

ПРОТОКОЛ № 11633/2023

проведения совместных испытаний программного обеспечения «Positive Technologies Extended Detection and Response» версии 4.0 и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7)

г. Москва

16.04.2023

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 10.04.2023 по 16.04.2023 совместных испытаний программного обеспечения «Positive Technologies Extended Detection and Response» версии 4.0 (далее – ПО), разработанного АО «Позитив Текнолоджиз», и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) (далее – Astra Linux SE 1.7.0), разработанной ООО «РусБИТех-Астра», включая Astra Linux SE 1.7.0 с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2022-1110SE17 (оперативное обновление 1.7.3) (далее – Astra Linux SE 1.7.3).

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 архива дистрибутива ПО	edr-installer.v3.2.0.666.tar.gz	377e662ccdafb4ac083e353bd5ecbf02	Сторона разработчика ПО
Файл архива дистрибутива ПО	edr-installer.v4.0.0.972.tar.gz	e312fc6a6c1ca29d9177f47d0726a384	Сторона разработчика ПО
Файл программного пакета дополнительных модулей ПО	vxagent-1.9.1.747_amd64.deb	e4167df7f66ea5845fbb947864cd201e	Сторона разработчика ПО
Официальное руководство по эксплуатации ПО в электронном формате	«Руководство администратора «Positive Technologies Extended Detection and Response» версии 3.1»	–	Сторона разработчика ПО



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 1.7.3, – в объеме, указанном в Приложении 1.

3.2 Перечень официальных репозиторий ПО, эксплуатировавшихся в упомянутых средах:

- в среде Astra Linux SE 1.7.0: base;
- в среде Astra Linux SE 1.7.3: base, update.

3.3 Неофициальные репозитории ПО для указанных сред не эксплуатировались.

3.4 С целью проведения указанных проверок при включённом режиме замкнутой программной среды (далее – ЗПС) упомянутых ОС, в ходе внедрения соответствующей электронной подписи (ЭП) в файлы ПО формата ELF, использовался комплект цифровых ключей программы Ready for Astra Linux ООО «РусБИТех-Астра».

3.5 Проверка корректности функционирования ПО в условиях активного механизма ЗПС указанных сред завершена с результатом «Неуспешно» в связи с тем, что агентское ПО после внедрения ЭП не подключается к серверу ПО, о чём свидетельствует соответствующий статус агента «Отключен», отображаемый в консоли управления ПО. Сервис агента ПО подсистемы инициализации «systemd» при этом функционирует корректно и не фиксирует каких-либо ошибок в системном журнале.

3.6 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.

3.7 Установка ПО в Astra Linux SE 1.7.0 завершена с результатом «Неуспешно» в связи с отсутствием в репозиториях Astra Linux SE 1.7.0 требуемой версии системы управления контейнерами «Docker Compose». В руководстве администратора на ПО, указанном в таблице 1, требуются версии 1.28 или 1.29.

4 Результаты испытаний

4.1 ПО корректно функционирует в среде Astra Linux SE 1.7.3.



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:

Карпенко Д. И. – руководитель сектора отдела тестирования на совместимость департамента развития технологического сотрудничества ДВиС ООО «РусБИТех-Астра»;

Показаньев Р. С. – инженер отдела тестирования на совместимость департамента развития технологического сотрудничества ДВиС ООО «РусБИТех-Астра».

ООО «РусБИТех-Астра»	
руководитель сектора отдела тестирования на совместимость департамента развития технологического сотрудничества ДВиС	
(должность)	
(подпись)	Карпенко Д. И. (фамилия, инициалы)



Перечень проверок совместимости ПО и Astra Linux SE 1.7.3

№ п/п	Наименование проверки	Результат проверки ПО и Astra Linux SE						
		1.7.3 с ядром ОС						
		5.4.0-110- generic	5.4.0-110- hardened	5.10.142-1- generic	5.10.142-1- hardened	5.15.0-33- generic	5.15.0-33- hardened	5.15.0-33- lowlatency
1.	Установка ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
2.	Запуск, остановка выполнения ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
3.	Эксплуатация минимальной базовой функциональности ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
4.	Функционирование ПО в условиях низкого уровня целостности механизма МКЦ ОС	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
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
6.	Отсутствие нарушений требований подраздела 17.3 «Руководство по КСЗ Ч. 1»	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
7.	Соответствие объектов ФС ОС дистрибутиву ОС при эксплуатации ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
8.	Удаление ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
9.	Функционирование ПО в условиях включённого механизма ЗПС ОС	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно
10.	Отсутствие нарушений требований подраздела 17.2 «Руководство по КСЗ Ч. 1»	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно



Инструкция по установке и удалению ПО в средах: Astra Linux SE 1.7.0, Astra Linux SE 1.7.3

1 Установка ПО:

1.1 Для установки серверной части выполнить системные команды, действия:

```
sudo -s
```

```
apt install docker.io docker-compose python3-pip
```

```
pip3 install ansible==2.9.22
```

```
mkdir edr-installer
```

```
tar xvf edr-installer.v3.2.0.666.tar.gz -C edr-installer/
```

```
cd edr-installer/
```

```
./edr_installer
```

```
tar xvf edr-installer.v4.0.0.972.tar.gz -C edr-installer-update/
```

```
cd edr-installer-update/
```

```
./edr_installer
```

1.2 Для установки агентской части выполнить системные команды, действия:

```
sudo -s
```

```
sudo VXSERVER_CONNECT=wss://<Адрес сервера агентов>:8443 dpkg -i  
./vxagent-1.9.1.747_amd64.deb
```

2 Удаление ПО:

2.1 Для удаления серверной части выполнить системные команды, действия:

```
sudo -s
```

```
apt purge -y docker.io
```

```
rm -fr /var/lib/docker/
```

```
rm -rf edr-installer edr-installer-update
```

```
rm edr-installer.v3.2.0.666.tar.gz edr-installer.v4.0.0.972.tar.gz
```

```
./edr-purge
```

2.2 Для удаления агентской части выполнить системные команды, действия:

```
sudo -s
```

```
apt purge -y vxagent
```



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 1.7.3 – операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2022-1110SE17 (оперативное обновление 1.7.3);

ДВиС – дивизион внедрения и сопровождения;

ЗПС – замкнутая программная среда;

КСЗ – комплекс средств защиты;

МКЦ – мандатный контроль целостности;


МРД – мандатное управление доступом;

ОС – операционная система;

ПО – программное обеспечение «Positive Technologies Extended Detection and Response» версии 4.0.

Идентификатор документа 9411dbf7-8e1e-4eb7-b63b-092f4ccb41c5

Документ подписан и передан через оператора ЭДО АО «ПФ «СКБ Контур»

Подписи отправителя:	Владелец сертификата: организация, сотрудник	Сертификат: серийный номер, период действия	Дата и время подписания
 ООО "РУСБИТЕХ-АСТРА" Карпенко Дмитрий Иванович, Руководитель сектора испытаний на совместимость с ПО		032EBA8C00EDAEDBA94363C6D0FD57B5 76 с 10.08.2022 11:22 по 10.08.2023 11:22 GMT+03:00	03.05.2023 09:26 GMT+03:00 Подпись соответствует файлу документа