АРХИТЕКТОРЫ ПРОГРАММНЫХ СИСТЕМ

Правообладатель — ООО «ОПТОР» (ИНН 1800058065)

Программа для ЭВМ «iCubix Учёт печати (Айкубикс Учёт печати)»

Руководство администратора

ГОСТ 19.503-79 · ВЕРСИЯ ПРОГРАММЫ 1.6.0

Редакция от 21.11.2026 · исходный текст 0101fc4
Актуальный комплект — arpsys.ru/icubix/uchet-pechati/dokumentaciya/ · поддержка: support@arpsys.ru

Руководство администратора

ГОСТ 19.503-79 («Руководство системного программиста»).

1. Общие сведения о программе

«iCubix Учёт печати» — веб-приложение для учёта и контроля печати. Устанавливается на сервер организации и работает без доступа в интернет. Назначение и функции — «Описание программы», порядок установки — «Инструкция по установке».

Состав:

- **сервер** — пакет `icubix`: веб-приложение и фоновые задачи, команда администратора `icubix`;
- **сборщики** — пакет `printaxis-collector` на площадках: опрашивают аппараты и передают показания на сервер;
- **агенты** — на рабочих местах Windows и Linux: передают задания печати и исполняют запрет печати по квотам.

Окружение сервера:

- ОС — Astra Linux SE 1.8, РЕД ОС 8 или Альт p11;
- PostgreSQL 15 или новее;
- nginx для HTTPS.

Аппаратные требования — «Инструкция по установке», раздел 1.

Администратор:

- устанавливает и обновляет программу;
- ведёт пользователей и права;
- подключает каталог, почту, SIEM;
- следит за резервными копиями и журналами.

Повседневная работа в интерфейсе — в руководстве пользователя.

2. Структура программы

Путь	Назначение
`/opt/icubix/`	Программа со своим интерпретатором Python (только чтение)
`/usr/bin/icubix`	Команда администратора: `icubix license`, `icubix manage …`
`/etc/icubix/icubix.conf`	Настройки (база, адрес системы, число процессов)
`/etc/icubix/secret_key`	Секретный ключ приложения (создаётся при установке; не передавать)
`/etc/icubix/data_key`	Ключ шифрования паролей в базе (SNMP, AD, SMTP); без него они не расшифровываются — хранить вместе с резервной копией базы, но отдельно от неё
`/etc/icubix/license.json`	Файл лицензии

Путь	Назначение
`/etc/icubix/ai_key`	Ключ API сервера модели ИИ, если он нужен (root:icubix, 0640; раздел 3.5)
`/var/lib/icubix/`	Рабочий каталог служб; `static/` — статические файлы для nginx
`/usr/lib/systemd/system/icubix*.{target,service}`	Службы
`/usr/share/icubix/nginx/icubix.conf`	Пример настройки nginx
`/usr/share/doc/icubix/`	Лицензионное соглашение, журнал изменений
`/opt/printaxis-collector/`, `/usr/bin/printaxis-collect`	Сборщик iCubix Учёт печати (пакет `printaxis-collector`, ставится на площадки)
`/etc/printaxis/collector.env`	Сервер и токен сборщика (root и группа `printaxis`, 0640)
`/var/lib/printaxis/`	Очередь неотправленных показаний и последний обход сборщика

Службы работают от учётной записи `icubix` без входа в систему и с ограничениями systemd: файловая система только для чтения (кроме `/var/lib/icubix`), без повышения привилегий и доступа к устройствам.

Служба	Назначение
`icubix.target`	Все службы вместе: `systemctl enable/start/stop/restart icubix.target`
`icubix-web.service`	Веб-приложение (gunicorn) на `127.0.0.1:8070`; при запуске обновляет схему базы
`icubix-worker.service`	Фоновые и периодические задачи (procrastinate)

3. Настройка программы

3.1. Лицензия

Файл лицензии, полученный от ООО «ОПТОР», поместить в `/etc/icubix/license.json` и проверить:

```
icubix license
```

Проверка выполняется без доступа в интернет.

3.2. Параметры

Все параметры — в `/etc/icubix/icubix.conf`, формат `ICUBIX_ИМЯ=значение` (пояснения — в самом файле). Файл читают службы и команды `icubix manage …`; запускать их — от root или пользователя из группы `icubix`. После изменения:

```
sudo systemctl restart icubix.target
```

История показаний (iCubix Учёт печати). Сборщик снимает показания раз в час. Последние `ICUBIX_PRINTAXIS_HOURLY_DAYS` дней (по умолчанию 90) хранятся все, старше — одно показание аппарата в сутки: последнее за день, а также показание в полночь, первое показание аппарата, показания вокруг замены счётчика и перенесённые из старой системы. Отчёты за период по дням от этого не меняются. Прореживание выполняет служба `icubix-worker` раз в час; накопленная история разбирается по 14 суток за запуск, каждый запуск — запись `printaxis.readings.thin` в журнале действий. Место в базе освобождается для новых данных; чтобы уменьшить файлы базы после первого прореживания большой истории — `VACUUM FULL printaxis_reading` в окно обслуживания. `ICUBIX_PRINTAXIS_HOURLY_DAYS=0` — хранить все показания.

3.3. Пользователи и права

Первый администратор — `sudo icubix manage createsuperuser`. Остальные пользователи, организации и группы прав — в разделе администрирования (`/admin/`). Пользователь видит данные только своей организации.

Завершение сеанса. Сеанс пользователя завершается после `ICUBIX_SESSION_IDLE_MINUTES` минут без действий (по умолчанию 30) и в любом случае через 8 часов после входа. Автообновление сводки действием не считается. После простоя пользователь попадает на страницу входа с пояснением и после входа возвращается на ту же страницу; в журнале действий — запись `core.session_idle`. `ICUBIX_SESSION_IDLE_MINUTES=0` — не завершать по бездействию.

Персональные данные сотрудников (152-ФЗ). Когда сотрудник уволился или истёк срок хранения его ПДн, его обезличивают: «Настройки → Персональные данные» или `icubix manage anonymize --org "<организация>" <логин>`. - Что меняется: логин в заданиях печати, справочнике сотрудников, персональных квотах и уведомлениях заменяется одним случайным псевдонимом «обезличен-...», ФИО стирается. Учётная запись в iCubix переименовывается в псевдоним, ФИО и почта стираются, вход закрывается. - Что остаётся: страницы, отдел, аппараты и даты — отчёты за прошлые периоды не меняются. - Вычислить человека по псевдониму нельзя: псевдоним случайный и вместе с логином нигде не хранится. Отменить обезличивание нельзя. - Журнал действий не обезличивается: записи неизменяемы, а хранение журнала событий безопасности обязательно. Само обезличивание пишется в журнал как `core.anonymize` с псевдонимом и числом записей, без логина. - По сроку: `ICUBIX_ANONYMIZE_AFTER_DAYS=N` (не меньше 30; по умолчанию 0 — выключено). Тогда каждую ночь обезличиваются сотрудники без печати дольше N дней и без действующей учётной записи. Список таких сотрудников — на той же странице; вручную — `icubix manage anonymize --org "<организация>" --inactive-days N` (без `--yes` только показывает). - Право — «Обезличивание персональных данных сотрудников» (`core.anonymize_person`). По умолчанию оно есть только у суперпользователя; ответственному за ПДн его выдают в администрировании.

Второй фактор входа. Сотрудник подключает приложение-генератор кодов (TOTP, RFC 6238: «Яндекс Ключ», Aladdin 2FA, FreeOTP и др.) сам: «Безопасность входа» в шапке. После этого вход по паролю — локальному или доменному — требует ещё 6-значный код; вход через Windows (Kerberos) и вызовы API — без кода. Код годится один раз, неверные коды считаются вместе с неверными паролями (5 подряд — вход закрыт на 15 минут). Секрет хранится в базе зашифрованным. Обязательность — `ICUBIX_TOTP_REQUIRED` : `none` (по умолчанию, по желанию сотрудника), `staff` (администраторам), `all` (всем); без подключённого приложения такой пользователь попадает только на страницу подключения. Потерян телефон — «Администрирование → Пользователи», отметить пользователя, действие «Сбросить второй фактор». Подключение, отключение и сброс — записи `core.totp_enable` , `core.totp_disable` , `core.totp_reset` в журнале действий; вход с кодом — `core.login` со способом `totp` , верный пароль без кода — `core.login_password` .

3.4. Интеграции

Вход через домен. «Настройки → Вход через домен»: Active Directory, Samba AD, РЕД АДМ (вид «Active Directory») или FreeIPA и ALD Pro (вид «FreeIPA / ALD Pro»). Пароль проверяет контроллер домена, права даются по группам каталога с учётом вложенных. Канал только шифрованный: `ldaps://` или `ldap://` со StartTLS. Служебная учётка — только чтение: в AD — обычный пользователь, во FreeIPA и ALD Pro — системная учётка в `cn=sysaccounts,cn=etc,<база>`. Для FreeIPA и ALD Pro: база поиска — `cn=accounts,dc=…`, группа — `cn=<имя>,cn=groups,cn=accounts,dc=…`, домен — область Kerberos. Каждые 5 минут вошедшие перепроверяются: отключённая в каталоге или убранная из групп учётка теряет доступ.

Вход через Windows без пароля (Kerberos). Билет Kerberos проверяет Apache `mod_auth_gssapi` на локальном адресе, nginx передаёт ему только адрес `/sso/`. Права даются, как при входе через AD по паролю: по группам AD. Включается параметром `ICUBIX_SSO_SECRET` — общим секретом с Apache. Порядок настройки — в `/usr/share/doc/icubix/sso.md`.

Почта. Письма — оповещения, рассылка отчётов, обращения в поддержку — уходят через канал «письмо» раздела «События»: SMTP-сервер организации, порт, шифрование, учётная запись. Пароль хранится зашифрованным. Кнопка «Проверить» отправляет тестовое письмо.

Вебхуки и Service Desk заказчика. Канал «вебхук» — HTTP POST с JSON о событии на адрес системы заказчика. Канал «заявка в Service Desk iCubix» заводит заявки во встроенном Service Desk. Неотправленные сообщения повторяются; ошибки видны в «Событиях».

MAX. Канал «сообщение в MAX» отправляет события через бота платформы MAX для партнёров (`platform-api2.max.ru`). Это единственный канал, которому нужен доступ в интернет; в закрытом контуре он не используется. Токен бота хранится зашифрованным.

1С и BI. «Подключения» → «Ключи API» → выпустить ключ. Выгрузки: аппараты, отпечатки, сотрудники, задания — в JSON и CSV по `GET /api/v1/export/…` с заголовком `Authorization: Bearer <ключ>`. Примеры для 1С и Power BI — по запросу в поддержку. Ключ показывается один раз, на сервере хранится только его хеш; каждый вызов записывается в журнал.

SIEM. Журнал действий выгружается в SIEM по syslog (RFC 5424) раз в минуту.

- Подключение: `ICUBIX_SIEM=udp://…`, `tcp://…` или `tls://…:6514` в `/etc/icubix/icubix.conf`.
- Формат: `ICUBIX_SIEM_FORMAT=cef` (MaxPatrol SIEM, KUMA, RuSIEM) или `json`.
- Для TLS — `ICUBIX_SIEM_CA` и, если SIEM требует, сертификат клиента.
- Проверка — `icubix manage siem test`, состояние — `icubix manage siem status`.
- Повторная отправка с даты — `icubix manage siem rewind --since ГГГГ-ММ-ДД`.

ЕСИА, СМЭВ. Не используются: пользователи программы — сотрудники организации, они входят через её каталог.

3.5. ИИ и документы

ИИ — функция ядра iCubix для всех продуктов: черновик ответа на заявку Service Desk и ответы по документам организации со ссылкой на источник.

Модель не входит в поставку. iCubix обращается к серверу модели в сети организации по OpenAI-совместимому API (`/v1/chat/completions`): vLLM, Ollama, совместимый шлюз. В интернет iCubix не обращается. **По умолчанию ИИ выключен**: кнопок ИИ нет, функции отказывают.

Включение. В `/etc/icubix/icubix.conf`:

Параметр	Назначение	По умолчанию
`ICUBIX_AI`	1 — включить ИИ	0
`ICUBIX_AI_URL`	Адрес API сервера модели, например `http://gpu-server:8000/v1`	—
`ICUBIX_AI_MODEL`	Имя модели на этом сервере	—
`ICUBIX_AI_API_KEY_FILE`	Файл с ключом API, если сервер модели его требует	`/etc/icubix/ai_key`
`ICUBIX_AI_TIMEOUT`	Сколько секунд ждать ответа модели; повторов нет	60
`ICUBIX_AI_MAX_TOKENS`, `ICUBIX_AI_MAX_CHARS`	Предел длины ответа модели (токенов) и запроса (символов)	1024, 20000
`ICUBIX_AI_ANONYMIZE`	Обезличивание перед моделью; 0 — только для модели на своём сервере в том же контуре	1
`ICUBIX_AI_PROVIDER`	`openai` — сервер модели; `stub` — встроенная заглушка для проверки без сервера модели	`openai`
`ICUBIX_DOCS_MAX_MB`	Наибольший размер загружаемого документа, МБ	20
`ICUBIX_DOCS_OCR`	Распознавание сканов, если установлены программы (ниже); 0 — выключить	1
`ICUBIX_DOCS_OCR_MAX_PAGES`	Сколько страниц одного скана распознавать	50
`ICUBIX_DOCS_OCR_LANG`	Языки распознавания (установленные словари tesseract)	`rus+eng`

Ключ API хранится только в файле: в базе, журнале и логах его нет. После изменения — `systemctl restart icubix.target`. Затем группам сотрудников выдаются права (раздел 3.3):

Право	Что даёт
Пользоваться ИИ (`ai.use_ai`)	Кнопки «Черновик ИИ» и «Спросить по документам» (вместе с правами на заявки или документы)
Может просматривать / добавлять / удалять / изменять документ	Поиск и просмотр, загрузка, удаление, перенос документов между пространствами
Может добавлять / изменять / удалять пространство документов	Управление пространствами; «изменять» — ещё и доступ ко всем пространствам своей организации

Обезличивание. Перед отправкой в модель реквизиты заменяются псевдонимами (`[ИНН-1]`, `[ФИО-2]`), а в ответе подставляются обратно:

- ИНН, СНИЛС, ОГРН, ОГРНИП и номер карты — с проверкой контрольной суммы;
- паспорт, телефон, электронная почта — по формату;
- ФИО — точным совпадением со справочником организации (пользователи iCubix и сотрудники Учёта печати).

Если в заявке осталась строка из 10 и более цифр, не прошедшая проверку, — запрос в модель не отправляется, пользователь видит причину. В документах такие номера (расчётные счета, номера договоров) заменяются псевдонимом `[НОМЕР-n]`. Имена людей, которых нет в справочнике, не распознаются.

Документы. Файлы (PDF, DOCX, ODT, TXT и сканы JPEG, PNG, TIFF) хранятся в базе и входят в резервную копию (раздел 5). Текст разбирает служба `icubix-worker` — пока она остановлена, новые документы остаются в состоянии «Разбирается».

Распознавание сканов. Страницы PDF без текстового слоя и картинки распознаются программами из репозитория ОС — tesseract с русским словарём и `pdftoppm`. Пакет iCubix их рекомендует, но не требует; в поставку они не входят. Установка:

```
sudo apt install tesseract-ocr tesseract-ocr-rus poppler-utils    # Astra Linux 1.8
sudo apt-get install tesseract tesseract-langpack poppler         # Альт p11
sudo dnf install tesseract tesseract-langpack-rus poppler-utils   # РЕД ОС 8 (если пакеты
есть в репозитории)
tesseract --list-langs                                            # в списке должен быть
rus
sudo systemctl restart icubix-worker
```

Страница распознаётся за 3–8 секунд в зависимости от качества скана, поэтому большой скан разбирается минуты. Распознаются не больше `ICUBIX_DOCS_OCR_MAX_PAGES` страниц, остальные указываются в причине. В карточке документа пользователь видит «Текст распознан со скана», в журнале разбора — число распознанных страниц. Без программ скан получает состояние «Ошибка», и в причине названы пакеты, которые нужно поставить.

Пространства документов — разделы под отдел со своими группами участников и инструкцией для ИИ («Документы» → «Пространства»). Документы пространства видят только участники его групп и управляющие пространствами; документы без пространства — все, у кого есть право просмотра документов.

Облачные сервисы. `ICUBIX_AI_PROVIDER=deepseek` или `yandex` — облачные DeepSeek и YandexGPT. Они работают только вместе с `ICUBIX_AI_CLOUD=1`, обезличивание для них включено всегда. **В закрытом контуре и у государственного заказчика облачные сервисы не включать**: запрос уходит из сети организации, у DeepSeek — за рубеж. Для YandexGPT нужен ещё `ICUBIX_AI_YANDEX_FOLDER` — каталог Yandex Cloud.

Проверка ИИ без интерфейса. `icubix manage servicedesk_ai_eval` прогоняет встроенные вымышленные заявки через выбранную модель тем же запросом, что и кнопка, и показывает черновик, время ответа и что обезличено. Ключ `--show-request` — показать запрос к модели. Если реквизит попал в запрос не обезличенным, команда пишет «УТЕЧКА» и этот запрос в модель не отправляет. В базу ничего не пишется.

4. Проверка программы

```
systemctl status icubix-web icubix-worker   # обе службы active (running)
curl -s http://127.0.0.1:8070/healthz       # «ok»: приложение отвечает и база доступна
icubix manage check --deploy                # проверка настроек безопасности
icubix manage audit_verify                  # целостность журнала действий
icubix license
```

Адрес `/healthz` открыт без входа и подходит для систем мониторинга.

5. Резервное копирование и восстановление

Копия — один файл `icubix-backup-ГГГГММДД-ЧЧММСС.tar` с правами 600. В нём:

- дамп базы — все данные, включая журнал действий;
- `/etc/icubix/icubix.conf`;
- ключи `secret_key` и `data_key`;
- опись с контрольными суммами.

Без `data_key` пароли SNMP, почты и подключений из базы не расшифровать. Поэтому копию хранят как пароль: отдельно от сервера, с ограниченным доступом. Файл лицензии в копию не входит: его хранят отдельно, при утере запрашивают у поставщика.

```
sudo icubix manage backup create                    # копия в ICUBIX_BACKUP_DIR
(/var/backups/icubix)
sudo icubix manage backup verify <файл>             # целостность копии и версия, с
которой она снята
sudo systemctl enable --now icubix-backup.timer     # ежедневно в 03:30, хранить
ICUBIX_BACKUP_KEEP (14) копий
```

Восстановление останавливает службы, заменяет базу и настройки копией и запускает службы снова:

```
sudo icubix manage backup restore <файл> --yes
```

Параметры подключения к базе в копии не восстанавливаются — берутся с этого сервера. Поэтому копию можно восстановить на новом сервере после установки пакета. Копия снимается на версии программы, указанной в описи; восстанавливать её — на той же или более новой версии.

6. Обновление

Сделать резервную копию (раздел 5) и установить пакет новой версии поверх текущей (`apt install ./…deb`, `dnf install ./…rpm`). Работающие службы перезапускаются сами, схема базы обновляется при запуске `icubix-web`. Настройки, лицензия и данные сохраняются.

7. Журналы и аудит

- **Журналы служб** — в journald:

`bash journalctl -u icubix-web # запросы (адрес клиента, путь, код ответа, время) и ошибки journalctl -u icubix-worker # фоновые задачи`

- **Журнал действий пользователей** — в базе (таблица `core_auditevent`), просмотр в разделе администрирования. Записи только добавляются: изменение и удаление запрещены триггером СУБД, подмену в обход СУБД выявляет цепочка хешей. Проверка — `icubix manage audit_verify` и автоматически каждую ночь в 02:30; нарушение — запись уровня ERROR в журнале `icubix-worker`.

- **Пользователи, группы и права в журнале действий.** Изменения в разделе администрирования (`/admin/`) и командами `icubix manage createsuperuser` / `changepassword` записываются в журнал с автором, адресом запроса, пользователем или группой и тем, что изменилось (было → стало; для групп и прав — добавлено / убрано). Пароли и их хеши не пишутся — только факт смены. Одно сохранение карточки даёт по записи на каждый вид изменения. Учётки из AD меняет сверка с контроллером — у неё свои записи `core.ldap.*`, здесь они не повторяются.

Запись	Когда	Важность в SIEM
`core.user.create`	Создан пользователь: логин, ФИО, организация, флаги, группы; `via` — `admin` или команда	5; суперпользователь — 9
`core.user.change`	Логин, ФИО, почта, источник входа	4
`core.user.activity`	Флаг «Активный» — блокировка или разблокировка	6
`core.user.rights`	`is_staff`, `is_superuser`, группы, отдельные права; `superuser_granted: true` при выдаче суперпользователя	8; выдача суперпользователя — 9
`core.user.org`	Организация и обслуживаемые организации	6
`core.user.password`	Пароль задан администратором или командой (`usable: false` — вход по паролю отключён)	6
`core.user.delete`	Удалён пользователь: логин, ФИО, организация, флаги, группы на момент удаления	7
`core.group.create`, `.change`, `.delete`	Группа создана (с правами), переименована, удалена (с правами и участниками)	6, 4, 8
`core.group.rights`	Права группы: добавлено, убрано, сколько участников затронуто	8

Изменения напрямую в базе или через `icubix manage shell` в журнал не попадают: доступ к серверу — только у администратора сервера. - **ИИ и документы в журнале действий.** Текст запросов, заявок и документов в журнал не пишется.

Запись	Когда
`ai.request`	Обращение к модели: пользователь, функция, объект, провайдер, обезличено ли и сколько, размер запроса и ответа, длительность, итог `ok` / `blocked` / `error`; для облачного сервиса — `external: true`
`servicedesk.ticket.comment`	Ответ в заявке; отметка, взят ли за основу черновик ИИ
`docs.document.upload`, `.index`, `.download`, `.delete`, `.move`	Загрузка, итог разбора, скачивание, удаление, перенос документа
`docs.search`	Поиск по документам: число найденного, без текста запроса
`docs.space.create`, `.update`, `.delete`	Пространство: название, группы, длина инструкции

8. Сообщения системному программисту

Сообщение	Причина	Действие
Файл лицензии не найден	Нет `/etc/icubix/license.json`	Поместить файл лицензии
Подпись лицензии недействительна	Файл изменён или от другого продукта	Запросить файл заново в поддержке
Срок действия лицензии истёк	Закончился срок	Продлить лицензию
Нет доступа к /etc/icubix/icubix.conf	Команда запущена обычным пользователем	Запускать от root (`sudo icubix …`)
Нет ключа: задайте ICUBIX_SECRET_KEY или создайте /etc/icubix/secret_key	Ключ удалён	Переустановить пакет — ключ создастся заново (сеансы пользователей сбросятся)
`/etc/icubix/icubix.conf, строка N: ожидается ICUBIX_ИМЯ=значение`	Ошибка в файле настроек	Исправить строку N
`icubix-web` не запускается, в журнале `connection refused` / `password authentication failed`	База недоступна или неверный пароль	Проверить PostgreSQL и параметры `ICUBIX_DB_*`
ИИ на этой установке выключен	`ICUBIX_AI` не задан	Включить ИИ (раздел 3.5), если это предусмотрено
ИИ не настроен: укажите ICUBIX_AI_URL и ICUBIX_AI_MODEL	Не задан адрес или модель	Задать параметры, перезапустить службы
Нет связи с сервером модели / Модель не ответила за N с	Сервер модели недоступен или перегружен	Проверить сервер модели и `ICUBIX_AI_URL` ; при долгих ответах увеличить `ICUBIX_AI_TIMEOUT`
Сервер модели отказал в доступе	Неверный ключ API	Проверить файл `ICUBIX_AI_API_KEY_FILE`
Облачный сервис … не разрешён на этой установке	Выбран облачный провайдер без `ICUBIX_AI_CLOUD=1`	Вернуть `ICUBIX_AI_PROVIDER=openai` или явно разрешить облако (не в закрытом контуре)
В файле нет текста — похоже на скан: распознавание сканов на сервере не установлено	Нет tesseract с русским словарём или pdftoppm	Установить пакеты (раздел 3.5), перезапустить `icubix-worker` , загрузить скан заново
Документ долго в состоянии «Разбирается»	Служба `icubix-worker` остановлена	`systemctl status icubix-worker` , запустить службу
Журнал действий нарушен: запись N	Записи журнала изменены в обход системы	Инцидент ИБ: сохранить копию базы, разобрать по журналам СУБД