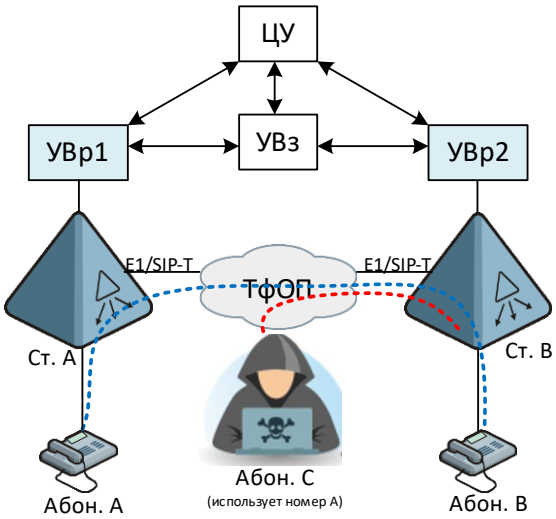
SP5000 «Антифрод»



Нормативно-правовые акты на SP5000 Антифрод:

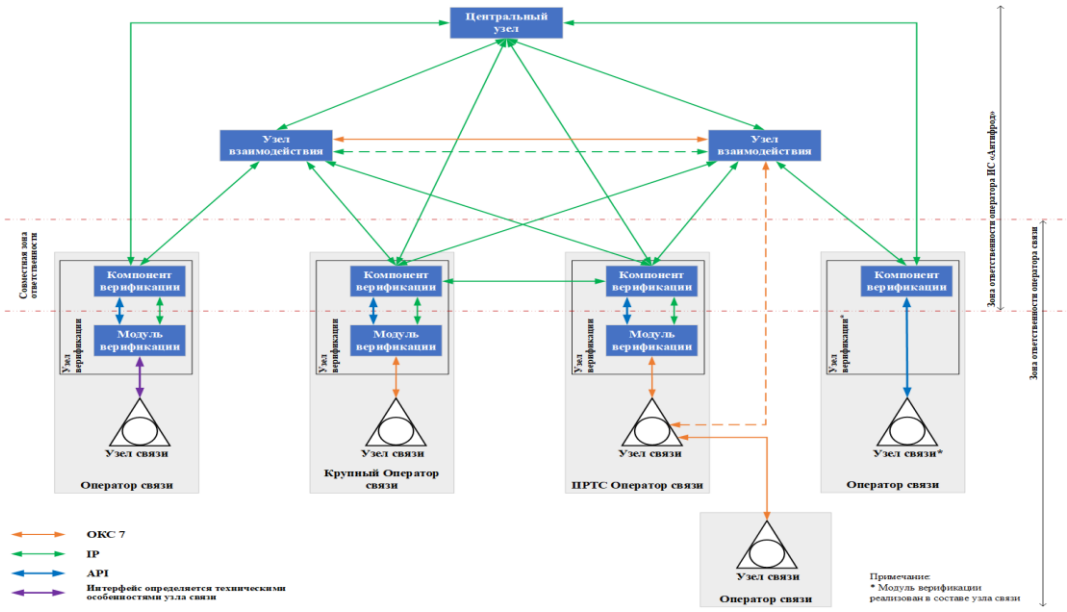
- Федеральный закон от 7 июля 2003 года № 126-ФЗ «О связи» (изменение от 02.07.2021 № 319-ФЗ)
- ППРФ от 03 ноября 2022 г. № 1978 - требования к системе и правила её функционирования
- ППРФ от 03 ноября 2022 г. № 1979 - правила направления и получения сведений из системы

SP5000 «Антифрод» - система, предназначенная для противодействия угрозам безопасности, связанным с подменой абонентских номеров (уникальных кодов идентификации) вызывающих абонентов в процессе инициирования и установления соединений в сети связи общего пользования Российской Федерации.

Участники взаимодействия с системой

- Радиочастотная служба (ГРЧЦ) - оператор системы;
- Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации;
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;
- Органы, осуществляющие оперативно-розыскную деятельность;
- Операторы связи.

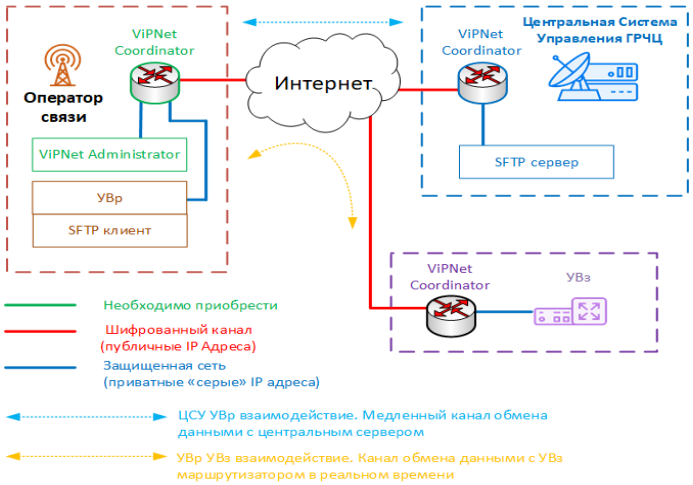
Компоненты системы ИС «Антифрод»



- **Центральный узел**: выявление нарушений при оказании услуг связи и услуг по пропуску трафика
- **Узлы верификации**: проверка достоверности сведений об инициировании телефонного вызова в сети связи общего пользования
- **Узлы взаимодействия**: обмен данными между узлами верификации при проверке достоверности сведений об инициировании соединений в случае отсутствия у них такой технической возможности

Необходимы действия оператору связи для выполнения требований ИС «Антифрод»

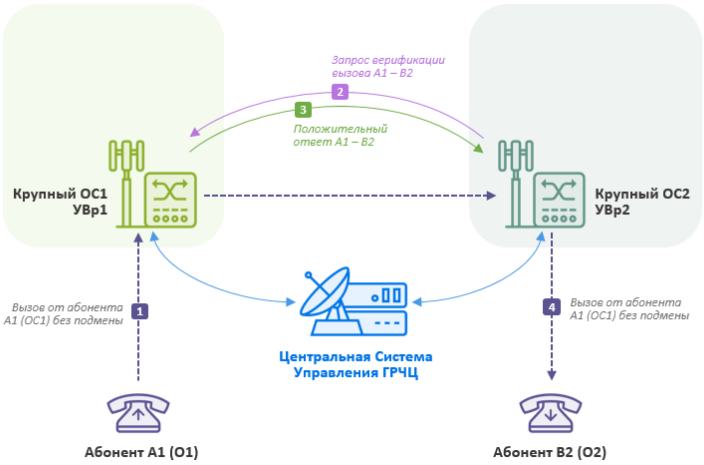
- Установить пакет обновления на **АТС SI3000 CS/cCS**
- Развернуть программный продукт **SP5000 «Антифрод»** от АО «Искра Технологии»
- Соединиться с **ИС «Антифрод** (ЦУ, УВз) через защищенные каналы (оборудование VipNet)



Принцип работы SP5000 «Антифрод»

Верифицированные соединения

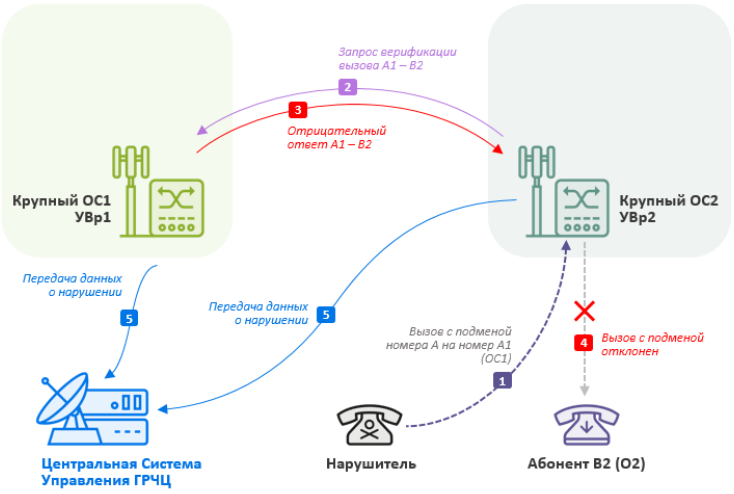
- Абонент А1 звонит Абоненту В2
- В момент формирования звонка станция А1 отправляет информацию о звонке в свой УВр (УВр1)
- Голосовой трафик идет, как обычно, через сеть ТфОП
- Когда звонок доходит до станции В2, оператор до установления соединения обязан верифицировать вызов через УВр станции В2 (УВр2)



- УВр2 анализирует номер А1 и по справочнику абонентов, определяет к какому УВр он относится
- УВр2 оправляет запрос на УВр1, есть ли у него в текущий момент такой звонок
- УВр1 проверяет информацию о звонке и отправляет на УВр2 подтверждение, что
- такой звонок есть
- УВр2, получив подтверждение от УВр1, разрешает АТС В1 проключить звонок на абонента В1

Вариант “плохого” звонка, когда злоумышленник, используя чужой номер А1, звонит абоненту В2

- В этом случае происходит вызов от оператора-нарушителя к абоненту оператора ОС2 с номером В2 с подменой номера А на номер А1 оператора ОС1В
- Голосовой трафик идет через сеть ТфОП
- Когда звонок доходит до станции В1, УВр станции В1 (УВр2), анализируя номер А по правочнику абонентов, определяет к какому УВр относится номер А



- УВр2 оправляет запрос на УВр1 есть ли у него в текущий момент такой звонок
- УВр1 проверяет информацию о звонке и отправляет на УВр2 информацию, что такого звонка у него в текущей базе нет
- УВр1 отправляет информацию в ЦУ что произошел инцидент подмены номера

Влияние решения SP5000 «Антифрод» на работу оборудования OPM COPM

Решение SP5000 «Антифрод» полностью соответствует требованиям COPM-1, COPM-3 и «закона Яровой» и направляет в сторону ПУ или хранилища всю необходимую информацию о инициации и разъединение

При использовании протокола **INAP** или **RADIUS возникает проблема в работе OPM COPM.**
А именно:
Если абонент В стоит под наблюдением, то при срабатывании INAP или RADIUS, инициации вызова в сторону абонента не будет, следовательно, ПУ никак не узнает о попытке вызова на абонента В.
УФСБ РФ требует, чтобы в сторону ПУ была и инициация вызова и разъединение с новым кодом **Н`07**

ИС «Антифрод», как Услуга от операторов Связи, точно также **не выполнит** требований OPM COPM

Архитектурная составляюшая продукта SP5000 «Антифрод»:

В рамках архитектуры продукта поддерживается два режима работы:

- **High availability** инсталляция.
- **Geo-redundancy** инсталяция

Конфигурация высокой доступности продукта **SP5000 «Антифрод»** на базе операционных систем AstraLinux/Debian и СУБД семейства PostgreSQL/Postrges Pro приведена ниже:

Архитектура продукта в рамках **High availability** инсталляции построена на решении для обеспечения высокой доступности **PostgreSQL — Patroni**. Для такого подхода требуется как минимум три физических или виртуальных узла.
В нашем продукте предлагается запустить SP5000 Антифрод на двух узлах, но третий узел будет использоваться в качестве контроллера, который будет работать в HA mode analyze (в режиме орбитра). Приложение SP5000 Антифрод будет отслеживать, какой из узлов в данный момент активен с помощью модуля HA mode analyze (в режиме Арбитра), и будет активен только на том же узле.
Конфигурация продукта в рамках **High availability** работает только **в L2 режиме сети.**

Архитектура продукта в рамках **Geo-redundancy** инсталляции построена так же, как и в ситуации с **High availability** инсталляцией. На каждой удаленной площадке необходимо развернуть SP5000 Антифрод на двух узлах, третий узел будет использоваться в качестве контроллера. Тоесть на каждой площадке будет развернут свой кластер **High availability** и между ними будет организована репликационная связанность.
Переключение между двумя площадками **осуществляется только в Ручном режиме**.

Описание среды работы продукта и характеристики оборудования

Сетевые интерфейсы	
Ethernet	10/100/1 000/ 10 000 Мбит/с
Система управления	
Протоколы управления	SSH, SFTP, Telnet
Интерфейсы управления	
Ethernet	10/100/1000 Мбит/с
Типы поддерживаемых ОС и СУБД	
Операционная система	Astra Linux Special Edition v.1.7, Debian 10, Wind River Linux 7
СУБД	PostgreSQL 11, Postgres Pro Standard 11
Поддерживаемые среды виртуализации и облачные системы	
Среда виртуализации	KVM, VMware 6.5 и выше, zVirt, Скала-Р
Облачные системы	Облачная платформа ICP

Характеристики виртуальных машины для SP5000 «Антифрод» (High availability)

Кол-во ресурсов (для одной виртуальной машины)	**Кол-во виртуальных машин**
УВр Антифрод	
8 vCPU, 32 Gb vRAM, 350Gb vHDD (SSD)	**2**
Арбитр Антифрод	
2 vCPU, 2 Gb vRAM, 60Gb vHDD (SSD)	1

Характеристики виртуальных машины для SP5000 «Антифрод» (Geo-redundancy)

Кол-во ресурсов (для одной виртуальной машины)	**Кол-во виртуальных машин**
УВр Антифрод	
8 vCPU, 32 Gb vRAM, 350Gb vHDD (SSD)	**4**
Арбитр Антифрод	
2 vCPU, 2 Gb vRAM, 60Gb vHDD (SSD)	**2**