

ООО «ЮНИТЕЛ»

**УЗЕЛ ВЕРИФИКАЦИИ
ЕПВВ ИС «АНТИФРОД»
ЮНИТ TS-AF**

Руководство пользователя

Версия 2.7

Москва 2024 г.

1. ВВЕДЕНИЕ

Узел верификации (УВр) Единой платформы верификации вызовов (ЕПВВ) ИС «Антифрод» ЮНИТ TS-AF предназначен для организации подключения оборудования оператора связи (ОС) к сети ЕПВВ ИС «Антифрод» в целях исполнения требований Постановления Правительства Российской Федерации от 03 ноября 2022 г. № 1978 «Об утверждении требований к системе обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования и Правил функционирования и взаимодействия системы обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования с информационными системами и иными системами, в том числе с системами операторов связи» и Постановления Правительства Российской Федерации от 03 ноября 2022 г. № 1979 «Об утверждении Правил направления в систему обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования и получения из указанной системы сведений».

Узел верификации ЮНИТ TS-AF разработан на основании Технических требований на подключение операторов связи к информационной системе «Антифрод», протоколов взаимодействия «центральный узел - узел верификации» (1137847334745.63.11.1.2023.1.001.ПВ.01), «узел верификации — узел взаимодействия (IP)» (1137847334745.63.11.1.2023.1.001.ПВ.09), «Методических указаний по пропуску вызовов» (1027739334479.63.11.1.2024.2.001.ПВ.10), с учетом «Технических условий на подключение к системе обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования».

2. ОБЩИЕ СВЕДЕНИЯ

Узел верификации ЮНИТ TS-AF представляет собой программно-аппаратный комплекс (ПАК), состоящий из серверной платформы, выбираемой сообразно решаемым на узле связи ОС задачам, и специального программного обеспечения (СПО), реализующего протоколы обмена с ИС «Антифрод» и взаимодействие с оборудованием ОС и БД.

Сервер поставляется высотой 1U или 2U для установки в 19» стойку.

С одной стороны УВр подключается к СОМ или IP портам АТС (для оборудования ЮНИТ TS-004), а с другой стороны — к IP-сети предприятия для дальнейшего выхода в сеть VipNet. Также УВр в своем составе имеет встроенный RADIUS и REST серверы. То есть имеется возможность подключать оборудование сторонних производителей по протоколам RADIUS и HTTP (REST) API. Вэтом случае УВр будут выступать в качестве «облачного» узла и может обслуживать несколько разных операторов связи.

При включении ПАК УВр СПО загружается автоматически и функционирует как служба (демон linux). В штатном режиме СПО не требует внимания оператора. При возникновении аварийных ситуаций на почтовый ящик технического персонала будет отправлено соответствующее уведомление.

3. РАБОТА С СПО УВр

В процессе работы может возникнуть ситуация, требующая выполнения ручных операций по загрузке/остановке демона СПО УВр. Для этих целей предусмотрены команды управления загрузкой СПО.

Модуль СПО называется **uvrd** и располагается в директории `/usr/local/bin`. При старте операционной системы этот модуль загружается автоматически. Для того, чтобы его принудительно остановить, необходимо выполнить команду:

`sudo /etc/init.d/uvrd.sh stop`

Запуск осуществляется командой **`sudo /etc/init.d/uvrd.sh start`**

Для перезагрузки необходимо выполнить команду **`sudo /etc/init.d/uvrd.sh restart`**

Существует возможность перечитать настройки конфигурационного файла, не перезагружая демон и, тем самым, не прерывая работу СПО. Для этой цели существует команда

`sudo /etc/init.d/uvrd.sh reload`

Для получения справки по командам необходимо набрать

`sudo /etc/init.d/uvrd.sh help`

В процессе функционирования СПО УВр связывается с SFTP сервером ЦСУ для обмена необходимыми данными. Некоторые операции, например, загрузка справочников номеров, может занимать длительное время. Для того, чтобы не прерывать такие операции, добавлены команды безопасного останова/перезагрузки демона `uvrd`. Для безопасного останова необходимо выполнить

`sudo /etc/init.d/uvrd.sh sstop,`

для перезагрузки -

`sudo /etc/init.d/uvrd.sh srestart.`

4. НАСТРОЙКА СПО

Настройка значений параметров модуля **uvrd** осуществляется через конфигурационный файл `/etc/uvrd/uvrd.conf`.

Ниже представлен вариант содержимого файла `uvrd.conf` с комментариями:

<code>[general]</code>	; основная секция
<code>log_out=0x06</code>	; маска направления вывода
	; диагностических данных
	; 0x01 — в порт отладки,
	; 0x02-в файл, 0x04 — в консоль
<code>log_level=2</code>	; уровень детализации вывода сообщений
<code>log_append=yes</code>	; удалять файл <code>uvrd.log</code> при перезагрузке
	; (no) или нет (yes)
<code>log_size=20K</code>	; размер log-файла для «ротации», то есть
	; при превышении указанного размера файл
	; будет сохранен под именем <code>uvrd.log.x</code> , где
	; x - следующий по порядку номер. Размер
	; указывается либо в байтах, либо с

log_cut_time=01:30	; применением модификаторов К - в ; килобайтах, М - в мегабайтах ; время «ротации» log-файла. В указанное ; время файл журнала будет усечен, если ; это необходимо
log_rotate=10	; количество сохраненных фрагментов log- ; файла после «ротации»
db_cut_time=00:30	; время суток для «очистки» БД
db_days=366	; срок хранения данных по соединениям в ; днях
addr_local="0.0.0.0"	; IP-адрес сетевого интерфейса, на котором ; будет запущен сервис ожидания ; поступления запросов на верификацию от ; УВз
local_port=8081	; IP-порт, на котором ожидается ; поступление запросов на верификацию от ; УВз
remote_port=8081	; IP-порт УВз
ats_num=2	; количество интерфейсов для подключения ; к АТС ЮНИТ
uvr_num=1	; количество поддерживаемых id УВр ; внутри одного физического УВр. ; УВр ОС может обслуживать более одного ; ID УВр. Выбор ID УВр осуществляется ; согласно установкам на ; соответствующем интерфейсе АТС для ; исходящих сообщений, либо согласно ; значению параметра Uvr_T для входящих ; сообщений. Параметры для УВр ; устанавливаются в соответствующей ; секции (см. ниже). Значение по-умолчанию ; равно 1.
encrypted=no	; включить (yes) или выключить (no) ; шифрование при обмене с УВз ; (serviceKey=0x81 при encrypted=yes)
hashed=yes	; включить (yes) или выключить (no) ; хэширование номера Б при запросе ; верификации
release_code=50	; значение кода разъединения
timeout_code=0	; значение кода при тайм-ауте ответа от ; УВз
error_code=0	; значение кода при ошибке
verify_own_number=yes	; проверка на принадлежность к номерной ; емкости ОС номера А при запросе

verify_own_a=yes

- ; верификации от удаленного УВр. Если эта
- ; опция выключена, то осуществляется
- ; проверка присутствия исходящего вызова
- ; на УВр с запрашиваемыми параметрами и
- ; отправка соответствующего результата
- ; (Continue, если вызов найден, Release, если
- ; не найден). Если опция включена, то
- ; проверяется принадлежность вызываемого
- ; номера из запроса к ОС. Если номер не
- ; принадлежит ОС, то на удаленный УВр
- ; отправляется сообщение об ошибке с
- ; кодом 5 «Номер не обслуживается.
- ; Ошибка конфигурации», а в БД
- ; сохраняется запись с кодом верификации 4
- ; «номер вызывающего абонента не
- ; обслуживается», на основании которого в
- ; последующем будет сформирован
- ; инцидент А. Если номер А принадлежит
- ; номерной емкости ОС, то выполняется
- ; операция поиска соответствующего
- ; вызова в реестре исходящих вызовов как
- ; это описано выше
- ; проверка на принадлежность к номерной
- ; емкости ОС номера А при входящем
- ; вызове.
- ; Если опция включена, то проверяется
- ; принадлежность вызываемого номера к
- ; номерной емкости оператора. Если номер
- ; принадлежит ОС, то осуществляется
- ; поиск исходящего соединения в реестре
- ; исходящих вызовов. Если вызов не найден,
- ; то происходит разъединение входящего
- ; вызова с кодом 50. если найден — вызов
- ; пропускается. При отключенной опции,
- ; такая проверка не осуществляется и вызов
- ; пропускается, так верификация вызовов со
- ; своей емкости в СИ «Антифрод» не
- ; производится. Данная возможность будет
- ; полезна для операторов с распределенной
- ; системой АТС, где номерная емкость ОС
- ; может обслуживаться территориально
- ; разнесенными узлами, а вызов между
- ; узлами проходит транзитом через сети
- ; связи сторонних операторов.

hash_on=yes	; включить «глобально» алгоритм ; хэширования
abc="495"	; глобальный параметр, содержащий ; значение ABC для нормализации номеров ; согласно E.164
w_size=1	; параметр «окна» одновременной отправки ; сообщений
ats_filtr=no	; фильтровать (yes)/пропускать (no) все ; сообщения от АТС ЮНИТ.
load_numbers=no	; опция загрузки БД номеров. Если значение ; установлено (yes), то файл numbers ; загружается при появлении в ; директории /numbers на SFTP. Если значение ; установлено в «no», то файл NUM_* не ; загружается и обновление БД номеров ; осуществляется только за счет данных из ; файлов DELTA_*
limit_sql=10000	; принудительное ограничение количества ; строк в операторе SELECT при ; формировании отчетов в ответ на запрос ; статистических данных. Значение «0» - не ; ограничивать
rest_addr="0.0.0.0"	; адрес сервера для приема запросов по ; протоколу REST (HTTP) API
rest_port=8085	; ip-порт сервера для приема запросов по ; протоколу REST (HTTP) API
radius_addr="0.0.0.0"	; адрес сервера для приема запросов по ; протоколу RADIUS
radius_port=1812	; ip-порт сервера для приема запросов по ; протоколу RADIUS
radius_secret="s3cr3t"	; пароль к RADIUS серверу
[timers]	; секция таймеров
main_timer=67	; таймер основного потока проверки ; наличия обновлений данных по ; операторам, УВр, УВз, запросам на ; выгрузку данных по соединениям
refresh_numbers=623	; таймер проверки обновлений данных ; numbers и delta
refresh_unload=854	; таймер выгрузки инцидентов и ; статистики
req_timer=1500	; тайм-аут ответа от УВз

call_timer=3600

; тайм-аут соединения. Максимальное время
; в секундах нахождения соединения в
; системе

[sftp]

; секция установок для обмена с SFTP-
; сервером ЕПБВ ИС «Антифрод»

private_key_path="grfc-key.pem"

; приватный ключ доступа к SFTP-серверу

in_path="/tmp"

; директория для загрузки и распаковки
; файлов с SFTP-сервера

pub_path="/home/unitel/run/database/pub"

; рабочая директория для хранения
; публичных ключей

out_path="/home/run/sftp"

; директория для подготовки и отправки
; файлов на SFTP-сервер

setup_path="/home/run/sftp/setup"

; директория для отправки SETUP-файла на
; SFTP-сервер ГРЧЦ. Для загрузки номерной
; емкости в БД ГРЧЦ достаточно
; положить в эту директорию
; сформированный согласно рекомендациям
; ГРЧЦ файл. Эта директория читается с
; периодичностью [timers].main_timer. При
; появлении в ней нового файла, он будет
; отправлен на SFTP-сервер и удален из
; этой директории

sftp_ip="198.51.100.228"

; IP-адрес SFTP-сервера

sftp_port=22

; IP-порт SFTP-сервера

sftp_timeout=2

; тайм-аут подключения к SFTP-серверу [с]

sftp_user="node_1067"

; имя (login) для доступа к SFTP-серверу

sftp_incidents="/incidents"

; далее следуют имена папок на SFTP-
; сервере, в которых располагаются файлы с
; данными ИС «Антифрод»

sftp_incidents_a="/incidents_a"

sftp_stats="/stats"

sftp_numbers="/numbers"

sftp_nodes="/nodes"

sftp_pub="/pub"

sftp_connections_requests="/connections/requests"

sftp_connections_responses="/connections/responses"

sftp_operators="/operators"

sftp_setup="/setup"

ping_on=yes

; запуск (yes) процесса тестирования
; доступности узла SFTP ЦСУ ГРЧЦ. При
; включенном параметре периодически
; осуществляется проверка связности по

ping_interval=10	; адресу sftp_ip. Если узел не доступен, то
ping_timeout=10	; подключение к SFTP не производится.
ping_attempts=3	; периодически посылки ping-пакета с
	; секундах
	; таймаут ожидания ответа на тестовый
	; пакет в секундах
	; количество неудачных попыток
	; тестирования после которых принимается
	; решение о недоступности узла
[last_numbers]	; секция описания номерной емкости, для
	; которой определяются
	; предустановленные ответы при запросе
	; входящей верификации. Применяется, если
	; необходимо выгрузить всю номерную
	; емкость, но для указанных номеров
	; состояния вызовов от коммутационного
	; оборудования пока не поступает
int_event=1	; тип ответа на запрос входящей
	; верификации: 0-отвечать continue, 1-не
	; отвечать (timeout), 2-отвечать release.
	; Применим для всех интервалов, если для
	; конкретного интервала не переопределен
int_num=1	; количество интервалов нумерации
int_0="74951234567-74959999999"	; интервал нумерации
int_event_0=2	; значение типа ответа для входящей
	; верификации для интервала 0.
[smtp]	; секция установок SMTP-клиента
on=yes	; включить SMTP-клиент
debug=no	; включить отладочный вывод
timer=1	; интервал отправки уведомлений в секундах
	; (при их наличии)
mail_to="info@ya.ru"	; почтовый адрес для доставки сообщения
mail_to_copy="unitalarm@ts004.ru"	; почтовый адрес для доставки сообщения
	; (копия)
mail_to_name="Unitels staff"	; имя адресата
[uvr_0]	; секция для 0-го ID УВр (по числу uvr_num)
uvr_id=1	; ID УВр
operator_id=11641	; идентификатор оператора (id_src)
private_rsa_key_path="1.pem"	; приватный ключ для симметричного
	; шифрования (используется при
	; encrypted=yes)

private_key_path="1-key.pem"

; приватный ключ для доступа к SFTP

[ats_0]

; секция 0-го интерфейса АТС (по числу

; ats_num)

type=1

; тип интерфейса (1-СОМ-порт, 0-IP-порт)

comport="/dev/ttyS0"

; имя устройства СОМ-порта

delay_tm=2000

; таймаут ожидания АТС ответа от УСП

cto_mono=no

; параметр «захвата» порта

uvr=0

; индекс УВр в списке обслуживаемых УВр

; (по числу uvr_num, больше 0 и меньше и

; равно uvr_num)

abc="495"

; значение ABC для нормализации номеров

; согласно Е.164

e4=11012

; установка значения ID оператора на

; поток E1

e5=11012

e6=11084

[ats_1]

type=0

; IP-адрес Ethernet порта АТС

ats_addr="XXX.XXX.XXX.XXX"

; IP-порт для подключения к Ethernet порту

ctrl_port=5503

; АТС

delay_tm=2000

cto_mono=no

e0=11012

e1=11012

e2=11084

int_event=1

; тип ответа на запрос входящей

; верификации: 0-отвечать continue, 1-не

; отвечать (timeout), 2-отвечать release.

; Применим для всех интервалов, если для

; конкретного интервала не переопределен.

; Параметры int_event, int_num,

; int_X,nt_event_X аналогичны глобальным

; установкам из секции [last_numbers] за

; исключением того, что они включаются в

; работу только при пропадании связи с АТС

; ЮНИТ, в секции которой они находятся

int_num=1

; количество интервалов нумерации

int_0="74951234567-74959999999"

; интервал нумерации

int_event_0=2

; значение типа ответа для входящей

; верификации для интервала 0.

<i>[ext_0]</i>	<i>; секция параметров подключения сервера</i>
	<i>; АТС к оборудованию (по числу ats_num)</i>
<i>local="0.0.0.0"</i>	<i>; адрес, на котором ожидают</i>
	<i>; подключения от сервер АТС</i>
<i>cdr_port=5501</i>	<i>; значения IP-портов для входящего</i>
	<i>; подключения по категориям</i>
<i>cto_port=5502</i>	
<i>ctrl_port=5503</i>	
<i>transcode=yes</i>	<i>; при включенном параметре (yes)</i>
	<i>; осуществляется перекодировка из Win1251</i>
	<i>; в UTF-8 и обратно</i>
<i>[ext_1]</i>	
<i>local="0.0.0.0"</i>	
<i>ctrl_port=5513</i>	

Значения параметров, выделенных жирным шрифтом, могут быть применены без остановки модуля **uvrd** с помощью команды **/etc/init.d/uvrd.sh reload**.

5. ОПИСАНИЕ ФАЙЛА UVRD.LOG

Файл журнала находится в директории **/var/log/uvrd/uvrd.log** и содержит вывод текущих операций СПО УВр. Анализ файла журнала позволяет контролировать работоспособность УВр.

Основная операция, которую выполняет УВр — это запрос верификации входящего вызова и ответ на запрос верификации входящего вызова.

Так, при поступлении входящего вызова на коммутационное оборудование оператора формируется запрос вида

```
(05.03.24 09:48:40) <= CHttpList::Sent out sock=21 to 198.51.100.3:8081 [POST /VerifyCallState HTTP/1.1
```

```
Host: 12.1.0.2
```

```
User-Agent: UNIT TS-AF
```

```
Content-Type: application/json
```

```
Content-Length: 193
```

```
{"request":{"serviceKey":      80,"uvrO":      1067,"uvrT":      1346,"sessionId":      "1AFEBCEC389B59D5","data":
"302241088000475989888202420A7E004463AB956F942C67430A7E0091F73DAAE02D048C","opcode": "Request"}}
] out=[5945532:271808598]
```

Результатом ответа на запрос будет

```
(05.03.24 09:48:40) => CIncomingCall::Recv from 198.51.100.3 sock=21: len=227 [HTTP/1.1 200 OK
```

```
Host: 11.1.1.24
```

```
Connection: close
```

```
Content-Length: 119
```

```
Content-Type: application/json
```

```
{"response":  
{"serviceKey":80,"uvrO":1067,"uvrT":1346,"sessionId":"1AFEBCEC389B59D5","data":"3000","opcode":"Continue"}}
```

если такой вызов найден и он должен быть пропущен.

Соответственно, входящий запрос верификации выглядит

```
(05.03.24 09:48:20) => CUvrNode::Recv from [198.51.100.2:39480]: len=291 [POST /VerifyCallState HTTP/1.1  
Host: 11.1.1.24  
Port: 8081  
Content-Length: 175  
Content-Type: application/json
```

```
{ "request": { "opcode": "Request", "uvrO": 11, "uvrT": 1067, "serviceKey": 80, "sessionId": "000b042b27ed7d35", "data":  
"301641088410479949499305420a7e00642242ef464958ed" } }
```

и ответ на него

```
(05.03.24 09:48:20) <= CHttpList::Sent in sock=21 to 198.51.100.2:39480 [HTTP/1.1 200 OK  
Host: 46.235.191.12  
User-Agent: UNIT TS-AF  
Content-Type: application/json  
Content-Length: 125
```

```
{"response":{"serviceKey": 80,"uvrO": 11,"uvrT": 1067,"sessionId": "000b042b27ed7d35","data": "3000","opcode":  
"Continue"}}
```

```
] in=[5945512:81594394] 4 ms
```

6. ФОРМАТ ОБМЕНА ПО ПРОТОКОЛУ REST API

Вызовы методов АПИ осуществляются с помощью HTTP POST запросов на адрес и порт REST API сервера, указанные в параметрах *rest_addr* и *rest_port* секции *[general]* файла конфигурации *uvrd.conf* соответственно.

В ответе на запрос могут передаваться поля *X-Error-Bits*, *X-Error-Messages*, *X-Warning-Bits*, *X-Warning-Messages*, в которых содержится дополнительная информация об ошибках и предупреждениях выполнения запроса. Поля *X-Error-Bits* и *X-Warning-Bits* содержат битовые поля, включающие шестнадцатеричные значения ошибок и предупреждений соответственно. В полях *X-Error-Messages* и *X-Warning-Messages* передается текстовая расшифровка битовых значений.

В текущей версии значения ошибок могут быть следующие:

```
0x00000001 - Header syntax error  
0x00000002 - Body syntax error  
0x00000004 - Not the owner of number A  
0x00000008 - Not the owner of number B  
0x00000010 - The owner of number A  
0x00000020 - The owner of number B
```

Значения предупреждений:

0x00000001 - Timeout

0x00000002 - Error

6.1. RegisterCall - Регистрация вызова

Регистрация вызова осуществляется HTTP POST запросом на адрес [\[http://x.x.x.x:8085/RegisterCall\]](http://x.x.x.x:8085/RegisterCall).

В запросе должны присутствовать следующие поля:

«a» - номер вызывающего абонента в формате E.164 (строка)

«b» - номер вызываемого абонента в формате E.164 (строка)

«id_dst» - идентификатор оператора связи согласно справочнику операторов, в сеть которого (в транк) осуществляется исходящий вызов (целое число)

«call_id» - уникальный идентификатор вызова (стока)

В случае успешной регистрации вызова будет возвращен HTTP Status code: **201** Created. В случае ошибки - HTTP Status code: **400** Bad Request. Подробная информация об ошибках содержится в X-Error-Bits, X-Error-Messages, X-Warning-Bits, X-Warning-Messages.

6.2. CheckCall - Верификация вызова

Верификация вызова осуществляется HTTP POST запросом на адрес [\[http://x.x.x.x:8085/CheckCall\]](http://x.x.x.x:8085/CheckCall)

Параметры запроса:

«a» - номер вызывающего абонента в формате E.164 (строка, обязательный)

«b» - номер вызываемого абонента в формате E.164 (строка, обязательный)

«c» - исходный (original) номер (до переадресации) вызываемого абонента в формате E.164 (строка, опциональный)

"d" - дополнительный номер вызываемого абонента, в формате E.164 (строка, опциональный)

«id_src» - идентификатор оператора связи согласно справочнику операторов, из сети которого (из транка) осуществляется входящий вызов (целое число, обязательный)

«call_id» - уникальный идентификатор вызова (стока, обязательный)

Возвращаемые значения:

- в случае успешной верификации вызова будет возвращен HTTP Status code: **200** OK
 - в случае неуспешной верификации вызова будет возвращен HTTP Status code: **404** Not found
 - в случае ошибки при обработке запроса будет возвращен HTTP Status code: **400** Bad Request.
- Подробная информация об ошибках содержится в X-Error-Bits, X-Error-Messages, X-Warning-Bits, X-Warning-Messages.

6.3. callUpdate - обновление вызова

Обновление вызова осуществляется HTTP POST запросом на адрес [\[http://x.x.x.x:8085/callUpdate\]](http://x.x.x.x:8085/callUpdate).

В запросе должны присутствовать следующие поля:

«**call_id**» - уникальный идентификатор вызова (стока)

Возвращаемые значения:

- в случае успеха будет возвращен HTTP Status code: **200** OK
- в случае ошибки будет возвращен HTTP Status code: **404** Not found

Подробная информация об ошибках содержится в X-Error-Bits, X-Error-Messages, X-Warning-Bits, X-Warning-Messages.

7. ФОРМАТ ОБМЕНА ПО ПРОТОКОЛУ RADIUS

Сервер обрабатывает RADIUS-запросы **Access-Request** с атрибутами:

h323-conf-id = "316004a8-571f97b3-cdd5364e-90ed2f02"

Calling-Station-Id = "7495111111"

Called-Station-Id = "7499222222"

h323-redirect-number = "7841333333"

Cisco-AVPair = "in-trunkgroup-label=1111"

Cisco-AVPair = "out-trunkgroup-label=2222"

Значения полей *Calling-Station-Id* и *Called-Station-Id* должны быть в формате E.164. Стратегия обработки вызовов следующая:

- если номер *Calling-Station-Id* принадлежит номерной емкости оператора, а номер *Called-Station-Id* — нет, то вызов считается исходящим и регистрируется на УВр.
- если номер *Calling-Station-Id* не принадлежит номерной емкости оператора, а номер *Called-Station-Id* — принадлежит, то вызов считается входящим и он отправляется на верификацию.
- если номера *Calling-Station-Id* и *Called-Station-Id* принадлежат номерной емкости оператора, то вызов является локальным и пропускается.
- если номера *Calling-Station-Id* и *Called-Station-Id* не принадлежат номерной емкости оператора, то вызов является транзитным и направление вызова определяется по значениям полей *in-trunkgroup-label* и *out-trunkgroup-label*. Если значение поля *in-trunkgroup-label*

равно идентификатору своего оператора, то вызов определяется как исходящий и регистрируется на УВр, если не равно, то вызов — входящий и он отправляется на верификацию.

В случае неуспешной верификации возвращается **Access-Reject**, во всех остальных случаях- **Access-Accept**.