ПРОТОКОЛ № 22390/2024

проведения совместных испытаний программного обеспечения «Security Capsule SIEM (Коррелятор и Сборщик)» версии 3.3 и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7)

г. Москва 28.04.2024

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 05.04.2024 по 28.04.2024 совместных испытаний программного обеспечения «Security Capsule SIEM (Коррелятор и Сборщик)» версии 3.3 (далее – ПО), разработанного ООО «ИТБ», и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) (далее – Astra Linux SE 1.7.0), включая Astra Linux SE 1.7.0 с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-1023SE17 (оперативное обновление 1.7.5) (далее – Astra Linux SE 1.7.5), 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	securitycapsulesiemcollector_2.0.0-4astraSE_amd64.deb	0c84b3f4ddbea2663cee3be9e829a32c	Сторона разработчика ПО
Файл программного пакета дистрибутива ПО	securitycapsulesiemcorrelator_2.0.2-4astraSE_amd64.deb	5602c02d6fe0296a6e4bdd51048dffdb	
Файл архива, содержащий дополнительное ПО	mongodb-4.2.24.tar	a33f022c4bd5bf97c350ea5d027ed616	
Официальное руководство по эксплуатации ПО	«SC_SIEM-PA_19_09_2023.docx»	–	

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности функционирования ПО в средах: Astra Linux SE 1.7.0, Astra Linux SE 1.7.5 в объеме, указанном в Приложении 1.

3.2 Перечень используемых репозиториев приведен в Приложении 2.

3.3 Неофициальные репозитории ПО для указанных сред не эксплуатировались.

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

3.5 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.

3.6 Недопустимо использовать ПО в условиях мандатного разграничения доступа по причине несоответствия указаний п.17.2.4.4 «Руководство по КСЗ Ч. 1».

3.7 ПО затрагивает требования по условиям функционирования п.17.3.2.1 «Руководство по КСЗ Ч. 1». Данные требования соблюдаются.

3.8 Проверка функционирования ПО в условиях низкого уровня целостности механизма МКЦ не проводилась.

4 Результаты испытаний

4.1 ПО корректно функционирует в средах: Astra Linux SE 1.7.0, Astra Linux SE 1.7.5.

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:

Жорин А. А. – главный специалист по внедрению ООО «ИТБ».

ООО «ИТБ»

главный специалист по внедрению

(должность)

(подпись)

Жорин А. А.

(фамилия, инициалы)

Приложение 1 к Протоколу № 22390/2024

Перечень проверок совместимости ПО и Astra Linux SE 1.7.0, Astra Linux SE 1.7.5

№ п/п	Наименование проверки	Результат проверки ПО и Astra Linux SE									
		1.7.0 с ядром ОС		1.7.5 с ядром ОС							
		5.4.0-54-generic	5.4.0-54-hardened	5.4.0-162-generic	5.4.0-162-hardened	5.10.190-1-generic	5.10.190-1-hardened	5.15.0-83-generic	5.15.0-83-hardened	5.15.0-83-lowlatency	6.1.50-1-generic
1.	Установка ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
2.	Запуск, остановка выполнения ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
3.	Эксплуатация минимальной базовой функциональности ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
4.	Функционирование ПО в условиях низкого уровня целостности механизма МКЦ ОС	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась
5.	Функционирование ПО в условиях ненулевого уровня конфиденциальности механизма МРД ОС	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась
6.	Отсутствие нарушений требований подраздела 17.3 «Руководство по КСЗ Ч. 1»	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
7.	Соответствие объектов ФС ОС дистрибутиву ОС при эксплуатации ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
8.	Удаление ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
9.	Функционирование ПО в условиях включённого механизма ЗПС ОС	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
10.	Отсутствие нарушений требований подраздела 17.2 «Руководство по КСЗ Ч. 1»	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно

Приложение 2 к Протоколу № 22390/2024

Инструкция по установке и удалению ПО в средах: Astra Linux SE 1.7.0, Astra Linux SE 1.7.5

1 Используемые репозитории:

в Astra Linux SE 1.7.0:

- deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.0/repository-base/1.7_x86-64 main contrib non-free

в Astra Linux SE 1.7.5:

- deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-base/1.7_x86-64 main contrib non-free

2 Установка ПО:

2.1 выполнить системные команды, действия:

Выполнить установку СУБД PostrgeSQL и действия по настройке согласно руководству администратора:

```
sudo apt install postgresql
```

Выполнить установку СУБД MongoDB и действия по настройке согласно руководству администратора:

```
sudo apt install ./mongod-org-*.deb
```

Выполнить установку пакетов коррелятора и сборщика событий:

```
sudo apt install ./securitycapsulesiemco*.deb
```

3 Удаление ПО:

3.1 выполнить системные команды, действия:

```
sudo apt purge -y mongodb-org-server mongodb-org-shell mongodb-org-tools securitycapsulesiemcollector securitycapsulesiemcorrelator
```

Приложение 3 к Протоколу № 22390/2024

Перечень используемых сокращений

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

Astra Linux SE 1.7.0 – операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7);

Astra Linux SE 1.7.5 – операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-1023SE17 (оперативное обновление 1.7.5);

ЗПС – замкнутая программная среда;

КСЗ – комплекс средств защиты;

МКЦ – мандатный контроль целостности;

МРД – мандатное управление доступом;

ОС – операционная система;

ПО – программное обеспечение «Security Capsule SIEM (Коррелятор и Сборщик)» версии 3.3.