Practical value: *the knowledge gained about swarm intelligence technologies can be used in setting tactical and technical tasks for promising models of weapons, military and special equipment under the responsibility of the Main Communications Directorate of the Armed Forces of the Russian Federation.*

References

1. Starkov I. A. Metody roevogo intellekta / I. A. Starkov // Nauka molodyh: sbornik statej Mezhregional'noj molodezhnoj nauchnoj konferencii, posvyashchennoj pamyati F. A. Babushkina, Syktyvkar, 29–30 maya 2025 goda. – Syktyvkar: Syktyvkarskij gosudarstvennyj universitet im. Pitirima Sorokina, 2025. – S. 9–12. – EDN EPIXIH.
2. A. Colorni, M. Dorigo et V. Maniezzo Distributed Optimization by Ant Colonies, actes de la première conférence européenne sur la vie artificielle, Paris, France, Elsevier Publishing, 1991. Pp. 134–142.
3. Kennedy J., Eberhart R. Particle Swarm Optimization. Proceedings of IEEE International Conference on Neural Networks, 1995. – Vol. IV. – Pp. 1942–1948.
4. Primenenie modeli markovskogo processa prinyatiya reshenij s cel'yu obespecheniya svoevremennosti obsluzhivaniya mul'tiservisnogo trafika v domene programmno-konfiguriruemoj infokommunikacionnoj seti special'nogo naznacheniya / D. S. Yagovitov, M. I. Rafal'skaya, D. A. Nesvit, I. V. Obrazcov // Sovremennoe sostoyanie i perspektivy razvitiya infokommunikacionnyh setej svyazi special'nogo naznacheniya: Sbornik materialov nauchno-prakticheskoj konferencii, Sankt-Peterburg, 23 marta 2023 g. – SPb: Federal'noe gosudarstvennoe kazennoe voennoe obrazovatel'noe uchrezhdenie vysshego obrazovaniya «Voennaya akademiya svyazi im. marshala Sovetskogo Soyuza S. M. Budennogo» Ministerstva oborony Rossijskoj Federacii, 2023. – S. 137–144. – EDN JESIAA.

АРХИТЕКТУРА СЕТИ ОТКРЫТОЙ АВТОМАТИЧЕСКОЙ ТЕЛЕФОННОЙ СВЯЗИ, ПОСТРОЕННОЙ С ПРИМЕНЕНИЕМ ПИРИНГОВЫХ ТЕХНОЛОГИЙ, И ПРЕДЛОЖЕНИЯ ПО ЕЕ ЗАЩИТЕ

Ашлапов М. В.[1], Елисеев Д. И.[2]

DOI:10.21681/3034-4050-2026-3-64-68

Ключевые слова: *телефонная связь, услуги телефонии, коммутация пакетов, кластер, аппаратные шлюзы, безопасность телефонной связи, аудиоконференц-связь.*

Аннотация

Цель работы: *анализ архитектуры пиринговой сети открытой автоматической телефонной связи и предложений по обеспечению защиты речевого и сигнального трафика.*

Метод исследования: *системный подход применен для анализа архитектуры сети пиринговой автоматической телефонной связи, на основе которого разработаны предложения по защите речевого и сигнального трафика в сети открытой телефонной связи.*

Результаты исследования: *рекомендуется применять аппаратно-программные средства обеспечения безопасности открытой телефонной связи.*

Научная новизна: *определяется глубиной обоснования применения пиринговых технологий для построения сетей открытой телефонной связи и рассмотрения особенностей обеспечения безопасности передачи речевого и сигнального трафика в такой сети.*

Введение

В современных условиях ведения боевых действий ключевое значение приобретает обеспечение своевременного и достоверного информационного обмена между должностными лицами на всех уровнях управления. Учитывая, что по-прежнему основой их информационного взаимодействия остается телефонная связь, решение вопросов доведения услуг телефонии непосредственно до линии боевого соприкосновения войск становится крайне важным [1, 2].

Одним из наиболее актуальных направлений совершенствования сети передачи данных в тактическом звене управления является развертывание на полевых пунктах управления сети открытой автоматической телефонной связи с использованием автоматических телефонных станций (далее – АТС) с поддержкой пиринговой технологии – АТС «Пирс» (рис. 1).

АТС «Пирс» обладает возможностью обеспечить услугами телефонной связи до 1000 IP-абонентов по протоколу сети с коммутацией пакетов SIP, а также 8 аналоговых абонентов. Кроме того, станция предоставляет большое количество дополнительных видов обслуживания, к которым относятся аудиоконференцсвязь, речевое оповещение, голосовой информатор, переадресация и другие.

Рис. 1. Внешний вид АТС «ПИРС»

Архитектура пиринговой сети открытой телефонной связи. Понятие кластера

В пиринговой архитектуре отсутствует выделенный центральный сервер, вместо этого каждый узел сети – будь то IP-телефон, программный клиент или шлюз – обладает достаточным уровнем интеллекта для самостоятельной маршрутизации вызовов [3]. Сигнальная информация передается по протоколу SIP, а медиапоток – по протоколу RTP, при этом обмен происходит непосредственно между узлами. Основными

1 ***Ашлапов Михаил Владимирович***, кандидат технических наук, доцент кафедры Военной академии связи. Санкт-Петербург, Россия. E-mail: mvashlapov@mail.ru

2 ***Елисеев Дмитрий Иванович***, кандидат технических наук, доцент, доцент кафедры Военной академии связи. Санкт-Петербург, Россия. E-mail: dimone73@mail.ru

преимуществами такой архитектуры являются высокая отказоустойчивость и масштабируемость. Поскольку нет центрального сервера, выход из строя одного из узлов не приводит к полному коллапсу всей телефонной сети. Добавление новых абонентов не требует увеличения мощностей центрального сервера, а прямая передача медиапотока минимизирует задержки и джиттер, что критически важно для поддержания качества обслуживания пользователей (QoS).

Ключевой особенностью архитектуры сети открытой телефонной связи, построенной с применением АТС «ПИРС», является возможность работы станций в кластере.

Кластер – понятие из области вычислительных сетей. В общем случае это группа серверов, объединенных высокоскоростными каналами связи и представляющих, с точки зрения пользователя, единый аппаратный ресурс[3]. Таким образом, кластер – это объединение не менее двух серверов на базе одинаковых процессоров под управлением одной операционной системы, имеющих общий доступ к носителям информации, используемым в кластере.

Работа вычислительных серверов в структуре кластера позволяет:

- скоординированно использовать общий ресурс серверов, входящих в кластер;
- осуществлять взаимный контроль работы серверов;
- осуществлять обмен данными о конфигурации серверов.
- кластер серверов отличается от обычной схемы резервирования:
- воспринимается пользователем как один сервер;
- управляется как единая система;
- обладает более высокой надежностью по сравнению с «клиент-серверной» архитектурой;
- имеет общую файловую систему.

Кластер АТС «ПИРС» представляет собой совокупность нескольких децентрализованных станций, развернутых в составе распределенной сети и пространственно разнесенных на значительной территории в зоне ответственности соединения (группировки, части). Для абонентов вся совокупность децентрализованных станций является единой АТС с точки зрения предоставляемых услуг связи, номерной емкости и аппаратного резервирования.

По принципам функционирования кластер АТС «ПИРС» во многом повторяет серверный кластер. Основу кластера составляет «пиринговая сеть», технология которой основывается на модели «Peer-to-Peer» (англ. – «равный-к-равному»). Указанная архитектура в значительной степени отличается от общепринятой в настоящее время архитектуры информационного обмена «клиент-сервер», на которой построены классические системы телефонии и коммуникаций.

Peer-to-Peer (P2P) представляет собой модель обмена информацией, в которой подключенные к сети узлы (пиры) обеспечивают непосредственную связь друг с другом и взаимный обмен информационными ресурсами. Особенностью технологии является то, что в ее состав входят равноправные узлы пиринговой сети. Центральная управляющая АТС (центральный блок) в пиринговой сети отсутствует, а в качестве узлов выступают все устройства пиринговой АТС.

Преимуществами архитектуры пиринговой телефонной сети по сравнению с традиционными сетями «клиент-сервер» являются способность неограниченного расширения сети, не требуя затрат централизованных ресурсов, высокая производительность и отказоустойчивость при любом количестве и сочетании доступных узлов. АТС «ПИРС» одного или даже разных типов (с аналоговыми окончаниями FXS, FXO, цифровыми интерфейсами E1 и др.) могут объединяться по сети передачи данных, образуя единую архитектуру пиринговых АТС с единым номерным планом, функциональностью дополнительных видов обслуживания (сервисами) и с общими физическими интерфейсами и каналами связи [1].

На сетевом уровне основную роль в организации автоматической телефонной связи посредством IP-сети играют маршрутизаторы, определяющие пути доставки данных до станций в составе кластера и до пользователей с определенным IP-адресом. Каждая пиринговая АТС имеет интерфейс Ethernet, посредством которого осуществляется подключение к транспортной сети связи, поиск других пиринговых АТС по IP-адресам, авторизация по специальному протоколу и логическое объединение с образованием кластера. Указанный алгоритм обеспечивает объединение в единую сеть ресурсов всех подключаемых устройств.

Пиринговая АТС «ПИРС» работает с различными оконечными устройствами. Это могут быть аналоговые телефонные аппараты и SIP-телефоны, некоторые из которых («Спектр-О», «Fanvil», Kirisun DH200 и др.) имеют встроенные профили автоматических настроек в системе.

Отличительными особенностями архитектуры телефонного кластера, построенного на основе АТС «Пирс», являются высокая отказоустойчивость и возможность информационного обмена в открытом сегменте сети передачи данных

3 АО «Линтех». Пиринговая система унифицированных коммуникаций Symway: официальная документация / АО «Линтех». – М., 2024. – Режим доступа: https://www.symway.com

Минобороны России, в том числе принимающим участие в специальной военной операции (так, по состоянию на 2025 год в группировках войск применялись более 1500 станций).

Вариант архитектуры сети открытой телефонной связи, построенной по принципу комплексного взаимодействия АТС «ПИРС», в составе распределенного кластера с классическими SIP серверами показан на рисунке 2.

Кроме АТС «ПИРС» в составе сети могут использоваться практически любые коммутаторы малой емкости, например, АТС П-380К из состава комплекса «Поле». По своей сути, АТС «ПИРС» будет являться шлюзом для объединения различных автоматических и ручных телефонных станций и предоставления им ресурсов кластера.

Однако именно децентрализация порождает уникальный профиль угроз. В отличие от централизованной АТС, где безопасность можно обеспечить на периметре одного сервера, в пиринговой сети каждый узел потенциально является точкой входа для злоумышленника. Это усложняет задачу администрирования и повышает вероятность атаки на кластер. Ключевые угрозы включают:

1. Перехват сигнальной информации: SIP-сообщения, такие как INVITE, ACK и BYE, передаются в открытом виде без шифрования (SIPS), что позволяет злоумышленнику, имеющему доступ к сетевому сегменту, перехватывать информацию о номерах абонентов, времени звонков и общем статусе линий [4].
2. Подмена абонента (Spoofing): отсутствие строгой взаимной аутентификации узлов позволяет злоумышленнику зарегистрироваться в сети под видом легитимного абонента и инициировать вызовы от его имени, что может привести к разглашению конфиденциальной информации.
3. Атаки на доступность (DoS/DDoS): узлы пиринговой сети часто функционируют на обычных рабочих станциях или серверах, которые имеют меньше вычислительных ресурсов по сравнению со специализированными серверами программных АТС. Целенаправленная атака на конкретный узел способна вывести его из строя.
4. Уязвимости программного обеспечения: распределение функционала пиринговой АТС между множеством оконечных устройств делает процесс обновления программного обеспечения и применения инструментов безопасности сложной и трудоемкой задачей. Наличие уязвимости в клиентском ПО на одном узле может стать причиной компрометации всего сегмента сети [5].

Для нейтрализации этих угроз необходим комплексный подход, который включает обеспечение конфиденциальности и целостности как сигнального, так и медиа-трафика.

На сегодняшний день для обеспечения безопасности передаваемой информации в глобальных сетях общего пользования достаточно широко применяются технологии OpenVPN, для защиты каналов применяются технологии IPsec, аппаратные шлюзы и связка TLS+SRTP. Выбор решения определяется криптографическими алгоритмами, архитектурой сети, статусом сертификации и применимостью в инфраструктуре сетей связи специального назначения.

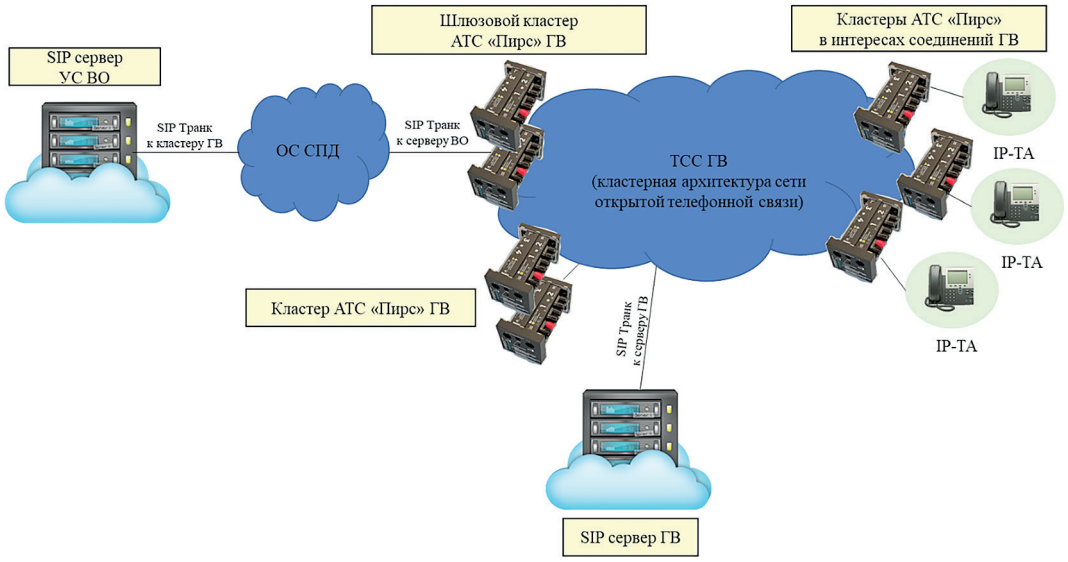

Рис. 2. Вариант архитектуры сети открытой телефонной связи ГВ

Криптографические механизмы и сертификация

OpenVPN – программное решение с открытым кодом, использующее библиотеку OpenSSL и протоколы TLS [6]. Оно поддерживает алгоритмы типа AES-256, но не имеет встроенной поддержки алгоритмов ГОСТ РФ и отдельных сертификатов ФСТЭК или ФСБ. Использование OpenVPN в сетях передачи данных специального назначения возможно только в составе сертифицированной конфигурации, что требует затрат на экспертизу.

IPsec, интегрированный на сетевом уровне ОС, шифрует заголовки пакетов, скрывая служебную информацию. Однако его применение в сетях передачи данных специального назначения требует сертификации всей системы, так как стандартные реализации не являются сертифицированными СКЗИ[4].

В свою очередь АПКШ «Континент» является сертифицированным аппаратно-программным комплексом (имеет сертификаты ФСТЭК и ФСБ). Комплекс гарантирует использование алгоритмов ГОСТ РФ (например, ГОСТ Р 34.12-2015) и защищает от вторжений через публичные сети. Наличие сертификатов делает «Континент» приоритетным выбором для применения на сетях связи специального назначения, в которых передается информация с ограничительными пометками[5,6].

Архитектурные особенности и надежность

Архитектура OpenVPN (пользовательский уровень, UDP) обуславливает недостаток – неустойчивость туннелей. При разрыве соединения требуется повторное установление сеанса протокола TLS, что занимает время и приводит к обрыву сеансов. Сравнительная оценка показывает, что время восстановления туннеля OpenVPN может достигать 5–10 секунд, что недопустимо для телефонии и приводит к потере пакетов RTP.

IPsec (уровень ядра, IKEv2) обладает повышенной отказоустойчивостью [7]. Протокол поддерживает быстрое переподключение и мобильность (MOBIKE), минимизируя простои до менее чем 1 секунды. АПКШ «Континент» обеспечивает максимальную стабильность за счет аппаратных криптографических модулей и кластеризации. В то время как программные решения зависят от ресурсов операционной системы, аппаратные шлюзы обеспечивают переключение за миллисекунды[6].

4 Федеральная служба по техническому и экспортному контролю. Требования к средствам криптографической защиты информации для обеспечения безопасности персональных данных при их передаче в сетях связи общего пользования: приказ ФСТЭК России от 11.02.2013 № 21. – М.: 2013. – 18 с.

5 ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – Введ. 2016-01-01. – М.: Стандартинформ, 2015. – 24 с.

6 АПКШ «Континент»: руководство администратора безопасности / ЗАО «Код Безопасности». – 4-е изд. – М.: 2022. – 156 с.

Для защиты речевого трафика используется связка TLS+SRTP. В отличие от IPsec, SRTP не шифрует заголовки RTP, но обеспечивает конфиденциальность медиапотока. Это решение эффективно для VoIP, но не заменяет VPN-технологии для защиты сетевого уровня.

На основе проведенного анализа можно сделать вывод, что для обеспечения безопасности открытой телефонной связи, как один из вариантов (рис. 3), может быть использована архитектура с каскадной схемой защиты услуг телефонной связи, как для сетей, построенных по классической клиент серверной архитектуре, так и для распределенных пиринговых сетей.

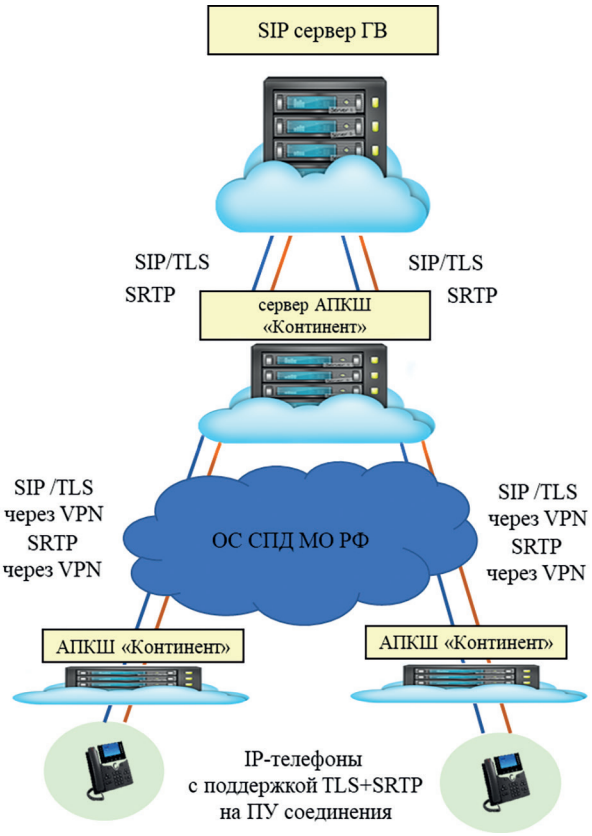

Рис. 3. Вариант архитектуры сети открытой телефонной связи с каскадной защитой услуг

Заключение

Очевидно, что для обеспечения защиты информации в сетях открытой телефонной связи наиболее предпочтительным решением является АПКШ «Континент» благодаря сертификации и поддержке ГОСТ РФ. Применение протокола IPsec рекомендуется как временное решение для защиты данных благодаря надежности туннелей. Применение OpenVPN для защиты голосового трафика не является приоритетным решением из-за проблем с устойчивостью