

Integrations, REST API and webhooks

How n7kel products exchange data with the POS system, 1C and ERP, security systems, notification channels and virtually any other client system. This document describes purpose and capabilities; the technical interface specification is provided upon connection.

Version 1.0, October 11, 2026. This document is for information purposes only, describes a standard delivery and does not constitute an offer. The scope of work and terms are set out in the contract.

1. Principle

1.1. Everything visible in the n7kel Vakhta web interface is available to external systems. Two exchange methods are provided:

- **REST API** — the external system requests data or sends it to the platform;
- **webhooks and notifications** — the platform itself reports events: to your system, by e-mail, to Telegram.

1.2. Integration is possible with virtually any client system: if a system has an API, a database, a file export or a message queue, it can be connected (section [10](#)).

1.3. A machine-readable interface specification and developer instructions are provided to the client's IT department upon connection. In the autonomous option, all interfaces operate within the client's network.

2. Typical integrations

SYSTEM	WHAT IS TRANSFERRED	METHOD
POS system, fiscal data	To the platform: receipts, refunds, voids, no-sale transactions, cashier logins, shifts	REST API in batches or a CSV/XLSX file export
1C, ERP	From the platform: violations, summaries, reports; to the platform: cash transactions and reference data	REST API, webhooks, CSV/XLSX exports; if needed, through an intermediate service
Security department, security console, access control	From the platform: violations and critical events in real time, status of cameras and n7kel on-site units	Webhooks, REST API

SYSTEM	WHAT IS TRANSFERRED	METHOD
Queue management, CRM, telephony	To the platform: tickets, visits, call recordings; from the platform: waiting times, events, transcripts (n7kel Flow, n7kel Voice)	REST API, webhooks, files
Government wanted-list databases	Checks of vehicle license plates and visitors' faces; match notification	Under an agreement with the authorized bodies, in the manner they approve
SIEM and IT monitoring	From the platform: events, integrity check errors, loss of connection to equipment	Webhooks, REST API
Service desk, occupational safety systems	From the platform: violations with priority and response deadline, review history	Webhooks, REST API
BI and reporting	From the platform: period analytics, reports by site, shift, employee, checkout	REST API, CSV/XLSX exports
E-mail, messenger	Short notifications in Russian with a link to the card in the interface	E-mail, Telegram

3. Access keys and permissions

- each external system is issued its own key with a separate set of permissions; keys are created by the organization administrator;
- a key is shown once; only its fingerprint is stored on the server;
- a key is bound to a single organization and has no access to any other organization's data;
- the request rate is limited separately for each key;
- every request, including rejected ones, is recorded in the request log;
- key revocation takes effect immediately; an expiry date can be set for a key.

4. Key permissions

The principle of least privilege: a POS system key can only submit transactions, and a BI key can only read analytics.

PERMISSION	WHAT IT GRANTS ACCESS TO
Events	The event log and the webhook delivery log
Evidence	Event frames and video clips. Without this permission, no image links are issued
Violations	Violations, their history, comments and statuses

PERMISSION	WHAT IT GRANTS ACCESS TO
Analytics	Period totals, breakdowns by site, shift, employee, type and time, trends, “what to change” recommendations, share of false alarms, checkout analytics
Reports	Report export in CSV and XLSX
Integrity	Signed integrity check reports
POS transaction submission	Receiving POS transactions only. Nothing can be read with this key

5. REST API capabilities

- events with filters by site, camera, post, employee, type, level and period; periodic polling for new data only;
- an event card with the evidence section: results of signature, chain and file verification; download of the frame and video clip if the permission is granted;
- violations with filters by status, priority, assignee, overdue response deadline, legal hold;
- analytics and reports, including Checkout analytics by checkout, cashier and shift;
- integrity check reports;
- receiving POS transactions.

Responses and error messages are in Russian. CSV tables open in Excel without any setup, with column headers in Russian. Text entered by people or sent by the POS is never turned into a formula when an export is opened.

6. Webhooks: what the platform reports

The auxiliary condition assessment signal is sent only on explicit subscription and only when the module is enabled.

TOPIC	WHEN IT IS SENT
Violation opened	A violation of any type has been opened: PPE, unattended post, absence, unauthorized person, hazardous zone, working under someone else's account, checkout violations
Violation updated / closed	An assignee has been set, the status changed or a comment added; the violation has been resolved or marked as a false alarm
POS reconciliation violations	Separate topics: drawer opened without a receipt, goods handed over without payment, refund without a customer, wrong employee at the till, frequent no-sale drawer openings
Camera events	On-site unit events by type, for example entry into a hazardous zone or a PPE violation

TOPIC	WHEN IT IS SENT
Equipment	An on-site unit or camera is offline, and the connection is restored
License	A change in the license status of an on-site unit
Integrity	The evidence integrity check found errors

7. Notification delivery

- every message is signed with the channel secret, so the recipient can verify that it was sent by your installation and has not been altered;
- channel filters: topics, minimum severity level, sites;
- every message is delivered at least once; each message has an identifier to protect against duplicate processing;
- failed deliveries are retried with an increasing interval; a channel that does not accept messages for a long time is disabled automatically, and the reason is visible to the administrator;
- the delivery log lets you check whether the receiver has missed any messages and retry delivery manually;
- messages contain no links to images: frames are obtained only with a key that has a separate permission;
- if the e-mail or Telegram channel is not configured, the delivery is marked as failed — the system does not pretend the message was sent.

A recommendation in the spirit of the “silence over noise” principle: send only high-priority violations to people (by e-mail and Telegram), and send the full event stream to machines through webhooks.

8. Connecting the POS system

8.1. The Fuel Station Checkout module needs POS transactions. Connection is done in one of two ways:

- **via API** — the POS system or an intermediate service sends transactions in batches of up to 500; resending the same transaction does not create duplicates;
- **as a CSV or XLSX file** — if the POS software cannot send requests. The platform offers column mapping and a dry-run check without saving, and automatically detects the encoding, the delimiter and Russian transaction names.

8.2. Mandatory transaction fields: transaction ID, till number, transaction type, time. Desirable: cashier login, receipt number, amount, payment method.

8.3. Till clocks often drift from the exact time. The platform estimates the clock offset of each till and takes it into account during reconciliation; the offset can also be set manually. Time synchronization on the tills is recommended.

8.4. The platform waits for late POS data: as long as there is no data for the moment being checked, a “no receipt” violation is not opened. A receipt that arrives after the violation was opened clears it automatically.

8.5. Accepted POS transactions are protected in the same way as on-site unit events: an accepted transaction cannot be changed or deleted unnoticed.

9. n7kel Fuel Station Control integrations

The control and anti-fraud platform for a fuel station network is designed for a network of hundreds of stations:

- reconciliation of POS receipts and fiscal data with registered operations: match, receipt without operation, duplicate, amount mismatch with the difference shown;
- a real-time dashboard and a cash transaction log;
- notifications by e-mail, Telegram and SMS with a verifiable delivery status;
- reports in Excel and PDF;
- speech analytics through n7kel Voice — service script compliance, forbidden phrases, conflicts in Russian, Kazakh and any other language; the price depends on the number of languages;
- station equipment telemetry;
- a cashier kiosk: cashier shift login by employee code and PIN; face login is enabled at the client's decision and only with the cashier's written consent;
- the central office sees the connection status of every till; till operation during a prolonged loss of connection is provided by the native till client and agreed during the site survey.

The scope of integration with a specific POS system and ERP is determined during the site survey.

10. Integration with any system

10.1. Beyond the standard integrations, n7kel connects virtually any client system, including in-house and legacy ones:

- **APIs** — REST, SOAP and other protocols;
- **databases** — reading and writing according to an agreed schema, with a dedicated account and minimal permissions;
- **file exchange** — CSV, XLSX, XML, JSON on a schedule or on an event;
- **message buses and queues** — for real-time event streams;

- **ERP and 1C, POS systems, access control, security monitoring consoles, video surveillance systems from other manufacturers;**
- **legacy systems** — through an intermediate service developed as part of the project.

10.2. The scope and method of integration are determined during the site survey and set out in the project design. All exchanges take place within the client's environment or over channels the client has approved; no external n7kel services are needed for this.

10.3. All events from n7kel products can be brought together in the n7kel Atlas platform for search, links and task distribution.

11. Government databases

11.1. If the client requires it, n7kel products can be connected to the wanted-list databases of the Ministry of Internal Affairs, the National Security Committee and other authorized bodies to check vehicle license plates and visitors' faces.

11.2. Connection is possible only if the client has an agreement with the relevant government authorities, and only in the manner established by law and by that agreement. The exchange method is determined by the authority; the exchange is performed by the platform server within the client's environment, and the check log is kept on the client's server.

11.3. In the event of a match, a notification goes to an authorized member of the client's security department and, as the agreement provides, to the authority. Every check and every match is recorded in the log.