**ПРОТОКОЛ № 31146/2025**

**проведения совместных испытаний программного обеспечения "Киберстаб" версии 3.0 и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8)**

г. Ярославль 12.11.2025

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения совместных испытаний в период с 20.03.2025 по 26.03.2025 программного обеспечения "Киберстаб" версии 3.0 (далее – ПО), разработанного ООО "Стандарт безопасности", и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8), разработанной ООО "РусБИТех-Астра".

2 Объект испытаний

2.1 Перечень компонентов ПО, эксплуатировавшихся в ходе проведения испытаний, представлен в Таблице 1.

Таблица 1 – Дистрибутив и документация ПО

| **Наименование файла** | **Контрольная сумма (MD5)** | **Ссылка на эксплуатационную документацию** |
|---|---|---|
| cyberstab.zip | aabdabbbe81efceffd6a65b46330b2fe | Сторона разработчика ПО |
| "Руководство пользователя для модулей программного комплекса «Киберстаб» версии 3.0" | – | Ресурс в сети "Интернет", адрес: "https://www.yarsec.ru/kiberstab/about_po.php/" |

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки ПО в среде Astra Linux SE 1.8 в объеме, указанном в Приложении 1.

3.2 Перечень используемых репозиториев приведен в Приложении 2.

3.3 Предоставленный на испытания дистрибутив ПО содержит электронную цифровую подпись для функционирования в среде операционной системы с активным режимом ЗПС.

3.4 Проверка корректности функционирования ПО с уровнем конфиденциальности 1-3 механизма мандатного разграничения доступа не проводилась по причине отсутствия поддержки ПО соответствующей функциональности ОС. Информация об отсутствии упомянутой поддержки была заявлена стороной разработчика ПО.

3.5 С целью проведения проверок при включённом режиме ЗПС использовался файл открытого ключа разработчика ПО.

4 Вывод

4.1 "Киберстаб" версии 3.0 функционирует в среде операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8) уровень защищенности "Усиленный" и признано совместимым, принимая во внимание информацию, содержащуюся в разделе 3.

5 Состав рабочей группы и подписи сторон

5.1 Данный протокол составлен участниками рабочей группы:

Чуфаровская А. А. – начальник отдела автоматизации и разработки ПО, ООО "Стандарт безопасности";

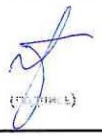
Никешина А. С. – бизнес-аналитик, ООО "Стандарт безопасности";

Тетеев А. А. – инженер по защите информации 2 категории, ООО "Стандарт безопасности".

ООО "Стандарт безопасности"

начальник отдела автоматизации и разработки ПО

(должность)



Чуфаровская А. А.

(подпись)

(фамилия, инициалы)

**Приложение 1 к Протоколу № 31146/2025**

## Перечень проверок совместимости ПО и Astra Linux SE 1.8

Таблица 1.1 - Результаты проверок ПО

| Перечень проверок | Версия ядер | | Статус механизмов безопасности | | |
|---|---|---|---|---|---|
| | 6.1.90-1-generic | 6.6.28-1-generic | ЗПС | МКЦ | МРД |
| Установка ПО | Успешно | Успешно | Активен | Активен | Активен |
| Эксплуатация ПО | Успешно | Успешно | Активен | | |
| Удаление ПО | Успешно | Успешно | Активен | | |
| Эксплуатация ПО. Уровень конфиденциальности 1-3 (опциональная проверка) | Не проводилась | Не проводилась | Активен | | |

**Приложение 2 к Протоколу № 31146/2025**

**Инструкция по установке и удалению ПО**

1. Используемые репозитории в Astra Linux SE 1.8:

   deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.1/main-repository/ 1.8_x86-64 main contrib non-free

2. Установка ПО:

выполнить системные команды, действия:

Установить, инициализировать, добавить в автозапуск и запустить СУБД PostgreSQL (на примере версии 15).

apt-get install postgresql

sudo pdpl-user -i 63 postgres

sudo su postgres

psql -c “ALTER ROLE postgres WITH PASSWORD 'ваш_пароль'”

\q

exit

sudo -i passwd postgres

В файле /etc/parsec/mswitch.conf у параметра zero_if_notfound выставьте значение yes. Данный параметр определяет мандатный атрибут пользователя в базах данных как 0 (минимальный уровень прав доступа), если таковой атрибут не был задан.

В файле /etc/postgresql/[№ версии]/main/pg_hba.conf в строке с комментарием «local is for Unix domain socket connections only» заменить peer на md5:

local all all peer

local all postgres peer

systemctl reload-or-restart postgresql

apt-get install libusb-0.1-4

Скопировать и разархивировать zip-файлы дистрибутива.

Переходим в директорию CyberstabServerLiux/dbupdater/ делаем файл исполняемым:

chmod +x CyberstabDbUpdaterLinux

Переходим в директорию CyberstabServerLiux/serverconsole/ делаем файл исполняемым и запускаем:

chmod +x CyberstabServerConsoleLinux

./CyberstabServerConsoleLinux

После запуска консоли вводим в ней команды:

setlevel "initialize"

setpgpass (потребуется ввести пароль пользователя postgres)

initserver

После успешной инициализации сервера (когда загрузка дойдет до 100%), закройте консоль:

quit

Перейдите в директорию CyberstabServerLiux/server/, сделайте файл сервера исполняемым и запустите из-под учетной записи суперпользователя:

chmod +x CyberstabServerLinux

sudo ./CyberstabServerLinux

Перейти в папку клиента и запустить клиентское приложение:

chmod +x CyberstabClientLinux

./CyberstabClientLinux

Удаление ПО:

выполнить системные команды, действия:

Удалить созданные папки с дистрибутивом.

Удалить СУБД:

sudo apt-get remove postgresql

**Приложение 3 к Протоколу № 31146/2025**

## Перечень используемых сокращений

Astra Linux SE 1.8 - операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8);

РКСЗ - Документ из состава эксплуатационной документации Astra Linux SE 1.8, Руководство по КСЗ. Часть 1;

КСЗ - комплекс средств защиты;

ОС - операционная система;

ЗПС - замкнутая программная среда;

МКЦ - мандатный контроль целостности;

МРД - мандатное управление доступом;

ПО - программное обеспечение "Киберстаб" версии 3.0.