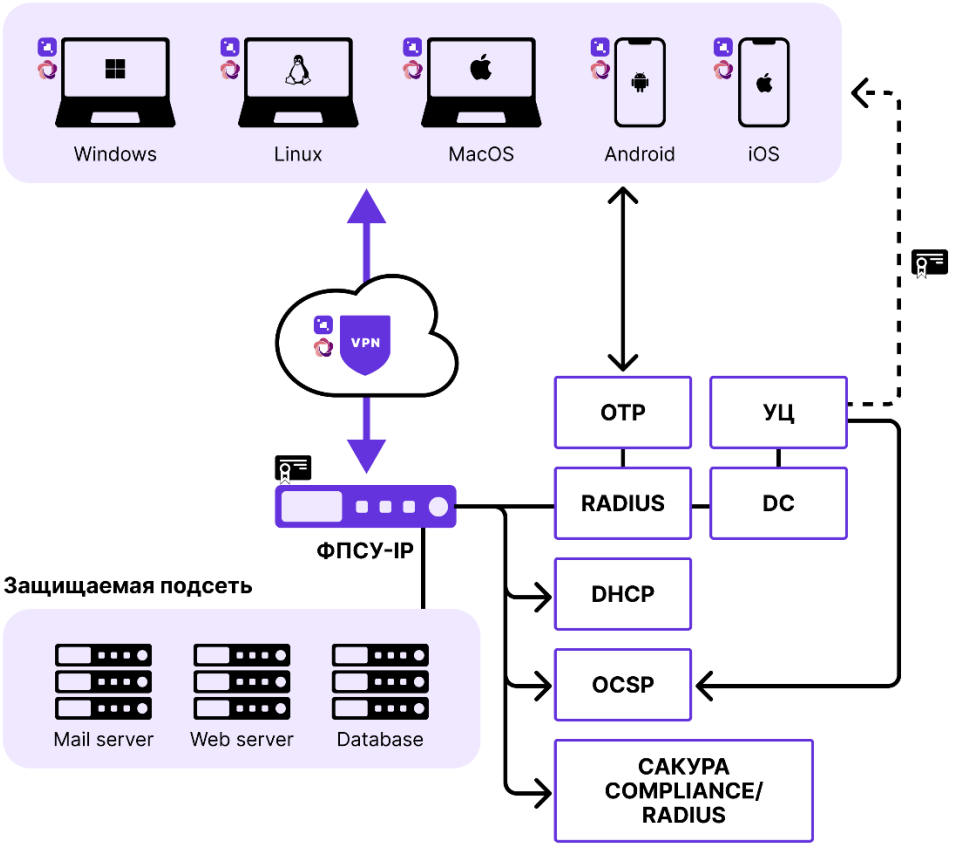
Описание программного обеспечения Системы удаленного доступа

1. Назначение

Программное обеспечение системы удаленного доступа «АМИКОННЕКТ» (далее Система) разработано в соответствии с ГОСТ Р 59795-2021 и предназначено для организации защищенных подключений пользователей к корпоративным ресурсам Заказчика. Система обеспечивает безопасный удаленный доступ с любых устройств (корпоративных или личных) с обязательным контролем их соответствия политикам безопасности («здоровья» или Compliance), что гарантирует защиту сети от небезопасных конечных точек.

2. Архитектура системы



Система построена по модульному принципу и состоит из следующих функциональных компонентов:

«ФПСУ-IP» (VPN-сервер): центральный узел безопасности. Отвечает за построение защищённых каналов связи, терминацию VPN-сессий, криптографическую защиту, обмен данными с серверами авторизации, а также фильтрацию трафика через встроенный межсетевой экран (МЭ).

«АМИКОННЕКТ» (VPN-клиент): программный клиент на устройстве пользователя. Обеспечивает инициацию защищённого VPN-соединения, передачу данных уровней L3–L7 модели OSI и взаимодействие с ФПСУ-IP для аутентификации и авторизации.

«Сакура» compliance-сервер: центр управления политиками безопасности. Формирует и распространяет политики проверок на агентов, принимает результаты проверок, рассчитывает уровень доверия устройства и передаёт его на ФПСУ-IP для применения соответствующих правил доступа.

«Сакура-агент»: программный модуль на устройстве пользователя, устанавливаемый параллельно с «АМИКОННЕКТ». Выполняет локальные проверки устройства на соответствие полученным от сервера политикам (наличие антивируса, обновлений ОС, запрещённого ПО и т.д.) и передаёт результаты на Compliance-сервер.

3. Основные функции и технические особенности

3.1. Криптографическая защита и аутентификация

- Поддержка как международных (RSA), так и российских стандартов криптографии (ГОСТ 34.10-2012), что позволяет использовать решение в смешанной и строго регулируемой средах.
- Инфраструктура открытых ключей (PKI): взаимная двухсторонняя аутентификация клиента и сервера на основе сертификатов. Автоматическая проверка статуса сертификатов через OCSP-серверы.
- Гибкая двухфакторная аутентификация (2FA):
    - 1-й фактор: Сертификат открытого ключа.
    - 2-й фактор (настраиваемый): Логин/пароль LDAP, одноразовый пароль (OTP) или аутентификация через RADIUS.
    - Интеграция: благодаря поддержке стандарта RADIUS, система совместима с внешними провайдерами MFA, включая «Мультифактор», Indeed, SberOK и другие решения.

3.2. Интеграция с системами контроля доступа

ФПСУ-IP взаимодействует с Комплексом информационной безопасности «Сакура» по протоколу RADIUS (RFC 5176).

- Уровни доверия: Compliance-сервер оценивает устройство по политикам безопасности и возвращает уровень доступа от 0 (наименее доверенный) до 100 (наиболее доверенный). По умолчанию при первичном подключении уровень устанавливается в 2 (доступ только в демилитаризованную зону для проверки).
- Применение политик на ФПСУ-IP: ФПСУ-IP содержит предустановленный набор правил межсетевого экрана. При получении уровня доверия от Сакуры ФПСУ-IP автоматически применяет соответствующие правила к трафику пользователя — без динамической перенастройки МЭ. Это обеспечивает высокую производительность и предсказуемость работы.

3.3. Сетевые технологии и производительность

- Транспортный протокол: VPN-туннель работает поверх UDP (порт 87), что обеспечивает высокую производительность и низкие накладные расходы.
- Устойчивость к каналам связи: протокол не чувствителен к задержкам (jitter) и пакетным потерям. Гарантируется стабильная работа на каналах с задержками до 300 мс и выше.
- Гибкая адресация: поддержка авторизации с реальным IP-адресом клиента или выдача адреса через внешний DHCP-сервер.

4. Поддерживаемые операционные системы

ФПСУ IP поставляется в виде программно-аппаратного комплекса или виртуального образа на базе операционной системы Linux (x86-64).

«АМИКОННЕКТ»:

- Windows: 10, 11;
- macOS: 13–26;
- Linux: Debian 12, 13; Ubuntu 24.04; SberOS 3.x, Astra Linux 1.7 и выше, РЕД ОС 8;
- iOS: 17–26;
- Android: 13–16.

5. Процесс подключения (Workflow)

1. Инициация: клиент «АМИКОННЕКТ» подключается к ФПСУ-IP. Предоставляется доступ только в демилитаризованную зону к Compliance-серверу.

2. Запуск проверок: агент Сакура получает от Compliance-сервера актуальные политики проверок и выполняет локальный анализ устройства.

3. Передача результатов: агент Сакура отправляет результаты проверок на Compliance-сервер.

4. Расчёт уровня доступа: Compliance-сервер рассчитывает уровень доверия (0–100) и передаёт его на ФПСУ-IP.

5. Применение политик: ФПСУ-IP применяет соответствующие правила встроенного МЭ к трафику пользователя на основе полученного уровня доверия (без динамической перенастройки правил).

6. Доступ: Пользователь получает доступ к ресурсам корпоративной сети в соответствии с назначенным ему уровнем (гибкая политика от полной изоляции до неограниченного доступа в зависимости от настроек, установленных администратором).