

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

к закупке услуг по организации и обслуживанию выделенного защищённого канала передачи видеоданных от объектов видеонаблюдения до Центра оперативного управления Департамента полиции

Регион оказания услуг: Туркестанская область (либо иной регион, указанный Заказчиком).

Объект(ы), количество, сроки и цена: устанавливаются документацией конкретной закупки и приложением с перечнем адресов.

1. Предмет и результат оказания услуги

Поставщик обеспечивает организацию, подключение, конфигурирование, эксплуатацию и техническое сопровождение логически выделенного канала передачи данных для доставки видеопотоков DVR/NVR/IP-камер Заказчика в ЦОУ ДП. Услуга является специализированной услугой передачи данных, а не предоставлением обычного доступа к сети Интернет.

Результат: работоспособная двусторонняя IP-связность между согласованными адресами объектов и ЦОУ, возможность просмотра согласованного количества потоков и документально подтверждённые параметры передачи.

2. Приоритетная архитектура сети

- Основной (предпочтительный) вариант — операторская частная сеть мобильной передачи данных RAN с закрытой абонентской группой, выделенной адресацией, изоляцией трафика от общедоступного Интернета и управляемой маршрутизацией до точки присоединения к ЦОУ.
- Поставщик организует соединение с ЦОУ посредством согласованного выделенного операторского стыка или эквивалентного частного межсетевого соединения (включая VRF/MPLS L3VPN либо иной закрытый транспорт). Конкретная реализация должна обеспечивать логическую изоляцию и контролируемые маршруты.
- Для объектов без технической возможности RAN допускается альтернативный выделенный канал (волоконно-оптическая линия, выделенный радиоканал, частная операторская L3VPN), отвечающий тем же требованиям безопасности и качества.
- Использование WireGuard поверх публичной IP-сети допускается только как исключение либо резервный вариант при отсутствии подходящего закрытого транспорта, при письменном согласовании с Заказчиком и принимающей стороной ЦОУ и соблюдении требований раздела 3.
- Исполнитель обеспечивает адресацию, межсетевые правила, отсутствие сквозного доступа между объектами без согласования, защиту административного доступа и отсутствие необходимости публиковать камеры/регистраторы через публичные IP-адреса.

3. Информационная безопасность и ограничения на публичные туннели

3.1. При передаче видеотрафика запрещается строить основной канал путём организации поверх общедоступной сети Интернет туннелей следующих типов (независимо от коммерческого названия услуги):

- PPTP; L2TP без IPsec; L2TP/IPsec; SSTP; OpenVPN (TCP/UDP); SSL VPN/TLS VPN общего назначения; SoftEther VPN; Cisco AnyConnect/OpenConnect и аналогичные удалённые VPN-клиенты;
- GRE и его варианты (в том числе GRE over IPsec), EoIP, IP-in-IP/IPIP, SIT/6in4, 6rd, 6to4, ISATAP, Teredo, GRE-TAP, VXLAN, GENEVE, L2TPv3 при их применении как туннелей через публичный Интернет;

- IPsec tunnel mode / IKEv1 / IKEv2, DMVPN, VTI, FlexVPN и аналогичные решения — если они используются как способ построения основного канала через общедоступный Интернет;
- SSH-туннели, SOCKS/HTTP CONNECT-прокси, reverse tunnels, коммерческие облачные overlay/mesh VPN и иные транзитные туннели через публичные серверы или узлы третьих лиц.

3.2. Перечень устанавливает ограничение на архитектуру доставки видеотрафика через публичный Интернет, а не утверждает, что каждый указанный протокол криптографически уязвим. Использование перечисленных технологий внутри изолированной сети оператора допускается, если это не нарушает условий изоляции, согласовано с принимающей стороной и не требует выхода видеотрафика в Интернет.

3.3. Допустимое исключение — WireGuard: современные параметры шифрования и управление ключами, индивидуальные ключи узлов, минимальные AllowedIPs, ограничения по firewall, отсутствие открытого управления регистраторами, журналирование административных действий и согласованный список конечных IP-адресов. Использование WireGuard само по себе не является доказательством соответствия всем требованиям защиты.

3.4. Не допускаются: NAT/port-forwarding камер и регистраторов в Интернет; прямой доступ к управлению NVR/DVR из Интернета; публичные облачные P2P-посредники для передачи основного потока без отдельного согласования; общие пароли по умолчанию; маршруты от объектов к посторонним сетям; предоставление третьим лицам доступа без разрешения.

3.5. Поставщик предоставляет схему с обозначением границ сетей и точек сопряжения (без раскрытия секретных ключей), описание способа изоляции, адресный план, матрицу доступов и результаты проверки отсутствия публичной экспозиции.

4. Параметры каналов и видеотрафика

- На каждом объекте: не менее 10 Мбит/с в направлении от объекта к ЦОУ и не менее 2 Мбит/с в обратном направлении; расчётная нагрузка — до пяти параллельных потоков по 2 Мбит/с каждый. При большем количестве камер пропускная способность уточняется с учётом кодеков, битрейтов и одновременных просмотров.
- На принимающей стороне ЦОУ: исходный ориентир — не менее 50 Мбит/с на приём видеопотоков и не менее 20 Мбит/с на передачу команд/данных; необходимая фактическая агрегированная ёмкость определяется количеством одновременно активных объектов и потоков.
- Целевые показатели на согласованном измерительном интервале при штатной нагрузке: потери пакетов не более 0,1%; RTT-задержка не более 150 мс; вариация задержки (jitter) не более 80 мс. Порядок, период и точки измерения фиксируются при приёме.
- Поддержка QoS/приоритизации видеотрафика в управляемой сети Поставщика; IPv4-маршрутизация согласно согласованному плану; поддержка необходимых портов и протоколов DVR/NVR без открытия их в Интернет.

5. Подключение и монтаж

- Поставщик обследует объект, согласует способ связи и точку установки оборудования, организует подключение клиентского маршрутизатора (CPE) к существующей локальной сети/видеорегистратору.
- Установка и настройка CPE, SIM-карт (при PAPN), маршрутизации, ACL/firewall, проверка регистрации абонентского устройства в закрытом сегменте оператора и доступности ЦОУ.
- Настройка сопряжения с действующими DVR/NVR и проверка вывода видеопотоков. Замена устаревших регистраторов и строительство новой СКС не входят автоматически в услугу связи и оговариваются в смете/отдельном задании.
- Начало подключения — в срок, определённый закупочной документацией, при условии доступа к объекту, исправности камер/регистратора и предоставления необходимых согласований и

реквизитов доступа. Рекомендованный ориентир — 3 календарных дня после выполнения этих условий.

6. Обслуживание, мониторинг и ответственность

- Мониторинг состояния управляемых каналов и доступности оборудования — 24/7; регистрация инцидентов и журнал работ.
- Приём обращений Заказчика — по указанным в договоре каналам; реакция на критическую аварию — в срок, установленный SLA. Исходный ориентир для начала устранения — не позднее 24 часов с момента регистрации обращения, с учётом доступности объекта.
- Поставщик отвечает за свою сеть и предоставленное СРЕ; Заказчик обеспечивает электропитание, физический доступ, исправность собственного видеорегистратора, камер и внутренней СКС, если иное не предусмотрено договором.
- Отключение/смена маршрутов к ЦОУ и существенные изменения схемы согласуются с принимающей стороной.

7. Приёмочные испытания и подтверждающие материалы

- Акт установки/настройки СРЕ и схема логического подключения, содержащая описание PAPN или согласованного альтернативного канала.
- Демонстрация вывода согласованного числа видеопотоков в ЦОУ, тесты связности, измерение пропускной способности, потерь, задержки и jitter.
- Подтверждение отсутствия доступности IP-адресов DVR/NVR через публичный Интернет и отсутствия неразрешённых маршрутов/публичных туннелей.
- Передача контактов технической поддержки, порядка регистрации заявок и границ ответственности.
- Окончательное подтверждение корректности вывода камер в ЦОУ выдает уполномоченная принимающая сторона; Поставщик содействует тестированию и оформлению результатов.

8. Требования к подтверждению соответствия участника

В составе предложения участник предоставляет описание предлагаемой архитектуры, документы/письма о возможности организации закрытого операторского транспорта либо иные подтверждения доступа к необходимой инфраструктуре, сведения о службе поддержки, о средствах мониторинга и гарантию соблюдения параметров качества. Не допускается требование использования оборудования или услуг только одной торговой марки при наличии функционально эквивалентного решения.

9. Примечания для окончательной редакции закупки

Настоящий документ — проект технической спецификации. До публикации следует заполнить список объектов, точку стыка с ЦОУ, длительность, SLA и модель оплаты; согласовать возможность PAPN с операторами и принимающей стороной; отдельно проверить со специалистом по госзакупкам РК, чтобы ограничения были соразмерны цели и не препятствовали конкуренции без объективного обоснования.

Основа: техническая спецификация из приложения № 1 к представленному договору (стр. 11–14). Разделы о PAPN, публичных туннелях, WireGuard, приёмке и границах ответственности переработаны для тендерной версии.