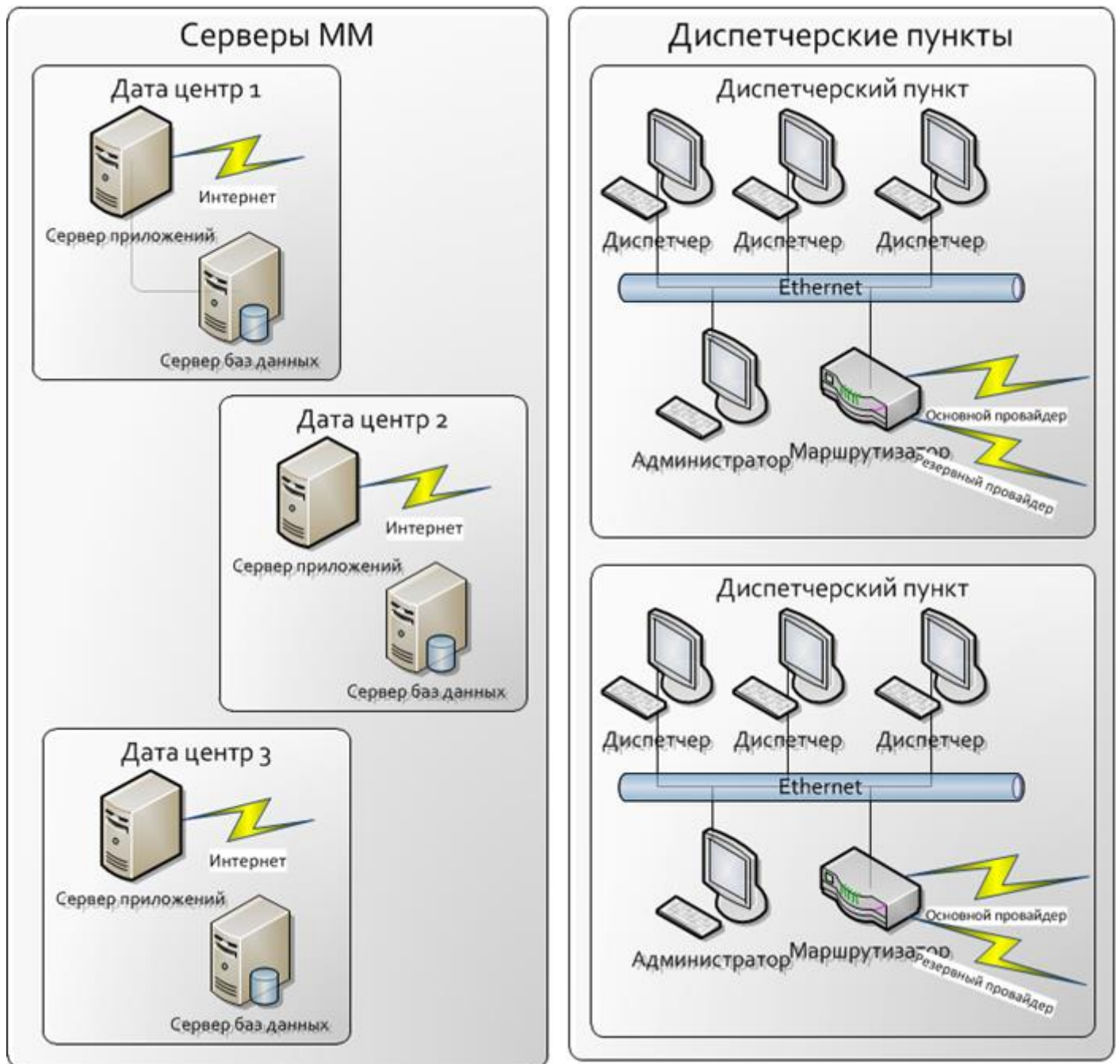


Рис. 6. Схема подключения диспетчерских пунктов.

## 9.4 Окно журнала событий

В окне журнала событий без фильтрации показываются события, полученные с ОУ.

Примеры событий (взято из описания ОУ пункта «Типы пакетов данных»).

- Состояние RS-устройства.
- Состояние БП.
- Срабатывание датчика, подключенного к ППК.

- Тревожные события с DVR.
- Смена провайдера.
- Ошибка подключения к серверу Системы.
- Разрыв подключения с сервером Системы.
- Неверный ввод PIN-кода.
- И др. (список пополнится по мере разработки системы).

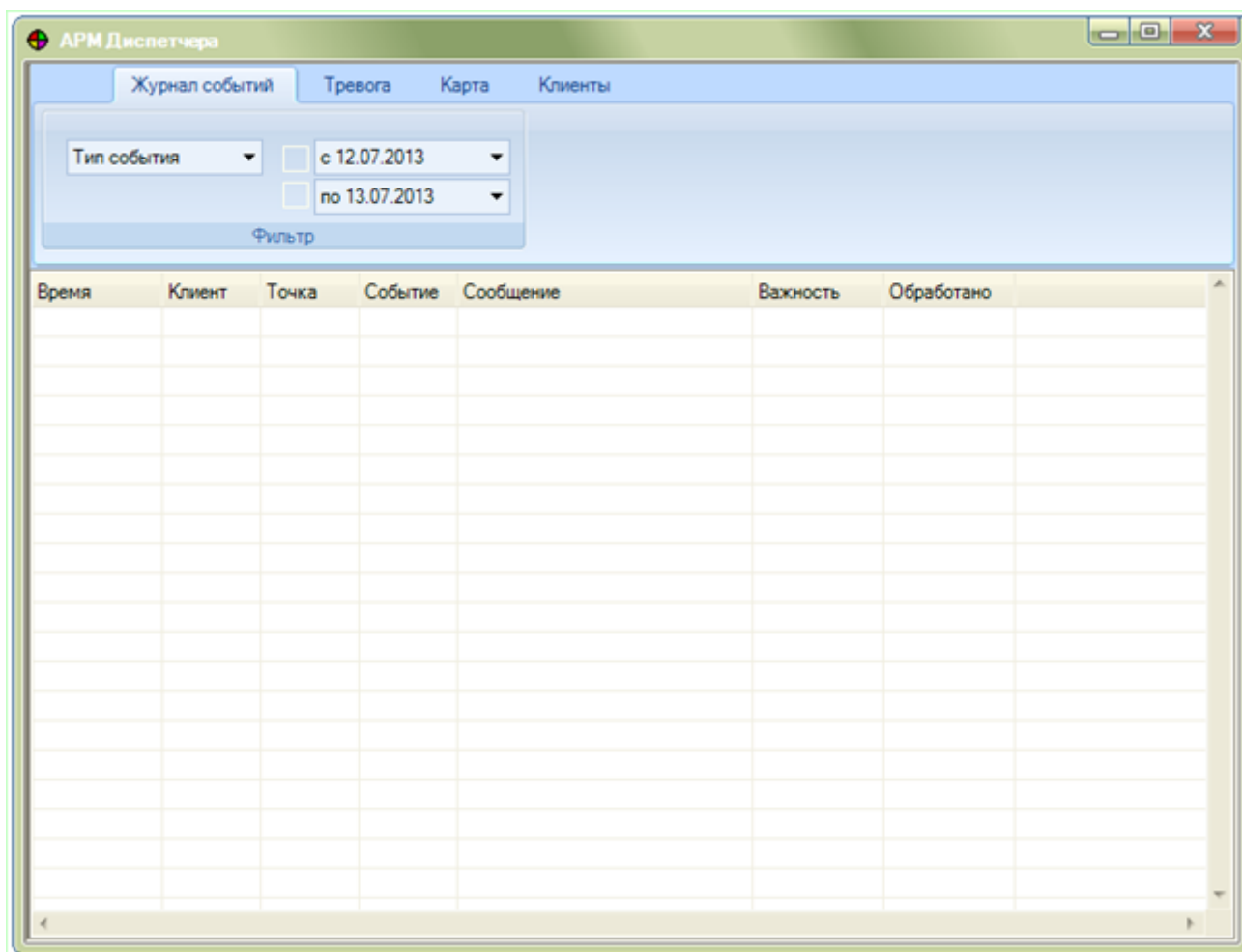


Рис. 7. Окно журнала событий.

Наблюдение за этим окном позволяет выявлять возникающие проблемы в работе Системы.

На отображаемые сообщения можно наложить фильтрацию, чтобы увидеть события одного типа или от одного устройства за заданный период времени.

#### 9.4.1 Настраиваемое окно журнала событий

Фильтры в окне событий могут быть сохранены для их последующей быстрой активации. Это необходимо, когда диспетчер хочет быстро просмотреть, например, все тревожные события на заданном охраняемом объекте.

Фильтры могут быть как общими — настраиваться администратором и распространяться по всем АРМ диспетчера, так и индивидуальными, настраиваться непосредственно диспетчером.

## 9.5 Окно тревог

В окне тревог отображаются все тревожные ситуации, возникающие в Системе. Тревоги отображаются всем диспетчерам. Процесс взятия тревоги в обработку диспетчером описан в следующем пункте «[Захват тревоги в работу](#)».

**Замечание:** Время появления тревоги в окне тревог должно быть минимальным. Для этого, во-первых, при появлении новой тревоги на сервере ММ, она доставляется на другие сервера в течение времени PUSH-репликации, это примерно 100–250 мс, в зависимости от расстояния между серверами.

Во-вторых, АРМ диспетчера опрашивает сервер ММ, к которому оно подключено, каждую секунду. В результате опроса сервер ММ может вернуть пакет с тревогой, которая немедленно появляется в окне тревог.

В итоге любая тревога доставляется до диспетчера максимум за 1–2 секунды с момента её возникновения на сервере ММ.

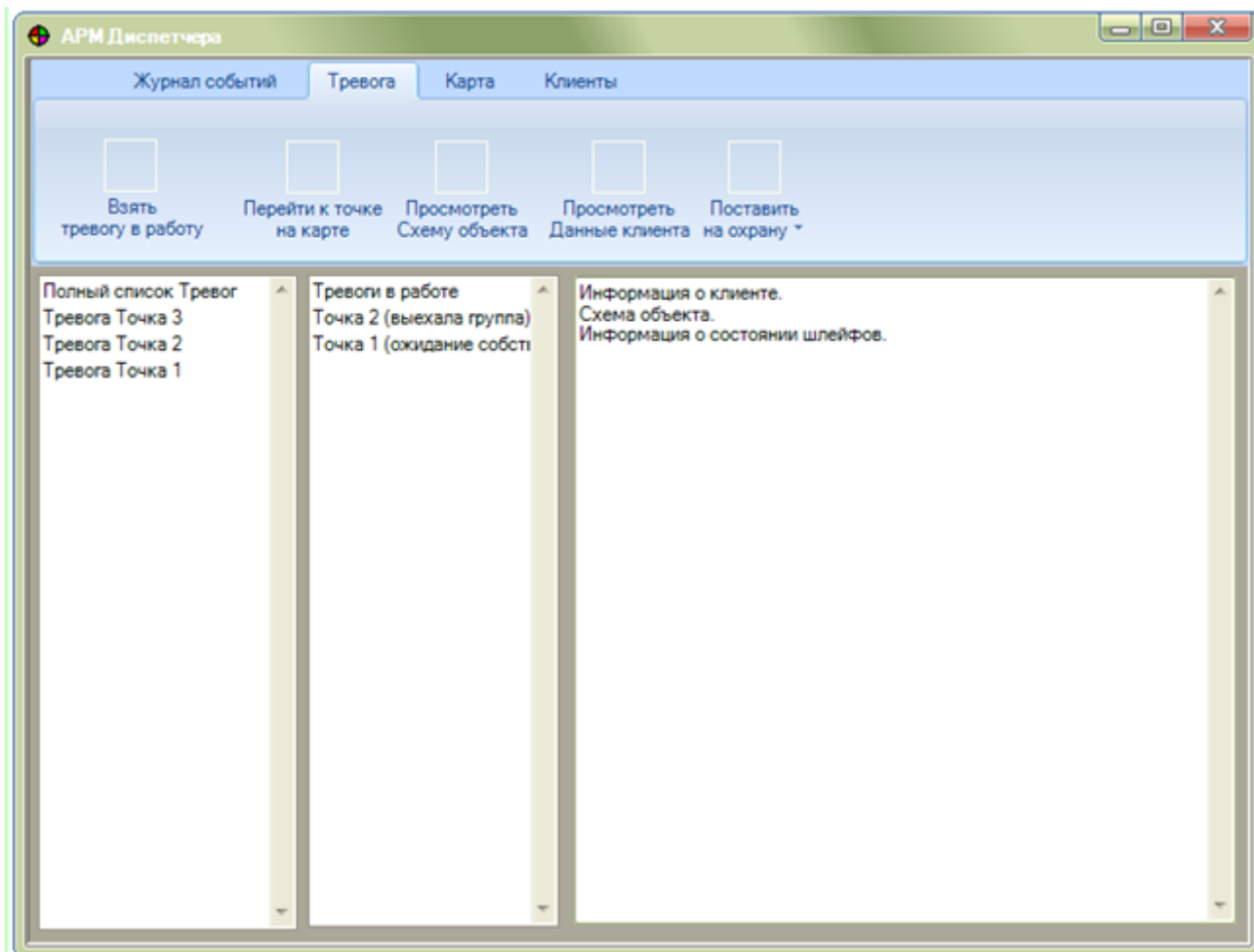


Рис. 8. Окно обработки тревог.

В окне тревог может быть настроен фильтр по критериям, заданным администратором.

Критерии фильтрации могут гибко настраиваться. Например, при организации нескольких географически удалённых диспетчерских пунктов можно указать, чтобы диспетчер видел первичные тревоги только своего региона и все повторные, или чтобы отображались все тревоги, длящиеся более получаса, или не взятые в работу более 1 минуты и т.п.

## 9.6 Захват тревоги в работу

Любой диспетчер может взять тревогу в работу после её появления в окне тревог. При попытке взять тревогу в работу сервер ММ, к которому подключено АРМ диспетчера, рассылает сообщения о захвате тревоги на другие сервера ММ. Если на другом сервере кто-то попытался захватить эту же тревогу, то срабатывает правило приоритета захвата: тревога передается первому захватившему ее диспетчеру.

После захвата тревоги для всех остальных диспетчеров в окне тревог выдаётся соответствующее оповещение.

Время передачи сообщения о захвате тревоги должно быть минимальным.

## 9.7 Отслеживание отключения АРМ диспетчера, вброс повторных тревог

Как было написано ранее, АРМ диспетчера в начале своей работы подключается к серверу ММ.

АРМ диспетчера периодически посылает на сервер ММ сообщение о своём нормальном функционировании, которое реплицируется между всеми серверами ММ. Такая схема позволяет отслеживать отключение АРМ диспетчера.

Если происходит неожиданное отключение АРМ диспетчера, который уже взял в обработку одну или несколько тревог, то сервер ММ заново вбрасывает эти тревоги в общий список тревог для обработки другим диспетчерами. Такие тревоги называются повторными.

Если АРМ диспетчера, которое неожиданно отключилось, так и не появляется в Системе (не зафиксирован факт подключения к серверу ММ) в течение 2–3 заданных таймаутов, то сервером ММ генерируется новая тревога вида «Пропал диспетчер». Эта тревога вбрасывается в общую очередь тревог и становится видна всем диспетчерам. Дополнительно сервер ММ производит извещение супервайзера (администратора) диспетчера через модуль оповещения (МО). В извещении указывается, какой диспетчер пропал, какие тревоги были на него назначены, и в какое время произошло отключение диспетчера.

## 9.8 Отслеживание временного регламента

Любая тревога должна пройти цикл обработки диспетчером. Каждый этап цикла имеет заданное максимальное время выполнения (таймаут). Пошаговая обработка диспетчером тревоги в строгом соответствии со временем называется временным регламентом.

Таймауты каждого этапа цикла обработки тревоги задаются администратором на сервере ММ, далее информация реплицируется между всеми серверами.

Сервер ММ, к которому подключен диспетчер, начинает следить за выполнением временного регламента в момент захвата тревоги диспетчером.

Если диспетчер не уложился в таймаут какого-либо этапа, то в АРМ диспетчера в диалоговом окне выдаётся предупреждение, на которое он должен отреагировать. Если реакции не последовало, то сервером ММ формируется новая тревога на основе просроченной, и она поступает в обработку всеми диспетчерами. Таким образом, гарантируется, что тревога будет кем-то захвачена и обработана.

Также сервер ММ, используя МО, извещает супервайзера диспетчера о нарушении временного регламента с указанием информации о диспетчере, обрабатываемой им тревоге и времени, когда был нарушен регламент.

**Внимание!** Любая тревога должна быть обязательно обработана до конца. Недопустима потеря или частичная обработка тревоги.

Ниже приводится пример списка состояний тревоги, в которые её переводит диспетчер. Этот список поможет понять, как задаётся цикл обработки тревоги.

- Зафиксирована. Тревога пришла на пульт, но ни один диспетчер ещё не начал ее обработку.
- Захват тревоги в работу. Диспетчер взял на себя тревогу.
- Отправлен экипаж. Диспетчер направил экипаж на точку.
- Экипаж прибыл. Экипаж сообщил диспетчеру, что прибыл на место.
- Нарушение периметра. Обнаружено, что было проникновение.
- Нет нарушения периметра. Двери закрыты, окна целы, имеется ложное срабатывание.
- Охрана до прибытия. Оставление одного сотрудника для охраны объекта до перепостановки объекта на охрану.

Список не полон, может дополняться администратором и лишь формализует состояние, в котором находится тревога. Для каждого состояния администратором выбирается временной интервал до появления предупреждений или переназначения тревоги другому диспетчеру.

## 9.9 Протоколирование действий диспетчера

Все значимые действия диспетчера должны протоколироваться и отправляться на сервер ММ. Значимыми действиями являются:

- открытие карточки объекта;
- открытие схемы объекта;
- отправка команд на ОУ;
- отправка сообщений в Мессенджере;
- голосовые вызовы;



- изменения состояния тревоги.

Действия диспетчера администратор в дальнейшем может просмотреть в текстовом виде с привязкой каждого действия ко времени.

## 9.10 Окно карты

Окно карты предназначено для отображения на карте местоположения охраняемых объектов, текущего положения автомобилей ГБР.

В качестве подложки карты может использоваться один из следующих сервисов:

- Яндекс.Карты;
- Google Maps;
- 2ГИС.

Положение автомобилей ГБР отслеживается модулем геопозиции (МГП). АРМ диспетчера непрерывно получает данные из МГП для отображения на карте геопозиции автомобилей ГБР в реальном времени.

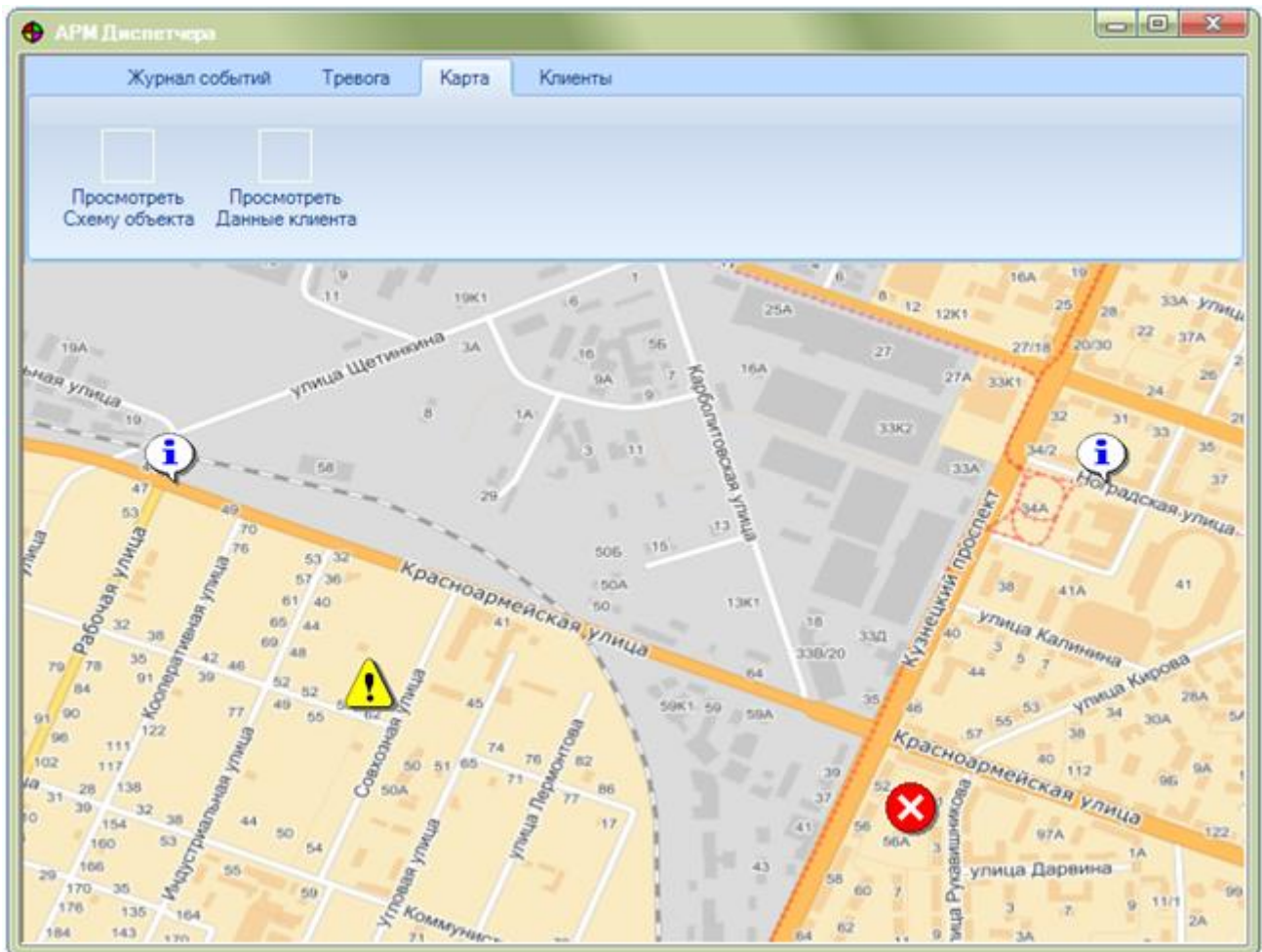


Рис. 9. Окно карты.



Положение неподвижных охраняемых объектов и подъезды к нему вносятся в базу данных администратором при настройке объекта.

Если положение охраняемого объекта не является фиксированным, т.е. данные о его положении постоянно посылаются GPS-адаптером, подключенным к ОУ, — то позиция такого объекта на карте отрисовывается динамически, как и для случая автомобилей ГБР. Данные о положении такого охраняемого объекта передаются из МГП.

На карте диспетчеру отображаются только объекты с тревогой. Также над автомобилями и объектами на карте отображается имя диспетчера, который работает с ними в данный момент. Таким образом, диспетчер всегда может понять, с какими объектами работает только он.

Двойной щелчок по охраняемому объекту открывает окно просмотра топологии устройств на объекте.

## **9.11 Модуль оповещения клиентов**

В случае тревоги на объекте, технических работ или сбоев в работе сервиса необходимо оповестить об этом клиента. Для оповещения могут использоваться электронная почта или SMS.

### **9.11.1 Оповещения по электронной почте**

Клиент предоставляет список адресов электронной почты, куда требуется отправлять сообщения. Специальный сервис (сервисы) на серверах кластера производят рассылку электронной почты. Сообщения электронной почты могут формироваться автоматически или вручную диспетчером или администратором.

### **9.11.2 Оповещения по SMS**

Клиент предоставляет номера телефонов, на которые следует отправлять SMS сообщения. На одном или нескольких серверах кластера запущен сервис для отправки SMS через шлюз провайдера, например, <http://smc.ru/>. Сообщения могут формироваться автоматически, или вручную диспетчером, или администратором.

## 9.12 Поиск и просмотр информации о Клиенте компании

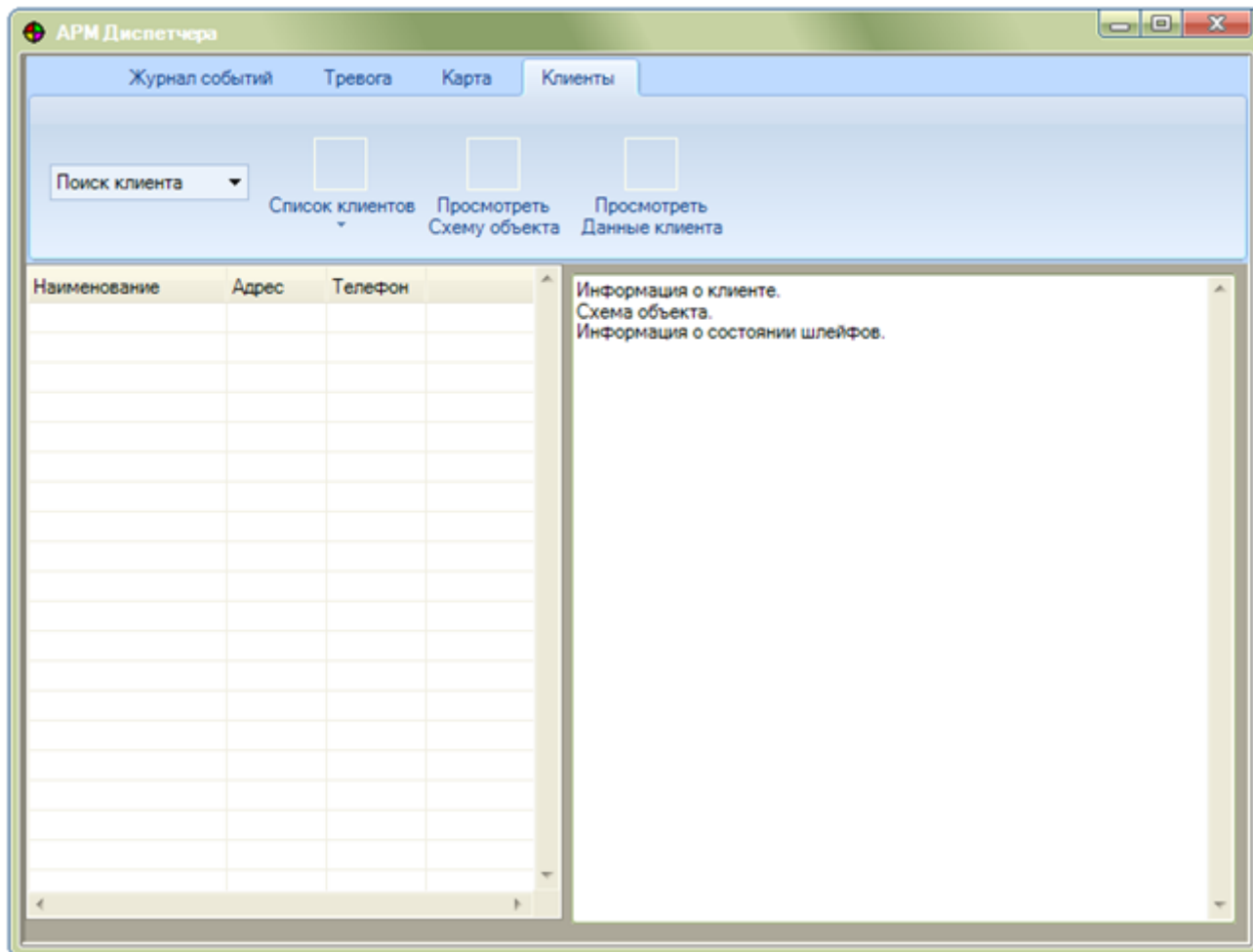


Рис. 10. Окно поиска и просмотра информации о клиенте.

Диспетчеру может потребоваться найти карточку клиента, чтобы просмотреть все необходимые данные о владельце, ответственном лице, телефоны и т.д. Для этого в приложении диспетчера существует окно поиска и просмотра информации о клиенте.

Данное окно также может быть вызвано прямо с карты при просмотре свойств охраняемого объекта.

Также в этом окне диспетчер может внести пометки, привязанные к клиенту или охраняемому объекту. Эти пометки становятся видимыми для всех диспетчеров.

Все внесённые диспетчером изменения журналируются на сервере ММ, чтобы можно было воспроизвести, кто, когда и что редактировал.

Из карточки Клиента компании диспетчер всегда может перейти на карту, где находится охраняемый объект этого клиента.

## 9.13 Просмотр топологии устройств охраняемого объекта

Диспетчер имеет возможность просмотреть схематичную топологию любого объекта. На топологии представлены следующие устройства.

- Схема подключения и связи между всеми устройствами.
- ОУ, его IP-адреса.
- Терминальные датчики охранно-пожарной сигнализации, текстовая расшифровка их назначения. Так диспетчер имеет возможность указать Клиенту компании, какой шлейф находится в тревожном состоянии, и указать, куда ведет этот шлейф, например, «окно в кабинете 3».
- RS-устройства (в частности, исполнительные устройства) и их состояние.
- Маршрутизатор и состояние всех его Интернет-подключений.
- Блоки питания и их состояние — питание от сети, от АКБ, состояние заряда АКБ.
- DVR, его состояние и состояние камер.
- Планшетный пульт управления и его состояние.

#### 9.14 Просмотр камер видеонаблюдения

В случае тревоги диспетчер имеет возможность подключиться к камерам видеонаблюдения и посмотреть, что происходит на объекте.

Для этого в АРМ диспетчера добавляется возможность вызова готового ПО для просмотра видеоизображения, которое подключается к DVR на охраняемом объекте через служебный канал связи — подробности см. в [описании МВ](#).

#### 9.15 Синхронизация времени

Правильное время на компьютере диспетчера является критичным. Иначе диспетчер не сможет корректно воспринимать хронологию возникающих событий и тревог.

Компьютер диспетчера, где установлено АРМ диспетчера, должен быть настроен системным администратором на синхронизацию времени с доверенными серверами времени.

См. [«Синхронизация времени»](#) серверов ММ.

#### 9.16 Просмотр хронологической последовательности событий объекта

В АРМ диспетчера должен быть реализован плеер событий охраняемого объекта.

Плеер нужен для анализа и восстановления последовательности событий, возникших на объекте. В плеере должна быть возможность выбора времени и просмотра состояний всех устройств объекта на схеме его топологии.

В плеере должна быть возможность быстрой перемотки времени.

Плеер должен быть реализован так, чтобы в процессе воспроизведения можно было видеть изменение состояния датчиков, переключения между провайдерами, переход на питание с АКБ, состояние связи с серверами Системы, состояния тревоги и т.д. одновременно с действиями диспетчера.

Отображаемый момент времени может выбираться пользователем перемещением ползунка, либо указанием точного времени.

Дополнительно следует показывать все пометки диспетчера по этому объекту в виде журнала отработки тревоги.

### 9.17 Полный список функций

- Подключение к серверу ММ.
- Автоматическое подключение к другому серверу ММ при потере связи.
- Получение событий и тревог от сервера ММ.
- Захват тревоги в работу.
- Обработка тревоги.
- Протоколирование действий диспетчера по отработке тревог.
- Отображение карты с указанием положения ГБР и объектов в тревожном состоянии.
- Просмотр топологии устройств и их состояния на объекте.
- Отправка команд исполнительным устройствам на объекте.
- Просмотр видео с камер наблюдения на объекте.
- Просмотр журналов событий.
- Просмотр журналов обработки тревог.
- Отслеживание временного регламента обработки тревоги.
- Просмотр информации о клиенте.
- Просмотр информации об объекте.
- Редактирование дополнительной информации, клиента и объекта (пометки диспетчера).

## 10 АРМ администратора

---

АРМ администратора предназначено для конфигурирования серверов мониторинга и ОУ, просмотра журналов работы для диагностики ошибок и перераспределения нагрузки, ввода сервера в работу в кластере и выведения сервера из состава кластера.

### 10.1 Платформа

**Платформа:** .NET Framework 4.5, WinForms.

**Язык программирования:** C#.

**СУБД:** Microsoft SQL Server Compact 4.0.

**Операционная система:** Windows 7, Windows 8.

### 10.2 Функциональные требования

АРМ администратора позволяет.

- Вводить в состав кластера новые сервера мониторинга.
- Настраивать конфигурацию любого сервера мониторинга.
- Добавлять в базу данных новые оконечные устройства (идентификаторы и открытые ключи).
- Рисовать топологию устройств на объекте.
- Вводить в базу данных и редактировать информацию об охраняемых объектах.
- Вводить в базу данных топографические координаты объектов.
- Вводить в базу данных и редактировать информацию о контрагентах.
- Производить наблюдение за работой серверов. Отслеживать нахождение серверов мониторинга в режиме online.
- Просматривать журнал ошибок и предупреждений ОУ.
- Контролировать загрузку каждого сервера мониторинга по CPU, памяти, времени записи события в БД, времени ответа клиенту.
- Отслеживать количество подключений ОУ к каждому узлу кластера мониторинга.
- Отслеживать количество подключений АРМ диспетчера к каждому узлу кластера мониторинга.
- Отслеживать количество подключений мобильных клиентов к каждому узлу кластера.
- Определять сервер, к которому подключено конкретное оконечное устройство.
- Определять сервер, к которому подключено АРМ диспетчера.
- Отправлять команды конфигурирования ОУ.
- Публиковать обновления новых версий ПО ОУ.



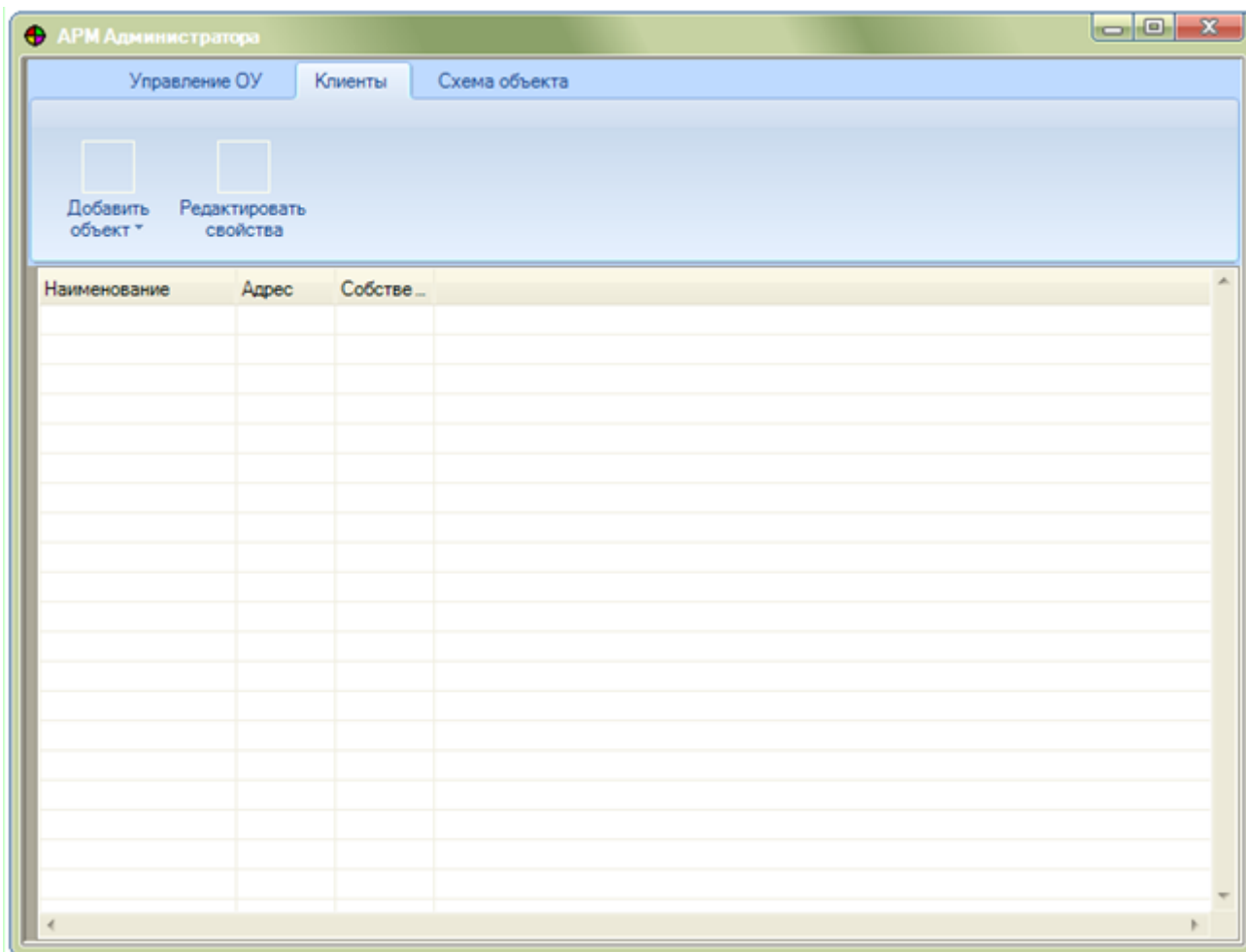


Рис. 12. Окно редактирования клиентов и объектов охраны.

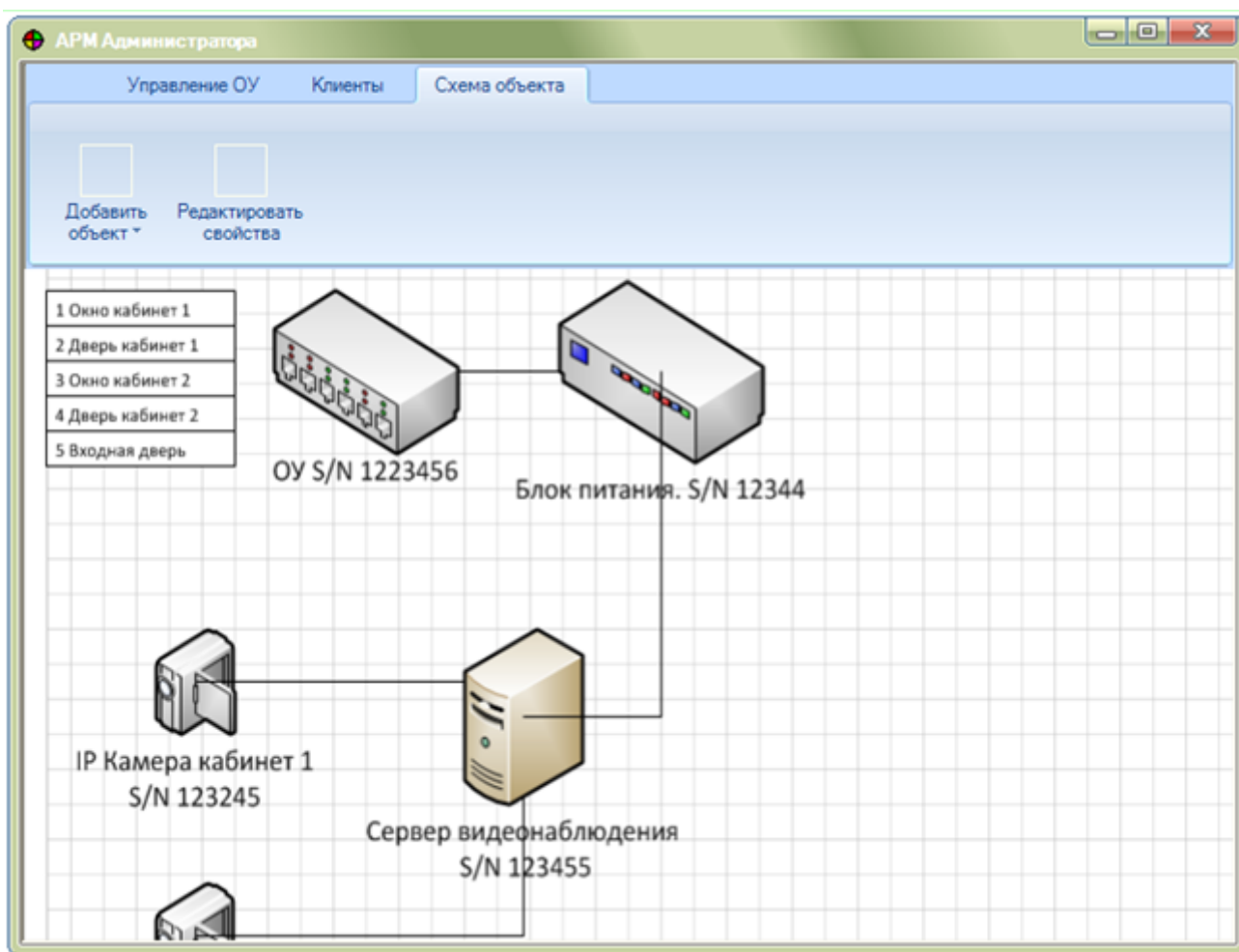


Рис. 13. Редактирование схемы объекта.

## 10.4 Справочная информация

### 10.4.1 Справочник организаций

Справочник организаций имеет следующие поля.

- Краткое наименование.
- Полное наименование.
- ИНН.
- ОГРН.
- Адрес юридический.
- Адрес местонахождения.
- Руководитель.
- Контактное лицо, телефон.
- Примечание.



- Выставлять счета (да/нет).
- Ежемесячная сумма обслуживания.

#### 10.4.2 Точки охраны

Справочник точек охраны имеет следующие поля.

- Наименование.
- Адрес.
- GPS координаты.
- Контактное лицо, телефон.
- Дата ввода в эксплуатацию.
- Статус обслуживания (обслуживается, не обслуживается, временно приостановлено, договор аннулирован и др.).
- Список установленного оборудования.
- Список людей, имеющих доступ на объект.
- Примечание.

#### 10.4.3 Схема подключения устройств

Редактирование схемы подключения устройств производится схематически в специальном редакторе, где можно добавлять иконки устройств, рисовать между ними связи. Для каждого устройства на схеме добавляется соответствующая строка в списке оборудования. Для оборудования можно задать его серийный номер, примечание, указать его расположение. Пример схемы приведен на [рис. 14](#).

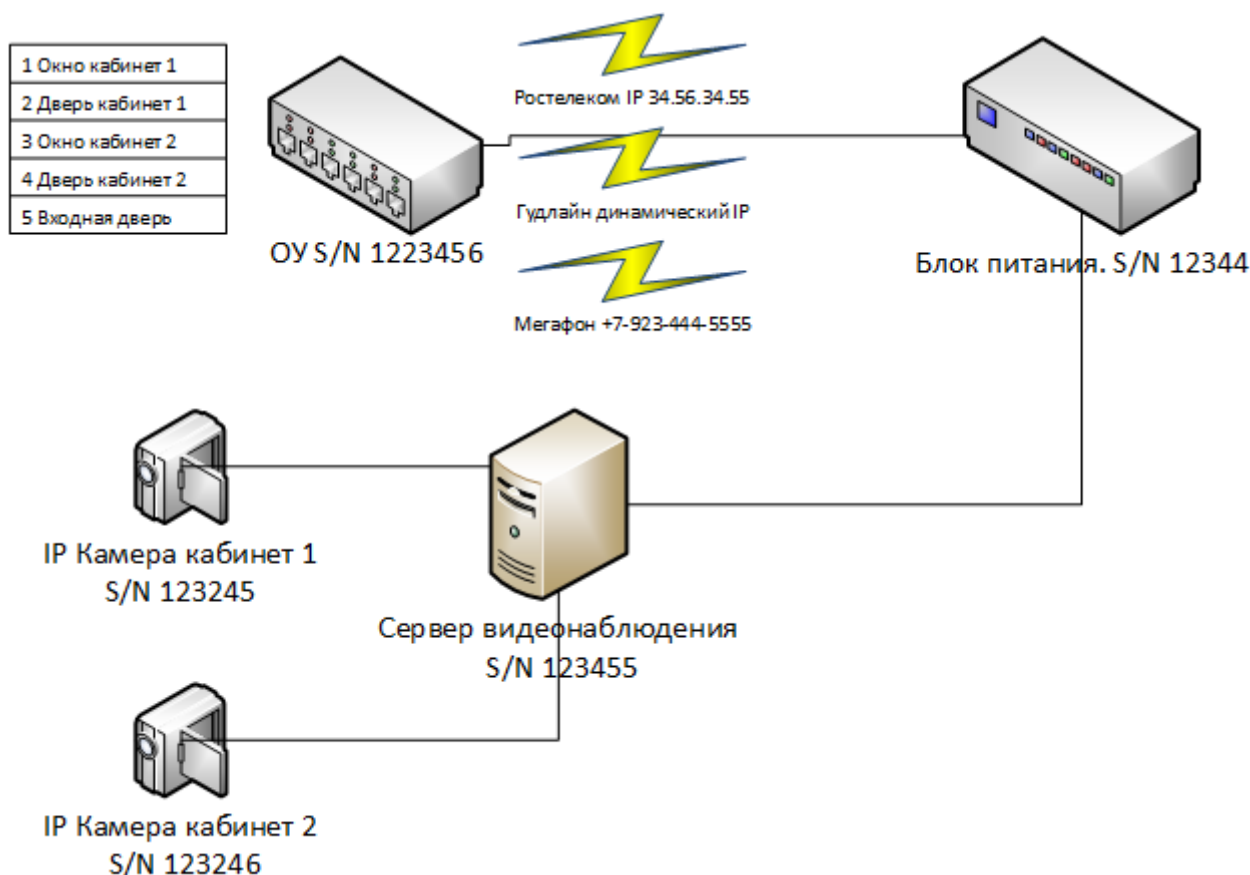


Рис. 14. Пример схемы подключения устройств.

#### 10.4.4 Списки доступа

В списке доступа редактируются пользователи и группы людей, имеющие доступ к охраняемому объекту. Для каждой группы задается PIN-код или регистрируется контактный/бесконтактный ключ доступа.

#### 10.4.5 Протоколирование изменений

Все изменения, вносимые в данные, должны протоколироваться, чтобы можно было узнать, что, когда и кто изменял. Журнал изменений сохраняется в текстовом виде.

#### 10.4.6 Интеграция с 1С

Договорной отдел обновляет поле «Выставлять счета». В 1С разрабатывается схема обработки, которая импортирует данные о клиентах и выставлении счетов из системы.

1С подключается к базе данных, списку организаций, выбирает организации с флагом «Выставлять счета» и генерирует счета автоматически.

Изменения в справочнике организаций журналируются с указанием сотрудника и временем внесения изменений.

## 11 Модуль оповещения (МО)

---

В случае тревоги на объекте, технических работ или сбоев в работе сервиса необходимо оповестить об этом клиента. Для оповещения используются все доступные способы: электронная почта, SMS и месенджер. SMS-рассылка реализуется с помощью SMS2SERVE.

Модуль оповещения клиентов располагается на отдельном сервере и поддерживает три типа рассылки сообщений:

- через шлюз по запросу программного обеспечения под паролем;
- ручная отправка сообщения администратором или диспетчером;
- групповая рассылка оповещений всем пользователям.

Модуль оповещения клиентов реплицирует данные об экстренных контактах клиентов и сотрудников один раз в несколько часов из основной базы данных кластера.

В карточку клиентов добавить IM, SMS и e-mail для экстренных уведомлений.

Прописать ниже каталог сотрудников.

## 12 Модуль связи

---

### 12.1 Голосовая связь

#### 12.1.1 Call-центр

Рабочее место каждого диспетчера оборудовано IP-телефоном, либо гарнитурой и SIP-клиентом для компьютера, и позволяет принимать звонки от клиента, звонящего на единый номер 8-800-xxxxxxx. Диспетчер может перевести звонок на другую линию или подключить к разговору другого диспетчера или инженера.

Диспетчер call-центра может принимать голосовые и видеовызовы от программы мессенджера со смартфона клиента или планшета пульта управления.

Диспетчер может сам сделать вызов клиента со своего IP-телефона. Набор номера может осуществляться из программы АРМ, двойным кликом по телефону клиента. При этом запись звонка привязывается к текущей обрабатываемой тревоге и отображается в журнале тревоги.

Входящие вызовы автоматически распределяются между свободными операторами. Все разговоры записываются и сохраняются в архив.

Call-центров может быть несколько, и они могут быть территориально распределены.

Все сервера call-центра должны быть зарезервированы так, чтобы сбой любого сервера не отражался на возможности принимать и совершать вызовы.

В качестве сервера call-центра используется свободное ПО Asterisk.

#### 12.1.2 Мобильная радиосвязь

Диспетчер имеет возможность, нажав на зарезервированную кнопку своего IP-телефона (или специальную кнопку выхода в эфир на компьютере), выйти в эфир и связаться с радиостанциями мобильных групп. Разговор при этом будет записан и привязан к обрабатываемой тревоге. Все разговоры в эфире так же пишутся и сохраняются в архив.

## 13 Мобильное приложение для смартфона

Мобильное приложение для смартфона предназначено для следующих задач:

- постановки/снятия объекта с охраны;
- отслеживания состояния объекта;
- просмотра видеоизображения с камер наблюдения. Реализуется с помощью ПО видеонаблюдения;
- голосового вызова диспетчера посредством SIP. Реализуется с помощью приложения телеконференций Protector.

### 13.1 Платформа

**Платформа:** Android, iOS.

**Язык программирования:** Java, Objective-C.

**Операционная система:** Android 4.2., iOS 6.

### 13.2 Внешний вид



Рис. 15. Примеры экранов мобильного приложения

### 13.3 Активация приложения

Для привязки экземпляра программы к конкретному объекту на смартфон системой отправляется SMS, содержащее необходимые данные. Эти данные вводятся в программное обеспечение, таким образом, производится подключение.

### 13.4 Постановка на охрану и снятие с охраны

С мобильного устройства осуществляется постановка на охрану и снятие объекта с охраны. Возможны два режима подключения смартфона к сети для постановки и снятия:

- через Интернет к одному из серверов. При этом у ОУ обязательно должно быть установлено соединение с сервером. Это предпочтительный режим работы;

- через WiFi роутер напрямую к ОУ.

Возможны два режима функционирования постановки/снятия.

- Online. Для постановки на охрану требуется соединение ОУ с сервером. Если в данный момент соединение с сервером отсутствует, то поставить на охрану не удастся. Снятие с охраны не требует соединения с сервером. Однако разрыв связи во время охраны приведет к тревоге и выезду группы реагирования.
- Offline. Для постановки на охрану не требуется установленного соединения между ОУ и сервером. Данные о постановке на охрану будут отправлены на сервер сразу после установки соединения. Снятие с охраны также не требует соединения с сервером, но разрыв связи во время охраны приведет к тревоге. В таком режиме постановки на охрану мобильное устройство должно быть подключено к локальной WiFi-сети.

## 14 Мессенджер

---

На смартфоны клиентов устанавливается программа для связи с оператором — мессенджер. Программа основывается на свободном SIP-клиенте Linphone. Внешний вид программы дорабатывается так, чтобы подходил под стиль бренда Protector. Программа должна запускаться под iOS 5.0 и выше, Android 4.2 и выше и под Windows 7 и выше. Также мессенджер может быть установлен на планшетном компьютере пульта управления.

Программа мессенджера позволяет связаться с диспетчером посредством: чата, голосового или видеовызова. Добавление дополнительных контактов, кроме предустановленных диспетчеров, запрещено.

На стороне диспетчерского пункта связь обеспечивается SIP-сервером Asterisk.

## 15 Планшетный пульт управления

---

Планшетный компьютер пульта управления устанавливается на объекте и подключается к локальной сети через WiFi маршрутизатора.

### 15.1 Платформа

**Платформа:** Linux.

**Язык программирования:** C++.

**Операционная система:** Linux.

### 15.2 Активация программы

Планшет настраивается администратором на работу с конкретным экземпляром ОУ. В память планшета прописывается открытый ключ ОУ, а в ОУ администратором прописывается открытый ключ планшета. Таким образом, планшет не сможет работать у другого клиента с другим ОУ, а ОУ не будет принимать команды планшетов, чьи открытые ключи ему не известны.

На планшет при инициализации устанавливается необходимое программное обеспечение, включая: ПО стороннего видеонаблюдения, ПО телеконференций Protector и ПО пульта управления Protector.

### 15.3 Постановка на охрану и снятие с охраны

С планшета производится постановка на охрану и снятие объекта с охраны. Возможны два режима функционирования постановки/снятия.

- **Online.** Для постановки на охрану требуется соединение ОУ с сервером. Если в данный момент соединение с сервером отсутствует, то поставить на охрану не удастся. Снятие с охраны не требует соединения с сервером. Однако разрыв связи во время охраны приведет к тревоге и выезду группы реагирования.
- **Offline.** Для постановки на охрану не требуется установленного соединения между ОУ и сервером. Данные о постановке на охрану будут отправлены на сервер сразу после установки соединения. Снятие с охраны также не требует соединения с сервером, но разрыв связи во время охраны приведет к тревоге.

Режим, в котором разрешена постановка на охрану, настраивается администратором для каждого ОУ.

### 15.4 Видеонаблюдение

Планшетный компьютер может использоваться для просмотра видеосигнала с камер наблюдения посредством сторонней программы сервиса видеонаблюдения.

### 15.5 Связь с диспетчером

С планшетного компьютера имеется возможность установить текстовую и голосовую связь с диспетчером посредством SIP-программы, доработанного клиента Linphone.



## 16 Протоколы обмена

В качестве протокола обмена сообщениями будет выступать OpenDMTP via SSH2. Протокол OpenDMTP определяет формат сообщений и набор пакетов, которыми обмениваются сервер и ОУ, а протокол SSH2 обеспечивает безопасное установление соединения с возможностью шифрования сообщений. Иными словами SSH2 выступает безопасным туннелем для обмена сообщениями по протоколу OpenDMTP.

Протоколы, описанные ниже, являются примерными, при реализации по необходимости могут дорабатываться и дополняться разработчиком.

### 16.1 Протокол OpenDMTP

Основные характеристики протокола OpenDMTP:

- минимизация объёма передаваемых по сети данных;
- возможность как менять, так и расширять список передаваемых данных без потери эффективности;
- возможность определения новых типов пакетов помимо тех, что уже описаны в протоколе.

#### 16.1.1 Формат сообщений

Каждое сообщение (пакет) представляет собой двоичный набор данных следующего формата:

| Байт: Длина | Описание                          |
|-------------|-----------------------------------|
| 0:1         | Заголовок пакета                  |
| 1:1         | Тип пакета                        |
| 2:1         | Длина полезной нагрузки           |
| 3:X         | Полезная нагрузка размером X байт |

#### 16.1.2 Пример пакета

К примеру, шестнадцатеричное представление пакета с уникальным идентификатором ОУ может выглядеть следующим образом:

0xE013084F70656E444D5450

Где:

- E0 — заголовок пакета;4
- 13 — тип пакета (пакет с идентификатором ОУ);
- 084F70656E444D5450 — 16-тиричное представление уникального идентификатора ОУ.

Данный формат сообщений должен соблюдаться при посылке сообщений как клиентом серверу, так и в обратную сторону.

### 16.1.3 Двусторонняя связь

Протокол OpenDMTP при наличии установленного TCP-подключения принимает и отправляет команды во время сеанса связи. Таким образом, достигается двусторонняя связь.

## 16.2 Протокол обмена сообщениями между ОУ и сервером

Набор параметров ОУ определяет его поведение. Некоторые параметры ОУ доступны только для чтения. Например, уникальный идентификатор ОУ не может быть перезаписан в ходе сеанса связи с сервером.

Вместе с тем существуют параметры, доступные для записи, которые могут быть изменены в ходе сеанса связи с сервером. ОУ считывает новое значение параметра из пакета специального типа. Иначе процесс задания параметра ОУ можно назвать посылкой команды сервером. Например, закрытие двери в помещении может быть осуществлено через посылку специального пакета сервером, который задаёт новое значение для исполнительного устройства «Состояние двери».

### 16.2.1 Процесс установления двусторонней связи

- Подключение инициируется только ОУ, т.е. ОУ посылает первый пакет для установления связи с сервером.
- В процессе установления подключения ОУ сначала идентифицирует сервер по его открытому ключу. Если идентификация проваливается, то ОУ пытается подключиться к следующему серверу из списка.
- После успешной идентификации сервера уже сервер начинает проводить идентификацию ОУ. Если идентификация проваливается, то сервер отвергает подключение. При этом ОУ будет пытаться подключиться к следующему серверу из списка. Если ни один из серверов не принимает подключение от ОУ, то ОУ через заданный период времени снова начинает пытаться подключиться к серверам из списка.
- После успешной идентификации между ОУ и сервером устанавливается безопасное соединение с шифрованием передаваемых данных. Это достигается возможностями протокола SSH2.

Далее начинается двусторонний обмен сообщениями по протоколу OpenDMTP.

Обычно данный обмен начинается с посылки ОУ на сервер новых данных о состоянии датчиков.

### 16.2.2 Основные типы параметров задаваемых на ОУ

- Интервал посылки данных.
- Состояние датчика X, подключенного к ОУ.
- Настройки сетевого подключения.
- Автоматическое обновление ПО, адрес сервера обновлений.
- Список открытых ключей планшетов и мобильных устройств. Только планшеты и мобильные устройства из этого списка смогут подключаться к данному ОУ и посылать на него команды постановки и снятия с охраны.

- Список зон. Каждая зона представляет собой набор идентификаторов датчиков, подключенных к ОУ. Зона определяет логический объект, который можно поставить или снять с охраны.
- Список PIN-кодов. Каждый PIN-код может соответствовать определённому пользователю или группе пользователей, имеющих право поставить или снять объект с охраны.
- Режим функционирования ОУ при снятии или постановке на охрану. Это одно из двух значений: online или offline.

### 16.2.3 Основные типы пакетов, передаваемых с ОУ на сервер

- Уникальный идентификатор ОУ.
- Данные с информацией о состоянии датчиков. Обычно такие данные посылаются через заданный интервал времени. Внеочередная посылка данных может быть связана с возникновением тревожного события, о котором следует оповестить немедленно.
- Конец передачи всех блоков данных. Больше данные передаваться не будут до следующего сеанса передачи.
- Конец передачи одного блока данных. Сеанс передачи ещё не закончен. Данный тип пакета нужен для того, чтобы сервер мог приостановить или прервать передачу данных. Например, сервер в этот момент может заново запросить у ОУ данные, которые были переданы с ошибкой.
- Значение запрошенного сервером параметра ОУ. Сервер может, например, запросить текущий список зон и их соответствие PIN-кодам, либо значение состояния какого-либо сенсора.
- Диагностический код, необходим только для этапа отладки и настройки оборудования.
- Код ошибки. Коды ошибок обычно сигнализируют о наличии технических проблем.
- Запрос времени.

### 16.2.4 Основные типы пакетов, передаваемых с сервера на ОУ

- Подтверждение получения сообщения.
- Запрос текущего значения заданного параметра ОУ.
- Задание нового значения параметра ОУ. Под заданием нового значения подразумевается и удалённое управление исполнительными устройствами, подключенными к ОУ.
- Пакет с новым списком открытых ключей планшетов и мобильных устройств. ОУ обязано полностью заменить свой старый список открытых ключей на новый.
- Пакет с новым списком зон. ОУ обязано полностью заменить старый список зон на новый.
- Пакет со списком PIN-кодов и их соответствие пользователям и группам. ОУ обязано полностью заменить старый список PIN-кодов на новый.
- Код ошибки.
- Конец передачи данных (будет закрыто соединение).
- Приостановить передачу блоков данных.
- Продолжить передачу блоков данных.

- Передача времени.

### 16.3 Протокол обмена между серверами

Каждый сервер при старте пытается установить соединение со всеми другими серверами. При ошибке соединения будут делаться бесконечное количество попыток с заданным таймаутом до успешного соединения. При разрыве соединения или, если удаленный сервер перестает отвечать на запросы и команды, делается повторное переподключение. Между двумя серверами устанавливается одно соединение. Допустима установка второго, высокоприоритетного соединения между серверами, для передачи оперативных данных.

#### 16.3.1 Типы пакетов, передаваемых между серверами

- Запрос порции данных для репликации.
- Ответ порции данных репликации.
- Широковещательная рассылка пакета данных, полученных от ОУ.
- Каскадные запросы данных для клиента диспетчера.
- Ответы на каскадные запросы данных.

### 16.4 Протокол обмена между АРМ диспетчера и сервером

Все запросы клиента сервер может обрабатывать асинхронно. АРМ диспетчера должно нумеровать запросы, отправляемые серверу. Сервер может изменять порядок ответа на запросы. Так, некоторые запросы могут требовать перенаправления к другим серверам и потому могут быть достаточно длительными.

#### 16.4.1 Типы пакетов, передаваемых между АРМ диспетчера и сервером

- Запрос ленты событий за период.
- Запрос полного журнала событий по определенному устройству за период.
- Обновление ленты событий.
- Захват тревоги в работу.
- Добавление сообщений в журнал тревоги.
- Чтение событий журнала тревоги.
- Чтение топологии устройств на точке.
- Чтение текущего состояния датчиков устройств.
- Чтение текущего статуса устройств.
- Запрос журнала состояния датчиков устройств за период.
- Запрос журнала постановок на охрану и снятия с охраны.
- Передача команды на ОУ.

## 16.5 Протокол обмена между пультом управления и ОУ

### 16.5.1 Параметры ОУ

- Список зон, доступных для постановки на охрану.
- Состояние шлейфов. Параметр только для чтения. Если какой-либо шлейф находится в тревожном состоянии, то постановка зоны на охрану невозможна.
- Состояние ОУ. Задаваемый параметр. Описание см. в [пункте 6.9](#).

### 16.5.2 Типы пакетов, передаваемых с ОУ на планшет

- Список шлейфов с состояниями.
- Текущее состояние ОУ.
- Подтверждение успеха или ошибки постановки/снятия зона на охрану.
- Подтверждение успеха или ошибки смены PIN-кода.

### 16.5.3 Основные типы пакетов, передаваемых с планшета на ОУ

- Запрос состояний зон и шлейфов.
- Задание нового состояния ОУ. Посылается при попытке поставить или снять ОУ с охраны.
- Запрос на смену PIN-кода. В данном запросе должен содержаться старый, ещё действующий PIN-код, а также значение нового PIN-кода.

## 16.6 Протокол обмена между мобильным приложением и ОУ

Протокол в большинстве команд повторяет протокол обмена между планшетом и ОУ.

## 16.7 Протокол обмена между мобильным приложением и сервером

Протокол в большинстве команд повторяет протокол обмена между планшетом и ОУ.