



VIPNet Client 5. Новое поколение продукта

Алексей Минаков
Менеджер продуктов

Технология ViPNet



Симметричная криптография:
Честный P2P VPN



Не сессионный VPN:
Работа на плохих и нестабильных
каналах



Централизованное обновление:
Ключи шифрования, справочники, ПО



Работа через NAT:
Соединение устройств за различными NAT



VipNet Client



- VPN-клиент для работы в защищенных сетях VipNet
- Прозрачен для приложений пользователя и сервисов ОС
- Независим от физических каналов связи
- Подключается к неограниченному количеству сегментов сети
- Разрабатывается в соответствии с требованиями **ФСБ России** к СКЗИ классов **КС1, КС2 и КС3**
- Поддерживает ОС **Windows, Linux, Android, Аврора, macOS, iOS, Kaspersky OS***

* В разработке



VIPNet Client 5

WHAT'S
NEW

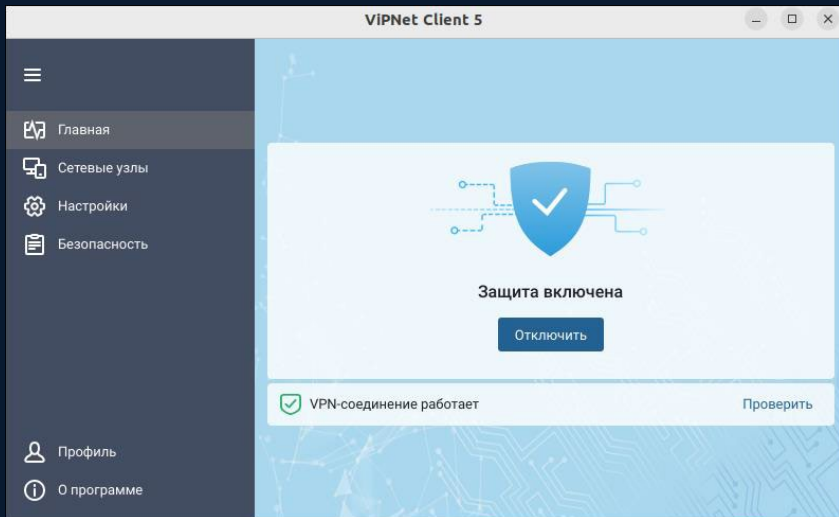


VIPNet Client на базе единого универсального исходного кода

- Установка из магазинов приложений или из инсталлятора
- Поддерживает большинство ОС, архитектур и платформ
- SDK для сторонних приложений
- Совместим с VIPNet ДП, CSS Connect, EPP
- Многофакторная аутентификация
- **Межсетевой экран для закрытого трафика**
Принимает правила от Policy Manager и Policy Management Module Prime
- Мониторинг через модуль **NVS** из Prime
- Поддержка групп серверов соединений
- Реализация функционала mDNS



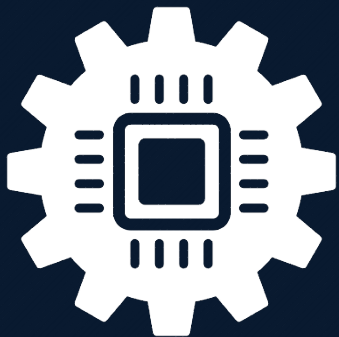
VIPNet Client 5



- Обновлён интерфейс программы
- Перенос ключей из VIPNet Client 4
- Новый протокол **IPLir6**
- Новые **ГОСТы**
- Поддержана универсальная лицензия для клиентов пятого поколения
- Несколько профилей на устройстве
- Все плюсы Client 4/4U + интеграция с VIPNet EPP (МЭ 4В ФСТЭК) + Compliance (ZTNA) - Блокировка трафика в случае отсутствия EPP или выключенных модулей защиты
- Разрабатывается в соответствии с требованиями ФСБ России к **СКЗИ** классов **КС1, КС2 и КС3**



VIPNet Client 5 Исполнения



Windows 10, 11



MIPS



МЦСТ
ЭЛЬБРУС



iOS, iPadOS 15.6 и выше
macOS 12.4 и выше



Android 8 - 14 (ARM64)



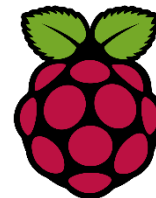
Авра 4, 5



Kaspersky OS



VIPNet Client 5 for Linux





VipNet Client 5 for Linux



- Используется виртуальный TUN\TAP интерфейс
- Поддержка широкого списка современных ОС Linux
- Не зависит от версии ядра ОС
- Корректная работа на низком уровне мандатного контроля целостности
- Поддержка архитектур x86, ARM, e2k, RISC-V, MIPS
- SDK для сторонних приложений
- Поддерживает многофакторную аутентификацию
- Совместим с Business mail for Linux

VIPNet Client 5 for Android for iOS/macOS



- Используется Google VPN API/ Apple VPN API
- Не требует прав суперпользователя (root)
- Оповещение о получении прав суперпользователя
- Настройка видимости IP-адресов туннелей
- Смена активного координатора из своей сети VIPNet
- Возможность блокировки открытого трафика при включенном VPN
- Распространение продукта через магазины приложений:



RuStore



SAMSUNG
Galaxy Store



NASHSTORE

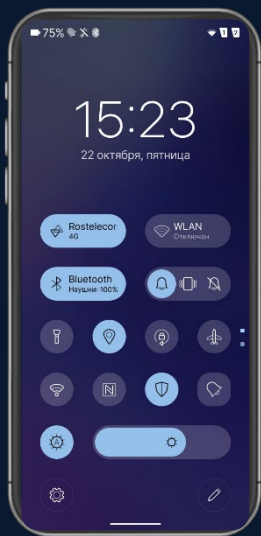


AppGallery





VIPNet Client 5 для ОС Аврора



Особенности продукта:

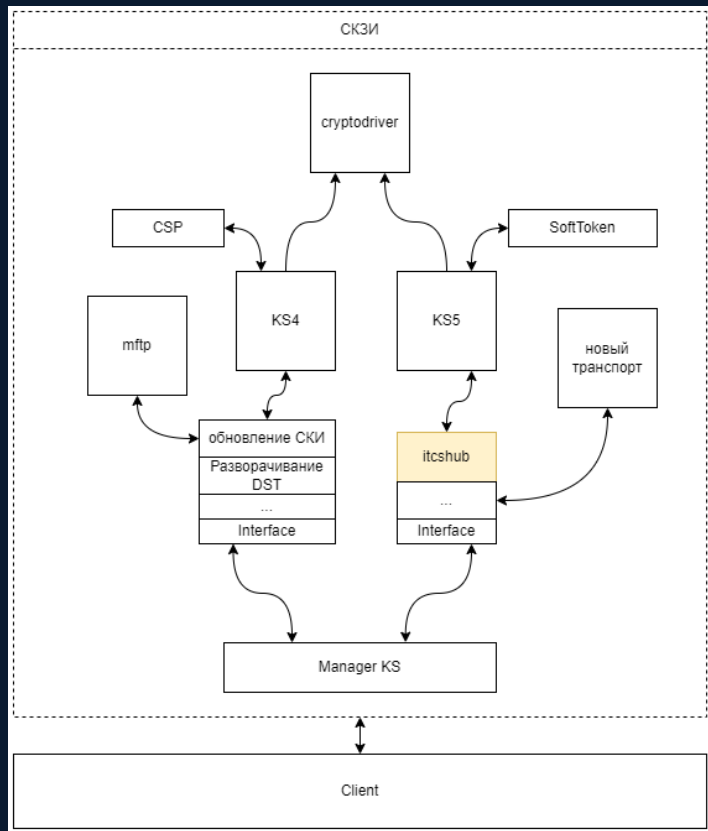
- Поддержка новой ОС Аврора 5 архитектур x32 и x64
- Поддержка ОС Аврора 4
- Работа с VIPNet CSS Connect 3.x
- Совместимость с ключевой системой KS4 и KS5
- Возможно использовать в сетях построенных при помощи VIPNet Administrator и VIPNet Prime
- Управление настройками VIPNet Client в управляющем ПО VIPNet Administrator и VIPNet Prime



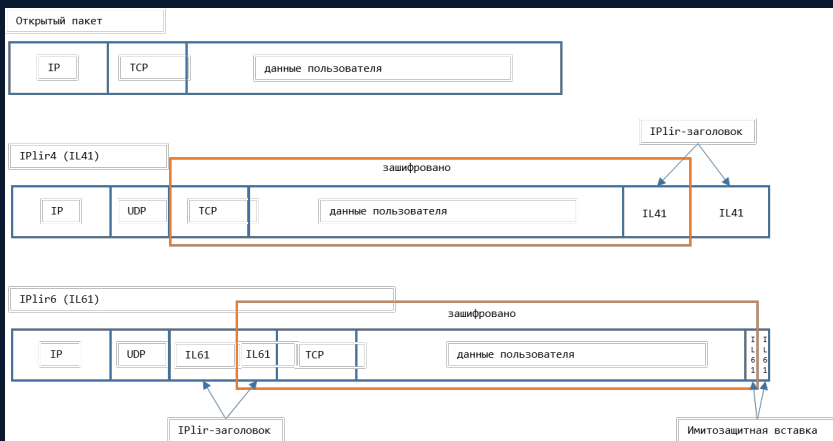
VIPNet Client 5

Особенности 5 поколения продуктов:

- Iplir6 + поддержка IPv6
- Новые ГОСТы («Магма» и «Кузнечик»)
- Новая ключевая система KS5
- Новый транспорт
- Новая система мониторинга NVS
- Единый VPN-клиент
- Широкие возможности централизованного управления



VIPNet Client 5



Основные преимущества IPlir6/INEP6 по сравнению с IPlir4/INEP4

- Новый формат IPlir-пакета - механизм защиты от повторов, поддержка актуальных криптоалгоритмов
- Новая маршрутизация INEP6 - Снижение нагрузки на сеть, уменьшение объема служебного трафика, поддержка IPv6, оптимизация маршрутов
- Новые алгоритмы - внедрение «Магма» и «Кузнечик» на уровне протокола
- Новая архитектура - повышение стабильности работы продуктов



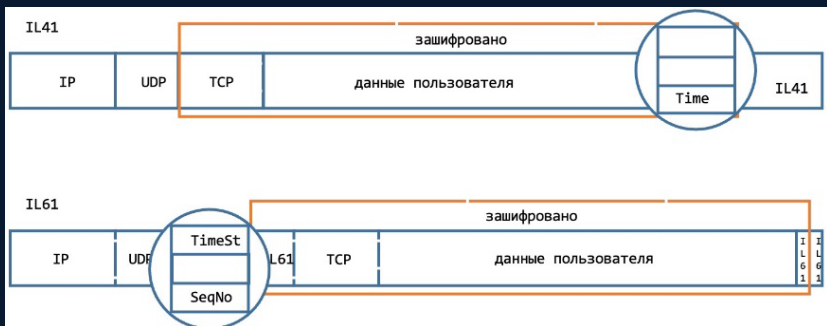


VIPNet Client 5

Механизм защиты от повторов

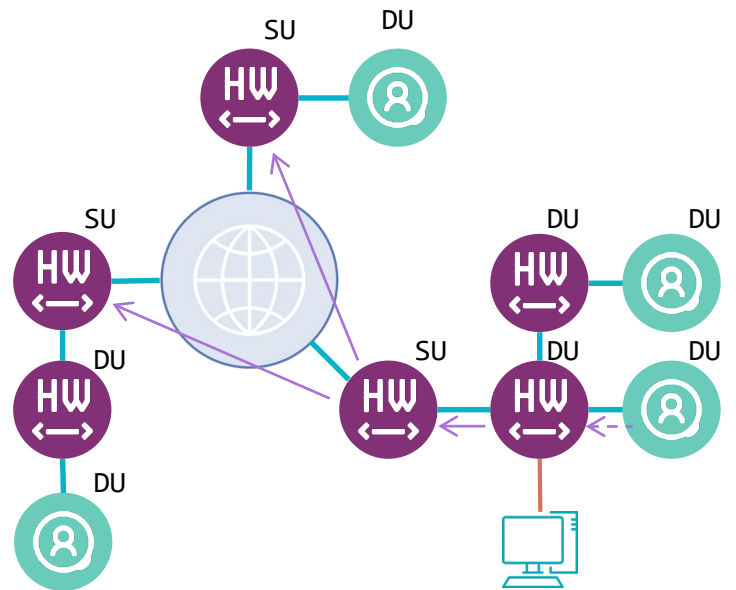
Улучшенный механизм защиты от повторов по требованиям регуляторов

В открытую часть заголовка пакета IP+TCP помимо метки времени добавлен порядковый номер пакета



Новая маршрутизация IPv6

Новые межзловые рассылки



SU Подключение напрямую или за статическим NAT

DU Подключение через сервер соединений

--> Клиентский трафик

→ Служебный трафик

Уменьшение количества служебного трафика при старте сети

Сокращение объема служебного трафика в несколько десятков раз (в зависимости от размеров сети)

Новый, расширяемый и удобный формат сервисных сообщений

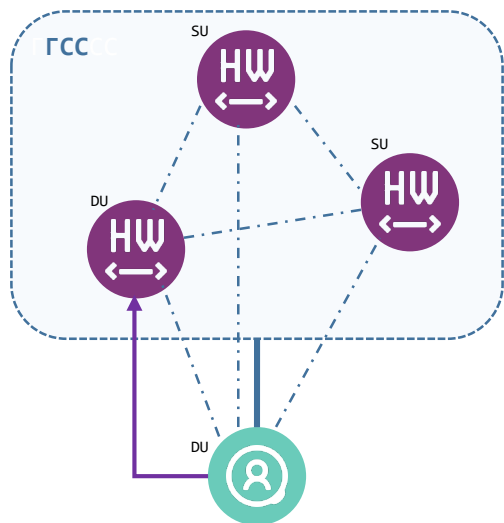
Повышение скорости и стабильности работы ViPNet VPN-узлов

Снижение нагрузки на координаторы и сервера соединений

Маршрутизация IPv6-трафика и работа в смешанных (IPv4 и IPv6) сетях

Новая маршрутизация IPv6

Группы серверов соединений (ГСС)



- Регистрация узла на ГСС
- Выбор сервера соединений из ГСС
- - - Связи ViPNet

Резервирование

Повышение стабильности ViPNet VPN-соединения благодаря возможности автоматического переключения между серверами соединений в процессе работы

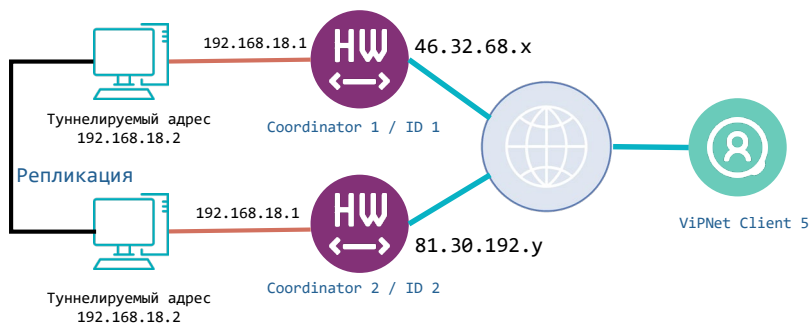
Балансировка нагрузки

Управление и оптимизация нагрузки на сервера соединений, обслуживающих клиентские узлы

Доступ к защищенной сети из Интернет

Стабильное подключение к ViPNet VPN-сети при переключении между различными сетями, например Wi-Fi ↔ LTE

Резервирование. Выбор пути к туннелю



Сценарий приоритезации туннелей для координатора с меньшим id - `tunnel_priority=min_id` (по умолчанию)

- У клиента в связях координаторы с одинаковыми адресами (пересекающиеся туннели)
- `tunnelPriority=min_id`
- Видимость туннелей - реальная

Сценарий резервирования - приоритезации туннелей для Активного координатора с использованием ГСС - `tunnel_priority=active_server`

- У клиента в связях координаторы с одинаковыми адресами (пересекающиеся туннели)
- Включен механизм ГСС
- `tunnelPriority=active_server`
- Видимость туннелей - реальная



VIPNet Client 5



Аутентификация с помощью токенов:

1. Администратор записывает персональный ключ пользователя на внешнее устройство и задает ПИН-код для него во время создания дистрибутива ключей
2. Пользователь самостоятельно меняет тип аутентификации

Многофакторная аутентификация

VipNet Client осуществляет взаимодействие с сервером аутентификации VipNet через REST API

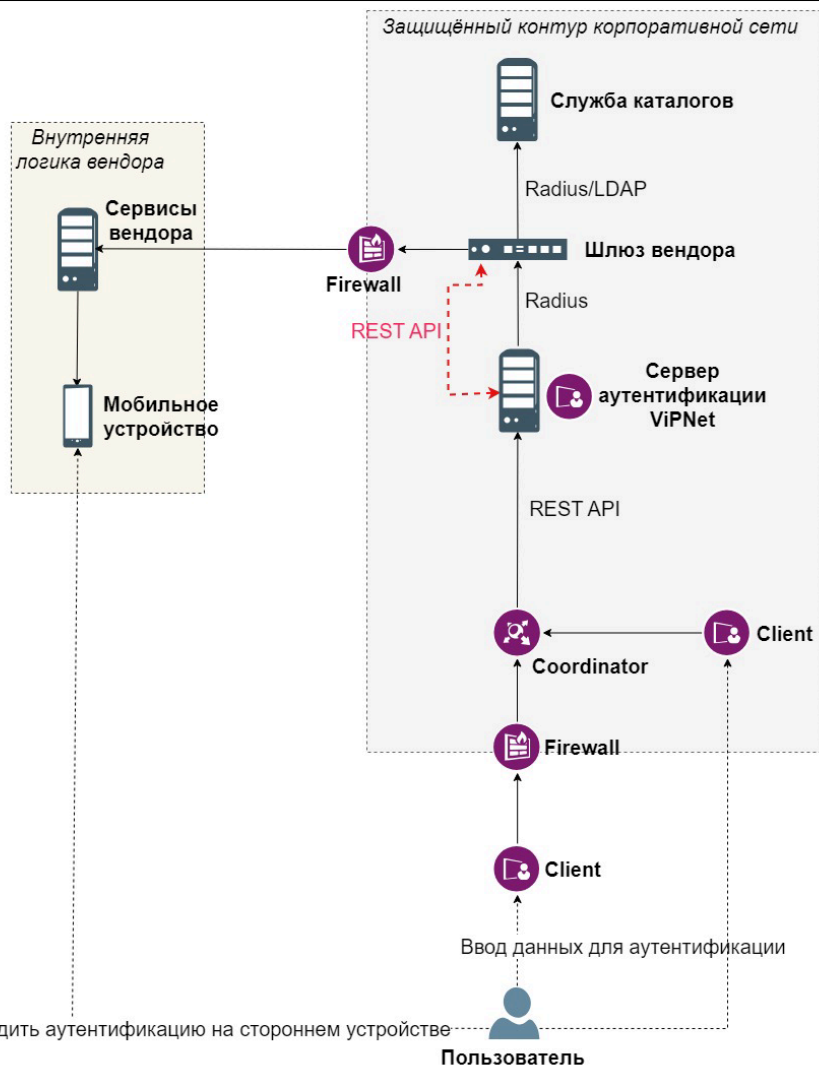
Сервер аутентификации должен обязательно находиться внутри защищённой сети VipNet

Сервер аутентификации преобразовывает запрос по REST API в запрос по протоколу RADIUS и отправляет на шлюз вендора

Multifactor Radius adapter реализовывает внутреннюю логику вендора Multifactor по процессу аутентификации - взаимодействуя с службой каталогов и облачным сервисом Multifactor

Сервер преобразует ответ RADIUS в ответ REST API и отправляет обратно в Client

На привязанном к аккаунту пользователя мобильном устройстве осуществляется генерация и/или подтверждение 2-го фактора (СМС, OTP, Push)





VIPNet Client 5

Управление детальными настройками VIPNet Client 5 через custom.yaml

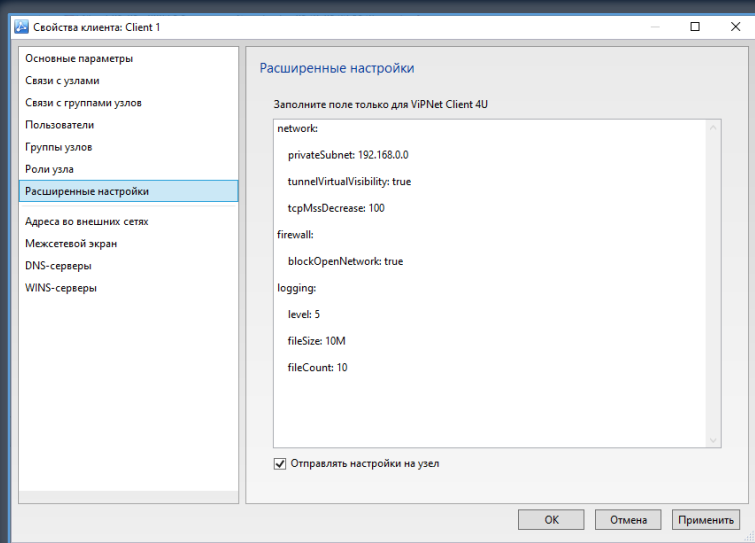
Секция **network**:

privateSubnet – диапазон частных IP-адресов для TUN интерфейса. Значение в VIPNet Client 4U по умолчанию – 7.0.0.0

tcpMssDecrease – уменьшение параметра MSS (максимальный размер сегмента) для протокола TCP на указанное число байт

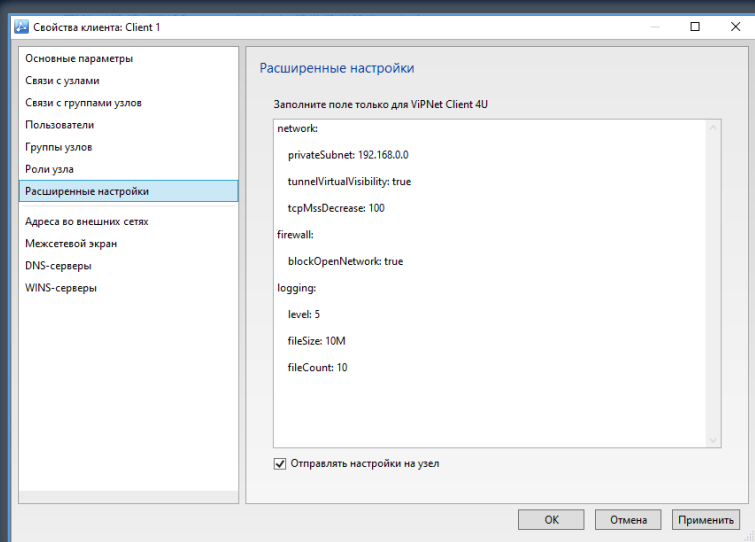
mtuOnTun – максимальный размер исходящего пакета на TUN-интерфейсе устройства в байтах. Значение в VIPNet Client 4U по умолчанию – 1500

enableDnsSD – поиск устройств VIPNet в локальной сети по протоколу DNS Service Discovery для последующего взаимодействия с ними напрямую (без участия координатора) по протоколам IPv4 и IPv6





VIPNet Client 5



Управление детальными настройками VIPNet Client 5 через custom.yaml

Секция **firewall**:

blockOpenNetwork – **блокировка** всего открытого IP-трафика устройства при включенном VIPNet-соединении
appsVpnAccessMode – режим доступа приложений на устройстве в сеть VIPNet. Вы можете указать один из трех режимов:

all – доступ в сеть VIPNet **разрешен** всем приложениям. (по умолчанию)

allowList – доступ в сеть VIPNet **запрещен** всем приложениям, кроме исключений, указанных в параметре `appsAllowList`

blockList – доступ в сеть VIPNet **разрешен** всем приложениям, кроме исключений, указанных в параметре `appsBlockList`

appsAllowList – список идентификаторов приложений, которым **разрешен** доступ в сеть VIPNet

appsBlockList – список идентификаторов приложений, которым **запрещен** доступ в сеть VIPNet





VIPNet Client 5



Управление VPN через SDK API

VIPNet Client 5 позволяет реализовать интеграцию с прикладным приложением, подписанным сертификатом ИнфоТеКС и обеспечить:

- Установку дистрибутива ключей из доступного файла
- Удаление дистрибутива ключей
- Включение VPN-соединения
- Отключение VPN-соединения
- Получение информации об узле
- Получение уникального идентификатора приложения VIPNet Client



VIPNet Client 5



Планы сертификации по требованиям ФСБ России

VIPNet Client 5 for Linux

- СКЗИ класса КС1-КС3
- МЭ 4 класса

VIPNet Client 5 for Windows

- СКЗИ класса КС1-КС3
- МЭ 4 класса

VIPNet Client 5 for Android

- СКЗИ класса КС1

VIPNet Client 5 для ОС Аврора

- СКЗИ класса КС1 и КС2

ТЕХНО infotecs
2024 Фест

Алексей Минаков
Менеджер продуктов

Aleksey.Minakov@infotecs.ru

Подписывайтесь на наши соцсети

