SI3000 Антифрод

Описание системы

АО «Искра Технологии», май 2024 г. KSS887800-LDR-020

Если используется копия документа, проверьте ее соответствие последней версии документа.

Документ выпущен компанией

ИСКРА ТЕХНОЛОГИИ

АО «Искра Технологии»

ул. Комвузовская, дом 9, строение А,
г. Екатеринбург, РФ 620066

Т: +7 343 210 69 51
Ф: +7 343 341 52 40

info@iskratechno.ru
www.iskratechno.ru

Содержание

Список рисунков

Список таблиц

1. О документе

1.1. Назначение

Данный документ содержит сведения о назначении, составе, функциях и применении продукта «SI3000 Антифрод».

1.2. Целевая аудитория

Документ предназначен для квалифицированных специалистов, ответственных за развёртывание, техобслуживание и конфигурирование решений, в состав которых входит продукт «SI3000 Антифрод».

1.3. Структура документа

Табл. 1.1. Структура документа

Глава	Описывает
«Общие сведения»	компоненты и функции продукта «SI3000 Антифрод», нормативные документы, в соответствии с которыми он был разработан и дополнительные сведения о его применении.
«Принципы работы системы»	процедуру проверки соединений для выявления случаев подмены номеров в ИС «Антифрод».
«Технические данные»	требования к виртуальным машинам для продукта «SI3000 Антифрод», а также основные параметры для подбора лицензий на продукт «SI3000 Антифрод» для конкретного заказчика, а также требования, которые должен выполнить оператор связи, чтобы начать применять продукт.

1.4. Сопутствующая документация

Табл. 1.2. Сопутствующая документация

Код	Название
KSS887500-LDR	«Руководство по установке и настройке»
KSS88750A-LDR	«Руководство администратора (CLI)»
KSS8878L0-LDR	«Инструкции по устранению ошибок»

1.5. Условные обозначения

1.5.1. Дополнительная маркировка текста

Табл. 1.3. Условные обозначения для маркировки текста

Знак	Текст	Описывает
	Предупреждение	Этот знак обозначает текст, который следует прочитать и принять к сведению для недопущения опасных последствий.
	Примечание	Этот знак обозначает дополнительное пояснение.

1.6. Список сокращений

Табл. 1.4. Список сокращений на английском языке

Сокращение	Расшифровка	Описание
cCS	Compact Call Server	Компактный программный коммутатор
COTS	Commercially off-the-shelf	Серийно выпускаемый, свободно доступный на рынке компонент
CS	Call Server	Программный коммутатор
DNS	Domain Name System	Система доменных имен
FMS	Fault Monitoring System	Система мониторинга неисправностей
GEO	Geographically redundant	Географическое резервирование
GUI	Graphical user interface	Графический интерфейс пользователя
HA	High availability	Высокая доступность
HSB	Hot stand-by	Горячее резервирование
ID	Identifier, Identification	Идентификатор
IP	Internet protocol	Протокол Интернета
KVM	Kernel-based Virtual Machine	«Виртуальная машина на основе ядра», ПО для виртуализации в среде Linux на платформе x86
LI	Lawful Interception	Средства законного перехвата в телекоммуникационных сетях
MNS	Management Node System	Система управления
NE	Network Element	Сетевой элемент
NEM	Network Element Manager	Менеджер сетевого элемента, приложения для управления конфигурацией CS и т.п
NTP	Network Time Protocol	Протокол сетевого времени
SFTP	SSH File Transfer Protocol	Протокол прикладного уровня передачи файлов, работающий поверх безопасного канала
SSH	Secure Shell	«Защищенная оболочка», протокол для удаленного управления ОС и туннелирования TCP-соединений
TCP	Transmission Control Protocol	Протокол управления передачей данных

Табл. 1.5. Список сокращений на русском языке

Сокращение	Описание
БД	База данных
ВМ	Виртуальная машина
ГБ	Гигабайт
ГРЧЦ	Главный радиочастотный центр
ИС	Информационная система
КВр	Компонент верификации
ОЗУ	Оперативное запоминающее устройство
ОРМ	Оперативно-розыскные мероприятия
ОС	Операционная система Оператор связи
ПО	Программное обеспечение
ТС	Технические средства
УВз	Узел взаимодействия

Сокращение	Описание
УВр	Узел верификации
ФГУП	Федеральное государственное унитарное предприятие
ФЗ	Федеральный закон
ЦП	Центральный процессор
ЦСУ	Центральная система управления
ЦУ	Центральный узел

2. Общие сведения

ИС «Антифрод» – система под централизованным управлением Радиочастотной службы (ФГУП «ГРЧЦ»), 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.

2.1. Нормативные документы

Нормативно-правовые акты, в соответствии с которыми был разработан продукт «SI3000 Антифрод»:

- Федеральный закон от 7 июля 2003 года № 126-ФЗ «О связи» (изменение от 02.07.2021 № 319-ФЗ).
- Постановление Правительства Российской Федерации от 03.11.2022 №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»;
- Постановление Правительства Российской Федерации от 03.11.2022 №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».

2.2. Компоненты системы

ИС «Антифрод» включает в себя следующие элементы:

- Центральная система управления (ЦСУ) – источник маршрутной, справочной и авторизационной информации. ЦСУ представляет собой Центральный узел (ЦУ) ИС «Антифрод». Центральный узел выполняет функцию выявления нарушений при оказании услуг связи и услуг по пропуску трафика.
- Узлы верификации (УВр) – выполняют верификацию вызовов, т.е. проверку достоверности сведений об инициировании телефонного вызова в сети связи общего пользования.
- Узлы взаимодействия (УВз) – обеспечивают связность всех УВр, т.е. обмен данными между узлами верификации при проверке достоверности сведений об инициировании соединений в случае отсутствия у них такой технической возможности.

Продукт «SI3000 Антифрод» представляет собой реализацию УВр.

Узел верификации, установленный на объекте оператора связи, включает в себя:

- Компонент верификации – ПО, разработанное согласно спецификациям ГРЧЦ, отвечающее за стыковку УВр с ЦСУ. Также он хранит информации о фактах установления соединений в течении 12 месяцев.
- Модуль регистрации и верификации вызовов (сокр. «Модуль верификации») – самостоятельно разработанное ПО, отвечающее за стыковку УВр со станциями оператора связи.

На рисунке ниже представлено взаимодействие продукта с другими компонентами ИС «Антифрод»:

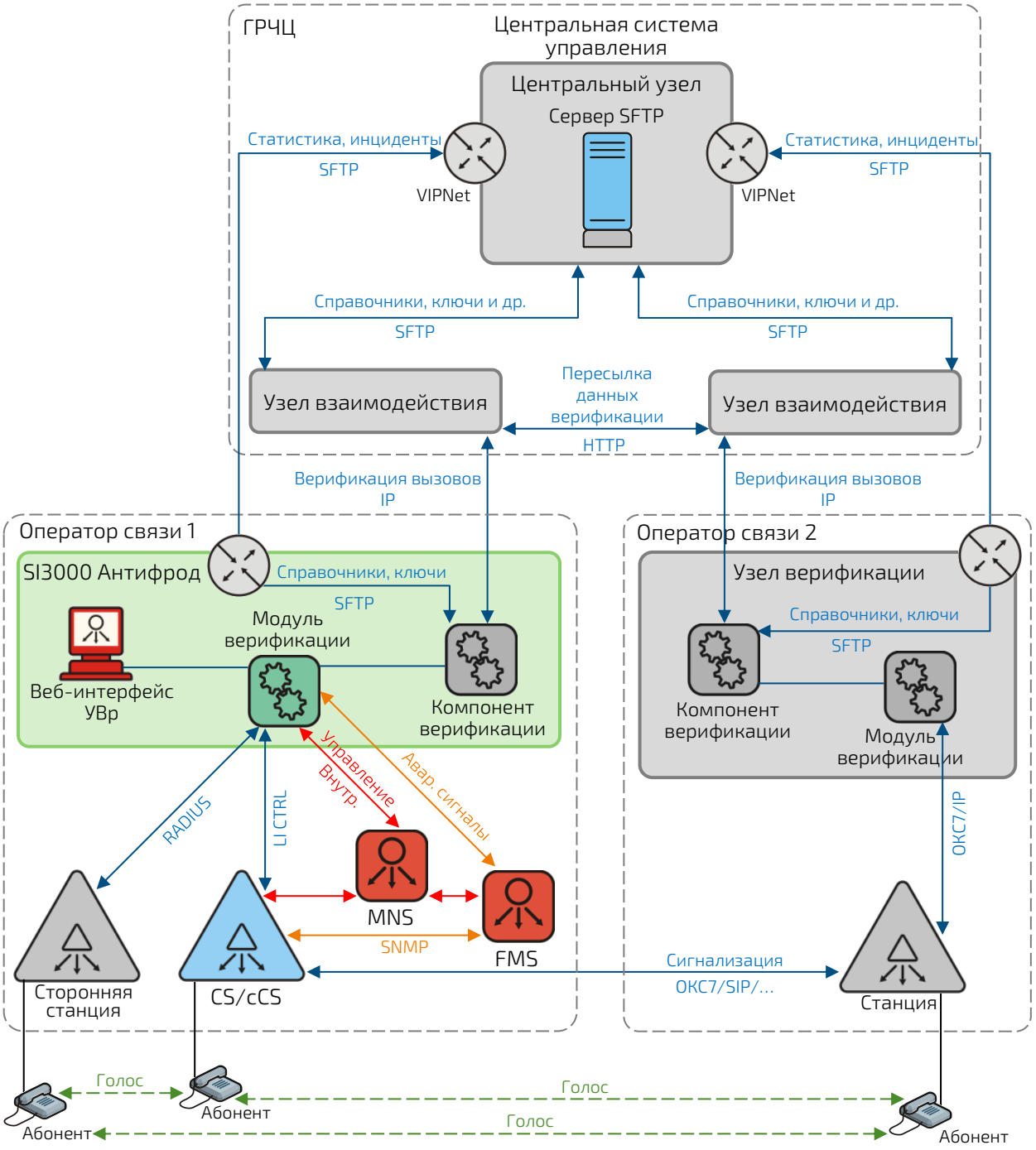

Рис. 2.1. Пример решения с продуктом «SI3000 Антифрод»

УВр «SI3000 Антифрод» взаимодействует со станциями SI3000 CS/cCS по внутреннему протоколу LI CTRL, а со станциями других производителей – по протоколу Radius:

- Станции направляют на УВр информацию о входящих и исходящих вызовах.
- УВр на основе данных от другого УВр разрешает или запрещает довести входящий вызов до абонентов станции.

УВр взаимодействует с другими УВр по протоколу TCP/IP, обмениваясь следующими сообщениями:

- запросы на верификацию вызова;
- ответы на запросы верификации вызова.

Запросы и ответы верификации при этом проходят через один или несколько УВз в неизменном виде.

УВр взаимодействует с ЦСУ по протоколу SFTP:

- Данные, в виде файлов предоставляемые центральным узлом с ЦСУ на УВр:
  - данные о нумерации: прежде всего телефонные номера абонентов, обозначение оператора связи, основной и резервный УВр;
  - данные об узлах верификации и узлах взаимодействия для маршрутизации вызовов к УВз или напрямую к УВр;
  - данные об операторах связи, подключенных к ИС «Антифрод»;
  - публичные ключи всех элементов системы.
- Данные, которые передаются с УВр на ЦСУ:
  - запросы о соединении абонентов, направленном с ЦСУ на УВр;
  - ответы УВр на запросы о соединении.

Для оперативного отслеживания работоспособности продукта «SI3000 Антифрод» и актуальности лицензии УВр взаимодействует с Системой управления SI3000 MNS по внутреннему протоколу и с Системой мониторинга неисправностей SI3000 FMS с помощью trap-сообщений протокола SNMP. Эти системы аналогичным образом взаимодействуют со станциями SI3000 CS/cCS.

Межстанционная сигнализация идет по конкретным транковым группам, идентификаторы которых должны быть прописаны в конфигурации УВр.

Голосовой трафик между абонентами идет через сеть ТфОП.

2.3. Варианты конфигурации системы

В зависимости от требований заказчика, заложенных в техническое решение, система может работать в одном из следующих режимов:

- **Одиночная конфигурация (автономная)**: используется только одна машина, т.е. без дублирования. Он отличается минимальными системными требованиями и простотой установки и обслуживания.
- **Конфигурация высокой доступности (HA)**: используется три машины – дублированный узел и узел-арбитр с функциями БД, установщика и репозитория. Такая конфигурация отличается повышенной отказоустойчивостью, но в то же время более сложными процедурами установки и поддержания работоспособности, а также повышенными системными требованиями.
- **Конфигурация с георезервированием (GEO)**: используется шесть машин, так как она представляет собой конфигурацию высокой доступности на двух географически удаленных друг от друга локациях. На каждой локации есть свой арбитр.

2.4. Влияние на работу ТС ОРМ

Решение SI3000 «Антифрод» полностью соответствует требованиям СОРМ-1, СОРМ-3 и «Закона Яровой» и направляет в сторону ПУ или хранилища всю необходимую информацию о инициации и разъединении вызовов при работе с собственными станциями при работе с собственными станциями SI3000. Согласно нормативным требованиям на ПУ поступает информация и об инициации вызова, и его разъединении с кодом «Н`07».

Однако при использовании протокола RADIUS для подключения к продукту сторонних станций возникает проблема в работе ТС ОРМ: если абонент Б стоит под наблюдением, то в случае выявления подмены номера инициации вызова не произойдет, и, следовательно, ПУ никак не узнает о попытке вызова абоненту Б.

ИС «Антифрод» как услуга от крупных операторов связи также не выполнит требований ТС ОРМ.

3. Принципы работы системы

Обычные соединения

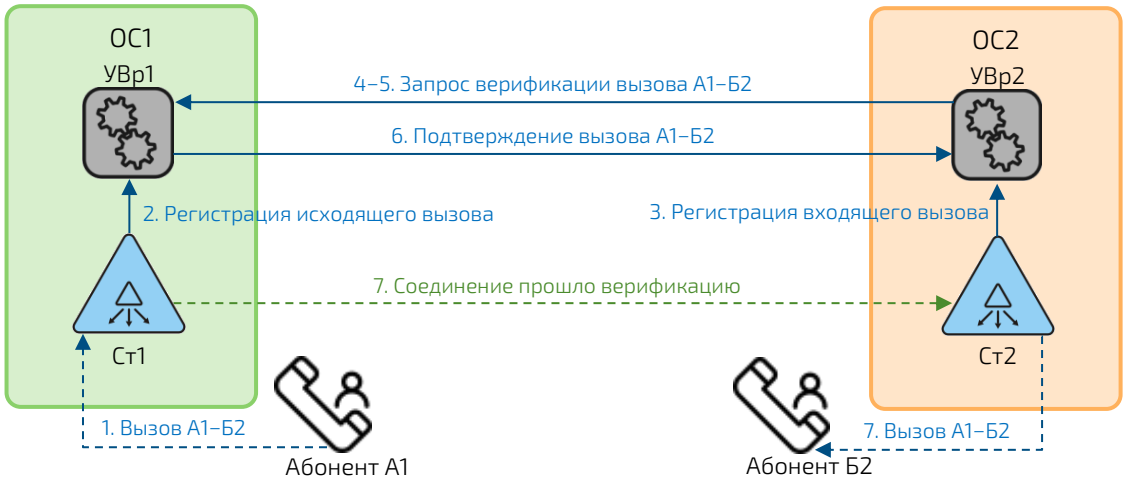

Рис. 3.1. Верификация соединения в ИС «Антифрод»

1. Абонент А1 инициирует вызов Абоненту Б2.
2. В момент формирования вызова станция А1 отправляет информацию о вызове на собственный УВр (УВр1).
3. Вызов доходит до станции Б2. Оператор до установления соединения обязан верифицировать вызов через УВр станции Б2 (УВр2).
4. УВр2 анализирует номер А1 и по справочнику абонентов и определяет, к какому УВр он относится.
5. УВр2 оправляет запрос на УВр1, чтобы выяснить, есть ли сейчас такой вызов на станции А1. Запрос при этом проходит через один или несколько УВз.
6. УВр1 проверяет информацию о вызове и отправляет на УВр2 подтверждение, что такой вызов существует. Ответ при этом проходит через один или несколько УВз.
7. УВр2, получив подтверждение от УВр1, разрешает станции В1 довести вызов до абонента В1.

Злонамеренные соединения

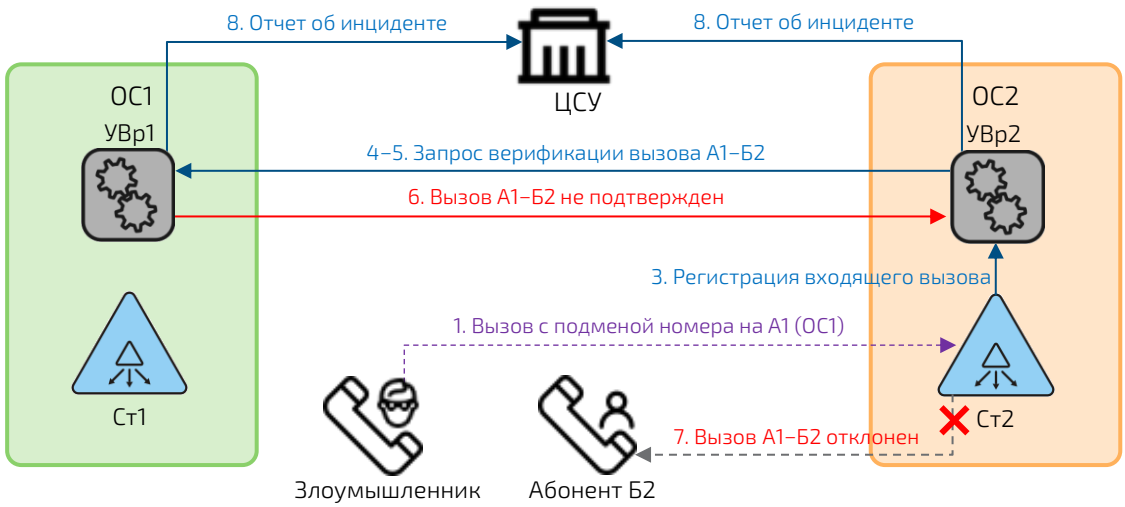

Рис. 3.2. Выявление злонамеренного соединения в ИС «Антифрод»

1. Злоумышленник, используя чужой номер абонента А1, звонит абоненту Б2.
2. Вызов от оператора-нарушителя направляется абоненту Б2 оператора ОС2 с подменой истинного номера на номер А1 оператора ОС1.
3. Вызов доходит до станции Б2. Оператор до установления соединения обязан верифицировать вызов через УВр станции Б2 (УВр2).
4. УВр2 анализирует номер А1 и по справочнику абонентов и определяет, к какому УВр он относится.
5. УВр2 оправляет запрос на УВр1, чтобы выяснить, есть ли сейчас такой вызов на станции А1. Запрос при этом проходит через один или несколько УВз.
6. УВр1 проверяет информацию о вызове и отправляет на УВр2 ответ о том, что такого вызова не существует. Ответ при этом проходит через один или несколько УВз.
7. УВр2, получив ответ от УВр1, запрещает станции В1 довести вызов до абонента В1.
8. УВр1 и УВр2 формируют отчеты об обнаруженном инциденте подмены номера, которые будут отправлены в ЦСУ в рамках процедур периодического обмена файлами между ЦСУ и УВр.

4. Технические данные

4.1. Системные требования

Программное обеспечения продукта «SI3000 Антифрод» устанавливается на стандартных серверах (COTS) промышленного класса. В качестве гипервизора может использоваться KVM, VMware или OpenStack. Для повышения надежности работы системы может быть реализована архитектура с резервированием или дублированием.

Табл. 4.1. Требования к ВМ для «SI3000 Антифрод» в различных конфигурациях

Тип конфигурации	ЦП	ОЗУ	Диск
Одиночный узел в компактной конфигурации	8 ядер	32 ГБ	350 ГБ
Дублированный узел (конфигурация высокой готовности)	18 ядер	66 ГБ	760 ГБ
Георезервированный узел (конфигурация высокой готовности в двух локациях)	36 ядер	132 ГБ	1520 ГБ

4.2. Лицензирование продукта «SI3000 Антифрод»

Для получения точного списка необходимых к приобретению лицензий для использования «SI3000 Антифрод» нужно определить:

- Вариант конфигурации продукта: одиночная, высокой доступности (т.е. с дублированием) или с георезервированием.
- Количество программных коммутаторов SI3000 CS/cCS, подключаемых к «SI3000 Антифрод».
- Количество программных коммутаторов других производителей, подключаемых к «SI3000 Антифрод».

Исходя из этих данных, приобретается нужное количество лицензий из следующего списка:

- Функциональная лицензия УВр «Антифрод», с подключением одного сетевого элемента CS/cCS.
- Функциональная лицензия УВр «Антифрод» с резервированием, с подключением одного сетевого элемента CS/cCS.
- Функциональная лицензия для географического резервирования УВр «Антифрод».
- Лицензия на функциональность «Антифрод» для установки на программный коммутатор SI3000 CS/cCS.
- Лицензия на подключение к УВр «Антифрод» дополнительного сетевого элемента CS/cCS, на один сетевой элемент.
- Лицензия на подключение к УВр «Антифрод» по протоколу RADIUS/API дополнительного сетевого элемента, на один сетевой элемент.

4.3. Требования к оператору связи

Чтобы подключиться к ИС «Антифрод» оператор связи должен выполнить следующие действия:

- Установить пакет обновления на АТС SI3000 CS/cCS.
- Развернуть программный продукт SI3000 «Антифрод».
- Зарегистрировать УВр в ГРЧЦ, в результате чего будет получен уникальный идентификатор УВр, который нужно прописать в файле конфигурации.
- Обеспечить связность с ИС «Антифрод (ЦУ, УВз) по защищенным каналам через оборудование VipNet.
- Передать в ГРЧЦ сгенерированные при инсталляции продукта открытые ключи для аутентификации УВр на сервере SFTP ЦСУ и взаимодействия с другими УВр и УВз.