Криптографический сервис НРД

Москва 2023

Оглавление

1. Введение

Криптографический сервис НРД (далее Крипто - сервис) – это приложение которое используется для обеспечения работы средств криптографии на веб-узлах:

- создание и проверка электронной подписи.
- зашифровка/расшифровка файлов.

Крипто-сервис работает с браузером Google Chrome и настройками по умолчанию. Обеспечивает единый контроль доступа (при работе с плагинами набор доступных прав зависит от настроек конкретного браузера).
Для получения доступа необходимо скачать Крипто - сервис (опытная эксплуатация) с сайта НРД на странице Программное обеспечение.
При возникновении вопросов всегда можно обратиться в техническую поддержку по телефону +7 495 956-09-34 или по электронной почте soed@nsd.ru. Полный перечень контактов можно найти на сайте НРД на странице Контакты НРД.

2. Технические требования

В таблице представлены технические требования для работы Крипто - сервиса.

Компонент	Требование
Операционные системы	Astra Linux Special Edition (очередное обновление 1.7)
Совместимые браузеры	Google Chrome

Технические требования для работы Крипто - сервиса

Также необходимо установить:

- справочник сертификатов;
- криптопровайдер.

Выбор ПО определяется типом криптографии операционной системы.

2.1 Типы криптографии

Для операционной системы AstraLinux необходимо установить:

- ПК «"Валидата Клиент L"
- Сертификаты ключей (НРД, пользовательские тестовые, боевые)

Используемые порты

Крипто-сервис запускается на 48737 порту. Он не должен быть закрыт в системе.

- Крипто-сервис на одном из портов в диапазоне с 47000 до 48700 (может быть запущено несколько, по одному от каждого пользователя машины);
- коммутатор на 48737 порту, определяет на каком порту запущен экземпляр Крипто - сервиса пользователя и обеспечивает маршрутизацию запросов от браузера к Крипто – сервису.

Настройки прокси сервера

Дополнительные настройки прокси - сервера не требуются. Но если вы используете прокси - сервер и у вас возникают проблемы с работой КС, то необходимо в настройках прокси проверить, что переключатель Bypass proxy server for local addresses (Пропускать запросы к локальным адресам) установлен.

3. Установка

Установка для Linux:

- Для установки на Astra Linux необходимо скачать дистрибутив с сайта НРД.
- Выполнить команду из директории со скаченным пакетом
  sudo dbkg -i crypto-service_83.0-24_amd64.deb

Добавление корневого сертификата в Браузер

Идем в настройки браузера – Конфиденциальность и безопасность – Безопасность и выбираем настроить сертификаты (выбрать «Центры сертификации»).

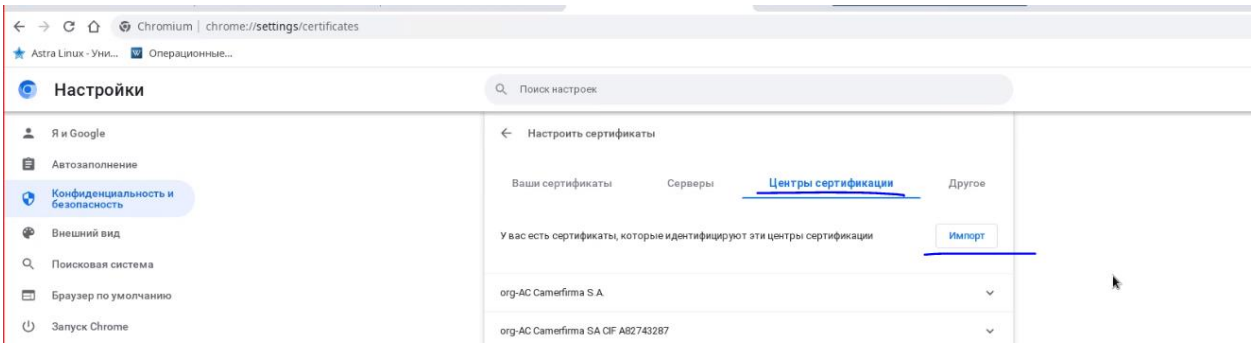

Рисунок 1 – настройки браузера

Добавить корневой сертификат NSD_local_services.cer

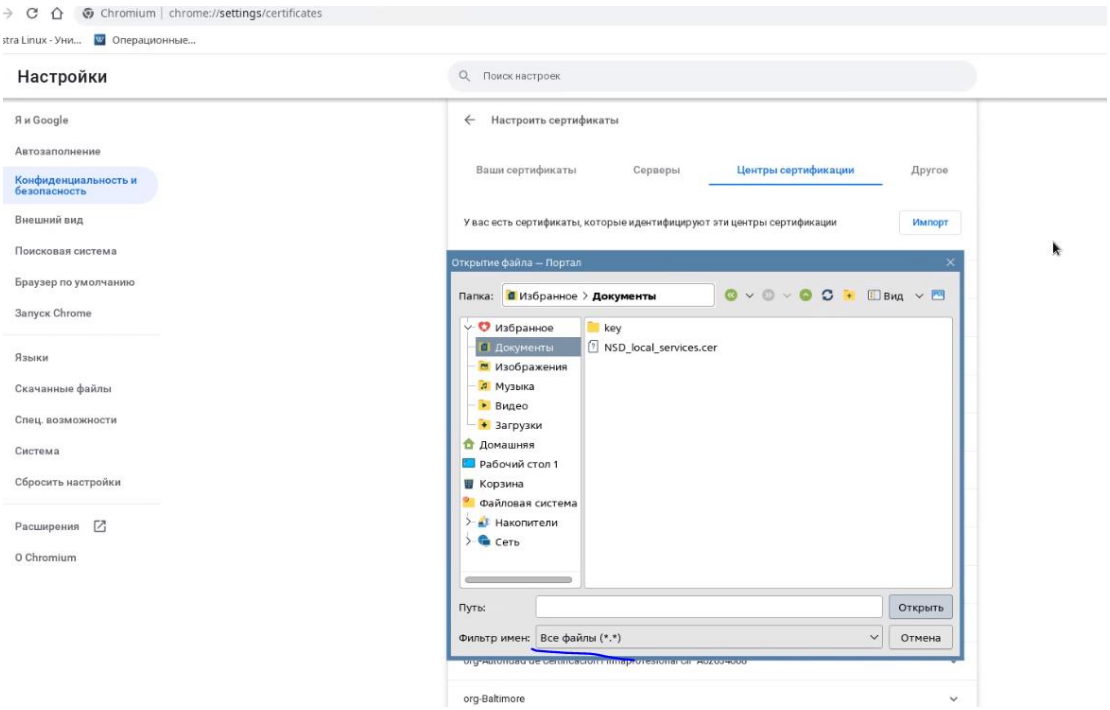

Рисунок 2 – выбор сертификата

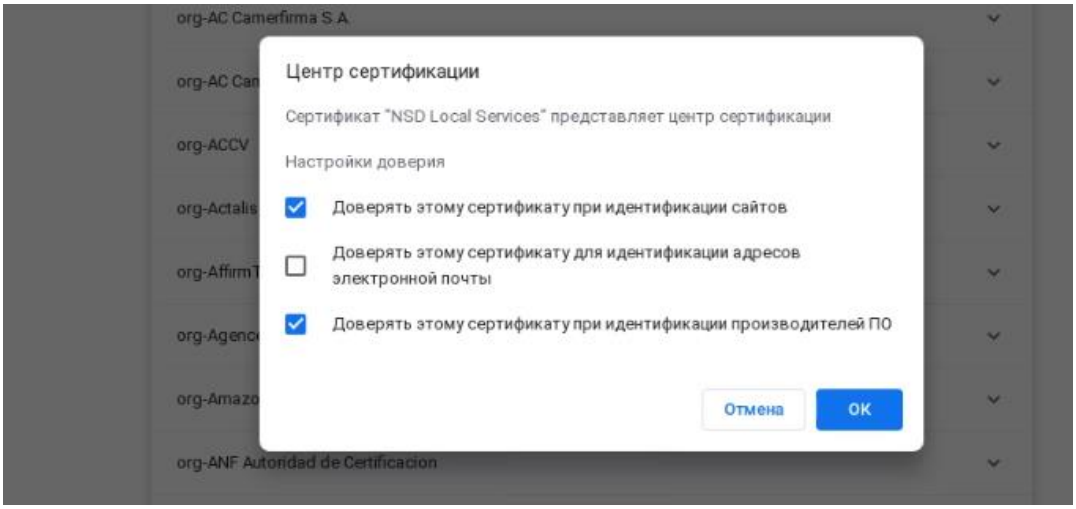

Рисунок 3 – настройка доверия к сертификату

4. Запуск и остановка Крипто - сервиса

Для запуска Крипто - сервиса следует нажать кнопку «Запустить».

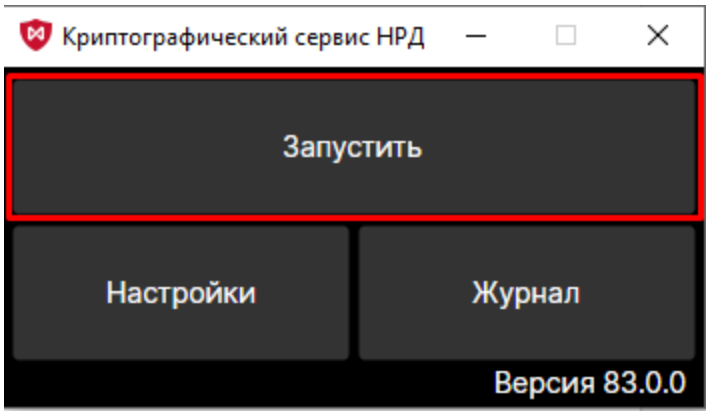

Рисунок 4 – запуск

Для остановки работы Крипто - сервиса следует нажать кнопку «Остановить».

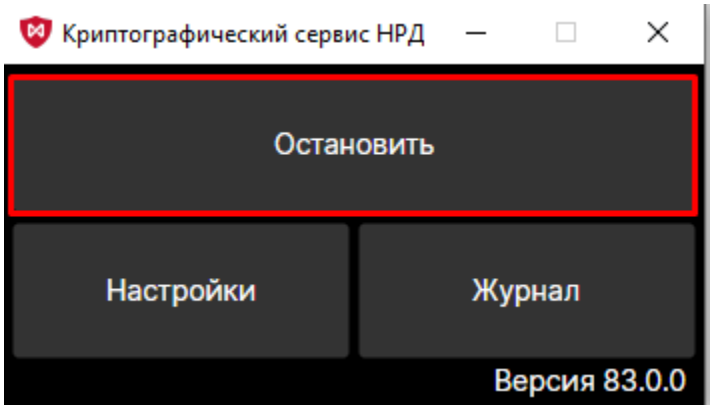

Рисунок 5 – остановка работы

Для выхода из приложения следует нажать кнопку ✕ .

5. Работа Крипто-сервиса

Для выполнения криптографических операций (подпись, зашифровка документов) JavaScript в браузере по HTTP(S) - протоколу обращается к Крипто - сервису. Если сайт не добавлен в список доверенных узлов (см. раздел Список доверенных сайтов), откроется запрос на разрешение доступа к справочнику сертификатов, ключам.

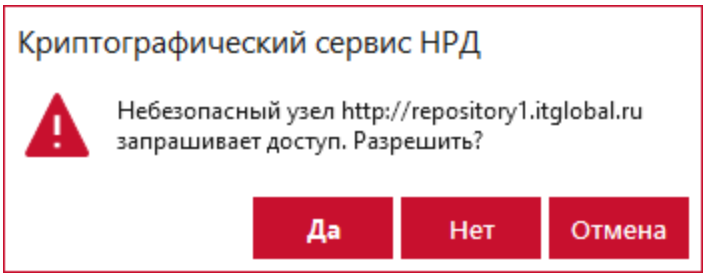

Рисунок 6 – запрос на разрешение доступа к справочнику сертификатов, ключам

Для разрешения доступа следует нажать кнопку «Да». Url будет автоматически добавлен в список «Доверенные узлы». При нажатии кнопки «Нет» url будет добавлен в список «Запрещенные узлы».
Для веб-узлов, добавленных в список доверенных сайтов, запрос доступа не производится. Разрешенным процессам предоставляет доступ к Validata CSP для выполнения криптографических операций.

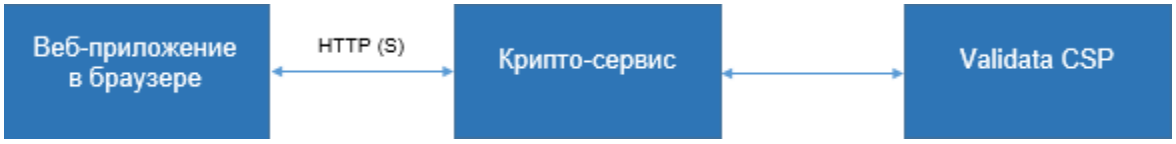

Рисунок 7 – взаимодействие компонентов

6. Настройки

Для перехода к параметрам настройки следует нажать кнопку «Настройки».

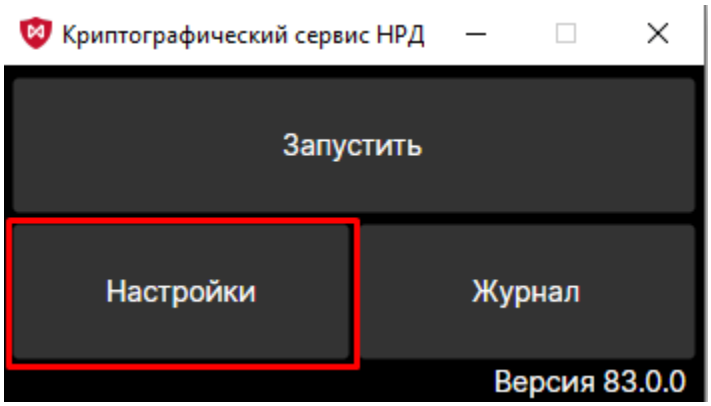

Рисунок 8 – настройки

Автозапуск

По умолчанию для запуска Крипто-сервиса следует:

- нажать дважды на ярлык на рабочем столе;

- в открывшемся окне нажать кнопку «Запустить».

Для того чтобы Крипто - сервис запускался автоматически при в ходе в систему, нужно установить переключатель «Запускать автоматически при старте Windows». Все настройки нужно сохранить, нажав кнопку «ОК».

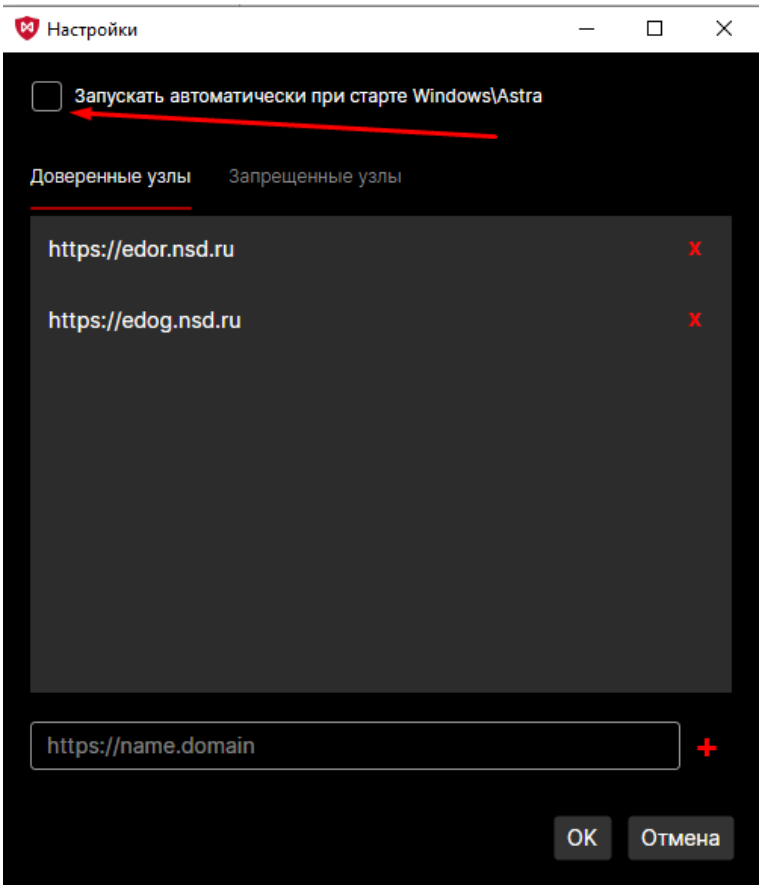

Рисунок 9 – автозапуск

Список доверенных сайтов

В списке «Доверенные узлы» представлены сайты, для которых доступен Крипто - сервис, в списке «Запрещенные узлы», для которых Крипто - сервис недоступен.

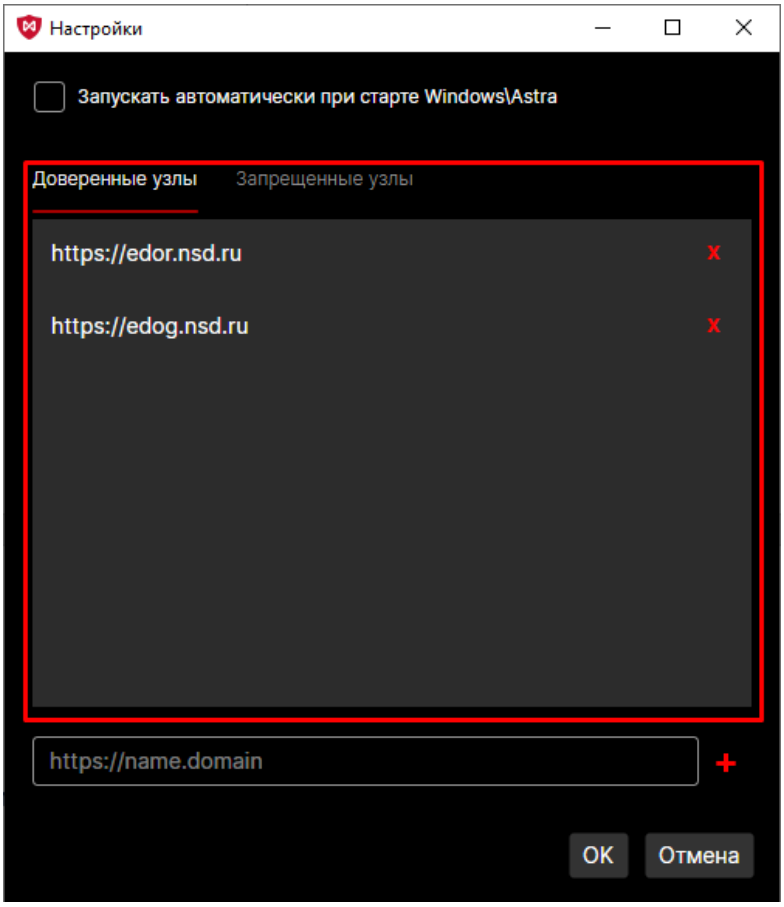

Рисунок 10 – список доверенных и запрещенных узлов

По умолчанию в списке доверенные узлы указан URL Web - кабинета https://edog.nsd.ru (ГОСТ, промышленный контур), https://edor.nsd.ru (RSA, промышленный контур).

Web-кабинет КД:

- URL (тестовый контур): https://gost-gt.nsd.ru/corpactions/ (GUEST)
- URL (промышленный контур): https://cabinet.nsd.ru/corpactions/

Web-кабинет Репозитария:

- URL (тестовый контур):
  - http://r-pl.itglobal.ru/lkr/ (PL)
  - http://r-gs.itglobal.ru/lkr/ (GUEST)
- URL (промышленный контур):
  - ГОСТ и RSA – https://cabinet.nsd.ru/repository/

Списки сайтов можно редактировать. Принцип добавления и удаления сайтов одинаков для списка доверенных и запрещенных узлов. Для добавления адреса необходимо в поле (рис. 17[1]) указать URL, нажать кнопку «Добавить» (рис. 17[2]).

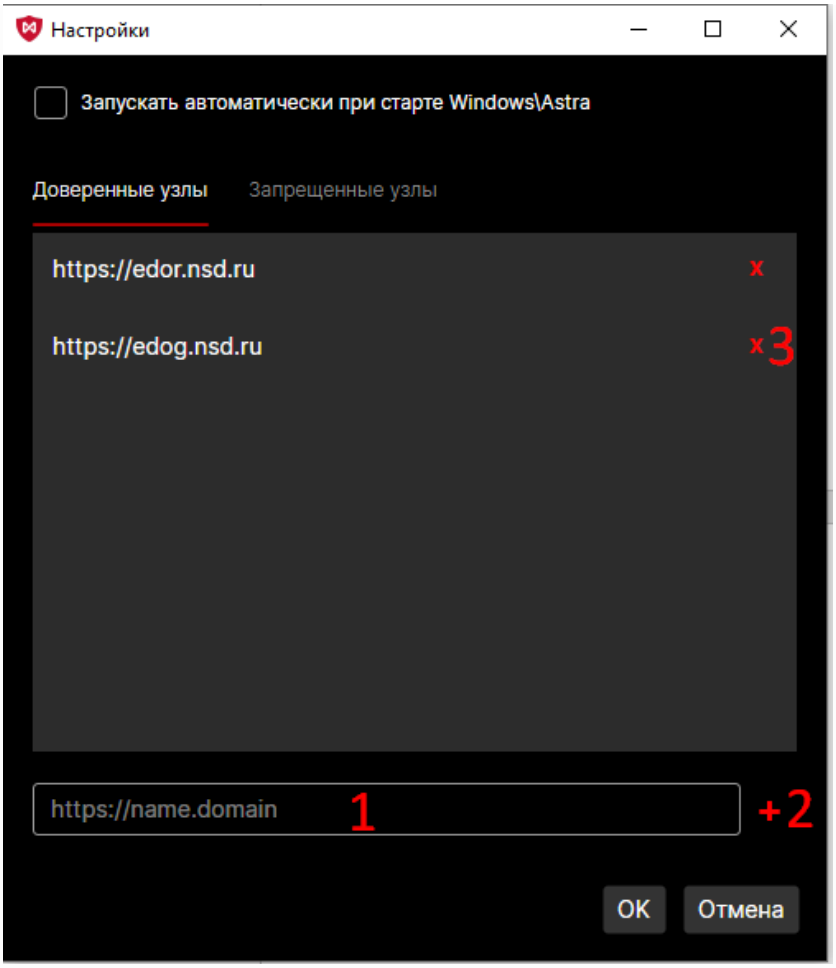

Рисунок 11 – редактирование списка доверенных и запрещенных узлов

В случае ввода некорректного адреса появится сообщение о ошибке.

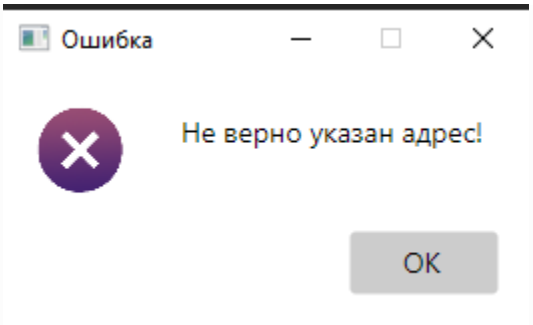

Рисунок 12 – ошибка ввода некорректного адреса

Для удаления сайта из списка следует нажать кнопку «X» (рис. 17[3]).

Все настройки нужно сохранить, нажав кнопку «ОК». Веб - узлы из списка надежных узлов не будут запрашивать подтверждения пользователя при открытии хранилища сертификатов и операциях с закрытым ключом пользователя.

7. Системный журнал (логирование)

В системном журнале хранятся записи о действиях системы.

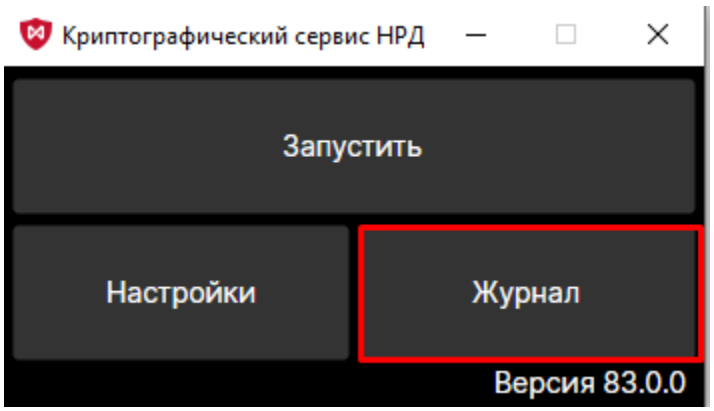

Рисунок 13 – вход в системный журнал

Для скачивания файлов необходимо нажать кнопку «Экспорт журнала». На компьютер будет загружен ZIP - архив с записями журнала событий за последние 3 дня.

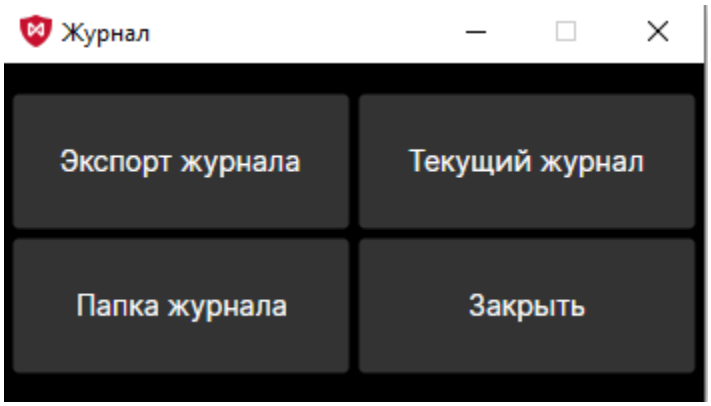

Рисунок 14 – разделы системного журнала

Для открытия текущего журнала необходимо нажать кнопку «Текущий журнал».
Для открытия папки где хранится Системный журнал необходимо нажать кнопку «Папка журнала».
Для закрытия текущего раздела необходимо нажать кнопку «Закрыть».