Рупор.БЛИЦ

Программный комплекс автоматического оповещения и анкетирования

STC-S9520

Руководство администратора

НЦДА.00737-01 91

ЦРТ инновации

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Общие положения

Данное руководство предназначено для администраторов программного комплекса автоматического оповещения и анкетирования **Рупор.БЛИЦ** STC-S9520 (далее – комплекс оповещения, комплекс **Рупор.БЛИЦ**), осуществляющих первоначальную настройку комплекса и его администрирование.

Предприятие-изготовитель оставляет за собой право без дополнительного уведомления вносить в данный документ изменения, связанные с улучшением комплекса. Внесенные изменения будут опубликованы в новой редакции документа и на сайте компании: http://www.speechpro.ru.

Соглашения и обозначения

В руководстве приняты следующие типографские соглашения:

Формат	Значение
Обычный	Основной текст документа.
Курсив	Применяется для выделения первого появления *термина*, значение которого поясняется здесь же или даётся в приложении. Также применяется для привлечения *внимания* и оформления *примечаний*.
Полужирный	Применяется для написания наименований **программных компонентов** и наименований **управляющих** и **информационных элементов** интерфейса (**заголовки**, **кнопки** и т.п.).
Полужирный курсив	Применяется для написания ***имён файлов*** и ***путей доступа*** к ним.

Словосочетание «выбрать, выделить, нажать объект (или нажать на объект)» означает: «навести указатель манипулятора типа «мышь» на объект, и нажать кнопку манипулятора».

Выбор меню, который показан при помощи стрелки **>**, например, текст **Файл > Выход**, должен пониматься так: выбрать меню **Файл**, затем команду **Выход** из меню **Файл**.

Ниже приведены примеры оформления материала руководства, указывающие на важность сведений.

Указания на другие документы в основном тексте.

Примечания; важные сведения; указания на действия, которые необходимо выполнить в обязательном порядке.

Требования, несоблюдение которых может привести к некорректной работе, повреждению или выходу из строя изделий или программного обеспечения.

Товарные знаки

Наименование «Рупор.БЛИЦ» является товарным знаком общества с ограниченной ответственностью «ЦРТ-инновации».

Все остальные названия компаний и названия продуктов, упомянутые в документе, являются собственностью их соответствующих владельцев.

Термины и определения

Абонент сети связи – физическое или юридическое лицо, имеющее договорные отношения с оператором связи на получение услуг определённого вида связи.

Администратор комплекса оповещения – должностное лицо организации, специалист по настройке и обслуживанию комплекса, отвечающий за его работу в штатном режиме и имеющий полные права доступа ко всем функциям комплекса.

Оператор комплекса оповещения – должностное лицо организации, функцией которого является управление процессом оповещения абонентов.

Оповещение – процесс уведомления абонентов по правилам, установленным в сценарии.

Пользователь комплекса оповещения – администратор или оператор комплекса **Рупор.БЛИЦ**.

Ситуация – заранее подготовленный набор правил оповещения, включающий отдельных абонентов и группы абонентов, оповещаемых по определённым сценариям определёнными сообщениями.

Сообщение голосовое – информация, которая должна быть передана абонентам сети связи по телефону.

Сообщение текстовое – информация, которая должна быть передана абонентам сети связи в текстовой форме (SMS, Email).

Сценарий – набор параметров, устанавливающих правила выполнения оповещения.

Файл оповещения – файл в формате CSV, который создаётся сотрудником, осуществляющим интеграцию комплекса **Рупор.БЛИЦ** со сторонней системой, и содержит данные абонентов для оповещения, тексты сообщений, название сценария, дату и время начала оповещения.

VitalVoice – продукт, созданный на основе технологии синтеза русской речи, разработанной в компании «ЦРТ-инновации».

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Сведения о программном обеспечении и его изготовителе

Наименование: Программный комплекс автоматического оповещения и анкетирования **Рупор.БЛИЦ** STC-S9520
Обозначение: НЦДА.00737-01
Изготовитель: Общество с ограниченной ответственностью «ЦРТ-инновации»
Адрес: 196084, г. Санкт-Петербург, ул. Красуцкого, дом 4, литера А
Телефон: (812) 325-88-48
Факс: (812) 327-92-97

1.2 Сервисное обслуживание и техническая поддержка

Если в процессе эксплуатации возникнут вопросы, обращайтесь в службу сервиса и технической поддержки предприятия-изготовителя.

Адрес службы сервисного обслуживания и технической поддержки в интернете:

Электронная почта: support@speechpro.com
Адрес в сети Интернет: http://www.speechpro.ru/support

Перед обращением в службу технической поддержки подготовьте следующую информацию:

– четкое описание возникшей проблемы;
– состав аппаратных и программных средств, используемых для оповещения;
– номера используемых версий программного обеспечения **Рупор.БЛИЦ**.

Ряд системно значимых файлов и функций комплекса защищён паролем в целях защиты от непреднамеренного изменения. Несогласованные со службой сервиса и технической поддержки предприятия-изготовителя действия, прямо не предусмотренные пользовательской документацией, в частности, сброс установленного пароля root, внесение изменений в настройки плана вызовов или работу базы данных, установка на сервер комплекса дополнительного ПО, могут привести к нарушениям в работе комплекса вплоть до полного отказа в обслуживании. В случае выявления фактов несанкционированного совершения пользователем вышеупомянутых действий, предприятие-изготовитель полностью снимает с себя ответственность за их последствия и оставляет за собой право прекратить техническую поддержку комплекса по вине пользователя.

1.3 Параметры доступа

Ниже представлены параметры доступа к комплексу **Рупор.БЛИЦ**.

Параметры доступа			
Параметр	SSH	веб-интерфейс (HTTPS)	сетевые папки
Имя пользователя	rupor_admin	admin	rupor_operator
Пароль	rupor	rupor	rupor

2 ОПИСАНИЕ КОМПЛЕКСА

2.1 Назначение комплекса

Программный комплекс автоматического оповещения и анкетирования **Рупор.БЛИЦ** STC-S9520 предназначен для:

– Совершения звонков абонентам и приема данных от IP АТС по каналам VoIP (SIP, H.323) и линиям цифрового потока E1 (при условии использования плат сопряжения с потоком E1).

– Передачи абонентам SMS-сообщений с помощью совместимого VoIP GSM-шлюза и по SMPP-протоколу.

– Отправки Email-сообщений по протоколу SMTP.

2.2 Архитектура и компоненты комплекса

Комплекс **Рупор.БЛИЦ** имеет клиент-серверную архитектуру. Общая архитектура комплекса и его взаимодействие с другими системами представлено на рисунке 1.

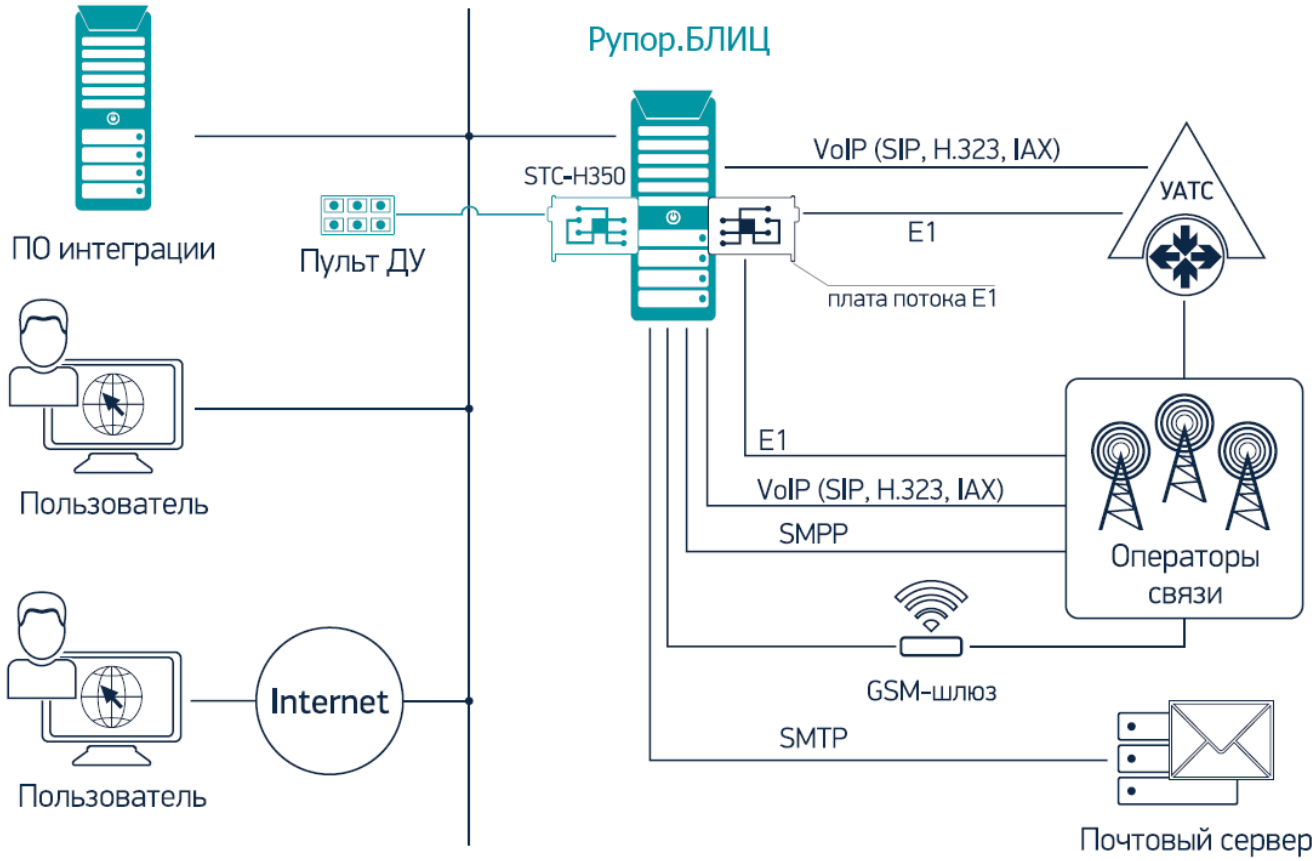

Рисунок 1 – Общая архитектура комплекса **Рупор.БЛИЦ** и его взаимодействие с другими системами

Взаимодействие основных компонентов комплекса **Рупор.БЛИЦ** между собой и с другими системами представлено на рисунке 2.

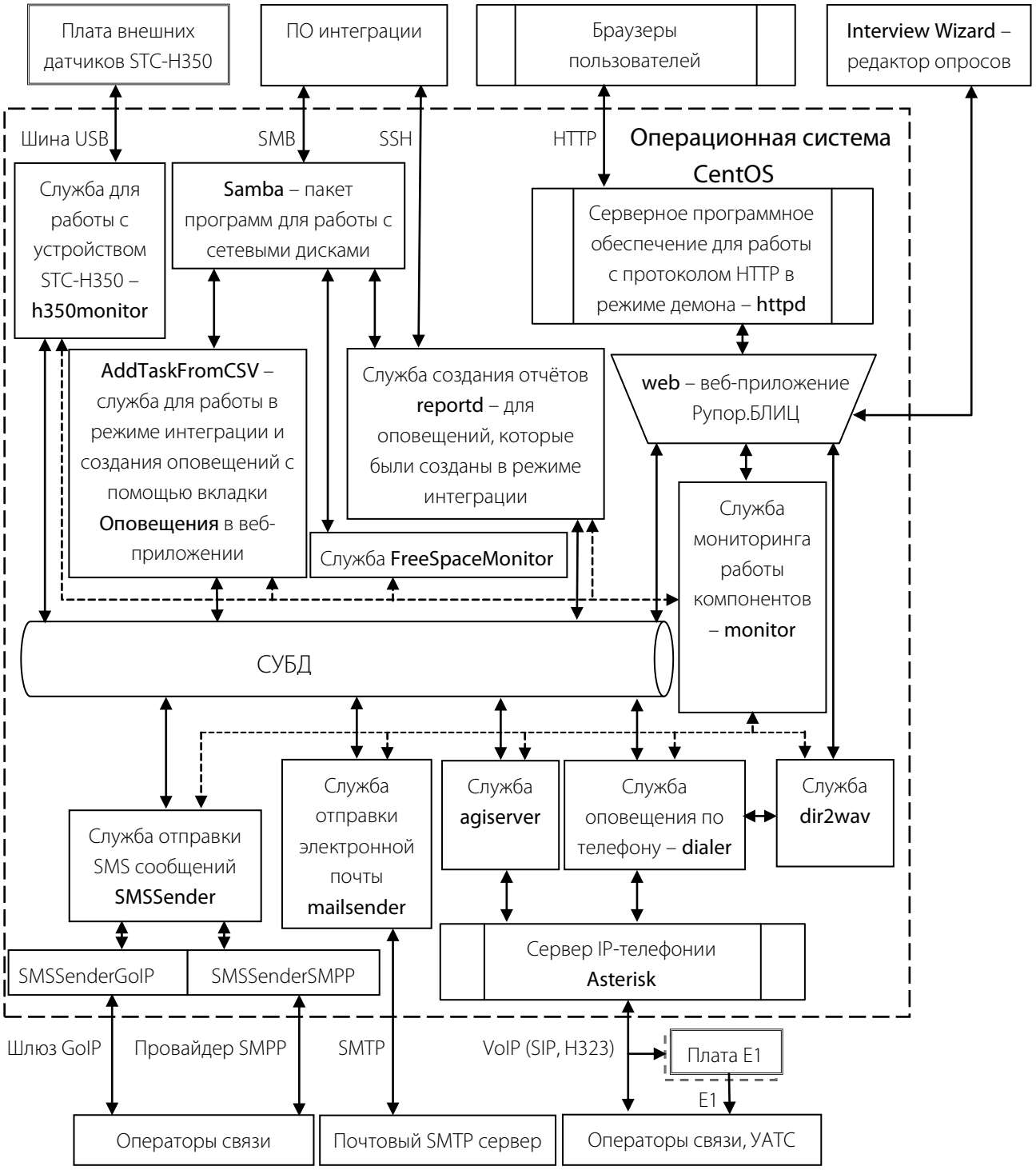

Рисунок 2 – Взаимодействие компонентов комплекса **Рупор.БЛИЦ** между собой и с другими системами

Серверная часть комплекса **Рупор.БЛИЦ** работает под управлением операционной системы **CentOS 7** и использует систему управления базами данных (СУБД) **PostgreSQL**. Все компоненты комплекса **Рупор.БЛИЦ**, размещённые на сервере, являются демонами (службами).

Комплекс **Рупор.БЛИЦ** рассчитан на использование в сетях, работающих по протоколу IP, при этом доступ пользователей к комплексу обеспечивается при помощи общедоступных веб-обозревателей (браузеров), которые являются клиентской частью комплекса.

Пользователи (администратор и операторы) взаимодействуют с комплексом через веб-приложение **Рупор.БЛИЦ** (**web**). Взаимодействие реализуется посредством серверного программного обеспечения для работы с протоколом HTTP в режиме демона (службы) – **httpd**.

Приложение **Interview Wizard** используется для составления и редактирования сценариев опроса абонентов по телефону. Приложение **Interview Wizard** работает на компьютере оператора и подключается к веб-приложению **Рупор.БЛИЦ** для публикации сценариев. Оператор создает сценарий, включающий вопросы, которые будут озвучиваться в ходе оповещения (анкетирования) абонентов, и допустимые варианты ответов, а затем публикует его на сервере.

Администратор комплекса может также инициировать оповещения на основе файлов оповещения формата CSV, созданных с помощью программного обеспечения (ПО) интеграции. Для реализации данного функционала используется следующее программное обеспечение:

а) **Samba** – пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных операционных системах по протоколу SMB/CIFS. Имеет клиентскую и серверную части.

б) **AddTaskFromCSV** – служба для работы в режиме интеграции и создания оповещений с помощью вкладки **Оповещения** в веб-приложении **Рупор.БЛИЦ**. Публикует файл со списком контактов в сетевую папку ***incoming***.

в) Служба создания отчётов **reportd** – для оповещений, которые были созданы в режиме интеграции. Получает при завершении оповещения сигнал от базы данных **PostgreSQL** и при необходимости создаёт отчёт в каталоге ***/var/rupor2/share/outgoing***, который доступен, либо через **samba** (сеть Windows), либо по протоколу **ssh** пользователю **rupor_operator**.

Запустить оповещение абонентов также можно посредством замыкания/размыкания сухого контакта платы внешних датчиков STC-H350 с помощью подключенных датчиков или кнопок. При этом используется служба **h350monitor** для работы с устройством STC-H350.

Комплекс **Рупор.БЛИЦ** оповещает абонентов с помощью голосовых сообщений по телефону и с помощью текстовых SMS и Email-сообщений.

Рассылка SMS выполняется службой отправки SMS сообщений – **SMSSender**. При этом используются подслужбы:

а) **SMSSenderGoIP** – для передачи SMS сообщений с помощью совместимого VoIP GSM-шлюза.

б) **SMSSenderSMPP** – для передачи SMS сообщений непосредственно через провайдера SMPP.

Комплекс **Рупор.БЛИЦ** интегрируется с учрежденческой АТС (УАТС) по каналам VoIP (SIP, H.323), линиям цифрового потока E1 (с использованием плат сопряжения с потоком E1). Для этого используется:

а) **Asterisk** – открытый программный сервер IP-телефонии, обеспечивающий подключение к телефонным сетям. В сервер **Asterisk** встроен компонент распознавания речи **ASR**.

б) Служба **dialer** – служба оповещения по телефону. Выбирает сценарий оповещения, передаёт в **Asterisk** команды на установление соединения с нужными телефонными номерами и сообщения.

в) Служба **agiserver** – фиксирует состояние вызова (набирается номер, вызов принят, вызов завершён), а также позволяет получать значения параметров комплекса **Рупор.БЛИЦ** в плане вызовов **Asterisk**. Читает и пишет данные из/в базу данных **PostgreSQL** и вызывается из **Asterisk**.

г) Служба **dir2wav** – отвечает за синтез сообщений. Получает от **dialer** или **web** текстовый файл и возвращает wav файл.

Служба отправки электронной почты **mailsender** обеспечивает взаимодействие комплекса **Рупор.БЛИЦ** с почтовым SMTP сервером.

Служба **monitor** осуществляет мониторинг работы компонентов комплекса **Рупор.БЛИЦ**.

Служба **FreeSpaceMonitor** осуществляет наблюдение за свободным местом на дисках и при необходимости запускает удаление старых файлов и/или оповещает администратора через режим интеграции (размещает файл с оповещением в ***/var/rupor2/share/incoming***).

2.3 Преимущества комплекса

Основными преимуществами комплекса оповещения **Рупор.БЛИЦ** являются:

– возможность удаленного инициирования, управления и мониторинга оповещения по сетям передачи данных;

– использование для оповещения различных типов голосовых сообщений (персонализированный синтез русской речи VitalVoice, аудиофайлы, запись с микрофона);

– создание сценариев опроса абонентов для проведения анкетирования в диалоговой форме;

– рассылка текстовых сообщений по SMS и Email;

– автоматический запуск оповещения после публикации CSV-файла оповещения со списком контактов, сообщений и сценариев;

– активация оповещений по телефону;

– оповещение в круглосуточном режиме с учетом часовых поясов;

– высокая скорость оповещения большого количества абонентов;

– применение нескольких каналов для передачи сообщений по телефону;

– поддержка подключения к нескольким провайдерам телефонии;

– многократное повторение голосовых сообщений по телефону с целью повышения вероятности оповещения;

– наличие условий успешного выполнения оповещения;

– получение подтверждения результатов оповещения;

– использование функции распознавания речи при подтверждении результатов оповещения и анкетировании;

– получение уведомлений о результатах оповещения;

– автоматизированное создание оповещений на основе сценариев;

– возможность создания персонального сценария для абонента;

– возможность создания персонального сообщения для абонента;

– формирование подробных отчетов о результатах оповещения с возможностью фильтрации по различным параметрам;

– экспорт в CSV-файл и вывод на печать результатов оповещения.

3 ВАРИАНТЫ ПОСТАВКИ КОМПЛЕКСА

Комплекс **Рупор.БЛИЦ** поставляется в следующих вариантах:

1. На DVD-диске совместно с операционной системой Linux CentOS 7 64 бита в качестве программного обеспечения для самостоятельной установки. Необходимые технические средства приобретаются заказчиком самостоятельно.
2. В виде программно-аппаратного комплекса на основе компьютера-сервера с предустановленным программным обеспечением **Рупор.БЛИЦ**.

Варианты поставки определяются условиями конкретного контракта (договора) на поставку.

Состав и технические характеристики программно-аппаратного комплекса **Рупор.БЛИЦ** указаны в формуляре НЦДА.465237.007ФО.

4 ТРЕБОВАНИЯ К ТЕХНИЧЕСКИМ И ПРОГРАММНЫМ СРЕДСТВАМ

4.1 Требования к техническим средствам серверного оборудования

Всё оборудование сервера должно быть совместимо с операционной системой Linux CentOS 7 или Red Hat Enterprise Linux 7. Операционная система CentOS входит в состав дистрибутива ПО **Рупор.БЛИЦ**.

Совместимость оборудования с операционной системой можно проверить на официальном ресурсе компании Red Hat:

https://access.redhat.com/ecosystem/search/#/category/Server?ecosystem=Red%20Hat%20Enterprise%20Linux,

а также на официальных сайтах производителей аппаратного обеспечения.

Ниже приведены рекомендуемые аппаратные требования к серверу комплекса в зависимости от количества каналов оповещения.

№ п/п	Условия использования	Характеристики сервера
1	До 60 каналов без распознавания; до 30 каналов с распознаванием	Процессор i3, i5 (4 ядра); оперативная память 12 ГБ
2	До 120 каналов без распознавания; 40-60 каналов с распознаванием	Процессор i5, i7 (6 ядер); оперативная память 18 ГБ
3	До 300-400 каналов без распознавания (в зависимости от количества ядер); до 120 каналов с распознаванием	Процессор i7, Xeon (8 и более ядер), оперативная память 24 ГБ

Минимальное количество выделяемой системе оперативной памяти должно быть не менее 2 ГБ на каждое физическое или виртуальное ядро процессора. Рекомендуемое значение: не менее 3ГБ на каждое физическое или виртуальное ядро процессора.

Минимальный объём свободного дискового пространства для установки комплекса на сервере составляет 35 ГБ.

При планировании ресурсов для развёртывания на компьютерах/физических или виртуальных серверах с процессорами с поддержкой многопоточной обработки (Hyper-threading) необходимо учитывать следующие особенности:

1. Рекомендуемые аппаратные требования приведены с расчётом на монопольное использование всех аппаратных ресурсов физической машины;

2. Операционная система считает доступное количество потоков обработки (threads) ядрами и исходя из этого потребляет оперативную память. Это следует учитывать при выделении системе оперативной памяти. К примеру, для процессора Intel с поддержкой Hyper-threading (2 ядра, 4 потока) минимальное количество оперативной памяти должно быть не менее 8 Гб, а рекомендованное не менее 12 Гб.

3. При развёртывании в виртуальных средах ядра виртуального процессора (vCPU) не эквивалентны ядрам физического процессора (CPU) в силу особенностей технологии,

подразумевающей динамическое выделение ресурсов. Поэтому при выделении виртуальных ядер следует считать их количество как удвоенное число требуемых физических ядер.

Для использования функции записи сеансов оповещений/анкетирования на этапе выбора аппаратного обеспечения и конфигурирования необходимо предусмотреть дополнительный запас дискового пространства, вычисляемый исходя из прогнозируемых объёмов записи и требуемого срока их хранения. Для непрерывной записи оповещений длительностью 1 час по 1 каналу необходимо 58 Мбайт дискового пространства. В этом случае минимальный объём свободного дискового пространства определяется по формуле:

V*N*t*1,13,

где V – объём хранения в единицу времени,

t – прогнозируемое время оповещения/анкетирования,

N – количество каналов оповещения/анкетирования,

1,13 – коэффициент, учитывающий потребности системы для дефрагментации диска.

Рассылка SMS-сообщений может осуществляться с помощью совместимого VoIP GSM-шлюза.

4.2 Требования к техническим средствам клиентского оборудования

Для работы с веб-приложением **Рупор.БЛИЦ** рабочее место пользователя должно быть оборудовано персональным компьютером с сетевой платой со скоростью передачи данных не менее 100 Мбит/с.

Также возможно использование любых коммуникационных устройств (ноутбук, коммуникатор и т.д.), оснащённых браузером и подключённых к сети передачи данных.

4.3 Требования к программным средствам

Для получения исходных текстов открытых частей комплекса (CentOS и Asterisk) обратитесь на сайты разработчиков: http://www.centos.org и http://www.asterisk.org. Данные компоненты поставляются в неизмененном виде.

Комплекс **Рупор.БЛИЦ** поддерживает следующие средства виртуализации:

- VMWare ESXI 5.5 и выше;
- Oracle VM VirtualBox 4.3.4 и выше.

Для получения доступа к командной строке операционной системы сервера **Рупор.БЛИЦ** необходимо использовать любой SSH-клиент, например, **PuTTY**. Подключение следует осуществлять по порту 22.

Вход в веб-приложение **Рупор.БЛИЦ** рекомендуется выполнять при помощи одного из следующих браузеров:

- Mozilla Firefox (рекомендуемый) версии 32 и выше;
- Google Chrome версии 32 и выше.

Для записи голосовых сообщений с помощью веб-приложения **Рупор.БЛИЦ** необходимо установить программу Adobe Flash Player версии 11 и выше, если она поддерживается используемым браузером.

5 ПОРЯДОК ДЕЙСТВИЙ ПО УСТАНОВКЕ И НАСТРОЙКЕ КОМПЛЕКСА

Параметры доступа к серверу, сетевым папкам и веб-интерфейсу комплекса, установленные по умолчанию, приведены в подразделе 1.3 Параметры доступа.

При установке и настройке комплекса рекомендуется соблюдать следующий порядок действий:

Если в комплект поставки входит аппаратный HASP-ключ, вставьте его в свободный USB-порт сервера.

Если в состав комплекса входит диск с программным обеспечением, установите ПО, как это описано в разделе 6 УСТАНОВКА КОМПЛЕКСА «Рупор.БЛИЦ».

Если в состав комплекса входит компьютер-сервер с предустановленным программным обеспечением (далее – *ПО*) комплекса **Рупор.БЛИЦ**, выполните следующие действия:

- Подключите сервер к локальной сети.
- Включите сервер. После включения сервера будет автоматически произведена попытка получения IP-адреса и регистрации имени сервера в локальной сети. Имя сервера присваивается по схеме ***rupor2-MAC-адрес_первой_сетевой_карты***. Если в сети не используется DHCP, для получения IP-адреса выполните действия, описанные в пункте 10.2.2 Изменение IP-адреса сервера комплекса оповещения.
- Если в комплект поставки входит аппаратный HASP-ключ, вставьте его в свободный USB-порт сервера. Если в комплект поставки не входит аппаратный HASP-ключ, установите программный HASP-ключ, как это описано в подразделе 7.1 Установка HASP-ключа. Если установка программного ключа была выполнена заблаговременно поставщиком комплекса, пропустите данный шаг установки.

Если оповещение будет осуществляться по линиям цифрового потока E1, подключите интерфейсную плату сопряжения с потоком E1 к серверу.

Если оповещение будет осуществляться с помощью устройства STC-H350, подключите внешние датчики или кнопки дистанционного управления КК-052 к устройству STC-H350, а затем подключите устройство STC-H350 к серверу. Для инициализации устройства после подключения перезагрузите сервер комплекса.

Устройство STC-H350 не поддерживает работу по стандарту USB 3.0. Поэтому перед началом работы с устройством необходимо отключить режим USB 3.0 (xHCI) в настройках BIOS/UEFI сервера либо использовать для подключения устройства концентратор, работающий по стандарту USB 2.0.

После подключения устройства служба **h350monitor** запустится автоматически. Убедитесь, что служба запустилась, а если этого не произошло, запустите службу вручную. Для этого:

- Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
- В консоли операционной системы выполните команду ***rupor2 status h350monitor***. Если служба запущена, то ответное сообщение будет содержать строки ***enabled:1***. и ***status:running***.
- Если ответное сообщение содержит строку ***enabled:0***, включите службу с помощью команды ***rupor2 enable h350monitor***. Служба будет включена и запущена.

События от устройства STC-H350 игнорируются в течение 20 секунд после запуска службы **h350monitor**. Это значит, что в течение некоторого времени после подключения устройства или перезапуска сервера активация оповещений будет недоступна.

Создайте и настройте транки (см. разделы 9 ИНТЕГРАЦИЯ С АТС и 10.9.2 Добавление транка).

Если с помощью комплекса будет осуществляться рассылка Email-оповещений, выполните настройку комплекса **Рупор.БЛИЦ** для работы с SMTP-сервером (см. подраздел 10.3 Настройка SMTP-сервера).

Если с помощью комплекса будет осуществляться рассылка SMS-оповещений с помощью совместимого VoIP GSM-шлюза, выполните подключение и настройку шлюза согласно инструкции, представленной в разделе 8 ПОДКЛЮЧЕНИЕ И НАСТРОЙКА GSM-ШЛЮЗА. Затем выполните настройку транков, как это указано в пункте 10.9.4 Настройка транков для отправки SMS.

Если с помощью комплекса будет осуществляться рассылка SMS-оповещений по SMPP, выполните настройку транков, как это указано в пункте 10.9.4 Настройка транков для отправки SMS.

Проверьте доступность веб-интерфейса комплекса. Для этого на любом компьютере в той же локальной сети введите в адресной строке браузера ***https://IP-адрес_сервера***. Для авторизации в веб-приложении используйте данные встроенной учетной записи администратора, которые приведены в подразделе 1.3 Параметры доступа.

Проверьте доступность сетевых папок файловой системы **Рупор.БЛИЦ**. Для этого на любом компьютере в той же локальной сети в проводнике введите ***\\IP-адрес_сервера\incoming*** и ***\\IP-адрес_сервера\outgoing***. Для авторизации используйте данные учетной записи, которые приведены в подразделе 1.3 Параметры доступа.

Доступ к серверу возможен только с частных IP-адресов.

Сетевая папка ***outgoing*** содержит каталог ***backup***. Это позволяет как создавать резервные копии конфигурации комплекса, так и восстанавливать конфигурацию из резервных копий.

Создайте оповещение одним из способов, описанных в разделе 11 СОЗДАНИЕ ОПОВЕЩЕНИЙ.

6 УСТАНОВКА КОМПЛЕКСА «РУПОР.БЛИЦ»

При установке комплекса **Рупор.БЛИЦ** с помощью DVD-диска на сервер устанавливается операционная система CentOS и программное обеспечение **Рупор.БЛИЦ**.

При установке комплекса на SATA-диски выберите в BIOS сервера режим AHCI для жёстких дисков. Обычно этот режим выбран по умолчанию.

Ручная установка рекомендуется только для опытных пользователей. При выборе некорректных значений параметров при установке работа комплекса может быть нарушена.

Для установки комплекса выполните следующие действия:

1. Подключите сервер к локальной сети.
2. Если в комплект поставки входит аппаратный HASP-ключ, вставьте его в свободный USB-порт сервера.
3. Вставьте установочный DVD-диск в оптический привод сервера и дождитесь появления меню выбора типа установки комплекса **Рупор.БЛИЦ** (рис. 3).

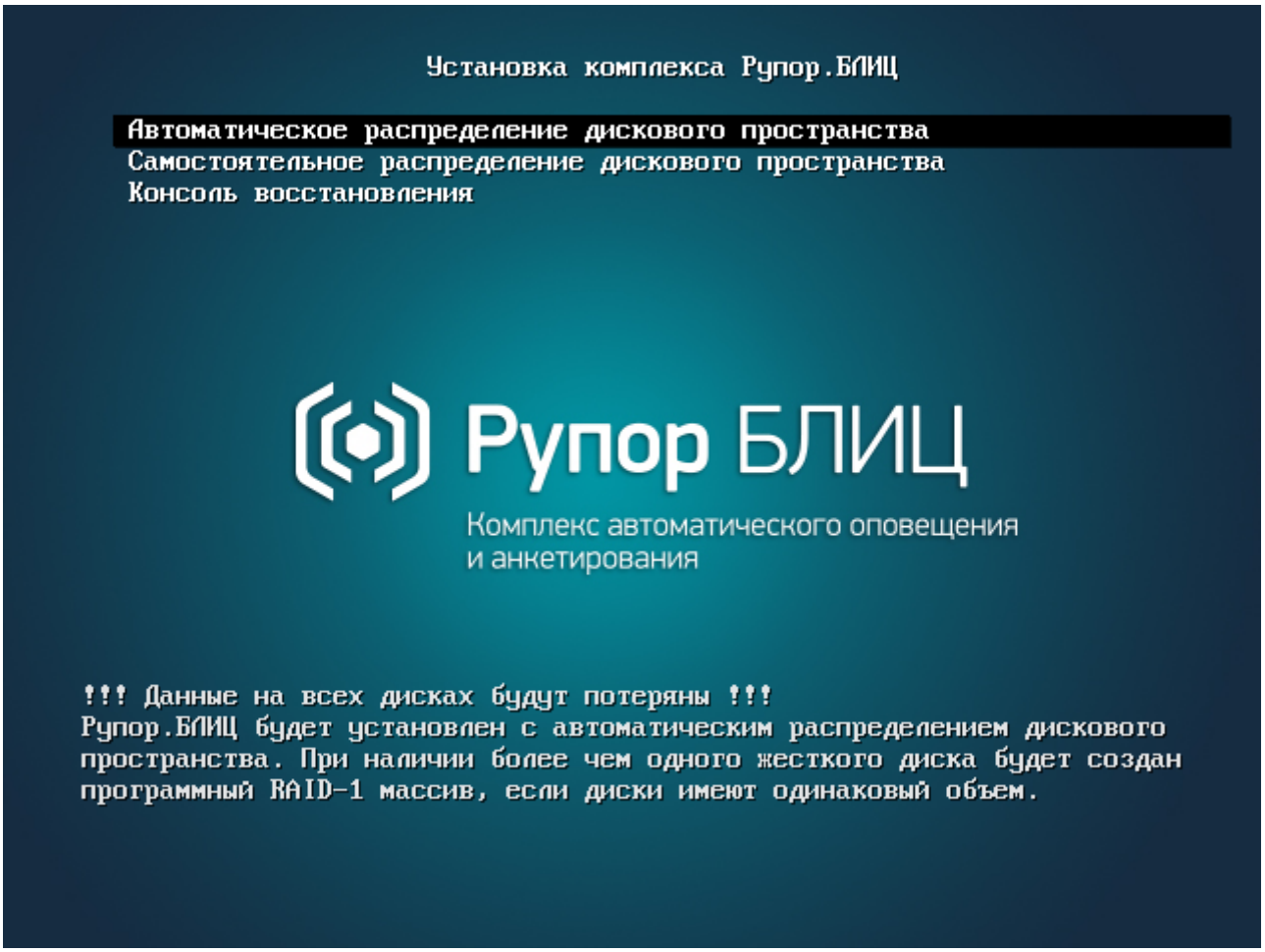

Рисунок 3 – Выбор типа установки

4. Выберите пункт **Автоматическое распределение дискового пространства** (рис. 3), если на сервере имеется один жёсткий диск, подключённый к интерфейсу SATA, или два диска одинакового размера, которые предполагается использовать в режиме зеркала. Нажмите клавишу ***Enter***. Начнётся автоматическая установка комплекса. Далее перейдите к п. 15.

   Выберите пункт **Самостоятельное распределение дискового пространства**, если:

   - на сервере имеется один диск, и требуется выполнить собственное разбиение диска на разделы (не рекомендуется);
   - на сервере имеется один диск, и установка в автоматическом режиме закончилась не успешно.

   Если на сервере имеется несколько дисков разного размера, обратитесь за консультацией по установке комплекса в отдел технической поддержки ООО «ЦРТ-инновации».

5. Для **Самостоятельного распределения дискового пространства** в окне **Обзор установки** (рис. 4) выберите пункт **Расположение установки**.

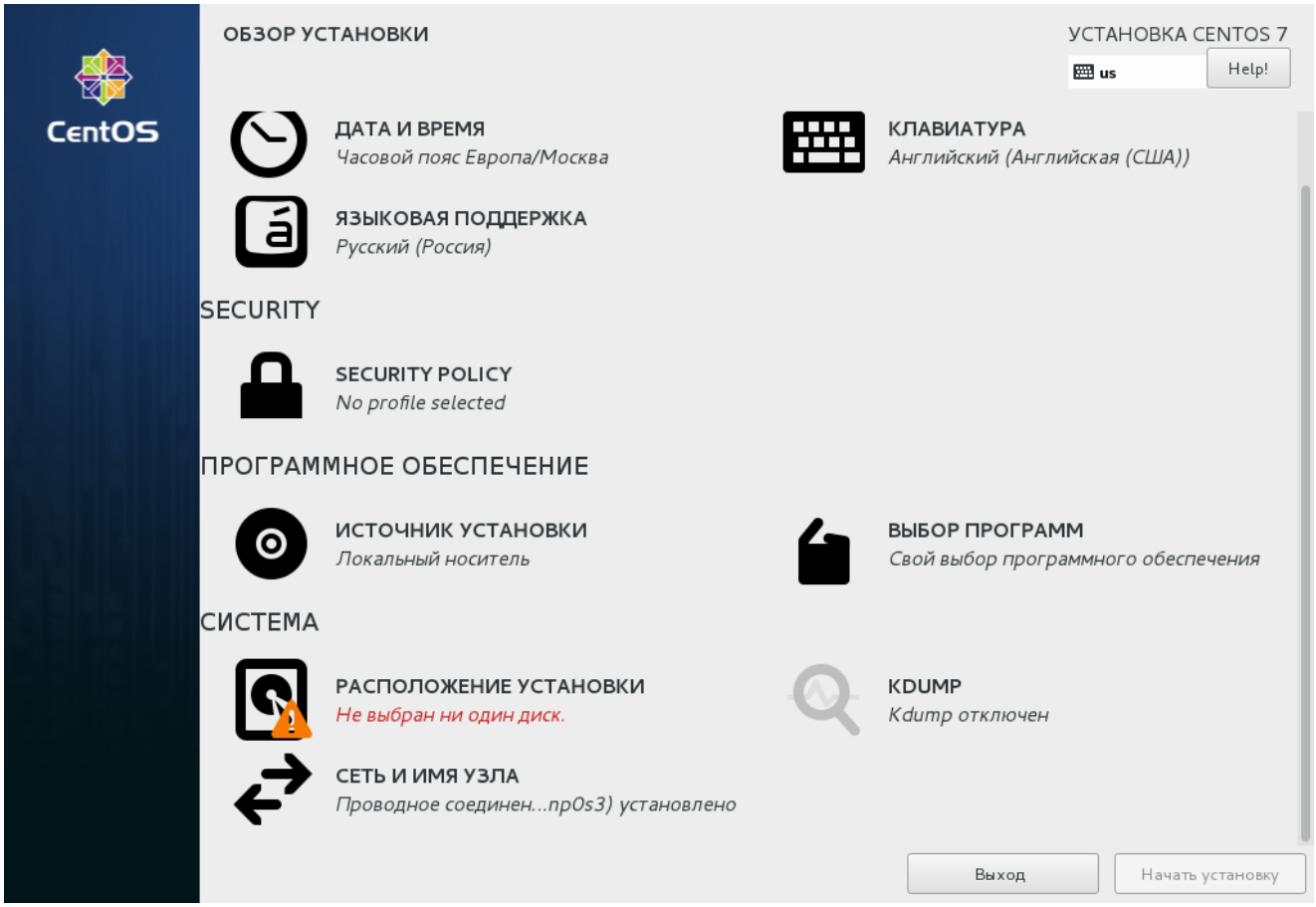

Рисунок 4 – Окно **Обзор установки**

6. В окне **Место установки** (рис. 5) выберите локальный диск и установите переключатель **Я настрою разделы**.

7. Нажмите на кнопку **Готово**.

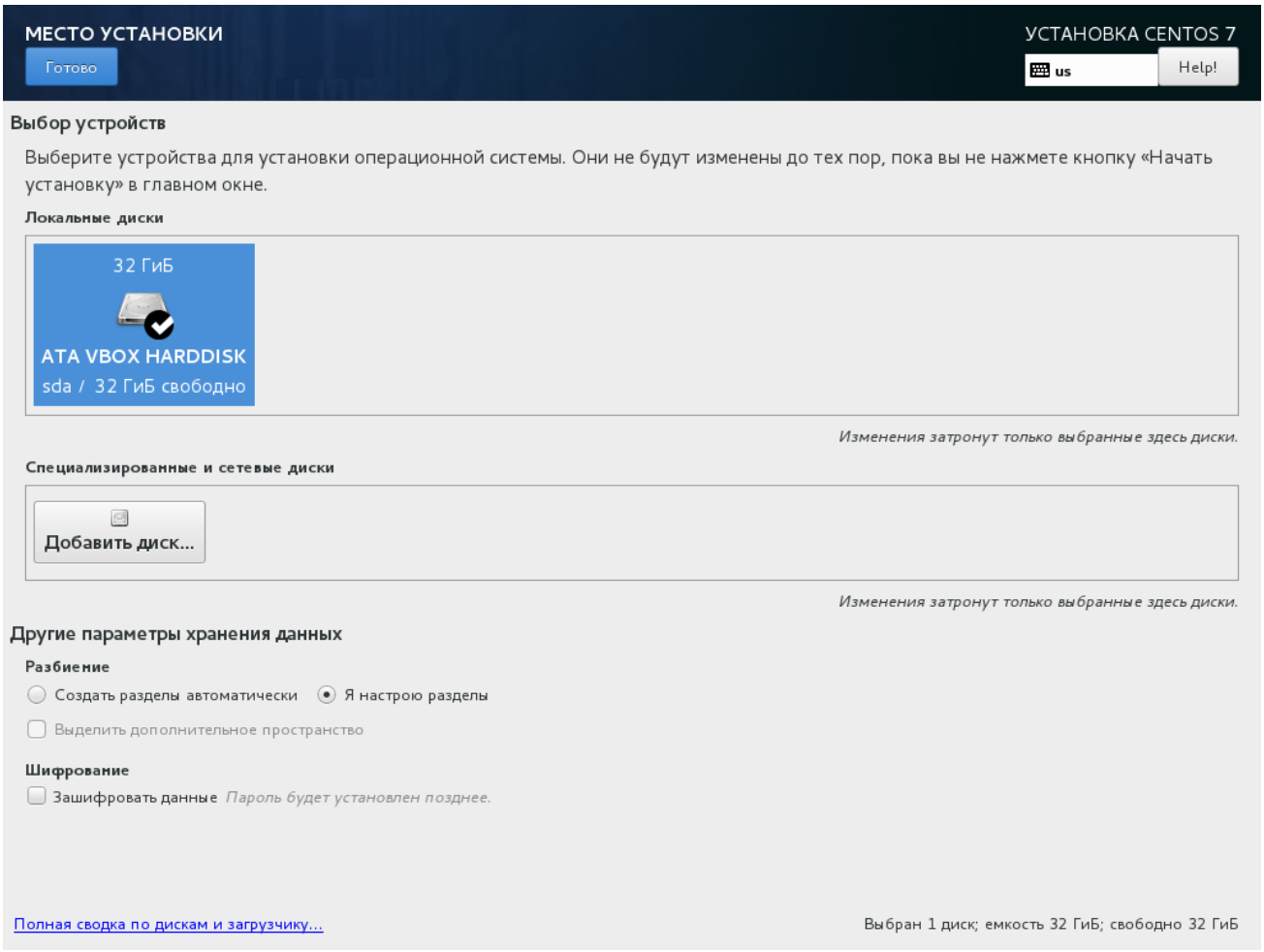

Рисунок 5 – Окно **Место установки**

8. В окне **Разметка вручную** (рис. 6) выберите **Стандартный раздел** и нажмите на кнопку **+**.

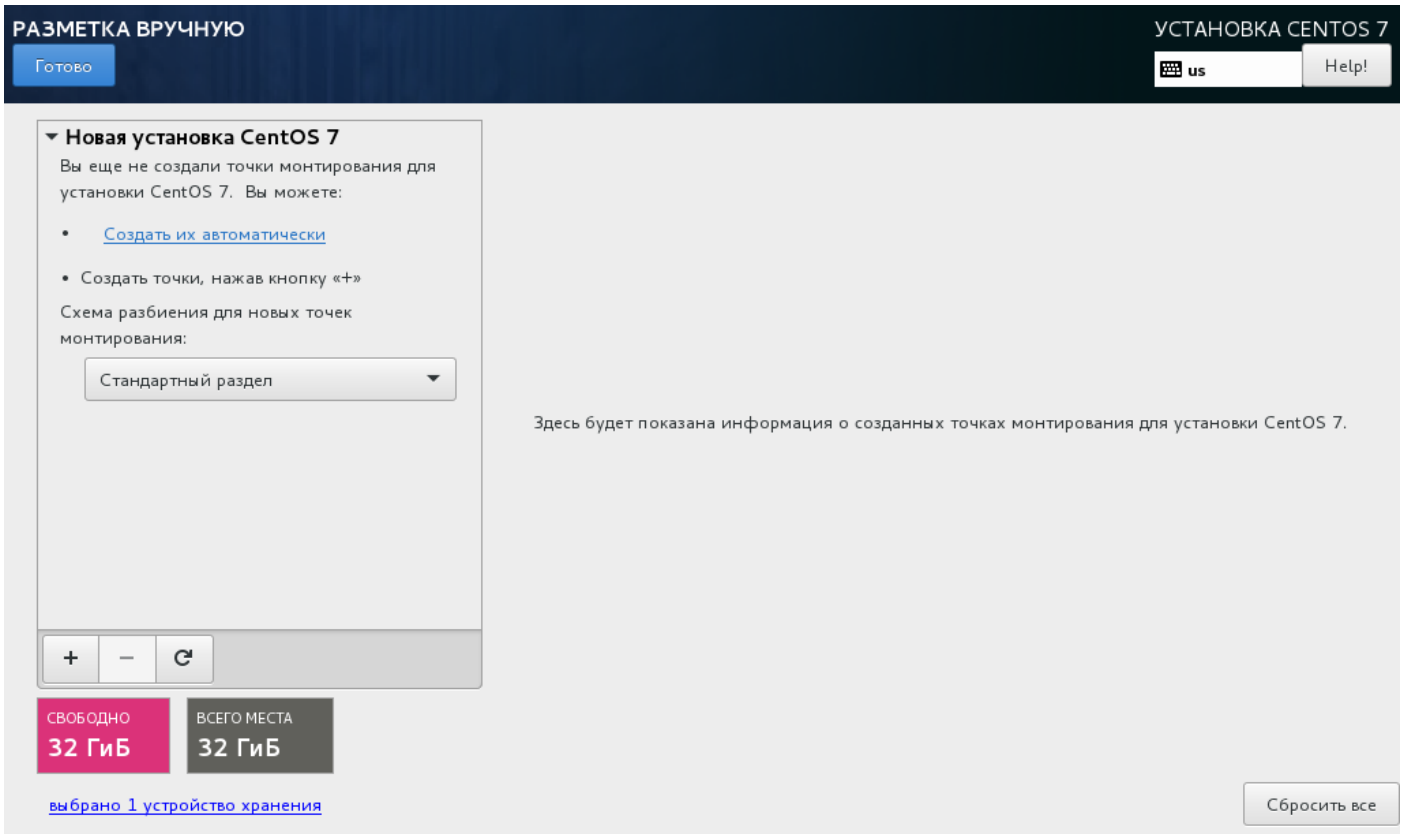

Рисунок 6 – Окно **Разметка вручную**

9. В окне **Создание точки монтирования** (рис. 7) выберите следующие параметры:
   - Точка монтирования: /
   - Размер (МБ): 10000

   Нажмите на кнопку **Добавить**.

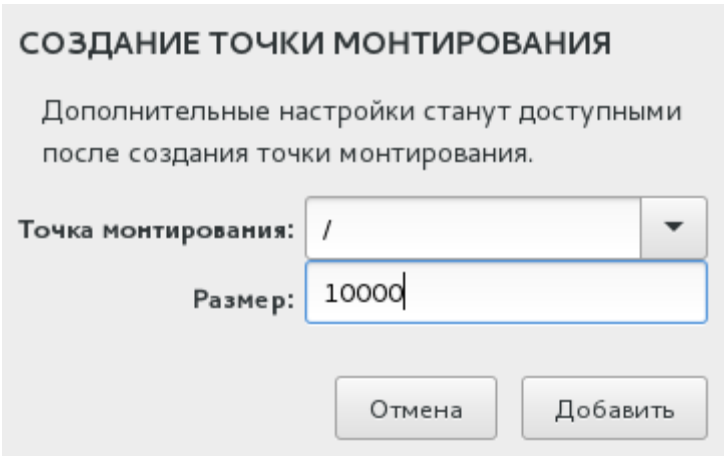

Рисунок 7 – Окно **Создание точки монтирования**

10. Далее выберите файловую систему для создаваемого раздела: ext4 (рис. 8).

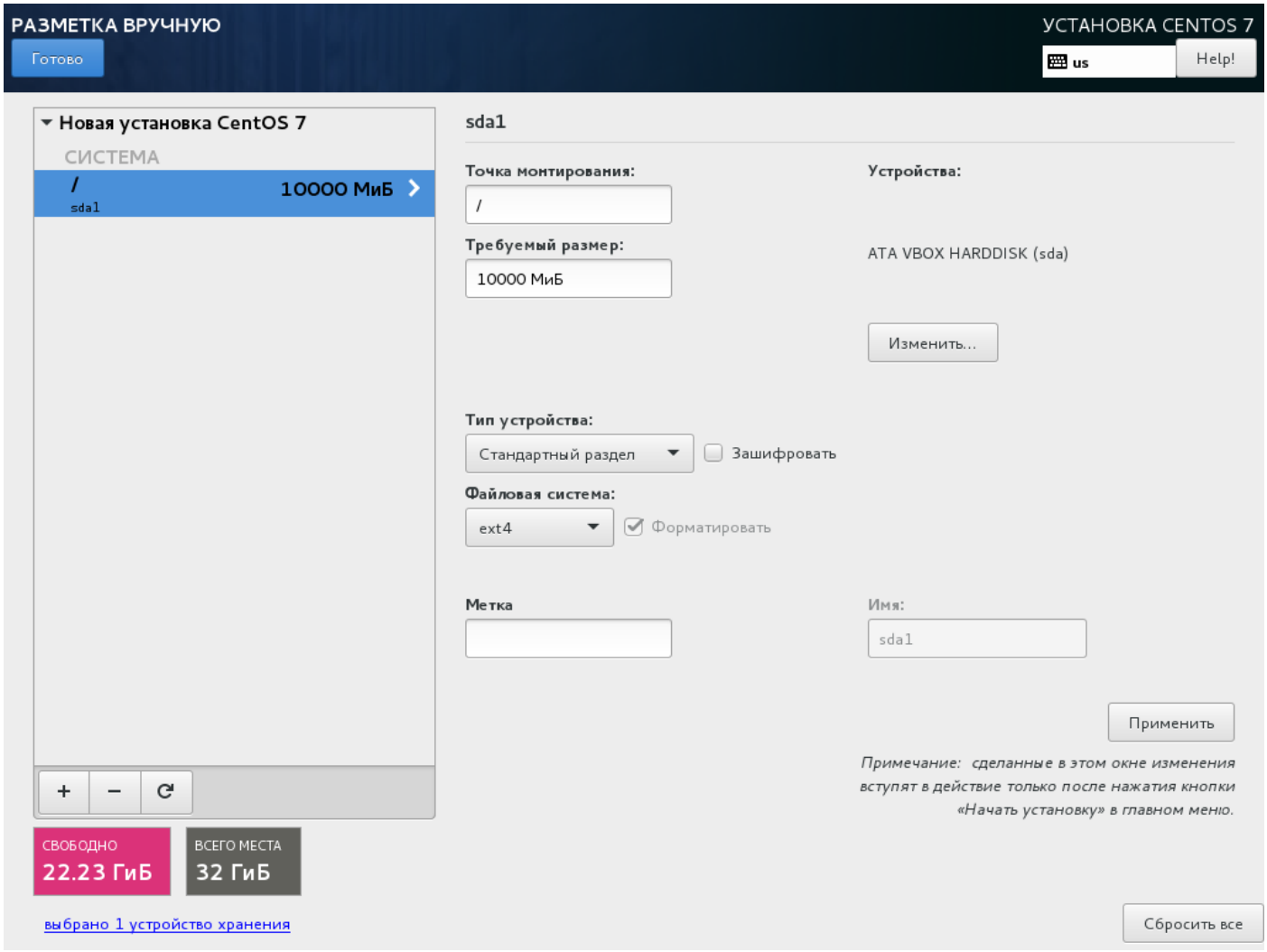

Рисунок 8 – Настройка параметров раздела

11. Аналогичным образом (п.п. 8–10) создайте раздел подкачки со следующими параметрами:
    - Точка монтирования: swap
    - Размер (МБ): выберите размер, равный количеству оперативной памяти
    - Тип ФС: swap
12. Аналогичным образом (п.п. 8–10) создайте раздел для точки монтирования ***/var*** со следующими параметрами:
    - Точка монтирования: /var
    - Размер (МБ): 400
    - Тип ФС: ext4

13. Нажмите на кнопку **Готово** (рис. 9).

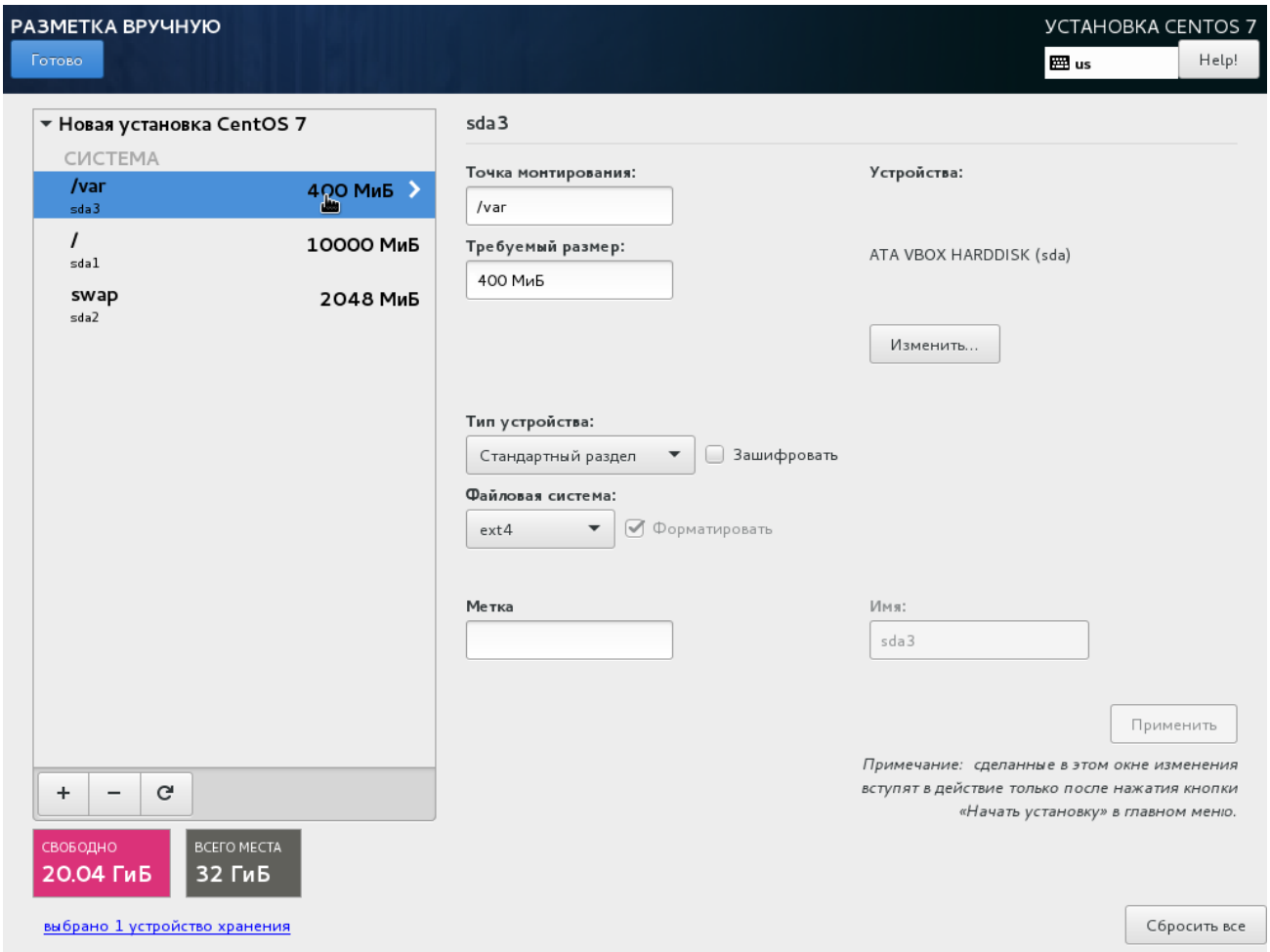

Рисунок 9 – Завершение настройки разделов

14. В окне **Обзор установки** нажмите на кнопку **Начать установку**.

    Начнётся установка комплекса (рис. 10).

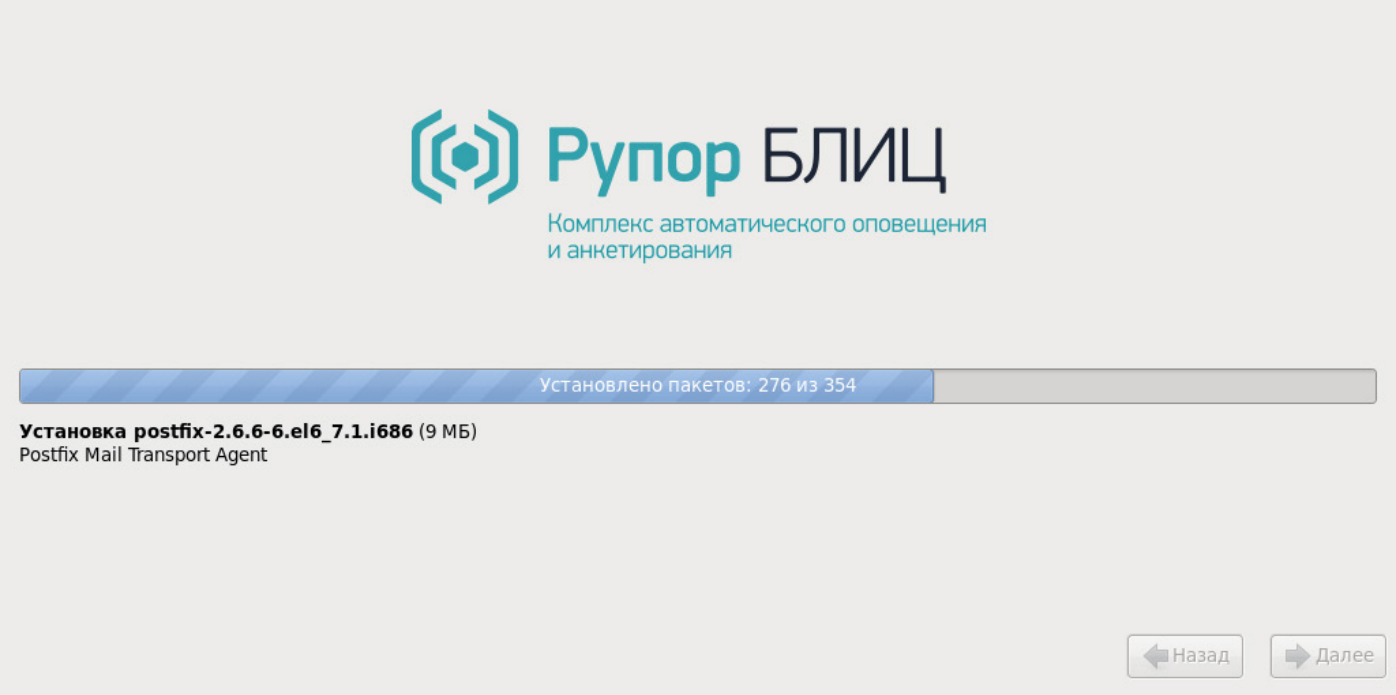

Рисунок 10 – Установка комплекса

15. По завершении установки сервер будет автоматически перезагружен. После того как начнётся перезагрузка, достаньте диск из оптического привода.

После перезагрузки сервера откроется консоль. В консоли отобразится информация о версии ПО **Рупор.БЛИЦ**, IP-адрес и имя сервера **Рупор.БЛИЦ** (рис. 11).

По умолчанию для настройки IP используется протокол DHCP, а имя сервера присваивается по схеме ***rupor2-MAC-адрес_первой_сетевой_карты***.

Если в сети не используется DHCP, для получения IP-адреса и регистрации имени сервера в локальной сети выполните действия, описанные в пунктах 10.2.2 Изменение IP-адреса сервера комплекса оповещения и 10.2.3 Изменение имени сервера комплекса «Рупор.БЛИЦ».

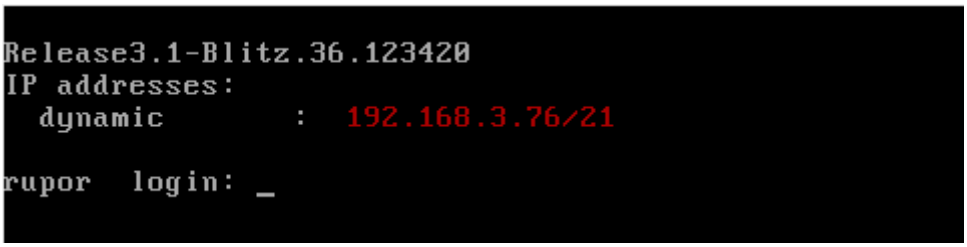

Рисунок 11 – IP-адрес и имя сервера

16. Если в комплект поставки не входит аппаратный HASP-ключ, установите программный HASP-ключ как это описано в подразделе 7.1 Установка HASP-ключа.

7 РАБОТА С HASP-КЛЮЧОМ

HASP-ключ предназначен для защиты программного обеспечения **Рупор.БЛИЦ**, которое устанавливается на компьютер-сервер. Защита программного обеспечения **Рупор.БЛИЦ** обеспечивается с помощью одного из следующих типов HASP-ключей:

- аппаратного ключа HASP HL Pro,
- программного ключа HASP SL Trial,
- постоянного программного ключа HASP SL Pro.

Ключ защиты должен быть установлен на компьютере-сервере в течение всего времени работы комплекса. Если в ходе работы HASP-ключ был случайно отсоединён, рекомендуется остановить все активные оповещения, перезагрузить сервер, а после перезагрузки снова запустить оповещения.

В памяти HASP-ключа содержится перечень и параметры лицензий, которые определяют, какие функции комплекса доступны в данном экземпляре программного обеспечения (см. также руководство по подбору оборудования и лицензий комплекса **Рупор.БЛИЦ**).

Для работы с HASP-ключом любого типа требуется следующее программное обеспечение:

- драйвер HASP-ключа,
- служба «Менеджер лицензий» («Sentinel License Manager»),
- утилита «Sentinel Admin Control Center».

Перечисленные программные компоненты входят в состав дистрибутива **Рупор.БЛИЦ** и устанавливаются на сервер при установке программного обеспечения комплекса.

Стандартным для поставки в составе комплекса является аппаратный ключ HASP HL Pro, устанавливаемый непосредственно в USB-порт аппаратного сервера комплекса. Использование других типов ключей защиты допускается только по согласованию со службой технической поддержки ООО «ЦРТ-инновации» и с учётом потенциально возможных рисков. ООО «ЦРТ-инновации» не несёт ответственности за негативные последствия рисковых событий и в рамках стандартной технической поддержки не оказывает услуг по восстановлению работоспособности комплекса, если иное не предусмотрено действующими договорами на оказание услуг технической поддержки и/или технического сопровождения.

Особенности внедрения комплекса **Рупор.БЛИЦ** с учётом специфики применяемых способов защиты ПО и описание рисковых событий приведены в приложении С.

7.1 Установка HASP-ключа

Чтобы обеспечить работу аппаратного HASP-ключа, достаточно вставить его в свободный USB-порт сервера, на котором установлено ПО комплекса.

При установке ПО комплекса на виртуальную машину необходимо путём настройки обеспечить доступность соответствующего USB-порта и установленного в него аппаратного ключа защиты HASP HL Pro. Также в случае использования многосерверной конфигурации необходимо запретить

миграцию виртуальной машины с комплексом на другие физические сервера, т.к. это может привести к потере связи с ключом защиты и прекращению работоспособности комплекса.

Чтобы установить программный ключ HASP SL Trial, который будет обеспечивать работу четырёх каналов в течение двух недель, в консоли сервера следует выполнить команду **install_demo_key**. Чтобы продолжить работу с комплексом после завершения демонстрационного периода, следует приобрести ключ защиты постоянного действия с требуемым набором функциональных лицензий.

Чтобы установить постоянный программный ключ HASP SL Pro, выполните следующие действия:

1. Если в системе был ранее установлен другой программный ключ, в т.ч. демонстрационный, удалите его путём ввода команды:

```
remove_software_keys
```

2. В консоли сервера выполните команду:

```
HaspTool
```

3. Дождитесь появления следующего сообщения:

```
Please, press i-hasp information, f-save fingerprint info, c-save c2v file,
u-update v2c file, e-exit.
```

Нажмите на клавиатуре клавишу **f**, а затем клавишу **Enter**, чтобы сохранить слепок состояния компьютера.

4. Дождитесь отображения в консоли следующей информации:

```
Getting FingerPrint Info:Operation completed successfully

<?xml version="1.0" encoding="UTF-8" ?>

<hasp_info>

<host_fingerprint                                                type="SL-AdminMode"
crc="3436052761">MXhJSSOVlUqQwt+KAxiGVZVK0EAGsgTGCQC6S9AgVQMC1GIqFAbQIJUVO8BgQ
pgxKCKVlUqiqh29pmoakZVK0MoLkl8gAC+AStAgzy5ac0oHT3fQIJUbC4PEmsPRiCCVlXr2bt0XBwW
7</host_fingerprint>

</hasp_info>

Please enter c2v file name:
```

Введите имя для сгенерированного слепка состояния компьютера. Имя должно быть введено в формате **имя_файла.c2v**. Например: **123.c2v**.

Слепок состояния компьютера будет сохранен в виде файла с расширением c2v.

5. Дождитесь отображения в консоли следующей информации:

```
FingerPrint information stored into file: 123.c2v

Please, press i-hasp information, f-save fingerprint info, c-save c2v file,
u-update v2c file, e-exit.
```

6. Нажмите на клавиатуре клавишу **e**, а затем клавишу **Enter**.

7. Отправьте созданный c2v-файл в техническую поддержку ООО «ЦРТ-инновации» (контактные данные см. в подразделе 1.2 Сервисное обслуживание и техническая поддержка). Ответным письмом вам будет выслан файл формата .v2c, который содержит программный ключ HASP SL Pro. Сохраните его в локальной директории сервера.

8. В консоли сервера выполните команду:

```
HaspTool
```

9. Дождитесь появления следующего сообщения:

```
Please, press i-hasp information, f-save fingerprint info, c-save c2v file,
u-update v2c file, e-exit.
```

Чтобы применить v2c-файл, т.е. установить программный HASP-ключ, нажмите на клавиатуре клавишу **u**, а затем клавишу **Enter**.

10. Дождитесь появления в консоли следующего сообщения:

```
Please enter the name of an available V2C file:
```

11. Введите имя файла v2c (включая расширение).

7.2 Работа с «Менеджером лицензий»

Работа с «Менеджером лицензий» выполняется в браузере с помощью утилиты «Sentinel Admin Control Center». Вход в «Sentinel Admin Control Center» рекомендуется выполнять путём проброса портов на каком-либо компьютере комплекса, операционная система которого имеет графическую оболочку.

Рассмотрим, как выполнить проброс портов с помощью SSH-клиента PuTTY.

Запустите утилиту PuTTY (рис. 12).

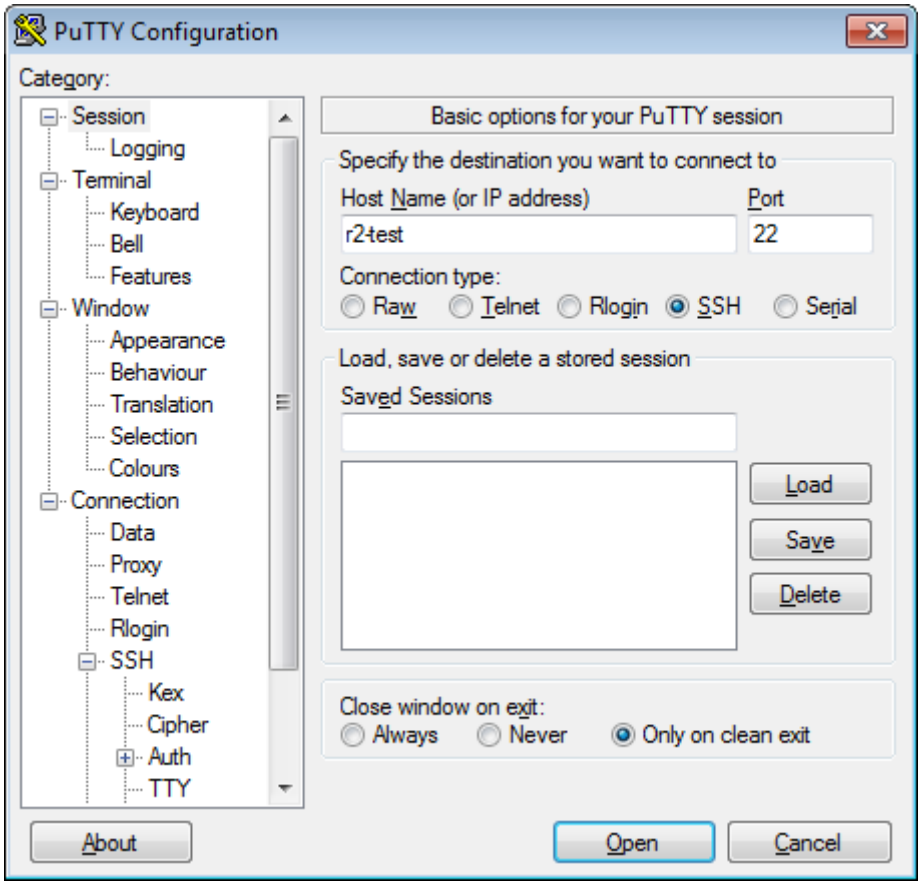

Рисунок 12 – Настройки подключения

В поле **Host name (or IP address)** укажите имя или IP-адрес сервера комплекса. В поле **Port** должен быть указан порт 22. Для подключения следует использовать **Connection Type** (**Тип соединения**) SSH.

На панели **Category** (**Категория**) выберите **Connection > SSH > Tunnels** (**Соединение > SSH > Туннели**) (рис. 13). В поле **Source port** (**Порт источника**) укажите любой неиспользуемый порт на локальном компьютере. В поле **Destination** (**Назначение**) введите строку вида **<address>:1947**, где **<address>** – IP-адрес или имя сервера комплекса. Нажмите кнопку **Add** (**Добавить**), затем кнопку **Open** (**Открыть**).

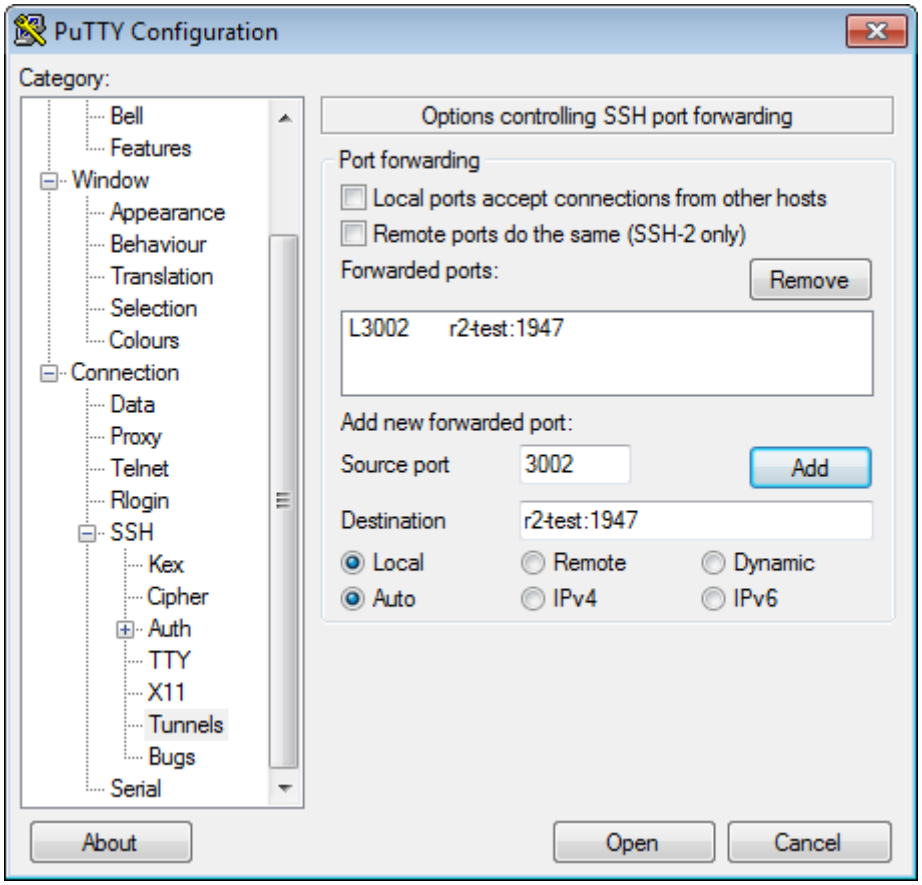

Рисунок 13 – Параметры проброса портов

В командной строке сервера укажите логин и пароль для входа в систему (см. раздел 1.3 Параметры доступа).

Затем на локальном компьютере откройте браузер и в адресной строке введите строку вида **http://localhost:<port>**, где **<port>** – порт, указанный в настройках PuTTY, в поле **Source port** (**Порт источника**) (рис. 13).

8 ПОДКЛЮЧЕНИЕ И НАСТРОЙКА GSM-ШЛЮЗА

В данном разделе приведён порядок действий по настройке и подключению VoIP GSM-шлюза на примере модели GoIP4.

Для подключения и настройки VoIP GSM-шлюза GoIP4 выполните следующие действия:

1. Отключите PIN-код на SIM-картах, предназначенных для GSM-шлюза.
2. Вставьте SIM-карты в предназначенные для них слоты GSM-шлюза.
3. Подключите шлюз к компьютеру через порт **PC**.
4. Подключите выход блока питания к разъему питания **DC 12V**.
5. *Если в сети не используется DHCP*, обратитесь к системному администратору для получения параметров подключения по локальной сети (перечень необходимых данных см. на рис. 16). В настройках операционной системы укажите следующие сетевые параметры для подключения по локальной сети: IP-адрес – **192.168.8.xxx**, шлюз по умолчанию – **192.168.8.1**.
6. Для перехода к веб-интерфейсу GSM-шлюза откройте браузер Internet Explorer и введите в адресной строке браузера **192.168.8.1** или **http://192.168.8.1** (**192.168.8.1** – IP-адрес порта **PC** по умолчанию).
7. Откроется окно аутентификации пользователя (рис. 14). В данном окне введите пароль и логин по умолчанию: **admin/admin**. Нажмите на кнопку **OK**.

Рисунок 14 – Окно аутентификации пользователя

8. Откроется страница настроек GSM-шлюза (рис. 15). *Если в сети не используется DHCP*, выберите в меню раздел **Configurations (Конфигурация) > Network (Сеть)** и выполните действия, описанные в п.п. 9-11. *Если в сети используется DHCP*, перейдите к п. 12.

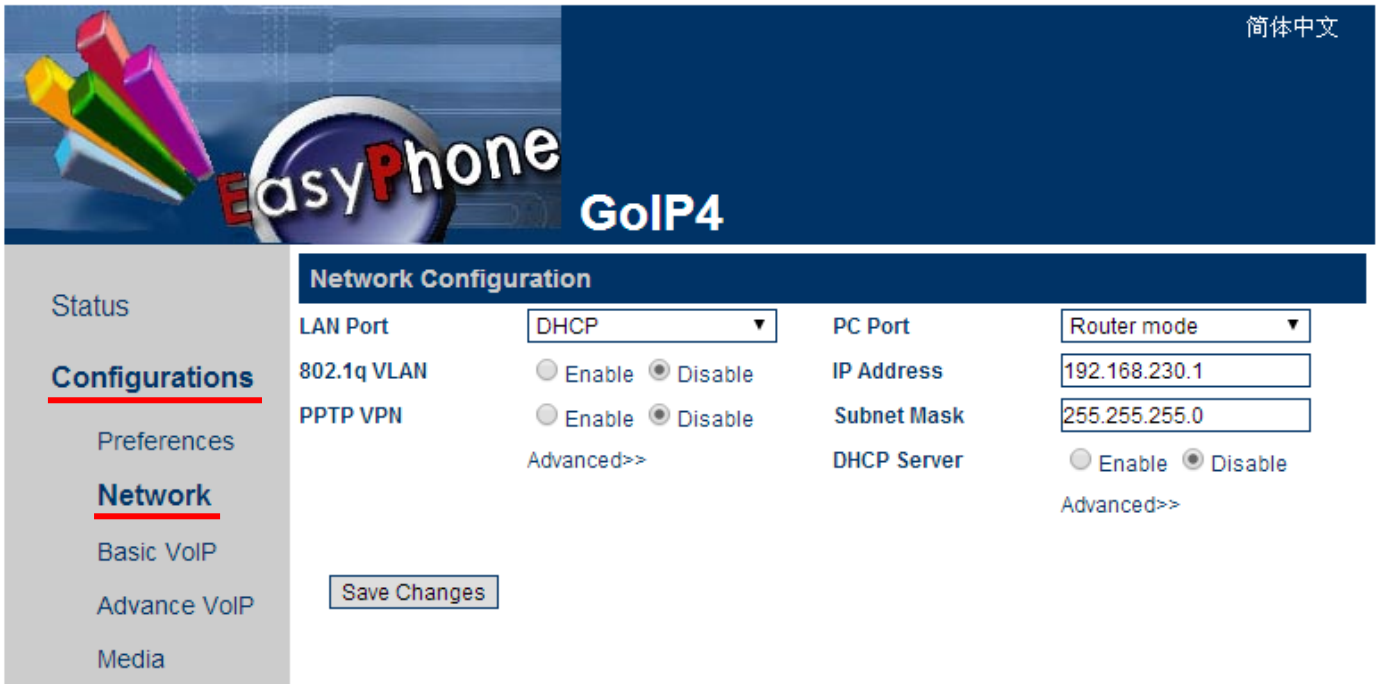

Рисунок 15 – Раздел **Network** (**Сеть**)

9. В поле **LAN Port (Порт LAN)** с помощью выпадающего списка выберите **Static IP (Постоянный IP-адрес)**.
10. В полях, которые отобразятся ниже, введите данные, полученные от системного администратора (рис. 16). Данные в группе настроек PC-порта оставьте без изменений.

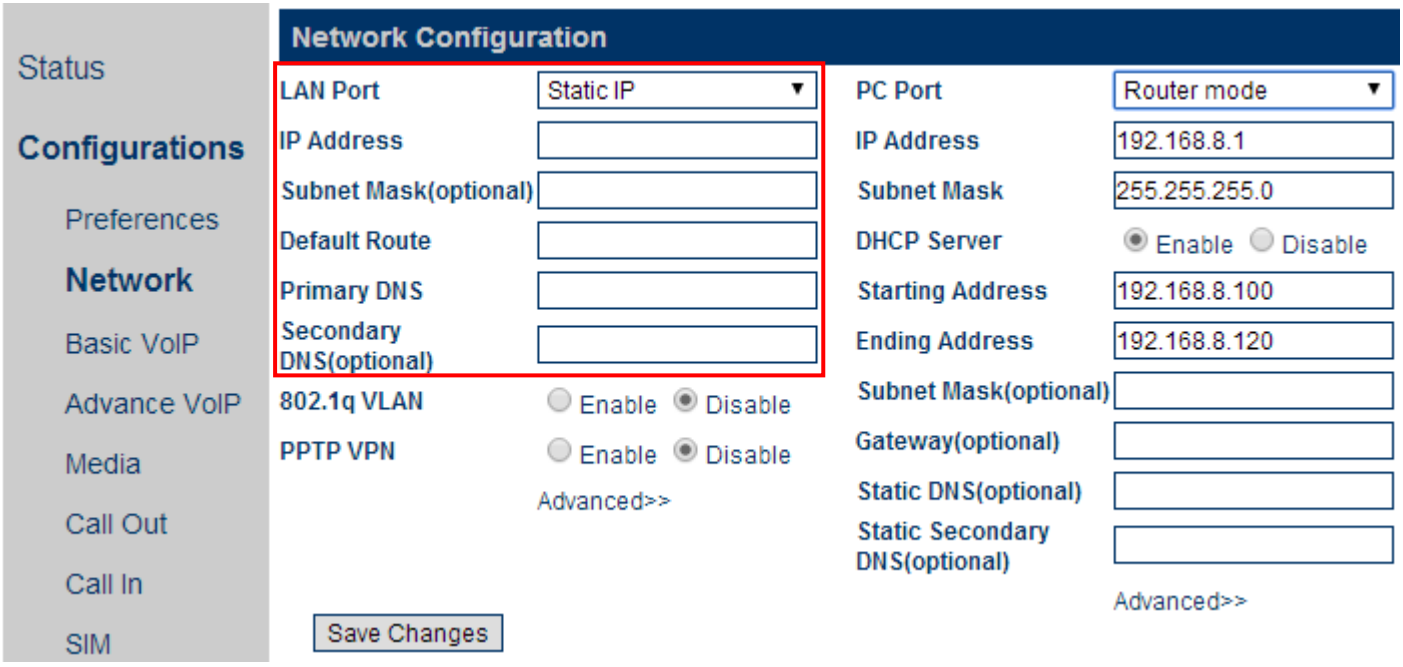

Рисунок 16 – Настройки LAN-порта

11. Нажмите на кнопку **Save Changes (Сохранить изменения)**.
12. В меню выберите раздел **Configurations (Конфигурация) > SMS** (рис. 17).

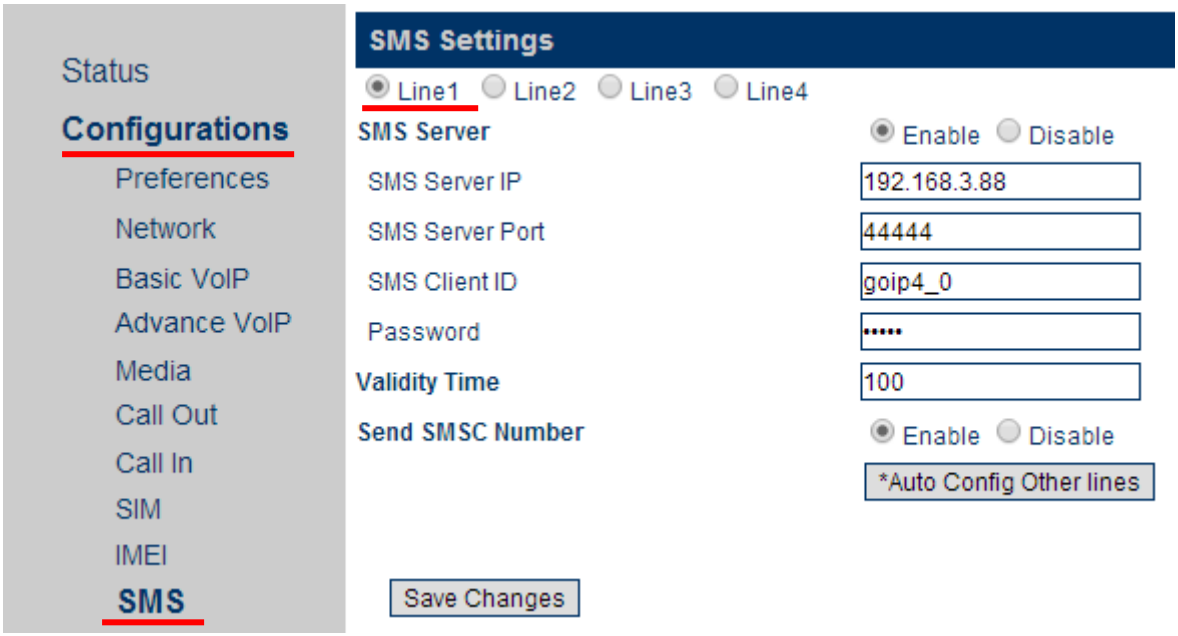

Рисунок 17 – Раздел **SMS**

13. Выполните настройку **Line 1 (Линии 1)**. Для этого установите переключатель **SMS Server (SMS-сервер)** в положение **Enable (Включить)**.
14. В поле **SMS Server IP (IP-адрес SMS-сервера)** введите IP-адрес сервера **Рупор.БЛИЦ**.
15. В поле **SMS Server Port (порт SMS-сервера)** оставьте порт, выбранный для сервера **Рупор.БЛИЦ** по умолчанию – 44444. Изменять порт не рекомендуется.
16. В поле **SMS Client ID (Идентификатор пользователя)** введите идентификатор шлюза или оставьте идентификатор, заданный по умолчанию. Идентификатор пользователя представляет собой цифро-буквенную последовательность латинским шрифтом в произвольной форме.

Идентификатор пользователя должен быть отличным от идентификаторов, используемых на других GSM-шлюзах, подключённых к ЛВС.

17. В поле **Password (Пароль пользователя)** введите пароль пользователя.

Ввод пароля пользователя обязателен.

18. В поле **Validity Time (Срок действия)** укажите период хранения SMS на сервере оператора. Рекомендуемое значение **143** (12 часов).

    Таблица значений:

Срок действия	Формула вычисления длительности	Время
0–143	(VP + 1) x 5 минут	5 минут–12 часов, интервалами по 5 минут
144–167	12 ч + (VP – 143) x 30 минут	12–24 часа
168–196	(VP – 166) x 1 день	2–30 дней
197–255	(VP – 192) x 1 неделя	5–63 недель

19. В группе настроек **Send SMSC Number (Отправить номер SMS-центра)** выберите **Enable (Включить)**.
20. Нажмите кнопку **Auto Config Other lines (Автоматическая настройка других линий)**, чтобы настройки линии 1 применились к линиям 2-4.

21. Нажмите на кнопку **Save Changes (Сохранить изменения)**.
22. Если GSM-шлюз не будет использоваться для передачи голосовых оповещений, перейдите к п. 28. Если GSM-шлюз будет использоваться для передачи голосовых оповещений, выберите раздел **Configurations (Конфигурация) > Basic VoIP** (рис. 18).
23. В поле **Config Mode (Режим конфигурации)** с помощью выпадающего списка выберите **Single Server Mode (Режим «Один сервер»)**.
24. В полях **Phone Number**, **Display Name** и **Authentication ID** введите значение 0000.
25. В поле **Password (Пароль)** введите пароль.
26. В полях **SIP Proxy (IP-адрес прокси-сервера SIP)**, **SIP Registrar Server (Сервер регистрации SIP)** и **Outbound Proxy (Исходящий прокси-сервер)** введите IP-адрес сервера **Рупор.БЛИЦ**.
27. Нажмите на кнопку **Save Changes (Сохранить изменения)**.

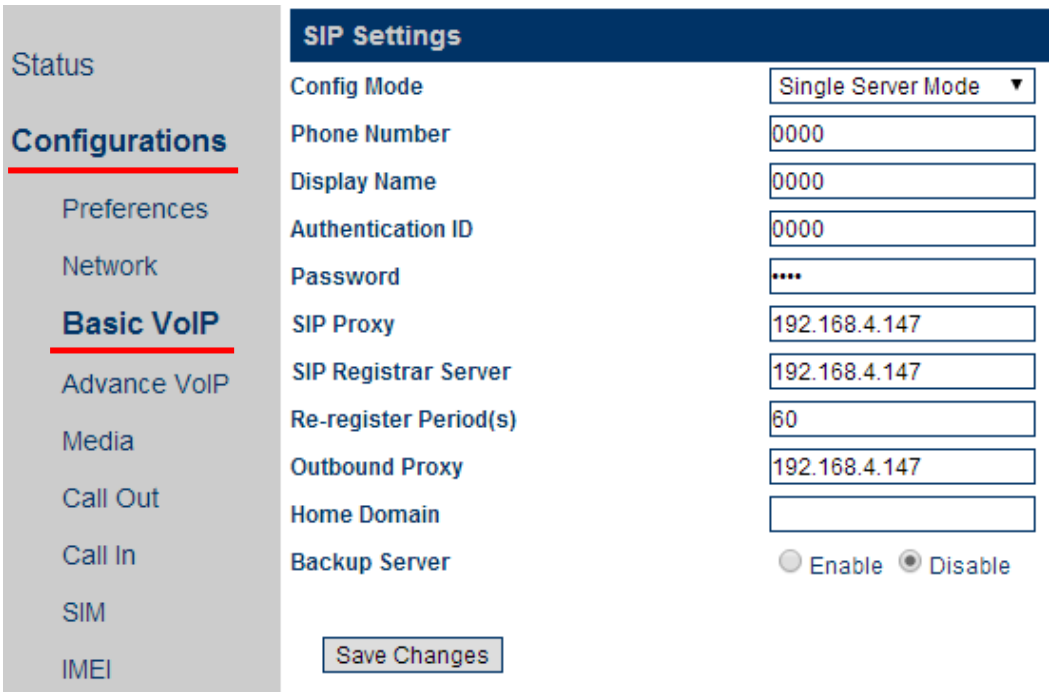

Рисунок 18 – Раздел **Basic VoIP**

28. Шлюз GoIP4 в конфигурации по умолчанию при получении сигнала «занято» на GSM линии сам инициирует повторный вызов, повторяя попытку дозвона 3 раза. При этом для комплекса **Рупор.БЛИЦ** это выглядит как одна попытка, а для абонента – как очень назойливый звонок. Рекомендуется отключать автоматический повтор набора номера. Для этого:
    - выберите раздел **Configurations (Конфигурация) > Call Out** (рис. 19);
    - в пункте **GSM Auto Redial > Disable** нажмите на кнопку **Save Changes (Сохранить изменения)**.

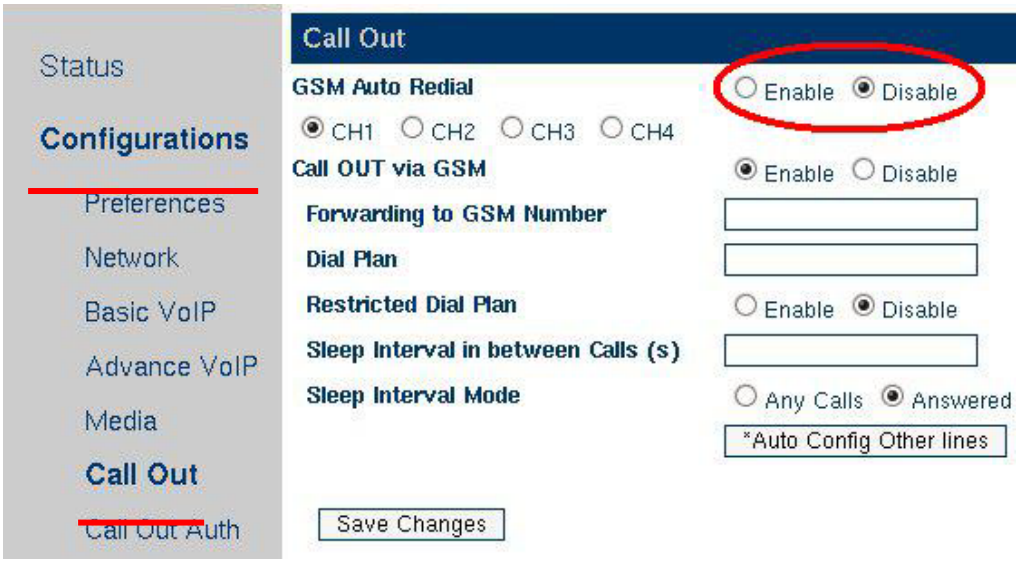

Рисунок 19 – Раздел **Call Out**

29. Рекомендуется отключить настроенный по умолчанию автоматический перезапуск шлюза. Для этого выберите раздел **Configurations (Конфигурация) > Preferences** (рис. 20).
30. В группе настроек **Auto Reboot (Автоматическая перезагрузка)** выберите **Disable (Выключить)**.
31. Нажмите на кнопку **Save Changes (Сохранить изменения)**.

Рисунок 20 – Раздел **Call Out**

32. Закройте в браузере вкладку с настройками GSM-шлюза и отключите компьютер от шлюза.
33. Подключите шлюз к локальной сети через порт **LAN**. Подключение производится с помощью Ethernet-кабеля, входящего в комплект поставки.

Для GSM-шлюза GoIP можно настроить расписание перезагрузки на сервере комплекса (см. пункт 10.9.4 Настройка транков для отправки SMS).

9 ИНТЕГРАЦИЯ С АТС

Программные средства комплекса **Рупор.БЛИЦ** совместимы со всеми IP телефонными станциями, поддерживающими передачу данных по каналам VoIP (SIP, H.323) и линиям цифрового потока E1, использующим для передачи голосовой информации речевой кодек ITU-T G.711.

9.1 Настройка подключения по SIP

Сопряжение АТС с программными средствами комплекса **Рупор.БЛИЦ** по каналу SIP осуществляется посредством редактирования значения параметров конфигурационного файла ***/etc/asterisk/sip.conf***.

Для изменения настроек канала SIP выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. Откройте файл ***/etc/asterisk/sip.conf*** в текстовом редакторе **mcedit** или **vim** и редактируйте секцию **[general]** (пример см. ниже):
   - Если на шлюзе требуется регистрация, в секцию **[general]** добавьте команду регистрации ***register => username:secret@host:port***.
   - В описании идентификатора клиента **[0000]** редактируйте значения требуемых параметров.
   - Закомментируйте неиспользуемые параметры. Для этого введите перед ними символ **;**.
3. Чтобы изменения вступили в силу, перезагрузите модуль SIP с помощью консольной команды ***apply_sip_changes***.

Пример содержания секции **[general]** представлен ниже:

```
register => user_1:123456@192.168.1.1

[0000]
host=192.168.1.1
type=friend
nat=no
username=user_1
secret=123456
```

Основные параметры файла конфигурации ***sip.conf***:

Параметр	Описание
host	IP-адрес SIP-сервера (шлюза)
port	Порт для соединения со шлюзом по протоколу TCP (по умолчанию 5060)
username	Имя пользователя для сопряжения на шлюзе (если необходимо)

Параметр	Описание
secret	Пароль пользователя для сопряжения на шлюзе (если необходимо)

Для получения более подробной информации о настройке канала SIP обратитесь в службу технической поддержки ООО «ЦРТ-инновации» или самостоятельно ознакомьтесь с соответствующей документацией на сайте разработчика системы Asterisk:

http://asterisk.ru/knowledgebase/Asterisk+config+sip.conf.

Далее необходимо настроить транк для оповещения в соответствии с инструкциями в подразделе 10.9 Настройка транков.

9.2 Настройка подключения по H.323

9.2.1 Настройка модуля ooh323

Параметры подключения к АТС с регистрацией на гейткипере для Asterisk 11:

```
[root@rupor2 asterisk]# cat /etc/asterisk/ooh323.conf
[general]
port = 1720 ;порт, который мы слушаем
bindaddr = 192.168.54.201 ;наш адрес
fastStart = no
h245Tunnelling = yes
dtmfmode = rfc2833
type = h323 ;параметры регистрации
h323id = addpac54201 ;логин
e164 = 83952797774 ;алиас
gatekeeper = 192.168.54.2 ;адрес гейткипера
autoframing = yes
disallow = all ;запрещаем загрузку всех кодеков
allow = ulaw ;разрешаем загрузку необходимого кодека
allow = alaw ;разрешаем загрузку необходимого кодека
context = type-1 ;указываем контекст
rtptimeout = 60
```

После изменения и сохранения параметров выполните команду ***add_trunk OOH323/addpac54201***.

9.2.2 Подключение к AVAYA

```
[general]
port = 1720
bindaddr = 10.1.2.1 ; this SHALL contain a single, valid IP address for this machine
disallow=all
allow=alaw ; see doc/rtp-packetization for framing options
dtmfmode=inband
gatekeeper = DISABLE
```

```
    AcceptAnonymous = yes ;Вы уверены что контролируете входящий H.323 траффик?
    context=type-1 ;этот контекст справедлив только для прямого доступа к внутренним
номерам и исходящим маршрутам.
    ; При этом Вы не сможете создавать правила для входящих DID's.
    progress_alert = 8
    h245Tunneling = yes
    fastStart = yes

    [avaya]
    type=friend
    context=type-1
    host=10.1.2.2 ;адрес АТС
    port=1720 ;порт, который слушает АТС
    disallow=all ;запрещаем загрузку всех кодеков
    allow=alaw ;разрешаем загрузку необходимого кодека
    dtmfmode=inband
    faststart=no
    h245Tunneling = yes
```

После изменения и сохранения параметров выполните команду ***add_trunk OOH323/avaya***.

9.3 Настройка вариантов набора номера

Если при редактировании файлов конфигурации будут допущены ошибки, работоспособность комплекса **Рупор.БЛИЦ** будет нарушена.

Для изменения правил набора номеров абонентов, например, добавления префикса или применения различных правил набора номеров для внутренних и внешних абонентов, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. Отредактируйте файл ***/opt/rupor2/conf/user-ext.conf*** с помощью текстового редактора **mcedit** или **vim**.
3. В консоли операционной системы выполните команду ***apply_dialplan_changes***.

Пример файла конфигурации ***user-ext.conf*** представлен ниже:

```
    ;; Пример пользовательского dial plan
    ;; для активации нужно удалить ';' в начале строк с exten

    ;; Все семизначные номера телефонов преобразуются в 10-значный номер
    ;;(с кодом 812) и к ним добавляется префикс 7
    ;exten => _XXXXXXX,1,Macro(prepare-call)
    ;exten => _XXXXXXX,n,Dial(SIP/0000/7812${EXTEN})

    ;; Ко всем 10-значным номерам добавляется префикс 7
    ;exten => _XXXXXXXXXX,1,Macro(prepare-call)
```

```
;exten => _XXXXXXXXXX,n,Dial(SIP/0000/7${EXTEN})

;; Все четырехзначные номера, начинающиеся на 7,
;; преобразуются в начинающиеся на 6
exten => _7XXX,1,Macro(prepare-call)
exten => _7XXX,n,Dial(SIP/0000/6${EXTEN:1})

;; Остальные номера обрабатываются в основном файле
```

Для переадресации вызова на оператора и необходимости вносить изменения в номер телефона оператора (например, добавление префикса) выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. Отредактируйте файл ***/opt/rupor2/conf/user-oper.conf*** с помощью текстового редактора **mcedit** или **vim**.
3. В консоли операционной системы выполните команду ***apply_dialplan_changes***.

Пример файла конфигурации ***user-oper.conf*** представлен ниже:

```
;; Добавим префикс 7 к телефону оператора
;; (для активации нужно убрать ';' в следующей строке
exten => s,n,Set(OPERATOR=7${OPERATOR})
```

10 АДМИНИСТРИРОВАНИЕ СЕРВЕРА КОМПЛЕКСА ОПОВЕЩЕНИЯ

Для получения доступа к командной строке операционной системы сервера **Рупор.БЛИЦ** необходимо использовать любой SSH-клиент, например, **PuTTY**. Подключение следует осуществлять по порту 22. Данные учетной записи **rupor_admin** для подключения по SSH представлены в подразделе 1.3 Параметры доступа. По умолчанию SSH-сессия длится 20 минут.

Настоятельно рекомендуется выполнять настройку комплекса до начала оповещения абонентов.

10.1 Просмотр списка изменяемых параметров

Список части изменяемых параметров отображается при выполнении команды ***show_constants***. Справочник этих параметров приведён в приложении В.

Порядок изменения части отображаемых параметров описан в данном руководстве.

Для изменения прочих отображаемых параметров следует выполнить команду ***set_constant name value***, где ***name*** – имя параметра, ***value*** – значение параметра.

Для проверки успешности выполнения какой-либо команды следует выполнить команду ***command params && echo Ok***. Например, ***set_constant web_session_timeout 1000 && echo Ok***. Если значение параметра успешно изменено, будет возвращен ответ ***Ok***.

10.2 Общие настройки

10.2.1 Работа с сертификатами

Для защиты данных, которые передаются между веб-сервером и веб-приложением **Рупор.БЛИЦ**, используется протокол SSL. На сервере комплекса содержится самоподписанный сертификат и SSL-ключ.

Сертификат генерируется автоматически:

1. При первом включении сервера с предустановленным ПО **Рупор.БЛИЦ** и получении IP-адреса для сервера.
2. При установке ПО **Рупор.БЛИЦ** и получении IP-адреса для сервера.

10.2.1.1 Настройка работы по протоколу http

По умолчанию при передаче данных между веб-сервером и веб-приложением используется протокол https. Чтобы отключить автоматическое перенаправление веб-интерфейса на https, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.

2. В консоли операционной системы выполните команду ***allow_http 1***.

После выполнения данной команды при обмене данными между веб-сервером и веб-приложением по умолчанию будет использоваться протокол http. При указании вручную в адресной строке браузера протокола https будет использоваться протокол https.

Чтобы по умолчанию использовался только протокол https, следует выполнить команду ***allow_http 0***.

Настоятельно рекомендуется не использовать протокол **http**, т.к. в этом случае учётные данные между веб-клиентом и сервером передаются по сети передачи данных в открытом виде и могут быть перехвачены и скомпрометированы.

10.2.1.2 Установка собственных сертификатов

Если требуется заменить самоподписанный сертификат и ключ SSL веб-сервера на собственный сертификат и ключ, выполните следующие действия:

1. Поместите сертификат и ключ в какую-либо директорию на сервере комплекса.
2. Присвойте файлам сертификата и ключа имя ***server***. Пример: ***server.key***.
3. В консоли операционной системы выполните команды:

   sudo cp server.crt /etc/httpd/ssl/

   sudo cp server.key /etc/httpd/ssl/

4. Выполните перезапуск веб-сервера с помощью команды ***sudo service httpd restart***.

10.2.1.3 Удаление сертификата

Если серверу комплекса необходимо назначить новый IP-адрес, необходимо предварительно удалить имеющийся на сервере самоподписанный сертификат. После получения нового IP-адреса новый сертификат будет сгенерирован автоматически.

Чтобы удалить самоподписанный сертификат, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команды:

   sudo rm /etc/httpd/ssl/server.crt

   sudo rm /etc/httpd/ssl/server.key

3. Выполните перезапуск веб-сервера с помощью команды ***sudo service httpd restart***.

При перезапуске сервиса httpd после удаления сертификата его работа будет нарушена.
Для корректной работы необходимо установить сертификат и перезапустить службу.
При необходимости можно перезапустить сервер, в этом случае сертификаты будут созданы автоматически.

10.2.2 Изменение IP-адреса сервера комплекса оповещения

Если серверу комплекса необходимо назначить статический IP-адрес, следует предварительно удалить имеющийся на сервере самоподписанный сертификат (см. 10.2.1.3 Удаление сертификата). После назначения статического IP-адреса новый сертификат будет сгенерирован автоматически.

Для изменения IP-адреса сервера комплекса оповещения выполните следующие действия:

1. Подключите к серверу монитор и клавиатуру.

   Откройте консоль и введите данные учетной записи **rupor_admin**.

   Выполните команду ***change_ip [-i interface] {DHCP|ip netmask [gateway [dns1 [dns2]]]}***.

   - ***interface*** – название сетевого интерфейса. Указывается при назначении IP-адреса интерфейсу, отличному от ***eth0***. Например, ***eth1***;
   - ***DHCP*** – данный параметр указывается, если для назначения IP-адреса следует использовать DHCP;
   - ***ip*** – IP-адрес. Указывается, если назначение IP-адреса требуется выполнить вручную;
   - ***netmask*** – маска подсети. Указывается, если назначение IP-адреса требуется выполнить вручную;
   - ***gateway*** – IP-адрес основного шлюза;
   - ***dns1*** – IP-адрес первого DNS-сервера;
   - ***dns2*** – IP-адрес второго DNS-сервера.

   […] – необязательные параметры.

   Примеры:

   - ***change_ip 192.168.2.10 255.255.255.0*** – назначить интерфейсу ***eth0*** IP-адрес ***192.168.2.10***;
   - ***change_ip DHCP*** – назначить интерфейсу ***eth0*** IP-адрес автоматически;
   - ***change_ip -i eth1 192.168.2.100 255.255.255.0 192.168.2.1 192.168.2.1 192.168.2.10*** – назначить интерфейсу ***eth1*** IP-адрес ***192.168.2.100***; маска подсети – ***255.255.255.0,*** IP-адрес основного шлюза – ***192.168.2.1,*** IP-адрес первого DNS-сервера – ***192.168.2.1,*** IP-адрес второго DNS-сервера – ***192.168.2.10***.

   При выполнении команды проверяется только количество указанных параметров. Корректность указанных IP-адресов не проверяется.

   Проверьте доступность веб-интерфейса комплекса. Для этого на любом компьютере в той же локальной сети введите в адресной строке браузера ***https://IP-адрес_сервера***. Для авторизации в веб-приложении используйте данные встроенной учетной записи администратора, которые приведены в подразделе 1.3 Параметры доступа.

   Проверьте доступность сетевых папок файловой системы **Рупор.БЛИЦ**. Для этого на любом компьютере в той же локальной сети в проводнике введите ***\\IP-адрес_сервера incoming*** и ***\\IP-адрес_сервера\outgoing***. Для авторизации используйте данные учетной записи, которые приведены в подразделе 1.3 Параметры доступа.

Доступ к серверу возможен только с частных IP-адресов.

10.2.3 Изменение имени сервера комплекса «Рупор.БЛИЦ»

Для изменения имени сервера комплекса **Рупор.БЛИЦ** выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***change_hostname server_name.domain_name***, где ***server_name*** – новое имя сервера, ***domain_name*** – имя домена.

10.2.4 Изменение имени пользователя и пароля для доступа к файловой системе через samba

Чтобы изменить авторизационные данные пользователя для доступа к сетевым папкам, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***change_samba имя_пользователя пароль***, где ***имя_пользователя*** – новое имя пользователя, ***пароль*** – новый пароль пользователя. Пароль может содержать только латинские буквы и цифры.

10.2.5 Настройка proxy-сервера

Для настройки proxy-сервера выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***set_http_proxy http://адрес_proxy-сервера:порт***.

10.2.6 Настройка даты и времени

Активация ситуаций по расписанию осуществляется по времени, установленному на сервере. Администратору комплекса необходимо убедиться, что дата, время и часовой пояс на рабочих местах пользователей веб-приложения совпадает с датой, временем и часовым поясом на сервере комплекса.

Установку даты, времени и часового пояса на сервере необходимо выполнять до оповещения абонентов.

Для установки даты и времени используются следующие команды:

Команда	Значение
sudo date MMDDHHmm	Установка даты и времени
sudo hwclock -w	Запись текущего времени в энергонезависимые часы
sudo ntpdate адрес_сервера	Установка времени с сервера NTP
edit /etc/ntp.conf	Редактирование файла конфигурации NTP
sudo service ntpd start или stop или restart	Запуск, остановка или перезагрузка ntpd
sudo chkconfig ntpd on или off	Активация или деактивация демона ntpd при загрузке

Для изменения часового пояса, выставляемого по умолчанию, в консоли операционной системы выполните команду ***set_default_tz часовой_пояс***. В качестве аргументов используются **GMT+X** или **GMT-X**, где **X** – смещение от Гринвичского времени. После успешной замены временной зоны будет предложено перезагрузить сервер, что можно сделать командой ***sudo reboot***.

При переводе на сервере времени назад в ходе оповещения абонентов процесс выполнения некоторых оповещений может быть нарушен (для попыток дозвона будет отображаться статус «канал недоступен», перестанут отправляться SMS-сообщения).

В связи с этим при переводе времени система может выдавать соответствующие предупреждения. После перевода времени также требуется перезагрузка сервера.

10.2.7 Настройка уровня журналирования

Не рекомендуется без необходимости повышать уровни журналирования компонентов комплекса, так как это может привести к ухудшению производительности работы комплекса Рупор.БЛИЦ и дополнительному потреблению дискового пространства.

Для каждого компонента комплекса уровень журналирования указывается в конфигурационном файле ***/opt/rupor2/conf/log_название_компонента.conf***. Изменение уровня журналирования осуществляется с помощью утилиты ***set_log_level***.

Чтобы изменить уровень журналирования работы компонентов, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***set_log_level LEVEL [COMPONENT]***, где:
   - ***LEVEL*** – уровень журналирования: **DEBUG**, **INFO**, **ERROR**, **WARN** или **FATAL**.
   - ***COMPONENT*** – название компонента, для которого следует изменить уровень журналирования. Если компонент не указан, то уровень журналирования изменяется для всех компонентов.

Ниже приведён список компонентов, для которых администратор комплекса может самостоятельно изменить уровень журналирования, и их назначение.

- **AddTaskFromCSV** – работа в режиме интеграции и создание оповещений с помощью вкладки **Оповещения** в веб-приложении **Рупор.БЛИЦ**.
- **dialer** – служба оповещения по телефону.
- **h350monitor** – работа устройства STC H350.
- **mailsender** – отправка почты.
- **monitor** – мониторинг работы компонентов комплекса **Рупор.БЛИЦ**.
- **reportd** – создание отчетов для оповещений, которые были созданы в режиме интеграции.
- **smssender** – отправка SMS-сообщений.
- **web** – веб-интерфейс.

Список всех компонентов, для которых можно изменить уровень журналирования, отображается при выполнении команды ***set_log_level***.

Лог-файлы компонентов сохраняются в папку ***/var/log/rupor2***.

Настоятельно не рекомендуется без запроса службы техподдержки ООО «ЦРТ-инновации» изменять уровень журналирования компонентов, которые не описаны в данном разделе.

10.2.8 Настройка уведомлений службы очистки диска

Служба мониторинга свободного места на диске инициирует выполнение системного сценария оповещения при заполнении допустимого объёма диска (см. пункт 10.6.6 Настройка длительности хранения завершившихся оповещений). Системный сценарий выполняется также при обнаружении проблем с репликацией данных.

До тех пор пока проблема не будет устранена, оповещение по системному сценарию будет проводиться повторно (с некоторой периодичностью).

Системный сценарий называется ***_system_alert_***. Этот сценарий скрыт от пользователей веб-приложения **Рупор.БЛИЦ**. Сценарий предполагает совершение телефонного вызова (3 попытки), отправку SMS (2 попытки с ожиданием отчёта о доставке в течение 10 минут) и Email.

Чтобы указать получателей оповещения, выполните команду ***set_alert_contacts voice_list sms_list email_list***, где:

- ***voice_list*** – один или несколько номеров телефона, на которые следует инициировать звонок от комплекса **Рупор.БЛИЦ** при заполнении допустимого объёма диска.
- ***sms_list*** – один или несколько номеров телефона, на которые следует отправить SMS-сообщения от комплекса **Рупор.БЛИЦ** при заполнении допустимого объёма диска.
- ***email_list*** – один или несколько Email-адресов, на которые следует отправить электронное письмо от комплекса **Рупор.БЛИЦ** при заполнении допустимого объёма диска.

Для каждого типа контакта (***voice_list***/***sms_list***/***email_list***) должен быть указан как минимум один контакт. Контакты разных типов разделяются пробелом. Если требуется указать несколько контактов одного типа, их необходимо указать через запятую без пробела.

Например:

set_alert_contacts 4238 +79818394960,+79816907712 sidorov@mail.ru.

Чтобы просмотреть список контактов, заданных с помощью утилиты ***set_alert_contacts***, выполните команду ***view_alert_contacts***.

Чтобы удалить контакты, выполните команду ***set_alert_contacts*** и передайте значения **NULL** для тех типов контактов, которые требуется удалить (***voice_list***/***sms_list***/***email_list***).

Для осуществления отправки сообщений службой очистки диска необходимо наличие лицензии на динамический синтез.

10.3 Настройка SMTP-сервера

Для настройки параметров необходимо, чтобы SMTP-сервер был подключен к сети и доступен для соединения в момент настройки. Настройки, описанные в пунктах 10.3.1 и 10.3.3 являются обязательными для функционирования сервера.

Отправка оповещений по электронной почте на почтовые сервера в киррилической доменной зоне, например, username@живетв.рф, не поддерживается.

10.3.1 Настройка имени SMTP-сервера

Чтобы указать имя/IP-адрес SMTP-сервера, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***set_mail_host hostname/ip [port]***, где ***hostname/ip*** – доменное имя/IP-адрес SMTP-сервера.

10.3.2 Настройка метода авторизации

Для настройки работы с SMTP-сервером, который требует авторизации, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду

set_mail_auth method [username password [domain]], где:

- ***method*** – ***NONE***, ***NTLM***, ***PLAIN*** или ***LOGIN***;
- ***username*** – имя пользователя;
- ***password*** – пароль пользователя;
- ***domain*** – опциональный параметр для метода ***NTLM***.

Имя пользователя и пароль не требуются только для метода **NONE**.

10.3.3 Настройка адреса отправителя писем

Чтобы указать адрес отправителя писем, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учётной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***set_mail_from name, где name*** – это полный адрес отправителя (например, **test@test.ru**).

Команда ***set_mail_from name*** не проверяет корректность вводимого адреса отправителя писем.

10.4 Настройка веб-приложения

10.4.1 Изменение времени длительности сессии

По умолчанию время длительности сессии в веб-приложении **Рупор.БЛИЦ** при неактивности пользователя составляет одни сутки (86400 секунд).

Чтобы изменить время длительности сессии, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***set_constant web_session_timeout N***, где ***N*** – время длительности сессии.

10.4.2 Сброс пароля администратора для доступа к веб-интерфейсу комплекса

Чтобы сбросить пароль администратора для доступа к веб-интерфейсу комплекса **Рупор.БЛИЦ**, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***reset_pass***.

После выполнения этой команды пароль администратора для доступа к веб-интерфейсу комплекса оповещения будет сброшен к значению пароля по умолчанию, прописанному в формуляре на комплекс **Рупор.БЛИЦ**.

10.4.3 Выбор языка страницы авторизации

Администратор комплекса может установить язык интерфейса страницы авторизации пользователя веб-приложения. Для выбора доступны четыре языка: русский, финский, испанский или английский. По умолчанию используется русский язык.

Для изменения языка выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***set_language language***, где ***language*** – двухбуквенный код языка: ***ru***, ***en***, ***es***, ***fi***.

Язык интерфейса веб-приложения выбирается пользователем самостоятельно с помощью настроек веб-приложения. При первом входе в веб-приложение используется язык страницы авторизации.

10.4.4 Изменение приоритета оповещения абонента

При создании абонента в веб-приложении **Рупор.БЛИЦ** указывается приоритет оповещения абонента (см. руководство пользователя веб-приложения **Рупор.БЛИЦ**). По умолчанию наибольший приоритет оповещения имеют абоненты, для которых установлено значение 0, наименьший – абоненты, для которых установлено значение 2.

Чтобы изменить наибольшее и наименьшее числовое значение приоритета, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учётной записью **rupor_admin**.
2. Для изменения значения максимального приоритета выполните команду ***set_constant recipient_priority_max значение_параметра***, например, ***set_constant recipient_priority_max 2***.

   Для изменения значения минимального приоритета выполните команду ***set_constant recipient_priority_min значение_параметра***, например, ***set_constant recipient_priority_min 0***.

10.4.5 Изменение длины ПИН абонента

При создании абонента в веб-приложении **Рупор.БЛИЦ** доступен ввод личного ПИН-кода (см. руководство пользователя веб-приложения системы **Рупор.БЛИЦ**). По умолчанию длина ПИН-кода равна 4 символам.

Чтобы изменить максимальную длину ПИН-кода, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учётной записью **rupor_admin**.
2. Чтобы задать максимальную длину ПИН-кода, выполните команду ***set_constant recipient_pin_length значение_параметра***, например, ***set_constant recipient_pin_length 6***.

Минимальная длина ПИН-кода не регулируется и всегда равна 4. Таким образом, после выполнения команды, приведённой выше, для абонентов можно будет задавать ПИН-коды длиной от 4 до 6 знаков включительно.

10.5 Настройка активации ситуаций

10.5.1 Настройка типов телефонных номеров

При создании абонента в веб-приложении **Рупор.БЛИЦ** указывается один или несколько телефонных номеров, по которым следует осуществлять оповещение данного абонента с помощью комплекса **Рупор.БЛИЦ**. Для каждого номера телефона при этом можно указать его тип: домашний, рабочий, мобильный.

При создании или активации ситуации можно указать, по каким типам телефонных номеров следует оповещать выбранных абонентов.

Если тип телефонных номеров не выбран при создании или активации ситуации, оповещение абонентов может осуществляться:

1. По всем телефонным номерам, заданным для требуемых абонентов. Для этого в консоли операционной системы выполните команду

   set_constant use_all_phones_when_phone_types_is_not_set 1.

2. Только по телефонным номерам требуемых абонентов, для которых не указан тип (по умолчанию). Для этого в консоли операционной системы выполните команду ***set_constant use_all_phones_when_phone_types_is_not_set 0***.

10.5.2 Настройка активации ситуации с помощью STC-H350

При создании ситуации, которая будет активироваться путём замыкания/размыкания контакта устройства STC-H350, имеется возможность включить дополнительные опции:

- необходимость повторного (подтверждающего) замыкания/размыкания контакта для активации;
- задержку между активацией ситуации и фактическим началом оповещения.

Чтобы изменить период ожидания повторного (подтверждающего) замыкания/размыкания контакта после первого замыкания/размыкания контакта, выполните команду ***set_constant h350_confirmation_timeout значение_параметра***, например, ***set_constant h350_confirmation_timeout 10***. Значение параметра задаётся в секундах. По умолчанию значение параметра равно 5.

Чтобы изменить период задержки, предлагаемый по умолчанию при создании ситуации, выполните команду ***set_constant default_activation_delay значение_параметра***, например, ***set_constant default_activation_delay 60***. Значение параметра задаётся в секундах. По умолчанию значение параметра равно 120.

10.6 Настройка оповещений

10.6.1 Настройка идентификатора вызывающего абонента

Чтобы указать идентификатор вызывающего абонента при обзвоне, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***set_default_cid "name <number>"*** или ***set_default_cid number*** где ***name*** – имя комплекса оповещения, ***number*** – номер телефона комплекса оповещения. Например: ***set_default_cid "STC <3258848>"*** или ***set_default_cid 3258848***.

Имя комплекса оповещения **name** может содержать только латинские буквы и цифры, а номер телефона комплекса оповещения **number** только цифры. Совокупная длина идентификатора вызывающего абонента не должна превышать 100 символов.

Функция определения имени и номера комплекса оповещения зависит от возможностей и настроек АТС, к которой подключен комплекс **Рупор.БЛИЦ**.

В случае неуспешного выполнения команды будет сделана запись в журнале ***dialer.log***.

10.6.2 Настройка идентификатора вызывающего абонента для сценария

Чтобы указать идентификатор вызывающего абонента при оповещении по какому-либо сценарию, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***set_scenario_cid scenario_id "name <number>"*** или ***set_ scenario_cid number***, где:
   - ***scenario_id*** - имя сценария в формате ***USER:TEMPLATE***, где ***USER*** – учетная запись, от имени которой был создан сценарий, ***TEMPLATE*** – название сценария. Например: ***operator:scenario1***.
   - ***name*** – имя комплекса оповещения.
   - ***number*** – номер телефона комплекса оповещения.

Например: ***set_scenario_cid operator:scenario1 "STC <3258848>"*** или ***set_scenario_cid operator:scenario1 3258848***.

Название сценария должно состоять из одного слова.

При необходимости раздельного написания нескольких слов вместо пробела следует объединять их знаком "_" (нижнее подчёркивание). Использование кавычек и других специальных символов в названии сценария недопустимо.

10.6.3 Настройка количества каналов, используемых для оповещения

Чтобы указать максимальное количество каналов, которые следует использовать для оповещения, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***set_max_voice_channels number_of_channels***, где ***number_of_channels*** – максимальное количество каналов (от 1 до значения, определяемого аппаратным ключом HASP). Количество используемых каналов не должно превышать возможности АТС.

10.6.4 Настройка длительности оповещения

В комплексе существует ограничение максимальной длительности оповещения по телефону. По умолчанию оно составляет 300 секунд. Данное ограничение необходимо для принудительного завершения вызова по окончании информирования (например, чтобы линия не оставалась занятой длительное время, если вызов не был завершён абонентом).

Оповещение включает в себя этапы дозвона и непосредственно телефонного разговора. Ограничение длительности применяется отдельно для каждого из этих этапов: по умолчанию на дозвон отводится до 300 секунд и на телефонный разговор также отводится до 300 секунд.

Чтобы изменить максимальную длительность оповещения, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. Выполните команду ***set_constant MaxTimeCall значение_параметра***, например, ***set_constant MaxTimeCall 400***. Минимальное значение параметра – 300 секунд.

Если выполнен критерий успешности оповещения (например, абонент прослушал 100% от сообщения), то принудительное завершение вызова не повлияет на результат оповещения, т.е. в этом случае оповещение будет считаться успешным. Если же критерий успешности не выполнен (например, вызов принудительно завершён, пока сообщение ещё не было прослушано полностью), то попытка оповещения будет считаться неуспешной.

10.6.5 Настройка времени ожидания ответа от абонента

По умолчанию время ожидания ответа от абонента при оповещении по телефону составляет 60 секунд. Если в течение этого времени абонент не снимает трубку, звонок завершается, и абонент считается не оповещенным.

Чтобы изменить время ожидания ответа от абонента, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. Выполните команду ***set_constant answer_timeout значение_параметра***, например, ***set_constant answer_timeout 40***. Минимальное значение параметра – 10 секунд.

10.6.6 Настройка длительности хранения завершившихся оповещений

По умолчанию длительность хранения завершившихся оповещений составляет 15 суток.

Чтобы изменить длительность хранения завершившихся оповещений, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***set_storage_time N***, где ***N*** – число дней хранения завершившихся оповещений (от 1 до 365).

Длительность хранения завершившихся оповещений ограничивается не только временем, но и объемом жесткого диска. Если диск переполнится, оповещение абонентов с помощью комплекса **Рупор.БЛИЦ** осуществляться не будет.

Чтобы этого не происходило, предусмотрена служба мониторинга свободного места на диске, в которой по умолчанию настроена очистка диска от записей и кэша синтеза. Установлены следующие ограничения:

1. Допустимый объем жесткого диска для хранения завершившихся оповещений – 80%.
   - При заполнении допустимого объема хранения до 60% комплекс уведомляет об этом ответственное должностное лицо (см. раздел 10.2.8 Настройка уведомлений службы очистки диска). Например, объем жесткого диска составляет 1 ТБ. Тогда допустимый объем жесткого диска для хранения завершившихся оповещений составляет 800 ГБ, а порог для оповещения ответственного лица составляет 60% от 800 ГБ, т.е. 480 ГБ.
   - При заполнении допустимого объема хранения до 80% комплекс удаляет самые старые файлы. Например, если объем жесткого диска составляет 1 ТБ, то допустимый объем жесткого диска для хранения завершившихся оповещений составляет 800 ГБ, а удаление старых файлов начинается при заполнении 80% от 800 ГБ, т.е. 640 ГБ.
2. Объем кэш-памяти для синтезированных и скачанных звуковых файлов составляет 2 ГБ. При заполнении 100% объема кэш-памяти комплекс начинает удалять самые старые файлы.
3. Допустимый объем жесткого диска для хранения звуковых сообщений, которые были созданы в комплексе, составляет 7000 МБ. При заполнении 70% от допустимого объема хранения комплекс уведомляет об этом ответственное должностное лицо (см. раздел 10.2.8 Настройка уведомлений службы очистки диска).

10.7 Настройка доступа к функциям комплекса по телефону

10.7.1 Настройка длины ТПИН

В комплексе **Рупор.БЛИЦ** существует возможность записывать голосовые сообщения и активировать ситуации с помощью телефона. Как правило, при записи сообщений и активации ситуаций по телефону используются *ТПИН-коды* – личные телефонные ПИН-коды пользователей комплекса.

Если запись сообщений и активация ситуаций по телефону будет осуществляться только от имени администратора, можно установить длину ТПИН-кода равной нулю. В этом случае комплекс не будет запрашивать ТПИН-код. Сообщения, записанные по телефону, будут отображаться в веб-интерфейсе только для учетной записи администратора, а для активации будут доступны только ситуации, созданные администратором.

Если запись сообщений и активация ситуаций будет осуществляться и администратором, и операторами, длина ТПИН не должна быть равна нулю. При этом комплекс будет запрашивать ТПИН у каждого пользователя.

По умолчанию длина ТПИН составляет 4 цифры.

Для изменения длины ТПИН выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы для отключения запроса ТПИН-кода выполните команду ***set_tpin_length 0***, для установки ТПИН длиной от 4 до 32 цифр выполните команду ***set_tpin_length 4-32***.

После применения команды все сеансы веб-приложения **Рупор.БЛИЦ** будут принудительно завершены.

При изменении длины ТПИН, заданные ранее ТПИН-коды операторов станут недействительны.

10.7.2 Настройка ТПИН пользователя

Если длина ТПИН-кода не равна нулю (см. раздел 10.7.1 Настройка длины ТПИН), для пользователей, которые выполняют запись голосовых сообщений и активацию ситуаций по телефону, должны быть назначены ТПИН-коды.

ТПИН-коды можно назначить с помощью веб-приложения **Рупор.БЛИЦ** (см. руководство пользователя **Рупор.БЛИЦ**).

10.7.3 Настройка длины DTMF-кода активации ситуации по телефону

Существует возможность активировать ситуации с помощью телефона. При активации ситуации пользователь комплекса вводит DTMF-код активации ситуации. По умолчанию длина кода активации должна составлять 2 цифры.

Чтобы изменить длину кода активации, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.

   Чтобы длина кода активации составляла от 1 до 10 цифр, в консоли операционной системы выполните команду ***set_phone_activation_code_length 1-10***.

Чтобы запретить активацию ситуаций по телефону, установите длину кода активации равной нулю. Для этого выполните команду ***set_phone_activation_code_length 0***.

Если во внутреннем хранилище комплекса присутствуют ситуации, то при увеличении длины кода активации ко всем кодам добавляется соответствующее количество лидирующих нулей. В консоли при этом появляется соответствующее информационное сообщение.

При уменьшении длины кода активации в консоли появляется предупреждающее сообщение о том, что все существующие коды активации ситуаций будут удалены. Для подтверждения операции необходимо выполнить команду ***ACCEPT***. После выполнения команды в веб-приложении **Рупор.БЛИЦ** следует назначить требуемым ситуациям новые коды активации с учетом установленной длины.

В случае отсутствия во внутреннем хранилище комплекса ситуаций изменение длины кода активации происходит без подтверждения.

После применения команды все сеансы веб-интерфейса принудительно завершаются.

10.7.4 Настройка возможности записи голосовых сообщений

В комплексе **Рупор.БЛИЦ** существует возможность записи голосовых сообщений по телефону. По умолчанию данная возможность включена.

Если требуется запретить запись голосовых сообщений по телефону, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.

   В консоли операционной системы выполните команду ***enable_recording_of_messages 0***.

Чтобы разрешить запись голосовых сообщений по телефону, выполните команду ***enable_recording_of_messages 1***.

10.8 Настройка отчётов

10.8.1 Изменение кодировки файлов отчётов

В веб-приложении **Рупор.БЛИЦ** существует возможность сохранять отчёты, которые содержат результаты оповещения абонентов (см. руководство пользователя **Рупор.БЛИЦ**). Файлы отчётов сохраняются с расширением CSV. По умолчанию файлы отчётов имеют кодировку **Кириллица (Windows-1251)**. Кодировку можно изменить на **UTF-8**.

Чтобы изменить кодировку файлов отчётов, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.
2. В консоли операционной системы выполните команду ***set_csv_encoding UTF-8***.

Чтобы снова установить кодировку **Кириллица (Windows-1251)**, выполните команду ***set_csv_encoding CP1251***.

10.8.2 Настройка формирования отчёта при отсутствии HASP-ключа

Чтобы при старте комплекса оповещения при отсутствии HASP-ключа выставлялось состояние **SYSTEM FAILURE** для всех незавершённых оповещений, выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.

   В консоли операционной системы выполните команду ***touch /opt/rupor2/conf/terminate-tasks-on-protection-error***.

Если при следующей загрузке системы HASP-ключ не будет найден, то все незавершённые попытки оповещения получат состояние **SYSTEM FAILURE**, и будут созданы соответствующие отчёты.

10.9 Настройка транков

Настройка транков осуществляется из консоли операционной системы сервера. Для подключения используется SSH-клиент. Вход в систему осуществляется под учетной записью **rupor_admin**.

Комплекс **Рупор.БЛИЦ** принимает все входящие вызовы по всем настроенным транкам.

10.9.1 Просмотр списка транков

Для просмотра списка существующих транков используется команда ***show_trunks***.

10.9.2 Добавление транка

Чтобы новые транки использовались в оповещении, они должны быть сконфигурированы в системе Asterisk (см. раздел 9 ИНТЕГРАЦИЯ С АТС).

При добавлении нового транка убедитесь в наличии свободных лицензированных каналов. Если на момент добавления транка все лицензированные каналы уже заняты, транк будет неактивным, и максимальное количество одновременных вызовов по нему будет иметь нулевое значение.

При создании транка для проведения опросов необходимо учитывать количество лицензий на распознавание речи. Если лицензий на распознавание речи меньше, чем лицензий на каналы оповещения, то необходимо установить для транка ограничение на количество одновременных вызовов, равное количеству лицензий на распознавание речи (см. команду ***set_trunk_call_limit***).

Для добавления обычного или виртуального транка используется команда ***add_trunk name [asterisk_name ["description"]]***, где:

- ***name*** – уникальное имя транка, записанное латиницей. Если не указывается параметр ***asterisk_name***, то параметр ***name*** должен быть указан в формате **SIP/provider** или **dahdi/G1**. **SIP/provider** – формат имени транка, использующего технологию передачи данных по SIP (**provider** – это идентификатор клиента из файла ***/etc/asterisk/sip.conf***),

dahdi/G1 – формат имени транка, использующего технологию передачи данных с помощью цифрового канала E1. Имя транка должно состоять из сочетаний латинских букв и цифр , и не превышать 64 символов.

- ***asterisk_name*** – имя транка в конфигурации Asterisk, записанное латиницей. В имени транка должен быть указан тип транка: **SIP/provider** – формат имени транка, использующего технологию передачи данных по SIP (**provider** – это идентификатор клиента из файла ***/etc/asterisk/sip.conf***), **dahdi/G1** – формат имени транка, использующего технологию передачи данных с помощью цифрового канала E1.
- ***description*** – описание транка.

Недопустимо создание транков с одинаковыми именами.

Если указан параметр ***asterisk_name***, то при выполнении вызовов, которые должны идти через виртуальный транк, эти вызовы будут идти через реальный транк ***asterisk_name***. Это сделано для того, чтобы можно было ограничивать количество каналов, которые могут суммарно использовать некоторые оповещения.

Например, можно создать виртуальный транк, затем командой ***set_trunk_call_limit*** установить ограничение (например, 10 каналов), потом назначить этот транк какому-либо сценарию. В этом случае все оповещения, которые созданы по данному сценарию, не смогут использовать более 10 каналов суммарно.

10.9.3 Общие настройки транков

В таблице ниже приведён список команд, с помощью которых осуществляется общая настройка транков.

Команда	**Параметры**
Переименование транка	
rename_trunk name new_name [force]	***name*** – имя транка; ***new_name*** – новое имя транка; ***force = 1*** – переименовать транк, который назначен сценарию и в настоящее время используется для выполнения процесса оповещения. После переименования транка оповещения будут продолжаться с использованием нового имени транка.
Добавление или изменение описания транка	
set_trunk_description name "description"	***name*** – имя транка, ***description*** – описание транка.
Установка ограничения на количество одновременных вызовов по транку	

Команда	Параметры
set_trunk_call_limit name call_limit	***name*** – имя транка, ***call_limit*** – максимальное количество одновременных вызовов по выбранному транку.
Активация транка	
enable_trunk name	***name*** – имя транка.
Деактивация транка	
disable_trunk name	***name*** – имя транка.
Установка роли транка для резервирования	
set_trunk_backup_type name backup_type [use_only_for_backup]	***name*** – имя транка. ***backup_type*** – роль транка для резервирования: • **0** – транк не может быть использован как резервный; • **1** – транк может быть использован как резервный для отключенных транков; • **2** – транк может быть использован как резервный для отключенных транков или для транков, у которых не хватает емкости. ***use_only_for_backup = 1*** – признак использования транка только в качестве резервного (может быть полезен, например, при высокой стоимости услуг провайдера).
Установка приоритета транка	
set_trunk_priority name priority	***name*** – имя транка, ***priority*** – приоритет транка (от 1 до 1000). Более высокому значению параметра ***priority*** соответствует более высокий приоритет. Параметр ***priority*** определяет порядок распределения вызовов по транкам. Если сценарию не назначен транк, либо ресурсы назначенного транка исчерпаны, и в комплексе существует несколько резервных транков, оповещения будут выполняться с использованием транка с большим приоритетом. После достижения ограничения вывозов по данному транку, последующие оповещения будут выполняться с использованием транка со следующим в порядке убывания приоритетом.  Резервный транк используется для оперативного переключения на него в случае выхода из строя основного. Возможность использования резервных транков в качестве основных для избранных сценариев не предусмотрена.

Команда	Параметры
Получение информации о транке, назначенном сценарию	
assign_trunk scenario_id	***scenario_id*** – название сценария в формате ***USER:TEMPLATE***, где ***USER*** – учетная запись, от имени которой был создан сценарий, ***TEMPLATE*** – название сценария. Например: ***operator:scenario1***.
Назначение транка сценарию оповещения	
assign_trunk scenario_id [trunk_name [force_assign [reassign_active]]]	***scenario_id*** – название сценария в формате ***USER:TEMPLATE***, где ***USER*** – учетная запись, от имени которой был создан сценарий, ***TEMPLATE*** – название сценария. Например: ***operator:scenario1***. ***trunk_name*** – имя транка. ***force_assign***: • **1** – принудительно назначить транк сценарию, если ему уже назначен другой транк; • **0** – не назначать транк сценарию, если ему уже назначен другой транк. ***reassign_active***: • **1** – назначить транк всем активным оповещениям, в которых используется данный сценарий; • **0** – не назначать транк активным оповещениям.
Отмена назначения транка неактивным оповещениям	
assign_trunk scenario_id null 1	***scenario_id*** – название сценария в формате ***USER:TEMPLATE***, где ***USER*** – учетная запись, от имени которой был создан сценарий, ***TEMPLATE*** – название сценария. Например: ***operator:scenario1***.
Отмена назначения транка активным оповещениям	
assign_trunk scenario_id null 1 1	***scenario_id*** – название сценария в формате ***USER:TEMPLATE***, где ***USER*** – учетная запись, от имени которой был создан сценарий, ***TEMPLATE*** – название сценария. Например: ***operator:scenario1***.

Команда	Параметры
Удаление транка	
delete_trunk name [force]	***name*** – имя транка; ***force = null*** – удалить неиспользуемый транк; ***force = 1*** – удалить транк, который назначен сценарию и в настоящее время используется для выполнения процесса оповещения. При удалении используемого транка все телефонные соединения с абонентами, активные на момент выполнения команды, будут доведены до конца (если это возможно), либо завершатся с ошибкой. Все остальные абоненты, которые входят в оповещение (в том числе абоненты, которые оповещались в момент удаления транка и для которых остались попытки дозвона), будут оповещаться по всем доступным транкам.

Для дополнительных параметров основных команд (таких как ***force***, ***reassigne_active***, ***force_assign***), которые принимают значения ***0*** или ***1***, в случае если будет установлено значение отличное от ***0*** или ***1*** системой это будет восприниматься как ***1***.

10.9.4 Настройка транков для отправки SMS

Для управления транками используется команда ***sms_trunk operation [trunk_name [trunk_parameters]]***.

Возможные варианты команды:

Команда	Назначение
sms_trunk list	Посмотреть список всех транков
sms_trunk clear	Удалить все транки
sms_trunk add trunk_name trunk_type	Добавить транк, который будет находиться в отключённом состоянии. ***trunk_name*** – имя транка; ***trunk_type*** – ***GoIP*** или ***SMPP***.
sms_trunk enable trunk_name	Включить транк. ***trunk_name*** – имя транка.
sms_trunk disable trunk_name	Отключить транк. ***trunk_name*** – имя транка.
sms_trunk params trunk_name	Посмотреть параметры транка. ***trunk_name*** – имя транка. Получаемые параметры: ***SMPP_dest_addr_npi***; ***SMPP_dest_addr_ton***; ***SMPP_source_addr***;

Команда	Назначение
	SMPP_source_addr_npi; ***SMPP_source_addr_ton*** Параметры транка ***source*** и ***dest*** указывают соответствующие параметры для источника и получателя сообщений. Параметры транка ***npi*** и ***ton*** настраиваются в соответствии с требуемыми значениями, определяемыми провайдером.
sms_trunk set_prio trunk_name priority	Установить приоритет транка. ***trunk_name*** – имя транка; ***priority*** – приоритет транка (целое число от 0 до 30000).
sms_trunk set_param trunk_name reboot_schedule NN/hh:mm	Настроить расписание перезагрузки GSM-шлюза GoIP. ***trunk_name*** – имя транка; ***NN/hh:mm*** – расписание перезагрузки. Расписание можно настроить одним из трех способов: 1) Перезагрузка по определённым датам: ***DD/hh:mm***. Например, ***12/12:00*** – шлюз будет перезагружаться 12 числа каждого месяца в 12:00. 2) Перезагрузка каждый день в определённое время: ***00/hh:mm***. 3) Перезагрузка по определённым дням недели: ***day_of_week/hh:mm***. Например: ***Mo/11:00*** – шлюз будет перезагружаться по понедельникам в 11:00. Для обозначения дней недели используются двухбуквенные сокращения английских названий: Mo, Tu, We, Th, Fr, Sa, Su. Параметры расписания могут комбинироваться и перечисляться через запятую без пробелов. Например: ***sms_trunk set_param GoIP reboot_schedule Mo/11:00,00/18:00***.
sms_trunk set_param trunk_name dont_reboot_with_undelivered {0|1}	***trunk_name*** – имя транка. ***{0|1}***: ***1*** – не перезагружать GSM-шлюз GoIP до того момента, пока не будут получены отчёты о доставке всех SMS, которые были отправлены с данного шлюза ***0*** – перезагружать шлюз, даже если не получены отчёты о доставке всех SMS, которые были отправлены с данного шлюза

Команда	Назначение
sms_trunk set_param trunk_name param_name param_value	Установить параметры для транка. Список возможных параметров см. в таблице ниже. ***trunk_name*** – имя транка; ***param_name*** – имя параметра; ***param_value*** – значение параметра. Имена и значения параметров зависят от типа транка (***GoIP*** или ***SMPP***), но никак не проверяются.
sms_trunk delete trunk_name	Удалить транк. ***trunk_name*** – имя транка.

Список возможных параметров для транка:

Общие параметры	
logfile	Путь к файлу журнала. Изменять не рекомендуется
loglevel	Уровень журналирования: ***DEBUG***, ***INFO***, ***ERROR***
Параметры для типа GoIP	
local_port	Порт UDP, который будет использоваться для организации SMS-сервера и к которому будет подключаться GoIP (по умолчанию **44444**). Рекомендуется не менять, в том числе и потому, что межсетевой экран на сервере **Рупор.БЛИЦ** настроен так, что разрешены входящие пакеты на порт **44444**.
local_addr	Если параметр не задан, то IP-адрес определяется динамически при каждом запуске путём выбора первого нелокального IP-адреса из списка интерфейсов.
Параметры для типа SMPP	
host	IP-адрес SMPP-сервера
port	Порт SMPP-сервера, по умолчанию **2775**
username	Имя пользователя для соединения с SMPP-сервером
password	Пароль пользователя
session_timeout	Таймаут перезапуска сессии, в секундах (по умолчанию 600)
sms_limit	Количество «слотов» для отправки SMS (по умолчанию 100). После отправки очередного SMS-сообщения количество свободных «слотов» уменьшается. Затем комплекс ожидает получения информации о состоянии обработки SMS от SMPP-сервера. Состояние может быть окончательным («ошибка» или «доставлено») или промежуточным («принято для передачи»). «Слот» освобождается при получении информации о состоянии либо её отсутствии в течение времени ожидания отчёта о доставке. Когда все «слоты» заняты, SMS-сообщение остаётся в очереди на отправку.
message_rate	Число сообщений (в том числе частей составного сообщения), которые можно отправить в секунду (по умолчанию 5).

	Например, если используется значение по умолчанию, то за 1 секунду можно отправить 5 коротких сообщений (до 70 символов) либо 1 длинное сообщение, состоящее из 350 символов. Чтобы отключить это ограничение, установите значение 0.
smpp_type	Тип подключения, зависящий от провайдера SMPP. Допустимые значения: ***transceiver*** (значение по умолчанию) – для передачи сообщений на SMPP-сервер и для приёма сообщений от SMPP-сервера используется одно TCP-соединение; ***transmitter/receiver*** – для связи с SMPP-сервером используется два TCP-соединения: для передачи сообщений и для приёма сообщений.

Обратите внимание, что параметры, не приведенные в документации, являются внутренними и не подлежат изменению.

11 СОЗДАНИЕ ОПОВЕЩЕНИЙ

Перед созданием оповещений необходимо выполнить действия по настройке комплекса, описанные в разделе 5 ПОРЯДОК ДЕЙСТВИЙ ПО УСТАНОВКЕ И НАСТРОЙКЕ данного руководства.

В комплексе **Рупор.БЛИЦ** предусмотрены следующие способы создания оповещений:

1. С помощью веб-приложения **Рупор.БЛИЦ**.
2. Посредством загрузки *файлов оповещений* в веб-приложение **Рупор.БЛИЦ** вручную.
3. Посредством автоматической загрузки *файлов оповещений* в комплекс **Рупор.БЛИЦ**.

11.1 Создание оповещений с помощью веб-интерфейса

Создание оповещений с помощью веб-приложения описано в руководстве пользователя **Рупор.БЛИЦ**.

11.2 Создание оповещений посредством загрузки файлов оповещений

Для создания оповещений в комплексе **Рупор.БЛИЦ** могут быть использованы файлы оповещения.

Файл оповещения – это файл в формате CSV, который создается сотрудником, осуществляющим интеграцию комплекса **Рупор.БЛИЦ** со сторонней системой. Файл содержит данные абонентов для оповещения, тексты сообщений, которые необходимо озвучить и/или доставить абонентам, название сценария оповещения, дату и время начала оповещения.

Файл оповещения может загружаться в комплекс **Рупор.БЛИЦ** вручную или автоматически.

Чтобы осуществить оповещение абонентов с помощью файла оповещения, необходимо выполнить следующие действия:

1. Если оповещение абонентов следует выполнить по телефону с помощью предзаписанного голосового сообщения, администратору комплекса необходимо создать данное сообщение с помощью веб-приложения **Рупор.БЛИЦ** (см. руководство пользователя **Рупор.БЛИЦ**).

   Преимущество предзаписанного сообщения заключается в том, что оно может использоваться в неограниченном количестве оповещений. Если необходимости в создании предзаписанного сообщения нет, текст сообщения, который должен быть озвучен абонентам по телефону, может быть указан непосредственно в *файле оповещения*.
2. С помощью веб-приложения администратору комплекса следует создать сценарий оповещения.
3. С помощью ПО интеграции сотруднику, выполняющему интеграцию комплекса **Рупор.БЛИЦ** со сторонней системой, следует создать *файл оповещения* (см. руководство по интеграции **Рупор.БЛИЦ**).
4. *Файл оповещения* должен быть запущен на выполнение одним из следующих способов:
   - Загружен администратором комплекса в веб-приложение вручную.

- Загружен автоматически в сетевую папку ***incoming***, расположенную в файловой системе **Рупор.БЛИЦ**.

Управление выполнением созданных оповещений осуществляется администратором с помощью веб-приложения **Рупор.БЛИЦ**.

Отчёты о результатах оповещений, запущенных на выполнение путём загрузки *файлов оповещений* в сетевую папку ***incoming***, сохраняются в сетевую папку ***outgoing***.

Ошибки, которые могут возникнуть при обработке файлов оповещений, описаны в руководстве по интеграции комплекса **Рупор.БЛИЦ**.

12 ПОДГОТОВКА ЖУРНАЛОВ РАБОТЫ

Перед обращением в службу технической поддержки ООО «ЦРТ-инновации» необходимо подготовить к отправке журналы работы комплекса **Рупор.БЛИЦ**. Для этого выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.

   В консоли операционной системы наберите команду ***get_rupor_logs***.

После выполнения этой команды все журналы работы комплекса оповещения будут сохранены в сетевой папке ***outgoing*** на сервере комплекса в виде архива ***rupor2-logs.zip***.

13 ВОЗМОЖНЫЕ ПРОБЛЕМЫ И СПОСОБЫ ИХ РЕШЕНИЯ

Далее приведены проблемы, которые могут возникнуть в процессе работы комплекса **Рупор.БЛИЦ**.

13.1 Отсутствие доступа к файловой системе

В случае отсутствия доступа к папкам ***incoming*** и ***outgoing*** убедитесь, что вводимые IP-адрес или имя сервера комплекса оповещения и авторизационные данные корректны.

Если используемые IP-адрес или имя сервера комплекса оповещения и авторизационные данные корректны, проверьте работоспособность пакета программ **samba**. Для этого:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.

   В консоли операционной системы выполните команду ***service smb status*** и убедитесь, что служба ***smbd*** находится в статусе ***running***.

   Выполните команду ***smbstatus*** и убедитесь, что со службой **samba** есть установленные соединения.

Для получения более подробной информации о работе с программным модулем **samba** обратитесь на сайт разработчика http://www.samba.org/.

Если установить причину не удалось, свяжитесь со службой технической поддержки ООО «ЦРТ-инновации».

13.2 Обработка файла оповещения завершилась с ошибкой

Если обработка файла оповещения завершилась с ошибкой, перейдите в папку ***incoming*** и найдите файл с расширением ***.csv.errormessage***, имя которого идентично имени файла оповещения, завершившегося с ошибкой.

Просмотрите содержимое файла.

Если файл был обработан неуспешно из-за ошибки оператора, строка в файле ***.csv.errormessage*** имеет вид:

CLIENTERROR: < тексты сообщений об ошибках в кодировке UTF-8, разделенные |>.

Причина: файл имеет неверный формат или данные в файле заданы некорректно. Ознакомьтесь с описанием возможных ошибок и способами их решения в руководстве по интеграции комплекса **Рупор.БЛИЦ**.

Если файл был обработан неуспешно из-за ошибки комплекса **Рупор.БЛИЦ**, строка в файле имеет вид:

SERVERERROR: <текст сообщения об ошибке в кодировке UTF-8>.

Данная ошибка может возникнуть при системном сбое на сервере **Рупор.БЛИЦ**. Для решения проблемы свяжитесь со службой технической поддержки ООО «ЦРТ-инновации» и предоставьте журналы работы комплекса для анализа.

13.3 Ситуация не активируется по телефону

Чтобы узнать причину, по которой ситуацию не удалось активировать по телефону, ознакомьтесь с содержимым файла ***/var/rupor2/log/phone_activate_situation.log***.

Пример фрагмента файла:

Tue Dec 11 16:01:46 2012 can't find situation code 59 for user oper1

Tue Dec 11 16:01:46 2012 file /var/rupor2/share/situation/in/oper1-59.csv.processed does not exist

Tue Dec 11 16:01:46 2012 file store/oper1/59.csv is not readable

Tue Dec 11 16:01:46 2012 file store/oper1/59.type is not readable

13.4 Список контактов обработан успешно, но во время оповещения присутствовала систематическая ошибка

В случае систематического возникновения ошибки *для телефонных оповещений* проверьте правильность настроек компонента Asterisk. Для этого выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.

   Проанализируйте файл ***/var/rupor2/log/asterisk/messages*** на наличие ошибок и предупреждений.

В случае систематического возникновения ошибки *для SMS-оповещений* выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.

   Проанализируйте файл ***/var/log/rupor2/smssender.log*** на наличие ошибок.

В случае систематического возникновения ошибки *для Email-оповещений* выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.

   Проанализируйте файл ***/var/log/rupor2/mailsender.log*** на наличие ошибок.

Если установить причину не удалось, свяжитесь со службой технической поддержки ООО «ЦРТ-инновации» и предоставьте журналы работы комплекса **Рупор.БЛИЦ** для анализа (см. раздел 12 ПОДГОТОВКА ЖУРНАЛОВ РАБОТЫ).

13.5 Проблемы со звуком (оповещения не слышно)

Если при оповещении не слышно звука, убедитесь, что комплекс **Рупор.БЛИЦ** и АТС (или клиентское оборудование) используют совместимые кодеки для звука.

Со стороны клиента на телефоне, подключенном к комплексу **Рупор.БЛИЦ** напрямую, должен быть включен только тот кодек, в котором происходит оповещение. Например, по умолчанию, для peer

0000 в asterisk на **Рупор.БЛИЦ** разрешен только ulaw. В остальных случаях используются настройки VoIP АТС.

При возникновении каких-либо проблем свяжитесь со службой технической поддержки ООО «ЦРТ-инновации» и предоставьте журналы работы комплекса **Рупор.БЛИЦ** для анализа.

13.6 Транки настроены, ситуация активируется, но телефонный вызов не идёт

Убедитесь, что в системе не установлено нулевое значение максимально допустимого количества голосовых каналов, что могло произойти в случае нарушения порядка действий, описанного в п. 5 данного руководства.

Для этого выполните следующие действия:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.

2. В консоли операционной системы выполните команду **show_constants [часть_названия_константы]** (например: *show_constans chan*) и убедитесь, что значение **max_voice_channels** не равно нулю.

3. В случае нулевого значения измените значение **max_voice_channels** на положительное (см. п. 10.6.3 данного руководства).

Если предлагаемое решение не помогло, свяжитесь со службой технической поддержки ООО «ЦРТ-инновации» и предоставьте журналы работы комплекса **Рупор.БЛИЦ** для анализа (см. раздел 12 ПОДГОТОВКА ЖУРНАЛОВ РАБОТЫ).

13.7 Некорректное восстановление базы данных из резервной копии

Некорректное восстановление может быть связано с неполным удалением разделов БД повреждённой версии в следствие аппаратного либо программного сбоя. В этом случае рекомендуется перед восстановлением произвести полное удаление повреждённой БД для чего:

1. Выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**.

2. В консоли операционной системы выполните команду **clear_db**. Затем выполните команду **reboot** для перезагрузки системы.

После выполнения команды **clear_db** из базы данных будет удалена вся информация и пароль будет изменен на стандартный

3. После перезагрузки войдите в веб-интерфейс системы с использованием учётной записи администратора и произведите повторное восстановление БД в соответствии с указаниями руководством пользователя системы.

Если устранить проблему корректного восстановления БД не удалось, свяжитесь со службой технической поддержки ООО «ЦРТ-инновации».

13.8 Сообщение в отчёте "Успешная длительность больше допустимой длительности вызова"

В том случае, если длительность конкретного голосового сообщения (с учётом процента, заданного в качестве критерия успешности), превышает допустимую максимальную длительность оповещения (см. п. 10.6.4 Настройка длительности оповещения) система не будет совершать ни одной попытки вызова. При этом данному оповещению в отчёте проставляется состояние **Не оповещен по телефону**, а попытке оповещения – **Успешная длительность больше допустимой длительности вызова**.

Если данная ситуация имеет тенденцию к повторению, значит значение параметра **MaxTimeCall** было установлено неверно, без учёта реальной практики использования комплекса. В этом случае рекомендуется изменить значение параметра в большую сторону.

Следует обратить внимание, что увеличение значения параметра **MaxTimeCall** может приводить к увеличению общего времени, требуемого для оповещения всех абонентов.

В том случае, если такая ситуация является исключительной и для соблюдения общих сроков оповещения допустимо игнорировать превышения для отдельных оповещений необходимо выполнить корректирующие действия. Для этого:

– выполните подключение к операционной системе сервера через SSH-клиент под учетной записью **rupor_admin**;

– выполните команду **set_constant dialer_force_fail_if_duration_is_too_large 0**. В этом случае система **Рупор.БЛИЦ** будет совершать вызовы и принудительно завершать их по окончанию допустимой длительности в соответствии с значением параметра **MaxTimeCall**, независимо от длительности конкретного голосового сообщения.

ПРИЛОЖЕНИЕ А ОСОБЕННОСТИ ОТПРАВКИ SMS

Рассылку SMS рекомендуется осуществлять по SMPP-протоколу.

При отправке SMS-оповещений с помощью VoIP GSM-шлюза GoIP1/GoIP4 следует соблюдать следующие требования:

- Одно оповещение должно содержать не более 300 SMS.
- Длина одного SMS при этом не должна превышать 250 символов.

Оповещения, не удовлетворяющие этим требованиям, рекомендуется проводить через SMPP, в противном случае доставка SMS-сообщений не гарантируется.

В связи с особенностью работы SMS-протокола сообщения, содержащие более 70 символов кириллицей (140 латиницей), могут перемешиваться друг с другом как на конечном устройстве, так и в SMS-центре оператора.

Возможные способы решения:

- Не отправлять составные SMS.
- При использовании GSM-шлюза GoIP1/GoIP4 в настройках шлюза выставить время жизни SMS-сообщения не более 24 часов (см. раздел 8 ПОДКЛЮЧЕНИЕ И НАСТРОЙКА GSM-ШЛЮЗА).

При отправке каждая часть длинного SMS тарифицируется сотовыми операторами **отдельно**.

ООО «ЦРТ-инновации» не несет ответственности за недоставку SMS-сообщения по вине оператора и не может гарантировать доставку и прочтение SMS. Статистика отправки/доставки сообщения целиком и полностью опирается на данные, предоставленные мобильным оператором.

В случае преднамеренной либо непреднамеренной перезагрузки сервера во время проведения им рассылки SMS ввиду недоступности данных от SMS-центра оператора сотовой связи за период простоя, все SMS, для которых на момент отключения сервера не были получены подтверждения о доставке, будут отправлены повторно с целью избежания неоповещения абонентов по указанной технической причине.

ПРИЛОЖЕНИЕ Б СВЕДЕНИЯ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для защиты комплекса **Рупор.БЛИЦ** от несанкционированного доступа и нарушений штатной работы рекомендуется соблюдать приведённые ниже рекомендации по администрированию ОС, настройке сетевого взаимодействия и управлению учётными записями пользователей.

Установка и обновление ПО

Операционная система **CentOS** и все программные компоненты, необходимые для работы комплекса оповещения **Рупор.БЛИЦ**, содержатся в комплекте поставки. Не рекомендуется устанавливать на сервер комплекса дополнительное ПО во избежание конфликтов программных и вычислительных ресурсов.

В комплексе не предусмотрено автоматическое обновление каких-либо программных компонентов и ОС в целом. Обновлять ОС рекомендуется только в случае крайней необходимости (например, при выявлении критических уязвимостей).

Обновление микропрограммного ПО сервера комплекса выполняется по усмотрению владельца оборудования. Единственное требование – это совместимость микропрограммного ПО с операционной системой, поставляемой в составе дистрибутива **Рупор.БЛИЦ** (**CentOS 7** разрядностью 64 бита).

Антивирусная защита

Комплект поставки **Рупор.БЛИЦ** не содержит каких-либо средств антивирусной защиты. Их установка нецелесообразна и не должна проводиться самостоятельно. По умолчанию в комплексе настроен межсетевой экран, однако предполагается, что **Рупор.БЛИЦ** эксплуатируется в пределах доверенной сети с централизованными средствами антивирусной защиты.

Параметры сетевого взаимодействия

Ниже перечислены порты, которые должны быть открыты на сервере комплекса для обеспечения взаимодействия компонентов. Открытость входящего порта предполагает сохранение состояния, то есть комплекс **Рупор.БЛИЦ** должен иметь возможность отправлять ответы в рамках сеанса.

Порт	Протокол	Направление	Назначение
22	TCP	Входящий	Доступ через SSH-клиент к ОС сервера
5060	TCP, UDP	Входящий/исходящий (в зависимости от способа подключения к АТС)	Приём/передача SIP-трафика
Диапазон портов от 10000 до 20000	UDP	Входящий/исходящий	Приём/передача RTP-трафика

Порт	Протокол	Направление	Назначение
44444	UDP	Входящий	Работа GSM-шлюза с SMS. Этот порт не должен быть доступен из внешней сети, т.к. шлюз располагается во внутренней сети.
443	TCP	Входящий	Доступ пользователей к веб-приложению по протоколу HTTPS
80	TCP	Входящий	Доступ пользователей к веб-приложению по протоколу HTTP
137	UDP	Входящий	Работа с файлами с помощью пакета программ **Samba** в режиме интеграции (получение заданий и выдача отчётов)
138	UDP	Входящий	
139	TCP	Входящий	
445	TCP	Входящий	

Если комплекс используется для отправки сообщений по электронной почте, то дополнительно необходимо обеспечить доступ к SMTP-серверу (номер порта по умолчанию – 25).

Если комплекс используется для отправки SMS по протоколу SMPP, то дополнительно необходимо обеспечить доступ к SMPP-серверу (номер порта по умолчанию – 2775).

Разграничение прав пользователей

Для работы с комплексом применяются учётные записи пользователей, создаваемые администратором с помощью веб-приложения **Рупор.БЛИЦ**. Рекомендуется для каждого пользователя создавать отдельную учётную запись.

При создании учётной записи необходимо назначить пользователю права доступа к определённым функциям комплекса. Это позволяет разграничить полномочия пользователей в соответствии с их задачами, а также защитить данные, с которыми работают пользователи, от изменения, просмотра и модификации другими пользователями.

Для администратора предусмотрена встроенная учётная запись с полным набором прав (см. раздел 1.3 Параметры доступа). Рекомендуется непосредственно после установки комплекса сменить пароль администратора.

Пользователи могут самостоятельно изменять свои пароли средствами веб-приложения. Строгих требований по структуре, сложности пароля и периодичности изменения пароля не предъявляется.

Дополнительная информация о регистрации учётных записей приведена в руководстве пользователя веб-приложения **Рупор.БЛИЦ**.

ПРИЛОЖЕНИЕ В ПЕРЕЧЕНЬ ИЗМЕНЯЕМЫХ ПАРАМЕТРОВ

В таблице ниже приведён перечень изменяемых параметров комплекса. Просмотр перечня параметров также доступен с помощью команды ***show_constants***. При наличии более подробного описания параметра в тексте настоящего руководства, последний столбец таблицы содержит ссылки на соответствующие разделы.

Параметр	Значение по умолчанию	Описание	См. также
CSV_text_encoding	CP1251	Кодировка текста в CSV-файлах; для изменения используйте команду ***set_csv_encoding***	10.8.1
MaxTimeCall	300	Максимальная длительность телефонного соединения, после которой вызов будет принудительно завершён	10.6.4
Timezone	GMT+3	Локальный часовой пояс; для изменения используйте команду ***set_default_tz***	10.2.6
answer_timeout	60	Время ожидания ответа абонента в секундах	10.6.5
default_activation_delay	120	Период задержки между активацией ситуации и фактическим началом оповещения, предлагаемый по умолчанию при создании ситуации	10.5.2
dialer_force_fail_if_duration_is_too_large	1	Установить для оповещения состояние «Не оповещен по телефону», если для успешного оповещения необходимо прослушать сообщение длительностью более ***MaxTimeCall***	10.6.4
enable_phone_message_recording	1	***1*** – разрешить запись голосовых сообщений, ***0*** – запретить запись голосовых сообщений. Для изменения используйте команду ***enable_recording_of_messages***	10.7.4
h350_confirmation_timeout	5	Период ожидания подтверждающего замыкания/размыкания контакта устройства STC-H350 (в секундах)	10.5.2
h350_play_sound_when_confirmation_needed	0	***1*** – воспроизводить звуковой сигнал во время ожидания подтверждающего замыкания/размыкания контакта устройства STC-H350; ***0*** – не воспроизводить звуковой сигнал.	–
IfTimeTask	15	Срок хранения отчётов о результатах оповещения, проводимого в режиме интеграции (в днях)	–

Параметр	Значение по умолчанию	Описание	См. также
mail_auth_domain	–	Домен пользователя, для изменения используйте команду ***set_mail_auth***	10.3.2
mail_auth_id	–	Имя пользователя, для изменения используйте команду ***set_mail_auth***	10.3.2
mail_auth_method	NONE	Тип аутентификации на почтовом сервере, для изменения используйте команду ***set_mail_auth***	10.3.2
mail_auth_password	–	Пароль пользователя, для изменения используйте команду ***set_mail_auth***	10.3.2
mail_from	Alert System	Адрес отправителя, для изменения используйте команду ***set_mail_from***	10.3.3
mail_host	–	Доменное имя/IP-адрес SMTP-сервера, для изменения используйте команду ***set_mail_host***	10.3.1
mail_port	25	TCP-порт для доступа к SMTP-серверу, для изменения используйте команду ***set_mail_host***	10.3.1
mail_subject	Оповещение: %task_name%	Тема сообщения	–
max_upload_size	15728640	Максимальный размер голосового сообщения, загружаемого из внешнего источника при работе в режиме интеграции (в байтах)	–
max_voice_channels	–	Максимальное количество одновременных голосовых вызовов. Значение присваивается при первоначальном запуске равным разрешенному количеству каналов на ключе защиты, для изменения используйте команду ***set_max_voice_channels***	10.6.3
min_free_space	30720	Минимально допустимое свободное место в папке ***incoming*** для работы в режиме интеграции (в КБ)	–
phone_activation_code_length	2	Длина кода для активации ситуации по телефону, для изменения используйте команду ***set_phone_activation_code_length***	10.7.3
phone_password_length	4	Длина ТПИН для доступа к комплексу оповещения по телефону, для изменения используйте команду ***set_tpin_length***	10.7.1
recipient_priority_max	2	Максимальное числовое значение приоритета оповещения абонента (минимальный приоритет)	10.4.4

Параметр	Значение по умолчанию	Описание	См. также
recipient_priority_min	0	Минимальное числовое значение приоритета оповещения абонента (максимальный приоритет)	10.4.4
recipient_pin_length	4	Максимальная длина личного ПИН-кода абонента	10.4.5
sms_max_len	250	Максимальная длина сообщения для SMS	–
sms_pause_between_messages	0.1	Пауза между отправками SMS (в секундах, можно использовать нецелые числа)	–
text_max_len	1000	Максимальная длина сообщения для синтеза или email	–
use_all_phones_when_phone_types_is_not_set	0	Поведение комплекса оповещения в случае, если при активации ситуации не указаны типы телефонов: ***1*** – использовать все телефоны; ***0*** – использовать только те телефоны, для которых не указан тип.	10.5.1
web_session_timeout	86400	Время длительности сессии в веб-приложении **Рупор.БЛИЦ** (в секундах)	10.4.1

ПРИЛОЖЕНИЕ С ОСОБЕННОСТИ ВНЕДРЕНИЯ КОМПЛЕКСА С УЧЁТОМ СПЕЦИФИКИ ПРИМЕНЯЕМЫХ СПОСОБОВ ЗАЩИТЫ ПО

Особенности внедрения комплекса в технологическое окружение вытекают из специфики применяемых схем защиты программного обеспечения и используемых ключей защиты.

Использование ключа защиты HASP HL Pro

Стандартным способом защиты ПО от нелицензионного использования является аппаратный ключ защиты HASP HL Pro, устанавливаемый непосредственно в сервер комплекса и взаимодействующий с ним через USB-порт. Указанный способ защиты является наиболее надёжным и не зависящим от конфигурации конкретного сервера. Основным ограничением данного способа защиты в приложении к использованию комплекса в виртуальной среде является необходимость обеспечения доступности USB-порта для ПО комплекса (т.н. «проброса» USB порта в виртуальную машину), требующая настройки гипервизора, а также необходимость запрета миграции виртуальной машины между аппаратными серверами во избежание потери соединения ПО с ключом защиты (при многосерверной конфигурации).

Использование ключа защиты HASP SL Pro

При невозможности использования аппаратного ключа защиты, по согласованию с технической поддержкой ООО «ЦРТ-инновации», ПО комплекса может использоваться с программным ключом HASP SL Pro. Основным определяющим недостатком данного способа защиты является привязка программного ключа к широкому набору параметров физического сервера, на который устанавливается ключ, для обеспечения невозможности копирования. Соответственно внесение любого изменения в изначальные физические параметры сервера после активации ключа, например, в случае ремонта, замены или апгрейда аппаратных компонентов, а также при миграции виртуальной машины на другой аппаратный сервер приведут к блокировке ключа защиты с невозможностью его дальнейшего использования и остановке функционирования комплекса. Достоинством данного способа защиты является только отсутствие физически извлекаемого ключа и необходимости настройки «проброса» USB порта в виртуальную машину.

Использование ключа защиты HASP HL Net

В исключительных случаях, при необходимости развёртывания ПО комплекса в виртуальной среде с миграцией виртуальных машин между аппаратными серверами, при невозможности фиксации виртуальной машины на конкретном физическом сервере, по согласованию с технической поддержкой ООО «ЦРТ-инновации» может применяться аппаратный сетевой ключ защиты HASP HL Net. Определяющим недостатком данного способа защиты является потребность в непрерывном сетевом соединении между ПО комплекса и ключом, что может быть обеспечено только высокоразвитой, корректно настроенной, сетевой инфраструктурой. Достоинством HASP HL Net является его независимость от параметров физического сервера подобная стандартному ключу HASP HL Pro.

Обрыв сетевого соединения или выход из строя сервера лицензирования, в который установлен ключ, приведёт к остановке функционирования комплекса. Поэтому рекомендуется размещать сервер лицензирования с ключом защиты в одной подсети с комплексом **Рупор.БЛИЦ**, обеспечив возможность широковещательных рассылок и взаимообмена TCP/UDP трафиком между ПО комплекса и ключом защиты по порту 1947.

Любые преднамеренные или непреднамеренные события и/или действия пользователя, приведшие к порче ключа защиты и/или нарушению сетевого взаимодействия между ключом защиты/сервером лицензирования и ПО комплекса, не являются предметом стандартной технической поддержки продукта и не покрываются какими-либо обязательствами ООО «ЦРТ-инновации». Т.е. принимая осознанное решение по использованию HASP SL Pro или HASP HL Net, Пользователь принимает на свой счёт все сопутствующие использованию ключа риски и потенциальные последствия рисковых событий.