ПРОТОКОЛ № 35033/2026

проведения совместных испытаний программного обеспечения "CyberCodeReview" версии 3.3.2 и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8)

г. Екатеринбург 30.07.2026

1. Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения совместных испытаний 30.07.2026 программного обеспечения "CyberCodeReview" версии 3.3.2 (далее – ПО), разработанного ООО "СМЛ Секьюрити", и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2026-0224SE18 (оперативное обновление 1.8.5) (далее – Astra Linux SE 1.8.5), 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**
registry.cybercodereview.ru/ cybercodereview/security-center/back/securitycenter	5c2a2426dd73de0a70db988aa5b4a3a9e7afc2b9b990129ccce363d7327aabde	https://docs.cybercodereview.ru/
registry.cybercodereview.ru/ cybercodereview/security-center/back/jira_helper	ea58dfaa96d239baffc2cdfa8041fef6766eb6f52fcedf30df158843c461a988	
registry.cybercodereview.ru/ cybercodereview/security-center/back/importer	4b9d79fbd948c8c3104db269e5e2c400ecb9fa6d22954a550f11dcace07a17c8	
registry.cybercodereview.ru/ cybercodereview/security-center/back/db_helper	63da13ddb12a058c6fe46a00eb7391d70f598d793801dad2da448eb95d47f0e8	
registry.cybercodereview.ru/ cybercodereview/security-center/front	0f3b28193f43ffb467aa5233f8c0264597335eb0580d319b35fe59848eeabcc1	
registry.cybercodereview.ru/ cybercodereview/auditor/back/ auditor	7b516fc1b272b21a06c9760b5f57fb07ae0f32eed4895fd514b304033ec7b639	
registry.cybercodereview.ru/	a16b48d8ff9a039b0dba98a5f13202ed26	

cybercodereview/auditor/ worker/docker	1320bb5c5f4b0df25621c9d7925a48	
registry.cybercodereview.ru/ cybercodereview/security-center/back/aiproxy	40c2b8b8e19dfe101a0446e33cd9482e6ef66bab3d3fdf1634428a935a54bb5a	

3. Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки ПО в среде Astra Linux SE 1.8.5 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 Решение о совместимости ПО в настоящем протоколе принято на основании материалов тестирования предоставленных ООО "СМЛ Секьюрити".

3.6 В ходе проведения испытаний обнаружены ошибки в логах контейнеров, не влияющие на корректную работу ПО.

3.7 В ходе проведения испытаний фиксируются попытки запуска исполняемых файлов с использованием механизма создания анонимного файла в памяти memfd. При включённом режиме ЗПС запуск исполняемых файлов с использованием memfd невозможен.

4. Вывод

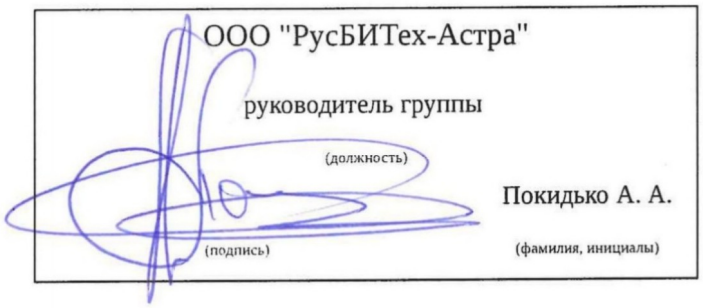
4.1 "CyberCodeReview" версии 3.3.2 функционирует в среде операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8) уровень защищенности "Базовый" и признано совместимым, принимая во внимание информацию, содержащуюся в разделе 3.

5. Состав рабочей группы и подписи сторон

5.1 Данный протокол составлен участниками рабочей группы:

Карабасов А. В. – директор, ООО "СМЛ Секьюрити";

Покидько А. А. – руководитель группы, ООО "РусБИТех-Астра".



Приложение 1 к Протоколу № 35033/2026

Перечень проверок совместимости ПО и Astra Linux SE 1.8.5

Таблица 1.1 - Результаты проверок ПО

Перечень проверок	**Версия ядра**	**Статус механизмов безопасности в процессе выполнения проверки**		
	6.1.158-1-generic	**ЗПС**	**МКЦ**	**МРД**
Установка ПО	Успешно	Активен	Активен	Активен
Эксплуатация ПО	Успешно	Активен		
Удаление ПО	Успешно	Активен		
Эксплуатация ПО. Уровень конфиденциальности 1-3	Неуспешно	Активен		

Приложение 2 к Протоколу № 35033/2026

Инструкция по установке и удалению ПО

1 Используемые репозитории в Astra Linux SE 1.8.5:

- deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.5/main-repository/ 1.8_x86-64 main contrib non-free non-free-firmware

2 Установка ПО:

2.1 Установить контейнеризацию Docker и git с помощью команды apt install docker.io docker-compose-v2 git;

2.2 Перейти в каталог /opt с помощью команды cd /opt

2.3 Загрузить компоненты Auditor из репозитория помощью команды git clone https://gitlab.cybercodereview.ru/cybercodereview/auditor.git;

2.4 Перейти в каталог Auditor с помощью команды cd auditor;

2.5 Создать текстовый файл .env и заполнить согласно образцу по ссылке: https://docs.cybercodereview.ru/docs-gramax/ustanovka/ustanovka-auditor/ustanovka-s-pomoschyu-docker-compose#шаг-3:-задайте-переменные-окружения;

2.6 Запустить компонент Auditor с помощью команды docker compose up -d;

2.7 Загрузить компоненты Security Center из репозитория помощью команды git clone https://gitlab.cybercodereview.ru/cybercodereview/security-center.git;

2.8 Перейти в каталог Security Center с помощью команды cd security-center;

2.9 Переместить файлы с помощью команды mv docker-compose/* ./;

2.10 Настроить переменные окружения запустив скрипт с помощью команды bash ./set_vars.sh;

2.11 Запустить компонент Security Center с помощью команды docker compose up -d;

2.12 Открыть веб-страницу, введя адрес сервера в браузере.

3 Удаление ПО:

3.1 Перейти в директорию Security Center с помощью команды cd /opt/security-center;

3.2 Остановить контейнеры с помощью команды docker compose down -v;

3.3 Перейти в папку на уровень выше с помощью команды cd ..;

3.4 Удалить папку Security Center с помощью команды rm -rf security-center;

3.5 Перейти в папку Auditor с помощью команды cd /opt/auditor;

3.6 Остановить контейнеры с помощью команды docker compose down -v;

3.7 Перейти в папку на уровень выше с помощью команды cd ..;

3.8 Удалить папку Auditor с помощью команды rm -rf auditor.

Приложение 3 к Протоколу № 35033/2026

Перечень используемых сокращений

Astra Linux SE 1.8.5 - операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2026-0224SE18 (оперативное обновление 1.8.5);

РКСЗ - Документ из состава эксплуатационной документации Astra Linux SE 1.8.5, 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 "CyberCodeReview" версии 3.3.2.