

УТВЕРЖДАЮ

Генеральный директор

В.А. Уфимцева

«17» апреля 2024 г.



ООО «АЙ ЭКС АЙ ИНФО»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ NG АТС

(ПО NG АТС)

ФУНКЦИОНАЛЬНЫЕ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПРОГРАММНОГО  
ОБЕСПЕЧЕНИЯ

Инв.№ подл.	Подл. и дата	Взам. инв. №	Инв.№ дубл.	Подл. дата

МОСКВА 2024 г.

## АННОТАЦИЯ

Настоящий документ разработан в рамках исполнения требований Постановления Правительства Российской Федерации от 28.12.2022 N 2461 и содержит описание функциональных и технических характеристик программного обеспечения.

Инв.№ подл.	Подп. и дата	Взам. инв. №	Инв.№ дубл.	Подп. дата	ПО NG АТС	Лист
						2
Изм	Лист	№ докум.	Подп.	Дата		

# СОДЕРЖАНИЕ

<b>1</b>	<b>ВВЕДЕНИЕ</b>	<b>5</b>
1.1	ОБЛАСТЬ ПРИМЕНЕНИЯ ДОКУМЕНТА	5
1.2	ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ ПЕРСОНАЛА	5
1.3	ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММНОМ ОБЕСПЕЧЕНИИ	5
<b>2</b>	<b>ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ ПО</b>	<b>6</b>
<b>3</b>	<b>ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПО</b>	<b>7</b>
	Лист регистрации изменений	<b>8</b>

Инва.№ подл.	Подп. и дата	Взам. инв. №	Инва.№ дубл.	Подп. дата	ПО NG АТС	Лист
						3
Изм	Лист	№ докум.	Подп.	Дата		

## ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Определение понятия
Система / NG-ATC	Система защищенной телефонной связи на базе ПО NG-ATC
TLS v1.2	Transport layer security - протокол защиты транспортного уровня
SSL	Secure Sockets Layer - протокол, обеспечивающий шифрование, защиту и аутентификацию интернет-соединений
TCP/IP	Стек протоколов TCP/IP - набор сетевых протоколов, используемых в интернете
DHCP	Dynamic Host Configuration Protocol — протокол динамической настройки узла - сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP
VOIP	Voice over Internet Protocol - протокол передачи голоса по IP-каналам
IP-телефония	Телефонная связь по протоколу IP
ZRTP	Криптографический протокол согласования ключей шифрования, используемый в системах передачи голоса по IP-сетям.
Double Ratchet	Алгоритм управления ключами
SIP	Session Initiation Protocol, протокол установления сеанса — протокол передачи данных, описывающий способ установления и завершения пользовательского сеанса связи
RTP	Real-time Transport Protocol, протокол передачи медиаданных в реальном времени.
ИБ	Информационная безопасность
ОС	Операционная система
ПО	Программное обеспечение

Инв.№ подл.	Подп. и дата	Взам. инв. №	Инв.№ дубл.	Подп. дата	ПО NG ATC	Лист
Изм	Лист	№ докум.	Подп.	Дата		

# 1 ВВЕДЕНИЕ

## 1.1 ОБЛАСТЬ ПРИМЕНЕНИЯ ДОКУМЕНТА

В настоящем документе рассматривается описание функциональных и технических характеристик ПО NG-АТС.

## 1.2 ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ ПЕРСОНАЛА

Описание рассчитано на специалистов, разбирающихся в схемотехнике IP-телефонии, понимании принципов работы VOIP-технологий, архитектуре VOIP-систем телефонии, разбирающихся в основных терминах и понятиях (SIP, RTP, codecs и др.), имеющих базовые знания сетевых протоколов (TCP/IP, DHCP и др.), стационарных устройств, имеющих навыки работы в среде операционных систем (ОС) Linux, владеющих методиками «прошивки» устройств.

## 1.3 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

ПО NG-АТС позволяет реализовать систему защищенной телефонной связи для организации корпоративного коммуникационного пространства на базе IP-АТС.

Компонентами (элементами) системы защищенной телефонной связи являются как существующие в организации системы и технические средства, так и вновь вводимые в эксплуатацию:

- сервер АТС на базе ПО NG-АТС (серверная инфраструктура NG-АТС)
- корпоративная сеть передачи данных;
- стационарные устройства;

Полностью отечественная разработка. Не имеет аналогов. Зарегистрирована в РОСПАТЕНТЕ (Федеральная служба по интеллектуальной собственности).

Свидетельство о государственной регистрации программ для ЭВМ №2018666156 от 03.12.2018г.

Инв.№ подл.	Подп. и дата	Взам. инв. №	Инв.№ дубл.	Подп. дата

						ПО NG АТС	Лист
							5
Изм	Лист	№ докум.	Подп.	Дата			

## 2 ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ ПО

ПО NG-ATC обеспечивает безопасный тип связи, защищенный от несанкционированного доступа как телеметрических данных (телефонные номера, кодеки, длительность разговора и т.д.), так и непосредственно голосовых и других данных, используя программное инкорпорирование трафика в трафик https, обфускацию трафика, протоколы TLS/SSL, а также защиту от атак типа MITM (англ. Man in the middle – «человек посередине»).

При несанкционированном доступе к трафику, NG-ATC не позволяет идентифицировать абонента (как по идентификаторам, так и в географической привязке, в т.ч. по IP адресу).

Функциональные возможности NG-ATC:

- поддерживает одновременную работу до 200 абонентов;
- предоставляет абонентам защищенную связь на базе открытого протокола TLSv1.2;
- обеспечивает конфиденциальность переговоров между абонентами NG-ATC (внутренние звонки) за счёт использования телефонных соединений, защищённых протоколами TLS v1.2/SSL;
- обеспечивает маскирование трафика телефонных соединений при нахождении абонента NG-ATC на неподконтрольной территории (в т.ч. на территории иностранных государств), за счёт использования для телефонных соединений, защищённых протоколом TLS v1.2, имитации трафика абонента NG-ATC, характерного для вебсайтов и торрент клиентов;
- обеспечивает контроль доступа абонента на уровне сервера NG-ATC ;
- обеспечивает контроль установки сессий на уровне сервера NG-ATC ;
- обеспечивает отказоустойчивую схему работы посредством дублирования (резервирования) серверов NG-ATC;
- обеспечивает расширенный контроль целостности NG-ATC;
- обеспечивает усиленный контроль доступа к NG-ATC со стороны администраторов и предотвращение несанкционированного доступа (в т.ч. к билинговой информации), за счёт использования усиленной системы контроля доступа, системы защиты от вирусных атак, спуфинга трафика и других атак;
- поддерживает работу стационарных устройств (Yealink);

Инв.№ подл.	Подп. и дата	Взам. инв. №	Инв.№ дубл.	Подп. дата

					ПО NG ATC	Лист
						6
Изм	Лист	№ докум.	Подп.	Дата		

### 3 ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПО

Серверная инфраструктура для установки ПО состоит из физического сервера. Физический сервер работает под управлением VMWare ESXi v7 и имеет одну гостевую ОС «Альт СП» Сервер, в которой работают прикладные сервисы: NG-ATC , WEB-API, WEB-консоль управления NG-ATC .

На сервере для дополнительной защиты настроен межсетевой экран на базе ПО IPTABLES для устойчивой работы стека TCP-IP ОС (защита от сетевых флудов, контроль TCP сессий, соединений на порт SSH с недоверенных IP).

Программное обеспечение представляет собой совокупность модулей, реализующих функции, способные работать, как на серверах платформы Intel, так и в виртуальной среде.

NG-ATC реализована на базе ПО с открытым кодом FreeSWITCH, где дополнительно разработан функционал для защиты голосового трафика, согласования ключей, реализации протокола Double Ratchet и т.д..

Система обеспечивает шифрование голосовых сообщений, для защиты от несанкционированного доступа. Шифрование медиапотоков и сообщений осуществляется с использованием алгоритмов AES\_CM\_128\_HMAC\_SHA1\_80, AES\_256\_GSM, TWOFISH\_CFB\_256\_HMAC\_SHA1\_80. Для обмена сообщениями используется алгоритм Double Ratchet.

Система управления ключами обеспечивает безопасное хранение, генерацию и обмен ключами шифрования для обеспечения конфиденциальности и целостности данных. Согласование ключей осуществляется по протоколу ZRTP. В протоколе обмена ключами ZRTP используется связка алгоритмов ECDSA\_571 (подпись), ECDHE\_256 (Elliptic-curve Diffie–Hellman (протокол обмена ключами Диффи-Хелмана на эллиптических кривых)).

ПО обеспечивает механизмы аутентификации пользователей, для предотвращения несанкционированного доступа к системе.

Система позволяет вести аудит действий пользователей и обеспечивать возможность журналирования отслеживания событий и выявления возможных угроз безопасности.

Инд. № подл.	Подп. и дата	Взам. инв. №	Инд. № дубл.	Подп. дата

						ПО NG ATC	Лист
Изм	Лист	№ докум.	Подп.	Дата			7

