

ПРОТОКОЛ № 27096/2025

проведения совместных испытаний программного обеспечения "KOMRAD Enterprise SIEM" версии 4.5 и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7)

г. Москва

28.01.2025

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 23.01.2025 по 28.01.2025 совместных испытаний программного обеспечения "KOMRAD Enterprise SIEM" версии 4.5 (далее – ПО), разработанного АО "НПО "Эшелон", и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2024-0830SE17 (оперативное обновление 1.7.6) (далее – Astra Linux SE 1.7.6), 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
Файл программного пакета дистрибутива ПО	komrad_v4.5.21_astra_1.7_a amd64.run	4854261a77ab08d5 fa84a540f80ae6966 45b2e4b848d94843 09e6959e33eedb3	Ресурс в сети "Интернет", адрес: "https://nexus.etecs.ru/repository/komrad/packaging/komrad/v4.5.21/astra_1.7/amd64/installers/komrad_v4.5.21_astra_1.7_amd64.run"
Официальное руководство по эксплуатации ПО в электронном формате	"Электронная документация для "KOMRAD Enterprise SIEM 4.3.58"	—	Ресурс в сети "Интернет", адрес: "https://docs.etecs.ru/komrad/docs/intro"

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности функционирования ПО в среде Astra Linux SE 1.7.6 в объеме, указанном в Приложении 1.

3.2 Перечень используемых репозиторий приведен в Приложении 2.

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

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.

3.5 При установке и эксплуатации ПО в рамках сценария не выполняются условия п. 17.2.4.4 "Руководство по КСЗ Ч. 1". Значения параметров защищенного сервера СУБД `enable_bitmapscan` и `ac_ignore_socket_maclabel` не соответствуют эксплуатационной документации.

4 Результаты испытаний

4.1 ПО корректно функционирует в среде Astra Linux SE 1.7.6.

5 Вывод

5.1 ПО и операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) 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:

Галданов Александр Александрович – Руководитель отдела тестирования, АО "НПО "Эшелон";

Яровая Полина Петровна – Специалист отдела тестирования, АО "НПО "Эшелон".

АО "НПО "Эшелон"	
Руководитель отдела тестирования	
	(подпись)
	(должность)
	Галданов А. А.
	(фамилия, инициалы)

Инструкция по установке и удалению ПО в среде Astra Linux SE 1.7.6

1 Используемые репозитории:

в Astra Linux SE 1.7.6:

- deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-base/ 1.7_x86-64
main contrib non-free
- deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-update/ 1.7_x86-64
main contrib non-free

2 Установка ПО:

2.1 выполнить системные команды:

```
chmod +x ./komrad_v4.5.21_astra_1.7_amd64.run sudo  
./komrad_v4.5.21_astra_1.7_amd64.run
```

3 Удаление ПО:

3.1 выполнить системные команды:

```
sudo su systemctl stop komrad-bus pauth-server komrad-server.service komrad-  
server.socket komrad-processor komrad-scanner komrad-reactor komrad-  
correlation-dispatcher komrad-incident-manager komrad-syslog-collector komrad-  
file-collector komrad-snmp-collector komrad-sql-collector komrad-xflow-collector  
komrad-http-collector komrad-ebpf-collector grafana komrad-backup komrad-waf-  
proxy clickhouse-server dpkg -P komrad-cli komrad-bus pauth-server komrad-  
server komrad-server komrad-processor komrad-scanner komrad-reactor komrad-  
correlation-dispatcher komrad-incident-manager komrad-syslog-collector komrad-  
file-collector komrad-snmp-collector komrad-sql-collector komrad-xflow-collector  
komrad-http-collector komrad-ebpf-collector grafana komrad-backup komrad-waf-  
proxy nmap clickhouse-client clickhouse-server clickhouse-common-static sudo -i -u  
postgres dropdb "komrad-preferences" sudo -i -u postgres dropdb "pauth-  
preferences" sudo -i -u postgres dropdb "scanner" sudo -i -u postgres dropdb  
"komrad-grafana" apt autoremove postgres* rm -rf /var/lib/echelon \ /etc/echelon \  
/etc/clickhouse-server/ \ /var/lib/clickhouse/ \ /etc/security/limits.d/clickhouse.conf \  
/var/lib/dpkg/info/komrad-* \ /usr/bin/komrad-* \ /usr/bin/pauth-* \ /var/log/echelon \  
/opt/echelon \ /usr/share/doc/komrad-* \ /usr/share/doc/nmap \ /usr/share/bash-  
completion/completions/nmap \ /usr/share/lintian/overrides/komrad-* \  
/usr/share/nmap \ /usr/lib/systemd/system/komrad-* \  
/sys/fs/cgroup/**/system.slice/komrad-** \ /sys/fs/cgroup/**/system.slice/pauth-** \
```

```
/etc/systemd/system/multi-user.target.wants/komrad-* \ /etc/systemd/system/multi-  
user.target.wants/pauth-* \ /etc/default/komrad-* \ /etc/default/pauth-* \  
/lib/systemd/system/komrad-* \ /lib/systemd/system/pauth-* systemctl daemon-  
reload userdel komrad-reactor userdel grafana userdel komrad groupdel komrad
```

Перечень используемых сокращений

Astra Linux SE 1.7.6 – операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2024-0830SE17 (оперативное обновление 1.7.6);

ЗПС – замкнутая программная среда;

МКЦ – мандатный контроль целостности;

МРД – мандатное управление доступом;

ОС – операционная система;

"Руководство по КСЗ. Ч. 1" – документ РУСБ.10015-01 97 01-1 "Операционная система специального назначения "Astra Linux Special Edition". Руководство по КСЗ. Часть 1";

ПО – программное обеспечение "KOMRAD Enterprise SIEM" версии 4.5.