



Развёртывание платформы Nova на хостинге

Требования к хостингу и пошаговая инструкция по установке, обновлению, резервному копированию и обслуживанию интернет-магазина nova-store и сервера лицензий

Требования

Какой хостинг подходит, ресурсы сервера, программы, сеть, домены и SSL

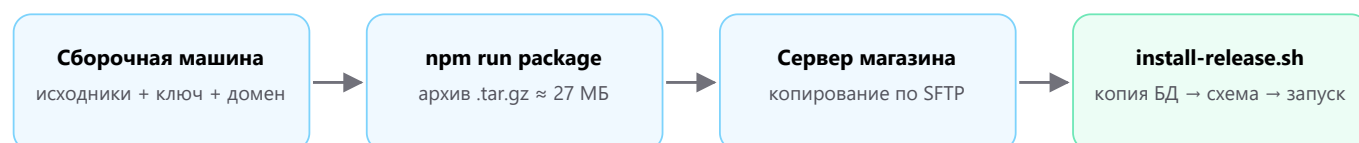
Установка

Подготовка Linux-сервера, сервер лицензий, сборка пакета и запуск магазина

Обслуживание

Обновления и откат, резервные копии, мониторинг, безопасность, решение проблем

Как магазин попадает на сервер



Содержание

1. Общие сведения

1.1 Из чего состоит платформа · 1.2 Варианты размещения · 1.3 Что подготовить заранее

2. Требования к хостингу

2.1 Тип хостинга · 2.2 Ресурсы сервера · 2.3 Операционная система и программы · 2.4 Сеть, порты и внешние сервисы · 2.5 Домены и SSL · 2.6 Персональные данные и выбор площадки

3. Подготовка сервера

3.1 Первый вход и обновление · 3.2 Защита SSH и брандмауэр · 3.3 Часовой пояс и файл подкачки · 3.4 Установка программ · 3.5 Служебный пользователь и папки · 3.6 DNS-записи

4. Сервер лицензий

4.1 Загрузка кода · 4.2 Файл настроек · 4.3 Сборка и запуск · 4.4 HTTPS и nginx · 4.5 Первый вход и проверка · 4.6 Открытый ключ для магазинов

5. Сборка пакета магазина

5.1 Сборочная машина · 5.2 Подготовка исходников · 5.3 Сборка пакета · 5.4 Что внутри пакета

6. Установка магазина

6.1 Папки и файл настроек · 6.2 Служба и установка пакета · 6.3 HTTPS и nginx · 6.4 Первый администратор · 6.5 Первичная настройка магазина · 6.6 Активация лицензии · 6.7 Проверка после запуска

7. Обновление и откат

8. Резервное копирование и восстановление

9. Мониторинг и обслуживание

10. Безопасность

11. Решение проблем

12. Дополнительно

12.1 Несколько магазинов на одном сервере · 12.2 PostgreSQL вместо SQLite · 12.3 Cloudflare и CDN · 12.4 Контейнеры и PaaS · 12.5 Чек-лист запуска

1 Общие сведения

1.1 Из чего состоит платформа

Платформа состоит из двух веб-приложений на Node.js (Next.js 15). Каждое работает как отдельная служба за веб-сервером nginx, который принимает HTTPS-запросы и передаёт их приложению.

Интернет-магазин nova-store

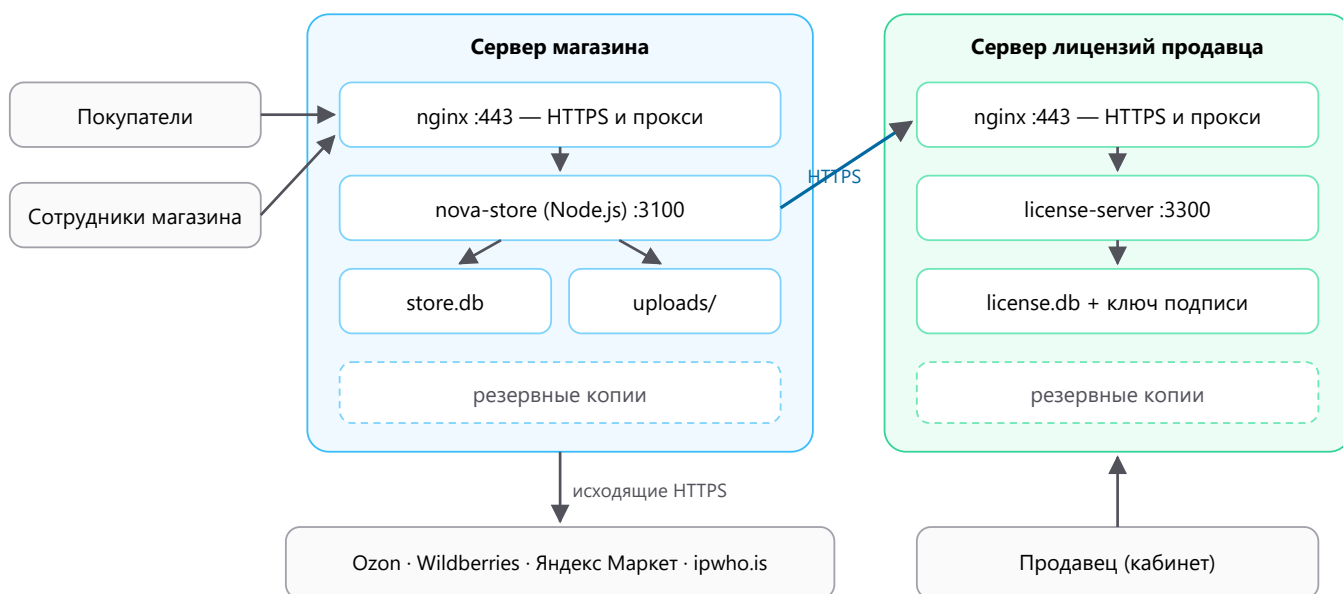
Витрина, корзина, заказы, админ-панель, склад, продажи и подключаемые модули. Данные хранятся в базе SQLite (один файл), загруженные изображения — в папке uploads. Внутри работают фоновые задачи: ежедневная проверка лицензии и автосинхронизация маркетплейсов.

Один магазин — одна установка на своём домене.

Сервер лицензий

Приложение продавца: клиенты, тарифы, выдача лицензий, учёт установок и продаж. Подписывает лицензии закрытым ключом и отвечает магазинам через API. База SQLite хранит в том числе закрытый ключ подписи.

Один сервер лицензий обслуживает все проданные магазины.



Магазин обращается к серверу лицензий при активации ключа и затем раз в сутки. Без связи онлайн-лицензия работает «Дней без связи с сервером» (по умолчанию 30), поэтому кратковременная недоступность сервера лицензий на магазины не влияет. Подробно механика описана в инструкции «Лицензирование интернет-магазина Nova».

1.2 Варианты размещения

Вариант	Кто и где размещает	Разделы инструкции
Сервер лицензий	Всегда продавец, на своём сервере с постоянным HTTPS-адресом. Адрес встраивается в каждую сборку магазина, поэтому менять его потом нельзя.	2, 3, 4, 7–10
Магазин у продавца	Продавец сам размещает магазины клиентов на своих серверах (управляемый хостинг). Можно разместить магазин на одном сервере с сервером лицензий.	2, 3, 5, 6, 7–10
Магазин у клиента	Клиент размещает магазин на своём хостинге. Продавец собирает пакет под домен клиента и передаёт архив, исходный код клиенту не передаётся. Установку выполняет администратор клиента по разделам 3 и 6.	Продавец: 5. Клиент: 2, 3, 6–10

Почему магазин ставится из пакета, а не из исходников

Пакет — это готовая production-сборка без исходного кода (Next.js standalone). На сервере магазина не нужны исходники, сборка и инструменты разработки, а обход лицензии через исходный код или режим разработки становится невозможен. Пакет запускается одной командой `node server.js` и весит около 27 МБ.

1.3 Что подготовить заранее

- ☐ Сервер (VPS) под каждое приложение или один общий — по требованиям раздела 2.
- ☐ Домены: для сервера лицензий (например, `license.example.ru`) и для каждого магазина (`shop.example.ru`). Доступ к управлению DNS-записями.
- ☐ Доступ к серверу по SSH с правами `sudo`, SSH-ключ на своём компьютере.
- ☐ Исходный код обоих приложений (git-репозиторий или архив).
- ☐ Linux-машина для сборки пакетов магазина (раздел 5.1). Подойдёт сам сервер лицензий.
- ☐ E-mail для уведомлений Let's Encrypt о сертификатах.
- ☐ Место для внешних резервных копий: второй сервер или S3-совместимое хранилище.

Во всех примерах используются домены `license.example.ru` и `shop.example.ru`, служебный пользователь `nova` и Ubuntu 24.04. Замените их своими значениями.

2 Требования к хостингу

2.1 Тип хостинга

Оба приложения — долгоживущие процессы Node.js, которые хранят данные на локальном диске. Магазины дополнительно нужны фоновые задачи по расписанию и кеши в памяти процесса. Отсюда главное требование: **постоянно работающий процесс Node.js в одном экземпляре и постоянный диск**.

Тип хостинга	Подходит	Пояснение
VPS/VDS (KVM) с root-доступом	Рекомендуется	Полный контроль над Node.js, nginx, диском и службами. Основной вариант этой инструкции.
Облачная виртуальная машина (Yandex Cloud, VK Cloud, Selectel и др.)	Да	То же, что VPS. Используйте сетевой диск SSD, а не временный локальный.
Выделенный сервер	Да	Для крупных магазинов или размещения многих магазинов на одном сервере.
PaaS с постоянным диском (облачные приложения хостеров)	С оговорками	Нужны постоянный том для базы и uploads, ровно один экземпляр, без автомасштабирования и «засыпания». Детально не описан, см. 12.4.
Виртуальный хостинг с поддержкой Node.js	Нет	Лимиты памяти, остановка простаивающих процессов (фоновые задачи перестают выполняться), нет управления nginx и службами.
Виртуальный хостинг PHP	Нет	Нет долгоживущих процессов Node.js.
Serverless (Vercel, Netlify, облачные функции)	Нет	Нет постоянного диска для SQLite и изображений, нет фоновых задач, запросы обслуживают разные экземпляры с разными кешами.

Только один экземпляр приложения

Не запускайте магазин в режиме кластера (PM2 cluster, несколько реплик, балансировка между серверами). SQLite рассчитан на один процесс-писатель, а проверка лицензии, синхронизация маркетплейсов и кеши живут внутри процесса. Один процесс Node.js спокойно обслуживает типичную нагрузку интернет-магазина.

2.2 Ресурсы сервера

Замеры на сборке 1.0.0: работающий магазин занимает около 200 МБ памяти, сервер лицензий — около 130 МБ. Сборка магазина требует до 2 ГБ памяти и 1,5–4 минуты, сборка сервера лицензий — около 1 ГБ и 0,5–2 минуты. Магазин собирается не на своём сервере, а на сборочной машине, поэтому серверу магазина память на сборку не нужна.

Назначение	vCPU	Память	Диск	Комментарий
Сервер лицензий	1	1 ГБ + 1 ГБ swap	10 ГБ SSD	Собирается на месте; без файла подкачки сборка может не уложиться в 1 ГБ.
Магазин, начальный небольшой каталог, 1–3 сотрудника	1–2	2 ГБ	20 ГБ SSD	Минимально разумная конфигурация.
Магазин, рабочий тысячи товаров, маркетплейсы, 5–10 сотрудников	2	4 ГБ	40 ГБ NVMe	Рекомендуемая конфигурация. Запас по памяти — под кеш файловой системы для базы и изображений.
Магазин, крупный высокая посещаемость, большой каталог	4+	8 ГБ	80+ ГБ NVMe	Рассмотрите PostgreSQL (12.2) и CDN (12.3).
Сервер лицензий и магазин вместе	2	4 ГБ	40 ГБ SSD	Для продавца, который сам размещает магазин. Здесь же можно собирать пакеты.
Сборочная машина	2+	4 ГБ	10 ГБ	Linux x64 с той же версией OpenSSL, что на серверах магазинов (раздел 5.1).

Из чего складывается место на диске магазина

- **Приложение:** около 95 МБ на версию; хранятся текущая и предыдущая — около 200 МБ. Кеш прт с Prisma CLI для обновлений — около 150 МБ.
- **База данных:** от единиц мегабайт на старте; растёт с заказами, документами и журналами.
- **Изображения:** до 5 МБ на файл. Это обычно самая большая часть данных.
- **Резервные копии:** по умолчанию 14 ежедневных копий базы и изображений. Для большого каталога увеличьте диск или храните копии изображений на внешнем хранилище.

2.3 Операционная система и программы

Программа	Версия	Назначение
Linux x86_64	Ubuntu 24.04 LTS или 22.04 LTS, Debian 12	Операционная система. Команды в инструкции — для Ubuntu/Debian. Другие дистрибутивы подходят, но пакет магазина нужно собирать под них (5.1).
Node.js	24 LTS (минимум 20)	Среда выполнения обоих приложений. Ставится из репозитория NodeSource; в стандартных репозиториях Ubuntu версия устаревшая.
nginx	1.18 и новее	Веб-сервер: HTTPS, сжатие, передача запросов приложениям.
certbot	из репозитория ОС	Бесплатные SSL-сертификаты Let's Encrypt и их автопродление.

Программа	Версия	Назначение
sqlite3	3.x	Горячие резервные копии баз и проверка их целостности.
git	любая	Получение и обновление кода сервера лицензий.
curl, tar, gzip	любые	Используются скриптами установки и резервного копирования.

Отдельная СУБД не нужна: обе базы — файлы SQLite. Docker, PM2 и панели управления не требуются: приложения запускаются службами systemd.

2.4 Сеть, порты и внешние сервисы

Входящие подключения

Порт	Назначение
22/tcp	SSH для администрирования. Желательно ограничить своими IP-адресами.
80/tcp	Перенаправление на HTTPS и проверка домена Let's Encrypt.
443/tcp	HTTPS: витрина и админка магазина; кабинет и API сервера лицензий. API должно быть доступно со всех серверов магазинов.

Порты приложений 3100 и 3300 слушают только `127.0.0.1` и снаружи недоступны. Нужен постоянный (статический) IPv4-адрес.

Исходящие подключения с сервера магазина (HTTPS, порт 443)

Адрес	Зачем	Если недоступен
Сервер лицензий (<code>license.example.ru</code>)	Активация ключа, ежедневная проверка, пробный период	Онлайн-лицензия работает до 30 дней, затем модули переходят в режим просмотра. Для закрытых сетей есть офлайн-лицензия.
<code>ipwho.is</code>	Город покупателя по IP	Город не определяется автоматически; покупатель выбирает его сам.
<code>api-seller.ozon.ru</code>	Модуль «Маркетплейсы»: Ozon	Обмен с Ozon не работает.
<code>common-api</code> , <code>content-api</code> , <code>marketplace-api</code> , <code>discounts-prices-api</code> <code>.wildberries.ru</code>	Модуль «Маркетплейсы»: Wildberries	Обмен с Wildberries не работает.
<code>api.partner.market.yandex.ru</code>	Модуль «Маркетплейсы»: Яндекс Маркет	Обмен с Яндекс Маркетом не работает.
<code>registry.npmjs.org</code>	Загрузка Prisma CLI при установке и обновлениях	Обновление схемы базы не выполнится (см. раздел 11).

Адрес	Зачем	Если недоступен
<code>acme-v02.api.letsencrypt.org</code>	Выпуск и продление SSL-сертификатов	Сертификат не продлится и через 90 дней истечёт.

Серверу лицензий нужны исходящие подключения к Let's Encrypt, `registry.npmjs.org` и вашему git-репозиторию. Счётчики Яндекс Метрики и Google Analytics загружает браузер покупателя, серверу доступ к ним не нужен.

2.5 Домены и SSL

- **HTTPS обязателен.** В production-сборке cookie входа помечены `Secure`, и браузер не отправляет их по HTTP: войти в админку по HTTP не получится. Камера для сканирования штрихкодов тоже работает только по HTTPS.
- **Домен магазина встраивается в сборку** (`NEXT_PUBLIC_SITE_URL`): по нему формируются `sitemap.xml`, `robots.txt`, канонические адреса, документы, и к нему привязывается лицензия. Новый домен — новый пакет.
- **Адрес сервера лицензий встраивается в каждую сборку магазина** (`NOVA_LICENSE_SERVER`). Выберите его один раз и навсегда, например `license.вашакомпания.ru`.
- Сертификаты Let's Encrypt бесплатны и продлеваются автоматически. Подойдёт и коммерческий сертификат — укажите его файлы в конфигурации nginx.

2.6 Персональные данные и выбор площадки

Магазин хранит персональные данные покупателей: имена, телефоны, адреса, e-mail, город по IP. По закону № 152-ФЗ запись и хранение персональных данных граждан России должны выполняться на серверах в России. Выбирайте хостинг с дата-центром в РФ и заранее подайте уведомление в Роскомнадзор как оператор персональных данных. Подходящие площадки — российские VPS- и облачные провайдеры с KVM-виртуализацией, SSD/NVMe-дисками и ежедневными снимками дисков.

Что спросить у хостера перед покупкой

- Виртуализация KVM, выделенные vCPU и память, SSD или NVMe.
- Ubuntu 24.04/22.04 или Debian 12 в списке образов, root-доступ.
- Статический IPv4, открытые входящие 80 и 443, без ограничений исходящего HTTPS.
- Снимки (snapshots) диска и резервное копирование на стороне хостера — как дополнительная страховка к копиям из раздела 8.
- Дата-центр в России.

3 Подготовка сервера

Эти шаги одинаковы для сервера лицензий и сервера магазина. Если оба приложения на одном сервере, выполните их один раз.

3.1 Первый вход и обновление

```
# с вашего компьютера: вход по данным от хостера
ssh root@203.0.113.10

# обновление системы
apt update && apt -y full-upgrade

# администратор с sudo (не работайте постоянно под root)
adduser deploy
usermod -aG sudo deploy
mkdir -p /home/deploy/.ssh && cp ~/.ssh/authorized_keys /home/deploy/.ssh/ 2>/dev/null
chown -R deploy:deploy /home/deploy/.ssh && chmod 700 /home/deploy/.ssh
```

Если хостер выдал только пароль, скопируйте свой ключ с компьютера: `ssh-copy-id deploy@203.0.113.10`.
Дальше входите как `deploy` и выполняйте команды через `sudo`.

3.2 Защита SSH и брандмауэр

```
# убедитесь, что вход по ключу работает, затем запретите пароли и вход под root
sudo sed -i 's/^#\?PasswordAuthentication .*/PasswordAuthentication no;/ s/^#\?PermitRootLogin .*/PermitRootLogin no/' /etc/ssh/sshd_config
sudo systemctl restart ssh

# брандмауэр: только SSH, HTTP и HTTPS
sudo apt -y install ufw
sudo ufw allow OpenSSH
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
sudo ufw enable

# автоматические обновления безопасности
sudo apt -y install unattended-upgrades
sudo dpkg-reconfigure -plow unattended-upgrades
```

Не закрывайте себе доступ

Перед перезапуском SSH откройте второе окно терминала и проверьте вход по ключу. Если хостер поддерживает свой брандмауэр в панели управления, откройте в нём те же порты.

3.3 Часовой пояс и файл подкачки

Даты в документах, отчётах и журналах считаются по времени сервера. Установите часовой пояс магазина (в юнитах служб он дополнительно задан переменной `TZ`).

```

sudo timedatectl set-timezone Europe/Moscow
timedatectl # проверка: Time zone: Europe/Moscow, System clock synchronized: yes

# файл подкачки 2 ГБ — обязателен на серверах с 1-2 ГБ памяти, где идёт сборка
sudo fallocate -l 2G /swapfile
sudo chmod 600 /swapfile
sudo mkswap /swapfile
sudo swapon /swapfile
echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
free -h

```

3.4 Установка программ

```

# Node.js 24 LTS из репозитория NodeSource
curl -fsSL https://deb.nodesource.com/setup_24.x | sudo -E bash -
sudo apt -y install nodejs
node -v # v24.x
npm -v

# веб-сервер, сертификаты, утилиты
sudo apt -y install nginx certbot sqlite3 git curl
sudo systemctl enable --now nginx

```

Откройте в браузере `http://203.0.113.10` — должна появиться стандартная страница nginx. Сайт по умолчанию пока оставьте: через него certbot подтвердит домены при первом выпуске сертификатов.

3.5 Служебный пользователь и папки

Приложения работают от отдельного пользователя `nova` без права входа в систему. Код, данные и настройки разнесены по разным папкам, поэтому обновления не затрагивают данные.

```

sudo useradd --system --create-home --shell /usr/sbin/nologin nova

```

Папка	Что хранится
<code>/opt/nova-license/app</code>	Код и сборка сервера лицензий (git-репозиторий)
<code>/var/lib/nova-license/</code>	База <code>license.db</code> с закрытым ключом подписи
<code>/etc/nova-license/</code>	<code>license.env</code> — секреты; <code>dist.env</code> — текущая папка сборки
<code>/opt/nova-store/app</code>	Текущая версия магазина из пакета. Путь постоянный: от него зависит отпечаток сервера в лицензии
<code>/opt/nova-store/app.prev</code>	Предыдущая версия для быстрого отката
<code>/var/lib/nova-store/</code>	База <code>store.db</code> и папка <code>uploads</code> с изображениями
<code>/etc/nova-store/store.env</code>	Секреты магазина
<code>/var/backups/nova-*</code>	Резервные копии

3.6 DNS-записи

В панели управления доменом создайте A-записи на IP-адрес сервера (и AAAA, если у сервера есть IPv6):

Имя	Тип	Значение
<code>license.example.ru</code>	A	IP сервера лицензий
<code>shop.example.ru</code>	A	IP сервера магазина
<code>www.shop.example.ru</code>	A или CNAME	Тот же адрес; nginx перенаправит на основной домен

Проверьте, что записи применились: `dig +short shop.example.ru` должен вернуть IP сервера. Обычно это занимает от нескольких минут до нескольких часов. Сертификаты выпускаются только после этого.

4 Сервер лицензий

Сервер лицензий разворачивается один раз и обслуживает все магазины. Он собирается прямо на своём сервере из исходного кода. Готовые файлы для развёртывания лежат в папке `license-server/deploy/` :

Файл	Назначение
<code>nova-license.service</code>	Служба systemd
<code>nginx-nova-license.conf</code>	Сайт nginx: HTTPS, ограничение частоты запросов, опциональный доступ к кабинету только с ваших IP
<code>nova-proxy.conf</code>	Общие заголовки проксирования для nginx
<code>update.sh</code>	Сборка и перезапуск: первая установка и обновления
<code>backup.sh</code>	Резервная копия базы и настроек

4.1 Загрузка кода

```
sudo mkdir -p /opt/nova-license /var/lib/nova-license /etc/nova-license
sudo chown nova:nova /opt/nova-license /var/lib/nova-license

# вариант 1: из git-репозитория (нужен доступ по ключу развёртывания или токenu)
sudo -u nova -H git clone https://git.example.ru/vendor/license-server.git /opt/nova-license/app

# вариант 2: архивом с вашего компьютера (в папке, где лежит license-server)
# tar --exclude=node_modules --exclude=".next*" --exclude="*.db" --exclude=.env -czf license-server.tar.gz license-server
# scp license-server.tar.gz deploy@203.0.113.10:/tmp/
sudo -u nova tar -xzf /tmp/license-server.tar.gz -C /opt/nova-license
sudo -u nova mv /opt/nova-license/license-server /opt/nova-license/app
```

4.2 Файл настроек

```
sudo tee /etc/nova-license/license.env >/dev/null <<EOF
DATABASE_URL="file:/var/lib/nova-license/license.db"
SESSION_SECRET="$(openssl rand -base64 48)"
VENDOR_ADMIN_EMAIL="admin@example.ru"
VENDOR_ADMIN_PASSWORD="$(openssl rand -base64 12)"
EOF
sudo chown root:nova /etc/nova-license/license.env
sudo chmod 640 /etc/nova-license/license.env
sudo ln -s /etc/nova-license/license.env /opt/nova-license/app/.env

sudo cat /etc/nova-license/license.env # запишите начальный пароль администратора
```

Переменная	Значение
<code>DATABASE_URL</code>	Путь к базе. Абсолютный путь вне папки кода, чтобы обновления не трогали данные.

Переменная	Значение
<code>SESSION_SECRET</code>	Секрет подписи сессий сотрудников продавца. Смена секрета разлогинит всех.
<code>VENDOR_ADMIN_EMAIL</code> , <code>VENDOR_ADMIN_PASSWORD</code>	Учётная запись администратора, которая создаётся при первом запуске. При первом входе система потребует сменить пароль.
<code>LICENSE_SIGNING_KEY</code>	Необязательно. Закрытый ключ Ed25519 (PEM). Если не задан, ключ создаётся при первом запуске и хранится в базе — тогда резервные копии базы обязательны (раздел 8).

Закрытый ключ подписи — самое ценное на сервере лицензий

Открытая часть ключа встроена во все проданные сборки магазина. Потеряете ключ — новые лицензии не подойдут к уже установленным магазинам, понадобится пересобрать и переустанавливать каждый. Утечёт ключ — любой сможет выпускать лицензии. Храните резервные копии базы в зашифрованном виде и в двух местах.

4.3 Сборка и запуск

```
sudo cp /opt/nova-license/app/deploy/nova-license.service /etc/systemd/system/
sudo systemctl daemon-reload
sudo systemctl enable nova-license
```

```
# установка зависимостей, создание базы, сборка и запуск
sudo bash /opt/nova-license/app/deploy/update.sh
```

Скрипт `update.sh` делает резервную копию (если база уже есть), выполняет `npm ci`, применяет схему базы (`prisma db push`), собирает приложение и перезапускает службу. Сборка идёт поочерёдно в папки `.next-a` и `.next-b` : пока собирается новая версия, работает прежняя, а при ошибке сборки служба не прерывается. Текущая папка записывается в `/etc/nova-license/dist.env` .

```
systemctl status nova-license          # active (running)
curl -s -o /dev/null -w "%{http_code}\n" http://127.0.0.1:3300/login  # 200
```

4.4 HTTPS и nginx

```
# сертификат: пока работает сайт nginx по умолчанию
sudo certbot certonly --webroot -w /var/www/html -d license.example.ru \
  -m admin@example.ru --agree-tos --no-eff-email --deploy-hook "systemctl reload nginx"

# конфигурация сайта
sudo cp /opt/nova-license/app/deploy/nova-proxy.conf /etc/nginx/snippets/
sudo cp /opt/nova-license/app/deploy/nginx-nova-license.conf /etc/nginx/sites-available/nova-license
sudo sed -i 's/license\.example\.ru/license.ВАШ-ДОМЕН.ru/g' /etc/nginx/sites-available/nova-license
sudo ln -s /etc/nginx/sites-available/nova-license /etc/nginx/sites-enabled/
sudo nginx -t && sudo systemctl reload nginx

# проверка автопродления
sudo certbot renew --dry-run
```

В конфигурации API `/api/` открыто для всех, кабинет продавца — тоже, но его можно закрыть: раскомментируйте строки `allow / deny` в блоке `location /` и укажите IP-адреса офиса. На API и вход действует ограничение 10 запросов в секунду с одного IP с запасом на всплески.

4.5 Первый вход и проверка

- 1 Откройте `https://license.example.ru` и войдите с `VENDOR_ADMIN_EMAIL` и паролем из файла настроек.
- 2 Система попросит сменить пароль — задайте постоянный. После этого удалите строку `VENDOR_ADMIN_PASSWORD` из `license.env`: она нужна только при первом запуске.
- 3 Проверьте тарифы и модули, при необходимости добавьте сотрудников в «Настройках».
- 4 Проверьте API с любого компьютера:

```
curl -s -X POST https://license.example.ru/api/v1/check -H "Content-Type: application/json" -d '{}'
# {"error": "Required"} — API доступно и отвечает
```

4.6 Открытый ключ для магазинов

Каждую сборку магазина нужно собрать с открытым ключом **этого** сервера лицензий. Получить файл `license-public.pem` можно двумя способами:

- в кабинете: «Настройки» → «Ключ подписи лицензий» → кнопка **license-public.pem**;
- на сервере: `cd /opt/nova-license/app && sudo -u nova -H npm run export-public-key -- /opt/nova-license/license-public.pem`.

Лицензии Nova

Обзор

Лицензии

Клиенты

Продажи

Тарифы

Журнал

Настройки

Настройки

Пароль, ключ подписи лицензий, сотрудники и API для магазинов

Ключ подписи лицензий

Ed25519. Закрытый ключ задан переменной LICENSE_SIGNING_KEY. Открытый ключ встраивается в каждую сборку nova-store: без него магазин не примет лицензию

-----BEGIN PUBLIC KEY-----
MCOwBQYOK2VwMyEAjQ4gRj9IHmngYsDRuPFV4fIHukaT48C188hvQ85EwdM+
-----END PUBLIC KEY-----

license-public.pem

Или из папки сервера: `npm run export-public-key` — запишет файл в `nova-store/license-public.pem`

Не меняйте ключ без необходимости: лицензии, подписанные старым ключом, перестанут приниматься новыми сборками, а старые сборки не примут новые лицензии.

Сотрудники продавца

Менеджер выдаёт лицензии и записывает продажи; администратор ещё и управляет тарифами, ключом и сотрудниками

Анна Соколова	Администратор	с 10.01.2026	
anna@nova-soft.ru			
Игорь Петров	Менеджер	с 02.02.2026	Заккрыть доступ
igor@nova-soft.ru			

API для магазинов

POST /api/v1/activate

Активация ключа на установке: `key, instancelid, fingerprint, domain` → `token`

POST /api/v1/check

Ежедневная проверка: продлевает работу без связи и передаёт новые условия; 410 — лицензия отозвана или приостановлена

POST /api/v1/deactivate

Отключение установки (перенос на другой сервер)

POST /api/v1/trial

Пробный период: один на установку, сервер и домен

Адрес сервера задаётся в сборке `nova-store` переменной `NOVA_LICENSE_SERVER`.

Сменить пароль

Текущий пароль

Новый пароль

Сменить пароль

Новый сотрудник

Имя

Email

Пароль

Роль

Менеджер

Добавить

Анна Соколова

Администратор

Выйти

Настройки сервера лицензий: открытый ключ и кнопка скачивания license-public.pem

Развёртывание платформы Nova

15 / 32

5 Сборка пакета магазина

Пакет — это архив с готовым к запуску магазином для одного домена. Его собирает продавец, а устанавливает тот, кто размещает магазин (раздел 6).

5.1 Сборочная машина

- **Linux x86_64 с той же линейкой OpenSSL, что и сервер магазина.** В пакет попадает движок базы данных Prisma, скомпилированный под систему сборочной машины. Ubuntu 22.04, 24.04 и Debian 12 используют OpenSSL 3 и взаимозаменяемы. Пакет, собранный на Windows или macOS, на Linux-сервере не запустится — скрипт предупредит об этом.
- Node.js той же основной версии, что на серверах магазинов (24 LTS).
- Около 2 ГБ свободной памяти на время сборки и 2 ГБ диска под исходники и зависимости.
- Подойдёт сервер лицензий (с файлом подкачки), отдельная виртуальная машина или CI-конвейер (GitLab CI, GitHub Actions на `ubuntu-24.04`).

Сервер магазина на другой системе

Если сервер магазина — другой дистрибутив (например, Alpine или старый Debian с OpenSSL 1.1), добавьте нужную платформу в `prisma/schema.prisma`: `binaryTargets = ["native", "debian-openssl-1.1.x"]` в блоке `generator client`, выполните `npm run prisma generate` и соберите пакет заново.

5.2 Подготовка исходников

```
# один раз: исходники и зависимости
git clone https://git.example.ru/vendor/nova-store.git
cd nova-store
npm ci

# пустая база со схемой для сборки (на данные клиентов не влияет)
cp .env.example .env
npm run db:push

# открытый ключ ВАШЕГО сервера лицензий (раздел 4.6)
cp /путь/к/license-public.pem ./license-public.pem
```

Замените ключ разработки

В репозитории лежит `license-public.pem` тестового сервера разработки. Магазин, собранный с ним, не примет лицензии вашего рабочего сервера: при активации будет ошибка подписи. Перед каждой сборкой для клиента убедитесь, что в корне проекта лежит ключ рабочего сервера лицензий.

5.3 Сборка пакета

```
NEXT_PUBLIC_SITE_URL=https://shop.example.ru \
NOVA_LICENSE_SERVER=https://license.example.ru \
npm run package
```

Через 2–4 минуты появится архив `dist/nova-store-1.0.0-shop.example.ru.tar.gz`. В имени — версия и домен, для которого он собран.

Переменная	Что задаёт
<code>NEXT_PUBLIC_SITE_URL</code>	Адрес магазина без <code>/</code> в конце, только <code>https://</code> . Используется в <code>sitemap</code> , <code>robots</code> , канонических адресах и документах; к домену привязывается лицензия.
<code>NOVA_LICENSE_SERVER</code>	Адрес сервера лицензий.
<code>NOVA_LICENSE_PUBLIC_KEY</code>	Необязательно: открытый ключ строкой вместо файла <code>license-public.pem</code> .

Один пакет — один домен

Значения встраиваются в сборку и не меняются настройками на сервере. Для другого магазина или смены домена соберите новый пакет. Перед отправкой клиенту проверьте `VERSION.txt` внутри пакета: там записаны домен, сервер лицензий и дата сборки.

5.4 Что внутри пакета

Файл или папка	Назначение
<code>server.js</code>	Точка входа: <code>node server.js</code>
<code>.next/</code> , <code>public/</code>	Собранное приложение и статические файлы
<code>node_modules/</code>	Только нужные для работы зависимости, включая движок Prisma
<code>prisma/schema.prisma</code>	Схема базы — для создания и обновления таблиц
<code>scripts/create-admin.mjs</code>	Создание первого администратора без демо-данных
<code>deploy/</code>	Служба <code>systemd</code> , конфигурация <code>nginx</code> , скрипты установки и резервного копирования
<code>.env.example</code>	Образец файла настроек
<code>VERSION.txt</code>	Версия, домен, сервер лицензий, дата и платформа сборки

Исходного кода, файла `.env` сборочной машины, баз данных и закрытых ключей в пакете нет.

6 Установка магазина

Сервер подготовлен по разделу 3, DNS-запись домена магазина указывает на него, пакет собран под этот домен.

6.1 Папки и файл настроек

```
sudo mkdir -p /opt/nova-store /var/lib/nova-store/uploads /etc/nova-store
sudo chown -R nova:nova /opt/nova-store /var/lib/nova-store

sudo tee /etc/nova-store/store.env >/dev/null <<EOF
DATABASE_URL="file:/var/lib/nova-store/store.db"
AUTH_SECRET="$(openssl rand -base64 48)"
EOF
sudo chown root:nova /etc/nova-store/store.env
sudo chmod 640 /etc/nova-store/store.env
```

Переменная	Значение
<code>DATABASE_URL</code>	Абсолютный путь к базе SQLite вне папки приложения.
<code>AUTH_SECRET</code>	Секрет сессий и шифрования API-ключей маркетплейсов. Не меняйте после запуска: все пользователи выйдут из аккаунтов, а сохранённые ключи маркетплейсов станут нечитаемыми.
<code>LICENSE_AUTOCHECK=0</code>	Необязательно. Отключить ежедневную проверку лицензии (для офлайн-лицензии).
<code>MARKETPLACE_AUTOSYNC=0</code>	Необязательно. Отключить автосинхронизацию маркетплейсов.
<code>INSECURE_COOKIES=1</code>	Только для временной проверки по HTTP до выпуска сертификата. Уберите сразу после подключения HTTPS.

Порт, адрес и режим работы (`PORT=3100` , `HOSTNAME=127.0.0.1` , `NODE_ENV=production`) заданы в юните службы: `server.js` читает их до загрузки `.env` .

6.2 Служба и установка пакета

```
# с компьютера, где собран пакет
scp dist/nova-store-1.0.0-shop.example.ru.tar.gz deploy@203.0.113.20:/tmp/

# на сервере: распаковка рядом с будущей папкой приложения
sudo tar -xzf /tmp/nova-store-1.0.0-shop.example.ru.tar.gz -C /opt/nova-store
PKG=/opt/nova-store/nova-store-1.0.0-shop.example.ru

# служба (один раз)
sudo cp $PKG/deploy/nova-store.service /etc/systemd/system/
sudo systemctl daemon-reload
sudo systemctl enable nova-store

# установка: база, схема, переключение и запуск
sudo bash $PKG/deploy/install-release.sh
```

Скрипт `install-release.sh` :

1. связывает пакет с настройками и данными: `.env` → `/etc/nova-store/store.env` , `uploads` → `/var/lib/nova-store/uploads` ;
2. если база уже есть — делает резервную копию через `deploy/backup.sh` ;
3. создаёт или обновляет таблицы: `npx prisma@6.19.3 db push` (при первом запуске загружает Prisma CLI из npm);
4. останавливает службу, переносит текущую версию в `app.prev` , новую — в `app` , запускает службу;
5. ждёт ответа магазина и сообщает результат.

```
systemctl status nova-store          # active (running)
curl -s http://127.0.0.1:3100/robots.txt | tail -n 1 # Sitemap: https://shop.example.ru/sitemap.xml
```

6.3 HTTPS и nginx

```
sudo certbot certonly --webroot -w /var/www/html -d shop.example.ru -d www.shop.example.ru \
-m admin@example.ru --agree-tos --no-eff-email --deploy-hook "systemctl reload nginx"

sudo cp /opt/nova-store/app/deploy/nginx-nova-store.conf /etc/nginx/sites-available/nova-store
sudo sed -i 's/shop\.example\.ru/ВАШ-ДОМЕН.ru/g' /etc/nginx/sites-available/nova-store
sudo ln -s /etc/nginx/sites-available/nova-store /etc/nginx/sites-enabled/
sudo rm -f /etc/nginx/sites-enabled/default # сайт по умолчанию больше не нужен
sudo nginx -t && sudo systemctl reload nginx
```

Что важно в конфигурации и почему:

Настройка	Зачем
<code>proxy_set_header Host \$host , X-Forwarded-Host , X-Forwarded-Proto</code>	Next.js сверяет адрес страницы с источником запроса при отправке форм. Без этих заголовков формы админки возвращают ошибку «Invalid Server Actions request».
<code>X-Forwarded-For \$remote_addr</code>	Магазин берёт IP посетителя из первого адреса этого заголовка (город покупателя, журнал). Заголовок перезаписывается реальным адресом, чтобы его нельзя было подделать.
<code>client_max_body_size 10m</code>	Изображения до 5 МБ; приложение принимает запросы до 8 МБ. При меньшем лимите загрузка падает с ошибкой 413.
Перенаправления <code>http</code> → <code>https</code> и <code>www</code> → без <code>www</code>	Один канонический адрес для поисковиков, совпадающий с <code>NEXT_PUBLIC_SITE_URL</code> .
<code>Strict-Transport-Security</code>	Браузер всегда открывает сайт по HTTPS.

Если домен магазина — с `www` , поменяйте местами перенаправление в конфигурации и укажите `https://www....` в `NEXT_PUBLIC_SITE_URL` .

6.4 Первый администратор

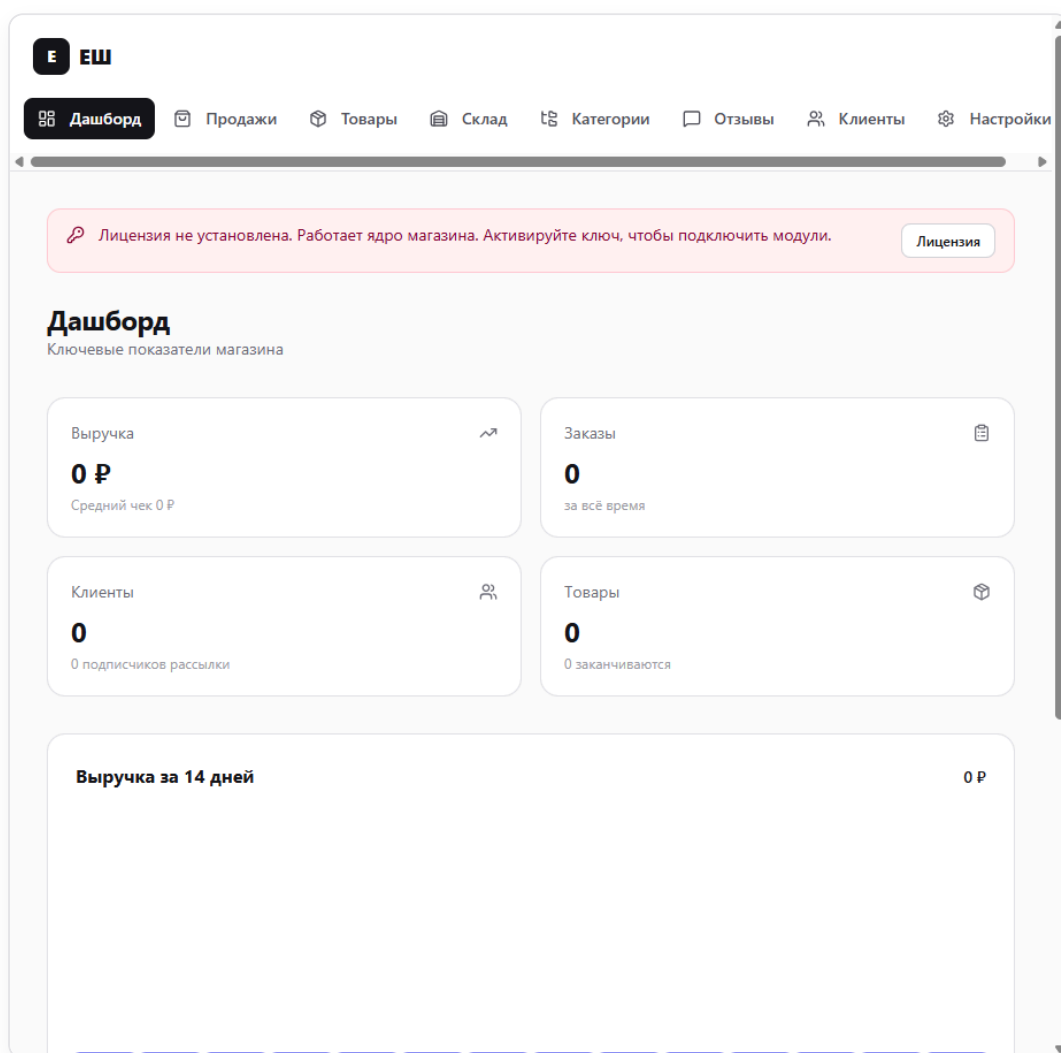
Новая база пустая: в ней нет ни демо-данных, ни пользователей. Администратора создаёт скрипт из пакета:

```
cd /opt/nova-store/app
sudo -u nova -H node scripts/create-admin.mjs --email owner@shop.example.ru --name "Иван Петров"
# Создан администратор owner@shop.example.ru
# Пароль: y8LSP0pTZXJ0X_7K
# Сохраните его — повторно он не показывается.
```

Пароль можно задать сразу: `--password "..."` (не короче 8 символов). Для существующего пользователя скрипт назначит роль администратора и сменит пароль — так же восстанавливается доступ, если пароль забыт.

Не запускайте на рабочем сервере команды с демо-данными

`npm run setup`, `db:seed` и `db:reset` **удаляют все данные** и загружают демонстрационный магазин. В пакете их нет. Ими пользуются только на компьютере разработчика.



Админ-панель нового магазина: данных ещё нет, лицензия не установлена

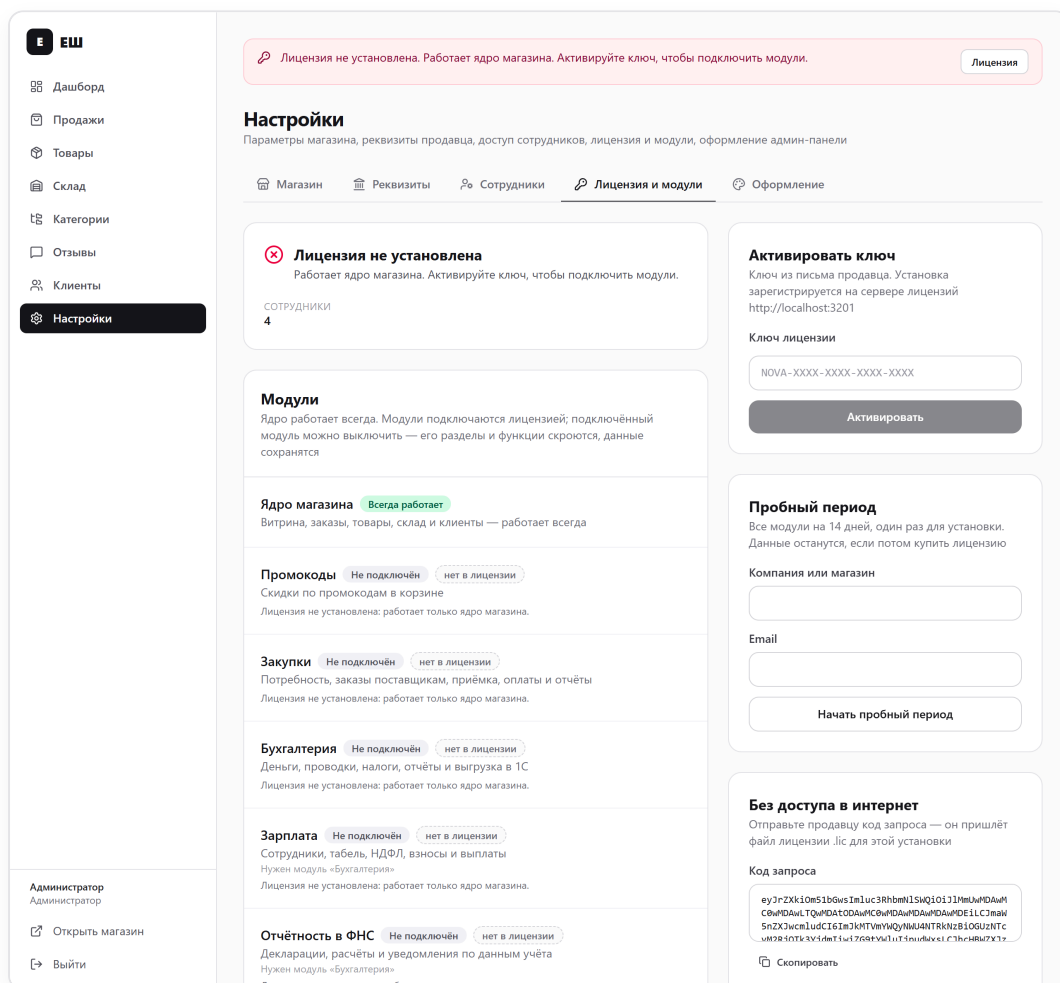
6.5 Первичная настройка магазина

Войдите на `https://shop.example.ru/login`. В новой базе действуют стандартные значения настроек — название «ЕШ», демонстрационные телефон, адрес и объявление в шапке. Их нужно заменить до открытия магазина:

- 1 **«Настройки» → «Магазин».** Выключите «Магазин включён» — покупатели увидят заглушку, сотрудники продолжат работать. Заполните название, слоган, описание, логотип, контакты, текст объявления в шапке (или выключите его), ссылки на соцсети.
- 2 **«Настройки» → «Реквизиты».** Наименование, ИНН, КПП, ОГРН, адрес, банк, система налогообложения и ставка НДС — они попадают в чеки, счета и УПД.
- 3 **«Настройки» → «Сотрудники».** Создайте учётные записи сотрудников с нужными ролями. Число сотрудников ограничено лицензией.
- 4 **Каталог.** Категории, товары с изображениями, остатки (через приход на склад).
- 5 **Остальное** по необходимости: SEO и счётчики, страницы конструктора, шаблоны документов, подключения маркетплейсов, сканер штрихкодов.
- 6 Когда всё готово — включите «Магазин включён».

6.6 Активация лицензии

Откройте «Настройки» → «Лицензия и модули», введите ключ `NOVA-XXXX-XXXX-XXXX-XXXX` из письма продавца и нажмите «Активировать». Магазин регистрирует установку на сервере лицензий с доменом из сборки. Если доступа в интернет нет, используйте блок «Без доступа в интернет» (офлайн-лицензия по коду запроса). Подробно — в разделе 5 инструкции по лицензированию.



Страница «Лицензия и модули» в админке магазина

6.7 Проверка после запуска

- ☐ `http://shop.example.ru` и `https://www.shop.example.ru` перенаправляют на `https://shop.example.ru`, замок в браузере без предупреждений.
- ☐ `/robots.txt` и `/sitemap.xml` содержат адреса с вашим доменом и `https`.
- ☐ Вход в админку работает, страница входа не показывает демо-доступы.
- ☐ Изображение товара загружается и появляется в `/var/lib/nova-store/uploads`.
- ☐ Лицензия активна; на сервере лицензий в карточке лицензии видна установка с правильным доменом.
- ☐ Тестовый заказ проходит от корзины до документов; после проверки отмените его.
- ☐ В карточке тестового заказа виден город по IP — значит, nginx передаёт адрес посетителя (если подключён модуль «Город покупателя»).
- ☐ После `sudo systemctl restart nova-store` все данные и изображения на месте.
- ☐ Резервная копия создаётся (раздел 8), задание cron настроено.
- ☐ Пробный запуск `sudo certbot renew --dry-run` проходит без ошибок.

7 Обновление и откат

7.1 Обновление магазина

Продавец собирает пакет новой версии под тот же домен (раздел 5.3) и передаёт архив. Установка — те же команды, что и в первый раз:

```
sudo tar -xzf /tmp/nova-store-1.1.0-shop.example.ru.tar.gz -C /opt/nova-store
sudo bash /opt/nova-store/nova-store-1.1.0-shop.example.ru/deploy/install-release.sh
```

Перед переключением скрипт делает резервную копию базы и изображений, затем обновляет схему базы, пока работает старая версия. Магазин недоступен только на время перезапуска — несколько секунд. Папка приложения остаётся прежней (`/opt/nova-store/app`), поэтому отпечаток сервера в лицензии не меняется.

Если обновление схемы требует удаления данных

Когда новая версия удаляет столбец или таблицу с данными, `prisma db push` останавливается с предупреждением о потере данных, и скрипт прерывается до переключения — магазин продолжает работать на старой версии. Не продолжайте вслепую: уточните у продавца, какие данные затрагиваются. Применить изменения можно вручную: `cd` в папку пакета и `sudo -u nova -H npx prisma@6.19.3 db push --schema prisma/schema.prisma --skip-generate --accept-data-loss`, затем снова запустить скрипт.

7.2 Откат магазина

```
sudo systemctl stop nova-store
sudo mv /opt/nova-store/app /opt/nova-store/app.failed
sudo mv /opt/nova-store/app.prev /opt/nova-store/app
sudo systemctl start nova-store
```

Обычно схема базы обновляется только добавлением полей, и старая версия работает с новой базой. Если после отката появляются ошибки базы, восстановите копию, сделанную перед обновлением (раздел 8.3): её имя с датой и временем обновления.

7.3 Обновление сервера лицензий

```
# из git: забрать изменения, собрать, перезапустить
sudo bash /opt/nova-license/app/deploy/update.sh --pull

# из архива: распакуйте новые файлы поверх /opt/nova-license/app (кроме .env), затем
sudo bash /opt/nova-license/app/deploy/update.sh
```

Скрипт делает резервную копию, обновляет зависимости и схему, собирает новую версию во вторую папку и перезапускает службу. Если сборка не удалась, работает прежняя версия. Откат на предыдущую сборку — команда, которую скрипт печатает при ошибке:

```
echo NEXT_DIST_DIR=.next-a | sudo tee /etc/nova-license/dist.env # или .next-b — прежняя папка
sudo systemctl restart nova-license
```

7.4 Обновление системы и Node.js

- Обновления безопасности ставятся автоматически (3.2). Раз в месяц выполняйте `sudo apt update && sudo apt full-upgrade` и перезагружайте сервер, если требуется (`/var/run/reboot-required`).
- Node.js обновляется вместе с системой в пределах основной версии. Переход на новую основную версию (например, 24 → 26) делайте одновременно на сборочной машине и серверах, затем пересоберите пакеты.

8 Резервное копирование и восстановление

8.1 Что копировать

Данные	Где	Почему важно
База магазина	<code>/var/lib/nova-store/store.db</code>	Все заказы, товары, клиенты, документы, учёт, состояние лицензии
Изображения магазина	<code>/var/lib/nova-store/uploads/</code>	Фото товаров, логотип, картинки страниц
Настройки магазина	<code>/etc/nova-store/store.env</code>	<code>AUTH_SECRET</code> нужен, чтобы прочитать ключи маркетплейсов из базы
База сервера лицензий	<code>/var/lib/nova-license/license.db</code>	Клиенты, лицензии, установки, продажи и закрытый ключ подписи
Настройки сервера лицензий	<code>/etc/nova-license/license.env</code>	Секрет сессий; ключ подписи, если задан переменной

Приложения копировать не нужно: магазин восстанавливается из пакета, сервер лицензий — из репозитория.

8.2 Ежедневные копии

Скрипты `deploy/backup.sh` делают горячую копию SQLite (`.backup` — безопасно при работающем приложении), проверяют её целостность, сжимают, копируют изображения и файл настроек и удаляют копии старше 14 дней (сервер лицензий — 30 дней).

```
# магазин: каждый день в 03:30
echo '30 3 * * * root /opt/nova-store/app/deploy/backup.sh >> /var/log/nova-store-backup.log 2>&1' \
| sudo tee /etc/cron.d/nova-store

# сервер лицензий: каждый день в 03:00
echo '0 3 * * * root /opt/nova-license/app/deploy/backup.sh >> /var/log/nova-license-backup.log 2>&1' \
| sudo tee /etc/cron.d/nova-license

# проверка вручную
sudo bash /opt/nova-store/app/deploy/backup.sh
ls -lh /var/backups/nova-store/
```

Копии вне сервера

Копии на том же диске не спасут при потере сервера. Ежедневно отправляйте их на другой сервер или в S3-совместимое хранилище российского провайдера. Копии сервера лицензий содержат закрытый ключ — шифруйте их.

```
# на другой сервер по SSH-ключу
rsync -a --delete /var/backups/nova-store/ backup@198.51.100.5:/backups/shop.example.ru/

# в S3 через rclone (настройка: rclone config)
rclone copy /var/backups/nova-store s3:nova-backups/shop.example.ru

# шифрование копий сервера лицензий паролем перед отправкой
gpg --batch --symmetric --passphrase-file /root/.backup-pass \
  -o license-2026-10-02-0300.db.gz.gpg /var/backups/nova-license/license-2026-10-02-0300.db.gz
```

Добавьте эти команды в скрипт после основного копирования. Раз в квартал проверяйте восстановление на отдельной машине: непроверенная копия — не копия.

8.3 Восстановление магазина

```
sudo systemctl stop nova-store
cd /var/lib/nova-store
sudo mv store.db store.db.broken
sudo rm -f store.db-journal
gunzip -c /var/backups/nova-store/store-2026-10-02-0330.db.gz | sudo tee store.db >/dev/null
sudo tar -xzf /var/backups/nova-store/uploads-2026-10-02-0330.tar.gz -C /var/lib/nova-store
sudo chown -R nova:nova /var/lib/nova-store
sudo systemctl start nova-store
```

Сервер лицензий восстанавливается так же: служба `nova-license`, файлы `/var/lib/nova-license/license.db` и копия `license-*.db.gz`.

8.4 Перенос на другой сервер

- 1 Подготовьте новый сервер (раздел 3) и установите тот же пакет (раздел 6) — без создания администратора.
- 2 На старом сервере в «Настройки» → «Лицензия и модули» нажмите «Удалить лицензию с сервера» — место установки освободится. Если старый сервер уже недоступен, продавец освобождает место кнопкой «Освободить» в карточке лицензии.
- 3 Остановите службу на старом сервере и сделайте копию; перенесите `store.db`, `uploads` и **тот же** `store.env` (с прежним `AUTH_SECRET`).
- 4 Восстановите данные на новом сервере (8.3), переключите DNS-запись домена на новый IP, выпустите сертификат.
- 5 Активируйте тот же ключ на новом сервере. Если перенести базу без удаления лицензии, магазин продолжит работать, а продавец увидит у установки отметку «Сменился сервер» (раздел 5.8 инструкции по лицензированию).

9 Мониторинг и обслуживание

9.1 Состояние и журналы

```
systemctl status nova-store nova-license nginx      # состояние служб
journalctl -u nova-store -f                        # журнал магазина в реальном времени
journalctl -u nova-store --since "1 hour ago"      # за последний час
journalctl -u nova-store --since today | grep -E "\[license\]|\[marketplaces\]|\[geo\]"
sudo tail -f /var/log/nginx/access.log /var/log/nginx/error.log
```

Метка в журнале	Что означает
[license]	Ошибка ежедневной проверки лицензии: нет связи с сервером лицензий, неверный ответ. Состояние лицензии видно в админке.
[marketplaces]	Ошибка обмена с маркетплейсом. Подробности — в журнале обмена раздела «Маркетплейсы».
[geo]	Сервис ipwho.is не ответил или не определил город. Единичные сообщения — норма.

Ограничьте размер системного журнала: в `/etc/systemd/journald.conf` задайте `SystemMaxUse=500M` и выполните `sudo systemctl restart systemd-journald`.

9.2 Внешний мониторинг

Подключите любой сервис проверки доступности (раз в 1–5 минут, уведомления в Telegram или на почту):

Адрес	Ожидаемый ответ
<code>https://shop.example.ru/robots.txt</code>	200, текст содержит <code>Sitemap:</code>
<code>https://license.example.ru/login</code>	200
Срок SSL-сертификатов	Больше 20 дней (certbot продлевает за 30)

9.3 Регулярные проверки

Как часто	Что проверить
Ежедневно	Уведомления мониторинга; в журнале копий нет ошибок (<code>/var/log/nova-*-backup.log</code>).
Еженедельно	Место на диске: <code>df -h</code> , <code>du -sh /var/lib/nova-store/* /var/backups/*</code> . Предупреждения в админке магазина (лицензия, маркетплейсы).
Ежемесячно	Обновление системы и перезагрузка; <code>sudo certbot renew --dry-run</code> ; журнал сервера лицензий на подозрительные активации.
Ежеквартально	Пробное восстановление из копии на отдельной машине; ревизия сотрудников и паролей.

10 Безопасность

- ☐ Вход на сервер только по SSH-ключам, вход под root и по паролю запрещён (3.2).
- ☐ Брандмауэр пропускает только 22, 80 и 443; приложения слушают только `127.0.0.1`.
- ☐ Приложения работают от пользователя `nova` без права входа; юниты `systemd` ограничивают запись папками приложения и данных.
- ☐ `AUTH_SECRET` и `SESSION_SECRET` — уникальные случайные строки для каждого сервера; файлы настроек доступны только root и `nova` (права 640).
- ☐ Администратор магазина создан скриптом с надёжным паролем; демо-данные и демо-учётные записи на рабочем сервере не загружались.
- ☐ Пароль администратора сервера лицензий сменён при первом входе, `VENDOR_ADMIN_PASSWORD` удалён из файла настроек.
- ☐ Кабинет сервера лицензий по возможности закрыт списком IP (4.4); у каждого сотрудника продавца своя учётная запись.
- ☐ Резервные копии сервера лицензий зашифрованы и хранятся минимум в двух местах.
- ☐ На сервере магазина нет исходного кода и режима разработки (`next dev`): в нём все модули работают без лицензии.
- ☐ HTTPS везде, HSTS включён, `INSECURE_COOKIES` не задан.
- ☐ Тестовые копии магазина закрыты от индексации («SEO» → «Индексация») и паролем на уровне `nginx` (`auth_basic`).
- ☐ Обновления безопасности системы ставятся автоматически.

11 Решение проблем

Симптом	Причина	Что сделать
502 Bad Gateway	Служба не запущена или упала	<code>systemctl status nova-store</code> , <code>journalctl -u nova-store -n 80</code> . Проверьте, что порт в <code>nginx</code> совпадает с юнитом (3100 / 3300).
После входа снова открывается форма входа	Сайт открыт по HTTP: cookie с флагом Secure не сохраняется	Откройте по <code>https://</code> . Для временной проверки без сертификата — <code>INSECURE_COOKIES=1</code> и перезапуск.
Формы админки не сохраняются, в журнале «Invalid Server Actions request»	<code>nginx</code> не передаёт <code>Host</code> / <code>X-Forwarded-Host</code> , или сайт открыт не по основному домену	Сверьте блок <code>location /</code> с <code>deploy/nginx-nova-store.conf</code> , перезагрузите <code>nginx</code> .
Ошибка 413 при загрузке изображения	Лимит размера запроса в <code>nginx</code>	<code>client_max_body_size 10m</code> ; в блоке <code>server</code> .
«Query engine library for current platform ... could not be found»	Пакет собран на другой ОС или с другим OpenSSL	Соберите пакет на Linux той же линейки (5.1) или добавьте <code>binaryTargets</code> .
«attempt to write a readonly database», «unable to open database file»	Нет прав у <code>nova</code> или неверный путь в <code>DATABASE_URL</code>	<code>sudo chown -R nova:nova /var/lib/nova-store</code> ; проверьте путь и что папка существует.
Изображения пропали после обновления	Пакет установлен вручную, без ссылки <code>uploads</code>	Устанавливайте через <code>install-release.sh</code> ; файлы лежат в <code>/var/lib/nova-store/uploads</code> .
Лицензия: «не удалось связаться с сервером лицензий»	Нет исходящего HTTPS, DNS или сертификат сервера лицензий недействителен	С сервера магазина: <code>curl -sI https://license.example.ru/login</code> . Проверьте брандмауэр хостера и сертификат.
Лицензия: неверная подпись	Пакет собран с ключом другого сервера лицензий (часто — с ключом разработки)	Пересоберите пакет с <code>license-public.pem</code> рабочего сервера (5.2).
Лицензия: домен не совпадает	<code>NEXT_PUBLIC_SITE_URL</code> сборки отличается от домена в лицензии	Соберите пакет под правильный домен или исправьте домен в лицензии на сервере.
На сервере лицензий после обновления магазина — «Сменился сервер»	Магазин запущен из другой папки или у сервера сменилось имя	Всегда запускайте из <code>/opt/nova-store/app</code> через <code>install-release.sh</code> . При переносе на другой сервер — 8.4.
Все пользователи вышли, ключи маркетплейсов не читаются	Изменён <code>AUTH_SECRET</code>	Верните прежнее значение из резервной копии <code>store-*.env</code> .
Сборка прерывается: «Killed», код 137, «heap out of memory»	Не хватает памяти	Добавьте файл подкачки (3.3) или соберите на машине с 4 ГБ памяти.

Симптом	Причина	Что сделать
<code>npx prisma</code> не загружается при установке	Нет доступа к <code>registry.npmjs.org</code>	Откройте доступ или заранее установите CLI: <code>sudo npm i -g prisma@6.19.3</code> и замените в скрипте <code>npx --yes prisma@6.19.3</code> на <code>prisma</code> .
Неверное время в документах и отчётах	Часовой пояс сервера	<code>timedatectl set-timezone ...</code> и <code>TZ</code> в юните, перезапуск службы.
Город покупателя не определяется	Нет доступа к <code>ipwho.is</code> или <code>nginx</code> не передаёт IP	Проверьте исходящий доступ и заголовок <code>X-Forwarded-For</code> ; за Cloudflare — источник «Заголовки хостинга» (12.3).
Сертификат не продлился	Порт 80 закрыт или удалён блок <code>/.well-known/acme-challenge/</code>	<code>sudo certbot renew --dry-run</code> покажет причину.

12 Дополнительно

12.1 Несколько магазинов на одном сервере

Каждому магазину нужны свои папки, база, порт и служба. Для второго магазина скопируйте юнит и скрипты, заменив имена и порт:

Параметр	Первый магазин → второй
Папки	<code>/opt/nova-store</code> , <code>/var/lib/nova-store</code> , <code>/etc/nova-store</code> → <code>.../nova-store-2</code>
Служба	<code>nova-store.service</code> → <code>nova-store-2.service</code>
Порт	<code>PORT=3100</code> → <code>3101</code> (в юните, в <code>proxy_pass</code> и в переменной <code>PORT</code> скрипта установки)
Переменные скриптов	<code>BASE</code> , <code>DATA</code> , <code>ENV_FILE</code> , <code>SERVICE</code> в <code>install-release.sh</code> ; <code>DATA</code> , <code>DEST</code> , <code>ENV_FILE</code> в <code>backup.sh</code>

Ориентир по памяти — 300–500 МБ на магазин с запасом под нагрузку.

12.2 PostgreSQL вместо SQLite

SQLite достаточно для большинства магазинов: база в одном файле, без отдельной СУБД, с простыми копиями. PostgreSQL имеет смысл при высокой нагрузке, большом объёме данных или требовании хранить базу на отдельном сервере. Переход выполняется в исходниках: `provider = "postgresql"` в `prisma/schema.prisma` , строка подключения в `DATABASE_URL` , затем пересборка пакета. Резервные копии — через `pg_dump` вместо `sqlite3 .backup` . Перенос существующих данных из SQLite — отдельная задача миграции.

12.3 Cloudflare и CDN

При работе через Cloudflare или другой CDN-прокси:

- режим SSL — **Full (strict)**, сертификат Let's Encrypt на сервере оставьте;
- настройте в nginx модуль `real_ip` (`set_real_ip_from` для адресов Cloudflare, `real_ip_header` `CF-Connecting-IP`), чтобы `$remote_addr` был адресом посетителя;
- в магазине в настройках геолокации выберите источник «Заголовки хостинга» и включите у Cloudflare заголовки местоположения — город будет определяться без `ipwho.is`;
- для Let's Encrypt через прокси используйте проверку DNS-01 или временно отключайте проксирование.

12.4 Контейнеры и PaaS

Пакет магазина подходит для контейнера: образ `node:24-bookworm-slim` , команда `node server.js` , переменные `PORT` , `HOSTNAME=0.0.0.0` , `NODE_ENV=production` , `DATABASE_URL` , `AUTH_SECRET` . Обязательные условия: постоянные тома для базы и `/app/uploads` , ровно одна реплика, постоянная рабочая папка и имя

хоста контейнера (иначе при каждом пересоздании меняется отпечаток сервера в лицензии). Готовые файлы Docker в поставку не входят.

12.5 Чек-лист запуска

Сервер лицензий

- ☐ VPS, DNS, сертификат, nginx
- ☐ Служба `nova-license` работает
- ☐ Пароль администратора сменён
- ☐ API отвечает снаружи
- ☐ `license-public.pem` выгружен
- ☐ Копии: cron, внешнее хранилище, шифрование
- ☐ Мониторинг доступности

Магазин

- ☐ Пакет собран с рабочим ключом и доменом
- ☐ VPS, DNS, сертификат, nginx
- ☐ Служба `nova-store` работает
- ☐ Администратор создан, настройки и реквизиты заполнены
- ☐ Лицензия активирована
- ☐ Проверки из 6.7 пройдены
- ☐ Копии и мониторинг настроены
- ☐ Оплата, касса, письма — по разделу «Перед запуском в продакшен» README