iCubix Учёт печати: сведения для службы информационной безопасности

Как программа работает в сети заказчика, что хранит и как защищает. Для согласования установки и пилота. Подробности — в руководстве администратора; ответим на вопросы по почте info@arpsys.ru.

1. Что это за программа

- iCubix Учёт печати — веб-приложение для учёта печати на сетевых принтерах и МФУ. Устанавливается на сервер заказчика под Astra Linux SE 1.8, РЕД ОС 8 или Альт p11, использует PostgreSQL 15+ и nginx из репозитория ОС. Правообладатель и разработчик — ООО «ОПТОР».
- Состав: сервер (пакет `icubix`), сборщики показаний на площадках (пакет `printaxis-collector`), агенты на рабочих местах Windows и Linux — только для модуля «Пользователи».
- **Интернет не нужен**: установка, проверка лицензии и обновления выполняются в закрытом контуре. Программа не передаёт данные за пределы сети заказчика и не обращается к сервисам ООО «ОПТОР». Удалённый доступ разработчика к серверам заказчика не требуется.

2. Сетевые взаимодействия

ОТКУДА	КУДА	ПРОТОКОЛ, ПОРТ	ЗАЧЕМ	НУЖНО
Браузер пользователя	Сервер iCubix	HTTPS, TCP 443 (nginx)	Работа в веб-интерфейсе	да
Сборщик на площадке	Сервер iCubix	HTTPS, TCP 443	Передача показаний; токен сборщика	да
Сборщик на площадке	Принтеры и МФУ	SNMP v2c/v3, UDP 161; HTTP/HTTPS, TCP 80/443	Чтение счётчиков и состояния; настройки аппаратов не меняются	да
Агент на ПК или сервере печати	Сервер iCubix	HTTPS, TCP 443	Задания печати по сотрудникам, квоты; токен агента	модуль «Пользователи»
Сервер iCubix	PostgreSQL	TCP 5432, scram-sha-256	База данных; может быть на том же сервере	да
Сервер iCubix	Каталог AD / FreeIPA / ALD Pro	LDAPS, TCP 636, или LDAP + StartTLS, TCP 389	Вход по доменной учётной записи; служебная учётка — только чтение	нет
Сервер iCubix	Почтовый сервер организации	SMTP, порт и шифрование — по настройке	Уведомления о событиях	нет
Сервер iCubix	Внешняя система заказчика	HTTPS, по адресу вебхука	Уведомления о событиях	нет
Сервер iCubix	SIEM	syslog: UDP/TCP 514 или TLS 6514	Выгрузка журнала действий (CEF или JSON)	нет

> Входящие соединения из интернета не нужны. Исходящих соединений в интернет программа не делает. Необязательные каналы, которым нужен интернет (сообщения в MAX, облачные ИИ-сервисы), по умолчанию выключены и в закрытом контуре не используются.

3. Вход и разграничение доступа

- Локальные пароли — не короче 12 символов, с проверкой на распространённые и чисто цифровые; хранятся хешем (PBKDF2-SHA256).
- После 5 неудачных попыток подряд вход по логину закрывается на 15 минут; после 30 неудач с одного адреса — вход с этого адреса. Каждая неудача пишется в журнал.
- Второй фактор — одноразовый код из приложения (TOTP): по желанию, обязательно для администраторов или для всех.
- Вход по доменной учётной записи (AD, FreeIPA, ALD Pro) только по шифрованному каналу, права — по группам каталога; каждые 5 минут вход перепроверяется, отключённая учётка теряет доступ. Возможен вход через Windows (Kerberos).
- Сеанс завершается после 30 минут бездействия (настраивается) и в любом случае через 8 часов после входа.
- Права назначаются группами. На одном сервере может работать несколько организаций: пользователь видит данные только своей.

4. Хранение секретов

- Пароли к аппаратам (SNMP v3), служебной учётке каталога и почтовому серверу хранятся в базе зашифрованными (AES-256-GCM). Ключ — отдельный файл `/etc/icubix/data_key` на сервере, в базе его нет.
- Токены сборщиков, агентов и ключи API показываются один раз; на сервере хранится только их хеш (SHA-256). Каждый токен отзывается отдельно.
- Лицензия — файл с электронной подписью (Ed25519), проверяется на сервере без обращения в интернет. Секретный ключ подписи — только у правообладателя.

5. Журнал действий

- В журнал действий пишутся: входы, неудачные попытки и блокировки, включение и сброс второго фактора, вход через каталог и изменение его настроек; изменения пользователей, групп и прав — создание, блокировка, выдача прав и суперпользователя, смена пароля администратором, удаление (пароли и хеши не пишутся); выпуск и отзыв ключей API и каждая выгрузка через API, резервные копии, обезличивание, изменения мест, профилей аппаратов, импорта и рассылок отчётов.
- Записи только добавляются: изменение и удаление запрещены триггером СУБД, подмену в обход СУБД выявляет цепочка хешей. Целостность проверяется каждую ночь и командой `icubix manage audit_verify`.
- Журнал выгружается в SIEM по syslog (RFC 5424) раз в минуту в формате CEF (MaxPatrol SIEM, KUMA, RuSIEM) или JSON. Изменение прав уходит с уровнем важности 8, выдача прав суперпользователя — 9.

6. Веб-интерфейс и сервер

- Приложение принимает соединения только с той же машины (127.0.0.1:8070); снаружи доступен только nginx с HTTPS, сертификат — заказчика.
- Заголовки: Content-Security-Policy (отдаёт сама программа) без встроенных скриптов и стилей и без сторонних ресурсов, HSTS, X-Frame-Options: DENY, nosniff; cookie сеанса — Secure и HttpOnly, защита от CSRF.

- Службы работают от отдельной учётной записи `icubix` без входа в систему, с ограничениями systemd: файловая система только для чтения (кроме рабочего каталога), без повышения привилегий и доступа к устройствам.
- Сборщики только читают данные аппаратов; настройки принтеров и МФУ программа не меняет.

7. Персональные данные

- Без модуля «Пользователи» программа учитывает аппараты, а не людей. Персональные данные — только учётные записи пользователей системы и, если его заполнить, ответственный за аппарат.
- С модулем «Пользователи» обрабатываются логины и ФИО сотрудников в заданиях печати. Уволенных сотрудников обезличивают — вручную или автоматически через заданный срок; журнал действий не обезличивается, так как он неизменяемый.

8. Поставка и обновления

- Пакеты .deb и .rpm с контрольными суммами SHA-256 и подписью ООО «ОПТОР» по ГОСТ (проверяется средствами КриптоПро CSP), к каждой версии — перечень компонентов (SBOM, CycloneDX).
- Обновление — установка пакета новой версии администратором заказчика. Принудительных и автоматических обновлений нет.
- Исправления безопасности для минорной версии выпускаются 3 года после её выхода.

9. Безопасная разработка и сертификация

- Разработка ведётся по процессу на основе ГОСТ Р 56939-2024: обязательное ревью изменений, статический анализ, проверка зависимостей на уязвимости, поиск секретов в коде, тесты; сборка — на собственном сервере в РФ из зафиксированных версий зависимостей.
- **Сертификата ФСТЭК России у программы нет.** Сертификация запланирована после включения в реестр российского ПО. Программа — прикладная, не средство защиты информации. Если сертификат требуется в вашей закупке или для вашей ИС, сообщите нам до закупки.
- Реестр российского ПО: заявка готовится.

ООО «ОПТОР», правообладатель iCubix Учёт печати. Сведения относятся к версии программы 1.6.0. Актуальная версия документа — arpsys.ru/docs/icubix-uchet-pechati-ib.pdf