

ПРОТОКОЛ № 26495/2024

проведения совместных испытаний программного обеспечения "RT Protect EDR" (сервер) версии 1.21 и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8)

г. Москва

27.11.2024

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 22.11.2024 по 27.11.2024 совместных испытаний программного обеспечения "RT Protect EDR" (сервер) версии 1.21 (далее – ПО), разработанного АО "РТ-Информационная безопасность", и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8) (далее – Astra Linux SE 1.8), разработанной ООО "РусБИТех-Астра".

2 Объект испытаний

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

Таблица 1 – Перечень компонентов, относящихся к ПО

Описание	Наименование	MD5	Источник
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/djangoapp	—	Сторона разработчика ПО
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/iaa-webapi	—	Сторона разработчика ПО
Docker-образ с ПО	<u>docker.rt-protect.ru:5000/main/eas-front</u>	—	Сторона разработчика ПО
Docker-образ с ПО	<u>docker.rt-protect.ru:5000/edr-backend/worker</u>	—	Сторона разработчика ПО
Docker-образ с ПО	<u>docker.rt-protect.ru:5000/edr-backend/webserver</u>	—	Сторона разработчика ПО
Docker-образ с ПО	<u>docker.rt-protect.ru:5000/edr-backend/loadbalancer</u>	—	Сторона разработчика ПО
Docker-образ с ПО	<u>docker.rt-protect.ru:5000/edr-backend/eventq</u>	—	Сторона разработчика ПО

Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/rating-dbmigrator	–	Сторона разработчика ПО
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/rating-webapi	–	Сторона разработчика ПО
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/rating-worker	–	Сторона разработчика ПО
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/elasticsearch	–	Сторона разработчика ПО
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/minio	–	Сторона разработчика ПО
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/cache	–	Сторона разработчика ПО
Официальное руководство по эксплуатации ПО в электронном формате	Руководство администратора	–	Сторона разработчика ПО

3 Ход испытаний

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

3.2 Перечень используемых репозиторий приведен в Приложении 2.

3.3 По информации от разработчика ПО не поддерживает работу с активным режимом ЗПС. Испытания проводились при отключенном режиме ЗПС.

3.4 Проверка корректности функционирования ПО в условиях ненулевого уровня конфиденциальности механизма мандатного разграничения доступа (далее – МРД) указанных сред не проводилась по причине отсутствия поддержки ПО соответствующей функциональности ОС. Информация об отсутствии упомянутой поддержки была заявлена стороной разработчика ПО.

4 Результаты испытаний

4.1 ПО корректно функционирует в среде Astra Linux SE 1.8.

5 Вывод

5.1 ПО и операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8) совместимы, принимая во внимание информацию, содержащуюся в разделах 3, 4 и Приложении 2.

6 Состав рабочей группы и подписи сторон

6.1 Данный протокол составлен участниками рабочей группы:

Жуков А. К. – Руководитель Департамента сервисов и продуктов АО "РТ-Информационная безопасность";

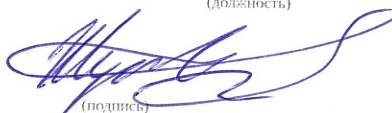
Сафонов К. А. – Инженер Центра мониторинга и реагирования на компьютерные инциденты АО "РТ-Информационная безопасность";

Валеева З.У. – Ведущий специалист Центра мониторинга и реагирования на компьютерные инциденты АО "РТ-Информационная безопасность".

АО "РТ-Информационная безопасность"

Руководитель Департамента сервисов и продуктов

(должность)



(подпись)

Жуков А. К.

(фамилия, инициалы)

Перечень проверок совместимости ПО и Astra Linux SE 1.8

№ п/п	Наименование проверки	Результат проверки ПО и Astra Linux SE	
		1.8 с ядром ОС	
		6.1.90-1-generic	6.6.28-1-generic
1.	Установка ПО	Успешно	Успешно
2.	Эксплуатация ПО	Успешно	Успешно
3.	Удаление ПО	Успешно	Успешно
4.	Требования безопасности ALSE	Успешно	Успешно
5.	Механизм безопасности ЗПС	Неуспешно	Неуспешно
6.	Механизм безопасности МКЦ	Неуспешно	Неуспешно
7.	Механизм безопасности МРД	Неуспешно	Неуспешно
8.	Механизм безопасности rootless (только для контейнерных приложений docker)	Неуспешно	Неуспешно

Инструкция по установке и удалению ПО в среде Astra Linux SE 1.8**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 non-free-firmware

2 Установка ПО:**2.1 выполнить системные команды:**

- `sudo apt update`
`sudo apt install ansible sshpass openssh-server ssh-keygen -t rsa -b 4096 ssh-copy-id user@ip ansible-playbook edr-install --extra-vars "@config/default/config.yml" -i ip, -u username --ask-become-pass`

3 Удаление ПО:**3.1 выполнить системные команды:**

- `docker container stop $(docker ps -a -q)`
`docker container prune`

Перечень используемых сокращений

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

ЗПС – замкнутая программная среда;

МКЦ – мандатный контроль целостности;

МРД – мандатное управление доступом;

ОС – операционная система;

Docker – программное обеспечение для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации;

Docker-образ – неизменяемый образ по шаблону которого создается docker-контейнер;

Docker-контейнер – контейнер, созданный на основе docker-образа;

ПО – программное обеспечение "RT Protect EDR" (сервер) версии 1.21.