

Безопасность и персональные данные

Что остаётся на объекте, кто и как получает доступ, как защищены доказательства, на каком основании работает распознавание и как обеспечиваются права людей. Документ для службы безопасности, ИТ, юристов и ответственного за обработку персональных данных.

Редакция 1.0 от 11.10.2026. Документ носит информационный характер, описывает типовую поставку и не является публичной офертой. Состав работ и условия фиксируются в договоре. Раздел о персональных данных — техническое описание и рекомендации, а не юридическое заключение.

Схема пути данных

Камеры объекта передают видео на аналитический блок n7kel на объекте. Сырое видео остаётся на объекте; на сервер уходят только подписанные события с кадром и коротким фрагментом. В автономном варианте сервер тоже находится у заказчика, и внешних соединений нет.



1. Главное

- Данные остаются у заказчика.** Вся информация конфиденциальна и не передаётся третьим лицам. Исключения — только те, что прямо предусмотрены договором и законом: передача сведений о совпадении уполномоченному органу при подключённом модуле

проверки по базам розыска (по соглашению с ним) и обработка по поручению заказчика в гибридном варианте. Необходимые ограничения устанавливаются по запросу заказчика.

2. **Распознавание посетителей выключено по умолчанию.** Оно включается только по решению заказчика как отдельный модуль и только на законном основании — согласии человека или соглашении с уполномоченными государственными органами. Сотрудники опознаются только с письменного согласия.
3. **Видео остаётся на объекте.** Постоянной записи нет: блок n7kel держит в памяти только последние секунды для видеофрагментов. Наружу — в гибридном варианте — уходят только событие, кадр и фрагмент около 10 секунд. В автономном варианте наружу не уходит ничего.
4. **Биометрия не покидает контур заказчика.** Эталоны хранятся в зашифрованном виде; фотографии не сохраняются; при отзыве согласия эталон удаляется.
5. **Каждый доступ к доказательствам записывается.** Просмотр и скачивание кадров и видеофрагментов фиксируются в журнале действий, в том числе действия специалистов поставщика.
6. **Записи защищены от правки задним числом.** Каждое событие подписано на блоке и сцеплено с предыдущим; проверка, в том числе независимая, выявляет изменение, удаление или вставку записи.
7. **Решение принимает человек.** Сигналы платформы — основание для проверки, а не для автоматических мер в отношении сотрудника.

2. Какие данные обрабатываются и где хранятся

Платформа не ведёт непрерывную видеозапись. Если на объекте есть видеорегистратор, он работает по своим правилам и вне платформы.

ДАННЫЕ	ГДЕ ХРАНЯТСЯ	ПОКИДАЮТ ЛИ ОБЪЕКТ
Видеопоток камер	Нигде: блок n7kel держит в памяти только последние секунды для видеофрагментов	Нет
Эталоны лиц сотрудников	Блок n7kel, в зашифрованном виде; фотографии не сохраняются	Нет
Эталоны лиц пациентов и клиентов (только при включённых модулях)	В контуре заказчика, в зашифрованном виде	Нет
Данные проверки по базам розыска (только при подключённом модуле)	Журнал проверок — сервер заказчика; порядок получения списков определяется соглашением с органом	Сведения о совпадении — уполномоченному органу согласно соглашению

ДАННЫЕ	ГДЕ ХРАНЯТСЯ	ПОКИДАЮТ ЛИ ОБЪЕКТ
Записи и расшифровки речи (n7kel Voice)	Сервер заказчика; в гибридном варианте — по договору	Автономный вариант — нет; гибридный — по договору
Кадр и видеофрагмент по событию	Блок n7kel (до отправки и 3 суток после) и сервер	Гибридный вариант — на сервер платформы; автономный — нет
Сведения о событиях: время, пост, тип, кто опознан	Блок n7kel, сервер	Гибридный вариант — на сервер платформы; автономный — нет
Справочник сотрудников, отметки о согласии	Сервер	Вводит заказчик
Операции кассы	Сервер	Передаёт кассовая система заказчика
Оценка состояния (только при включённом модуле)	Блок n7kel → сервер, без изображений	Гибридный вариант — на сервер платформы; автономный — нет
Аналитика за период	Сервер	Изображений не содержит

3. Сеть и внешние соединения

3.1. Блок n7kel соединяется только с сервером платформы (в автономном варианте — с сервером заказчика) и внутри объекта — с камерами, DNS и NTP. Ни один компонент блока не обращается к третьим сторонам: ни за обновлениями, ни за лицензиями, ни со статистикой использования. Обмен с государственными базами при подключённом модуле проверки по базам розыска выполняет сервер — по каналу, определённом соглашением с органом.

3.2. Входящих соединений к блоку из интернета не требуется. В протоколе обмена блока с сервером нет способа передать видеопоток.

3.3. Доступ пользователей и внешних систем к серверу — только по HTTPS. Рекомендуется выделить камеры в отдельный сегмент сети и ограничить соединения блока межсетевым экраном объекта.

3.4. При приёме выполняется проверка исходящих соединений блока; её результат прикладывается к протоколу приёма.

3.5. Распознавание выполняет ИИ n7kel на оборудовании заказчика: зарубежные и облачные сервисы распознавания, внешние API и подписки не используются, данные за рубеж не передаются. ИИ n7kel обучен и проверен на обычной 2D-картинке, поэтому подходят уже установленные камеры. 3D-камеры тоже поддерживаются — если они есть на объекте или нужны для задачи.

4. Роли и права доступа

Каждый раздел и каждый запрос проверяют роль пользователя и доступные ему объекты.

РОЛЬ	КТО ЭТО	ОСНОВНЫЕ ПРАВА
Администратор организации	Ответственный за систему у заказчика	Все разделы организации: справочники, пользователи, настройки, касса, API-ключи и вебхуки, сроки хранения; включение модуля оценки состояния
Специалист по охране труда / служба безопасности	Служба безопасности, охрана труда	Дашборд, разбор нарушений, журнал событий, аналитика, проверка целостности и выгрузка пакета доказательств
Руководитель объекта	Управляющий АЗС, начальник участка	Те же права, что у службы безопасности, но только по назначенным объектам
Аудитор	Ревизор, внутренний аудит	Только просмотр: дашборд, нарушения, журнал событий, аналитика, отчёты о целостности, касса, журнал действий

5. Учётные записи и доступ к доказательствам

- учётные записи персональные; передача учётных данных другим лицам не допускается;
- подбор пароля ограничен: после нескольких неверных попыток вход временно блокируется, время блокировки растёт с каждой ошибкой; блокировки записываются в журнал;
- смена пароля, отключение учётной записи, изменение роли или объектов немедленно завершают все сеансы пользователя;
- ссылка на кадр или видеофрагмент выдаётся конкретному пользователю, действует 15 минут и только пока у него есть доступ к объекту;
- в оповещениях (вебхуки, Telegram, почта) ссылок на изображения нет; внешние системы получают кадры только по ключу с отдельным правом;
- специалисты поставщика работают в отдельном разделе и получают доступ к данным заказчика только по его запросу; каждый такой доступ виден администратору и аудитору заказчика.

6. Журнал действий

6.1. Журнал действий фиксирует, кто, когда и что сделал в системе: входы, просмотр и скачивание доказательств, изменение статусов нарушений, справочников, сроков хранения, ключей доступа и настроек приватности.

6.2. Журнал сам построен как цепочка записей: его изменение выявляется проверкой. Срок хранения журнала по умолчанию — 1095 суток.

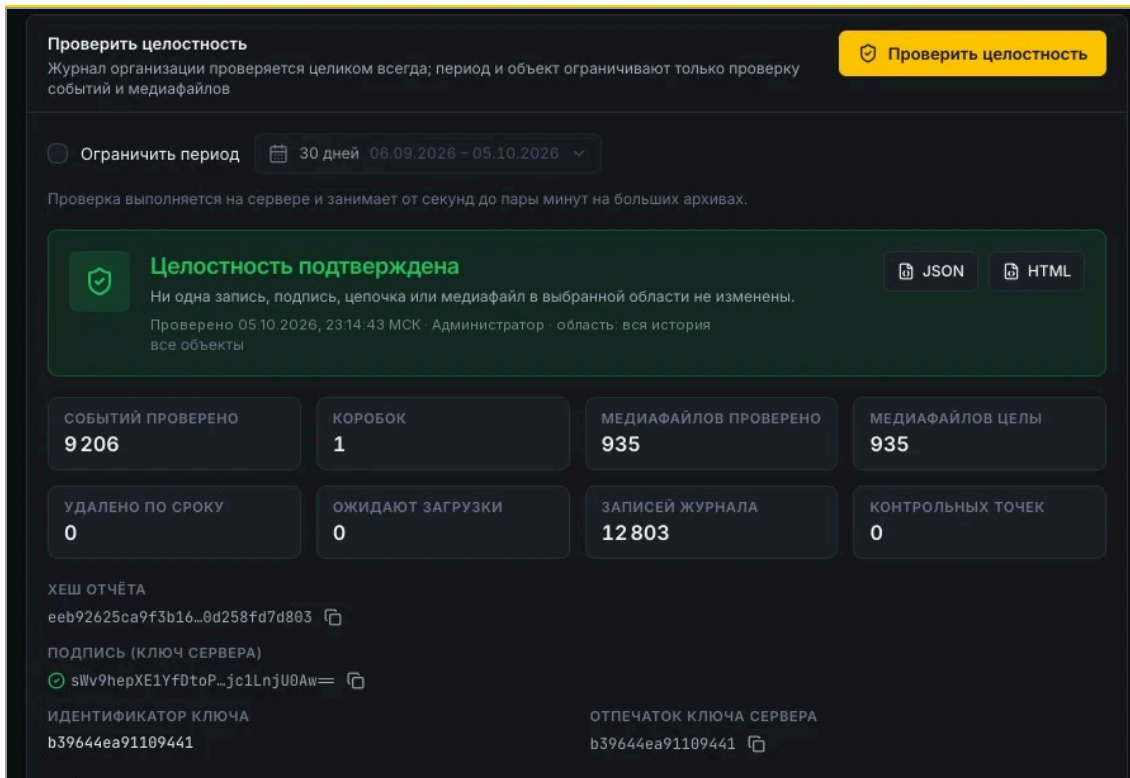
6.3. Каждый запрос внешней системы по API-ключу, включая отклонённые, записывается в журнал обращений (по умолчанию хранится 180 суток).

■ ДОКАЗАТЕЛЬСТВА

7. Целостность доказательств

Каждое событие сохраняется с кадром момента и видеофрагментом и защищено так, что правка задним числом выявляется проверкой.

- **Нумерация.** У каждого блока свой непрерывный счёт событий: пропуск номера сразу виден.
- **Сцепление.** Каждая запись содержит отпечаток предыдущей: изменить одну запись незаметно нельзя.
- **Подпись блока.** Событие подписывается ключом, который есть только на блоке; ни сервер, ни пользователи не могут создать или исправить запись от его имени.
- **Кадр и видео в подписи.** Отпечатки файлов входят в подписанную запись: замена кадра или обрезка видео выявляется.
- **Контрольные точки у заказчика.** Состояние общего журнала регулярно подписывается и хранится на оборудовании заказчика: незаметно переписать историю не может и поставщик.



«Защита записи» в карточке события. Демонстрационный стенд.

8. Проверка целостности и независимая проверка

8.1. В разделе «Целостность» уполномоченный пользователь выбирает период и объект и запускает проверку. Сервер заново проверяет подписи, непрерывность цепочек, наличие и неизменность кадров и видеофрагментов, совпадение данных в базе с подписанными записями, а также операции кассы. Результат — подписанный отчёт, который можно скачать и приложить к материалам.

8.2. Для разбирательства выгружается пакет доказательств за период: подписанные события, журнал, контрольные точки, кадры и видеофрагменты, инструкция по проверке.

8.3. Пакет проверяется **без сервера платформы и без участия поставщика**: юрист, аудитор или эксперт запускает программу проверки из комплекта поставки на любом компьютере. Программа не обращается к сети. Отпечаток ключа сервера сверяется с указанным в договоре — так подтверждается, что пакет выдан именно вашей установкой.

8.4. Что доказывает проверка: кадр и видеофрагмент — ровно те, что блок записал в момент события; ни одно событие не изменено, не удалено и не вставлено задним числом. Чего проверка не доказывает: что сцена перед камерой была подлинной и что ИИ n7kel понял её правильно — поэтому событие остаётся сигналом для проверки человеком.

9. Сроки хранения

Сроки устанавливает заказчик. Удаление по сроку выполняется автоматически и само фиксируется в журнале целостности, поэтому проверка отличает удаление по сроку от подделки. Отметка «юридическое удержание» сохраняет материалы спора до её снятия.

ДАННЫЕ	ПО УМОЛЧАНИЮ, СУТОК	ДОПУСТИМЫЙ ДИАПАЗОН, СУТОК
Видеофрагменты событий	30	1–3650
Кадры событий	90	1–3650
События, нарушения и операции кассы	365	7–3650
Сведения о состоянии оборудования	30	1–3650
Журнал обращений к API	180	7–3650
Журнал действий пользователей	1095	90–3650

10. Обезличивание

- лица и головы всех людей, кроме человека, к которому относится событие, размываются на блоке необратимо — до сохранения и подписи; хранится и показывается только размытая версия;
- для событий без конкретного человека (например, «пост пустует») размываются все;
- люди без согласия на опознание остаются в событиях анонимными («эталона нет»);
- аналитика за период содержит только числа, без изображений.

11. Опознание по лицу и согласие

11.1. Опознание сотрудников по лицу применяется только к тем, кто дал письменное добровольное согласие. Без отметки о согласии блок не регистрирует эталон, и сотрудник не опознаётся.

11.2. Предоставление биометрии не может быть обязательным. Без эталонов работают присутствие на посту, пустые посты, контроль СИЗ, опасные зоны и сверка с кассой — они не требуют установления личности.

11.3. При отзыве согласия эталоны сотрудника удаляются с блока, обычно в течение минуты.

11.4. Статус «эталона нет» никогда не считается несовпадением: такой человек не порождает событий «неопознанный человек», «работа под чужой учётной записью» и «за кассой не тот, кто вошёл в систему». Статус «не определено» (лицо не видно, человек спиной к камере) также не приводит к обвинению.

11.5. Распознавание посетителей, клиентов и пациентов по умолчанию выключено. Модули, которые его включают, описаны в разделе [17](#); каждый из них включается только по решению заказчика и только на законном основании.

12. Модуль оценки состояния: выключен по умолчанию

12.1. Вспомогательный модуль оценивает усталость и напряжение работника относительно его личной нормы. Распознавание эмоций работников ограничено законом в ряде юрисдикций, поэтому:

- модуль выключен по умолчанию и полностью отключается настройкой: при выключенном модуле его компоненты на блок не загружаются, данные не формируются, остальная система работает без изменений;
- включение возможно только при наличии функции в лицензии и решением администратора организации с подтверждением правового уведомления; подтверждение записывается в журнал;
- модуль никогда не создаёт, не усиливает и не повышает приоритет нарушений и не является основанием для дисциплинарных или кадровых решений;
- личная норма — несколько чисел в оперативной памяти блока, пока человек в кадре: на диск и на сервер она не попадает и для опознания не пригодна;
- по умолчанию аналитика показывает только сводные данные по сменам и часам; данные по отдельному сотруднику видит только администратор организации, и каждый такой просмотр записывается в журнал.

12.2. Включать модуль без отдельного правового анализа не рекомендуем.

13. Персональные данные и применимое законодательство

13.1. Оператором персональных данных является заказчик: он определяет цели обработки, состав сотрудников, посты, сроки хранения, круг лиц, имеющих доступ, и другие ограничения. Все данные остаются у заказчика, конфиденциальны и не передаются третьим лицам, кроме случаев, прямо предусмотренных соглашением и законом. В автономном варианте данные есть только у заказчика, поставщик к ним доступа не имеет. В гибридном варианте поставщик обрабатывает данные по поручению заказчика на основании договора.

13.2. Платформа рассчитана на требования законодательства о персональных данных страны заказчика:

- Республика Казахстан — Закон «О персональных данных и их защите», включая требование хранить персональные данные в базе на территории Республики Казахстан: в автономном варианте сервер стоит у заказчика, в гибридном — в центре обработки данных на территории страны;
- Республика Армения — Закон «О защите персональных данных»;
- другие юрисдикции — по запросу, при обследовании.

13.3. Рекомендуемые цели обработки для локального акта: охрана труда (СИЗ, опасные зоны), организация работы на постах, сохранность денежных средств (сверка с кассой); настройка распознавания на размеченных примерах объекта — если заказчик включил эту цель в локальный акт. Правила работают только внутри размеченных зон и в активные смены поста; вне зон ничего не фиксируется.

13.4. До ввода в эксплуатацию заказчику рекомендуется:

1. принять локальный акт о применении видеоаналитики: цели, зоны, сроки хранения, доступ, порядок разбора нарушений;
2. ознакомить сотрудников с уведомлением под подпись — шаблон предоставляем;
3. получить письменные согласия на опознание по лицу — только от желающих;
4. разместить таблички о видеонаблюдении в зонах обзора камер;
5. в гибридном варианте — оформить поручение на обработку персональных данных;
6. при включении n7kel Voice — уведомить сотрудников и клиентов о записи звука (таблички, информирование при звонке);
7. при включении распознавания пациентов или клиентов — утвердить порядок получения и отзыва согласия;
8. при включении проверки по базам розыска — заключить соглашение с уполномоченным органом.

13.5. Окончательную правовую оценку порядка применения, включая модуль оценки состояния, выполняет юрист заказчика. Мы предоставляем описание мер защиты и шаблон уведомления персонала.

14. Права субъектов данных

Права сотрудников, а также пациентов и клиентов, распознаваемых с их согласия:

- узнать, какие данные о нём обработаны, — через ответственного за обработку персональных данных у заказчика;
- увидеть кадр и видеофрагмент по событию, дать объяснение и оспорить нарушение; при споре может быть выгружен пакет доказательств с независимой проверкой;
- отозвать согласие на распознавание по лицу — эталон удаляется, дальше человек не распознаётся;

- рассчитывать на удаление данных по истечении установленных сроков хранения — оно выполняется автоматически и фиксируется в журнале.

Обращения сотрудников принимает заказчик как оператор персональных данных; платформа предоставляет для этого карточку сотрудника и выгрузку его событий.

15. Защита продукта и обновлений

- лицензия подписана и привязана к оборудованию блока: перенесённая на другую машину, она не работает;
- ИИ n7kel поставляется в зашифрованном виде и открывается только лицензией конкретного блока; программа блока поставляется в скомпилированном виде, без исходного кода;
- обновления подписаны: перед установкой проверяются подпись и контрольная сумма, понижение версии запрещено, при сбое — автоматический откат на предыдущую версию;
- программа блока работает от отдельного пользователя с минимальными правами.

Условия использования, запрет обратной разработки, порядок доступа к оборудованию и уничтожение накопителя при прекращении договора фиксируются в лицензионном договоре.

16. n7kel Контроль АЗС: меры защиты

- каждая кассовая операция получает цифровое доказательство в цепочке отпечатков SHA-256; целостность проверяется в один клик, подмена записи выявляется проверкой;
- доступ по ролям: администратор, служба безопасности, менеджер, диспетчер;
- речевая аналитика подключается через n7kel Voice: запись и анализ речи включаются только при уведомлении сотрудников и покупателей (таблички в зоне кассы) и при наличии правового основания, определённого заказчиком (раздел [18](#));
- статус доставки каждого оповещения по e-mail, Telegram и SMS можно проверить;
- опознание кассира по лицу предусмотрено архитектурой и применяется только с согласия сотрудников.

17. Модули распознавания посетителей и клиентов

17.1. Распознавание посетителей, клиентов и пациентов выключено по умолчанию. Его включает только заказчик, отдельно для каждого модуля, после правовой оценки своего юриста.

МОДУЛЬ	ЗАКОННОЕ ОСНОВАНИЕ	КОГО КАСАЕТСЯ
Вход пациентов по лицу (n7kel Access)	Согласие пациента, данное при записи на приём	Только пациенты, давшие согласие; остальные регистрируются как обычно
Персональная аналитика визита (n7kel Flow)	Согласие клиента, который сам предоставил лицо	Только клиенты, давшие согласие; остальные учитываются обезличенно
Проверка по базам розыска (n7kel Вахта, n7kel Access)	Соглашение с уполномоченными государственными органами и закон	Номера автомобилей и лица посетителей в зоне въезда и входа
Опознавание сотрудников	Письменное согласие сотрудника	Только сотрудники, давшие согласие

17.2. При проверке по базам розыска оповещение о совпадении получает уполномоченный сотрудник службы безопасности заказчика и — согласно соглашению — орган. Иная передача данных не производится. При отсутствии совпадения никаких выводов о человеке не делается.

17.3. Эталоны хранятся в контуре заказчика в зашифрованном виде и удаляются при отзыве согласия и по срокам, установленным заказчиком.

18. Звук и речь (n7kel Voice)

18.1. Системы n7kel могут работать со звуком: продукт n7kel Voice переводит речь в текст и анализирует её на любых языках. Модуль включается только по решению заказчика.

- запись и анализ звука — только при уведомлении сотрудников и клиентов (таблички в зоне обслуживания, информирование при звонке) в порядке, установленном законом страны;
- анализ ведётся только в размеченных зонах обслуживания и в рабочие смены;
- речь распознаётся на оборудовании заказчика, внешние сервисы распознавания не используются;
- сроки хранения записей и расшифровок и права доступа устанавливает заказчик; каждое прослушивание и скачивание записывается в журнал;
- правовое основание определяет заказчик как оператор персональных данных; окончательную оценку даёт его юрист.