

ПРОТОКОЛ № 16167/2024

проведения совместных испытаний программного обеспечения «Яхонт-мини» версии 0.0.1 и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ №20220829SE16 (оперативное обновление 11)

г. Москва

19.01.2024

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 11.01.2024 по 19.01.2024 совместных испытаний программного обеспечения «Яхонт-мини» версии 0.0.1 (далее – ПО), разработанного ЗАО "НОРСИ-ТРАНС", и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ №20220829SE16 (оперативное обновление 11) (далее – Astra Linux SE 1.6.11), 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	jahont_0.0.1-1_all.deb	493770468bcf2a438dff 2a40d0614db6	Сторона разработчика ПО
Подписанный исполняемый файл	archive-backup	86b95aada83f20095cad bdc68f173c28	Сторона разработчика ПО
Подписанный исполняемый файл	backend.cgi	a3aba727f92491cbc2 a22048781b62	Сторона разработчика ПО

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности функционирования ПО в средах: Astra Linux SE 1.6.11, – в объеме, указанном в Приложении 1.

3.2 Перечень официальных репозиторий ПО, эксплуатировавшихся в упомянутых средах:

- в среде Astra Linux SE 1.6.11: main, 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, использовался соответствующий файл открытого ключа, предоставленный стороной разработчика ПО.

3.5 Проверка корректности функционирования ПО в условиях ненулевого уровня конфиденциальности механизма мандатного разграничения доступа (далее – МРД) указанных сред проводилась согласно соответствующему сценарию, предоставленному стороной разработчика ПО.

3.6 Проверки в среде операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6) (Astra Linux SE 1.6.0) не проводились.

3.7 При проверке целостности выявлено нарушение у следующих файлов: /lib/systemd/system/krb5-admin-server.service, /lib/systemd/system/krb5-kdc.service связанное с инициализацией ALD, а также нарушение целостности файлов LibreOffice: /usr/share/maven-repo/org/libreoffice/juh/debian/juh-debian.pom, /usr/share/maven-repo/org/libreoffice/jurt/debian/jurt-debian.pom, /usr/share/maven-repo/org/libreoffice/ridl/debian/ridl-debian.pom, /usr/share/maven-repo/org/libreoffice/unoloader/debian/unoloader-debian.pom, данные нарушения не являются критичными.

3.8 Проверка в соответствии с подп. 17.3.2.3 документа "Операционная система специального назначения "Astra Linux Special Edition". Руководство по КСЗ. Часть 1" РУСБ.10015-01 97 01-1 выявила наличие у пользователя "oper" привилегии "PARSEC_CAP_SMMAC", это обосновано тем, что доменные пользователи, состоящие в системной группе role_oper и не являющиеся администраторами БД, должны обладать возможностью изменять уровень конфиденциальности записей в postgres. В связи с этим при создании пользователей данной группы, они наделяются привилегией PARSEC_CAP_SMMAC.

3.9 Проверка системного каталога /boot выявила изменения, вызванные модификацией /etc/default/grub, а именно, добавлением опции parsec.ccnr_relax=1. Использование данной опции обосновано тем, что пользователи любого уровня конфиденциальности, состоящие в системной группе role_admin, должны иметь возможность

посредством ПО создать файл бэкапа БД в специальную папку /var/backups. Этой папке присваивается флаг cspg и 3-й уровень конфиденциальности.

4 Результаты испытаний

4.1 ПО корректно функционирует в средах: Astra Linux SE 1.6.11.


5 Вывод

5.1 ПО и операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6) 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:

Пироженко М. В. – инженер-программист отдела разработки №1 ЗАО «НОРСИ-ТРАНС»

ЗАО «НОРСИ-ТРАНС»	
инженер-программист отдела разработки №1	
	(должность)
(подпись)	Пироженко М. В.
	(фамилия, инициалы)

Инструкция по установке и удалению ПО в средах: Astra Linux SE 1.6.0, Astra Linux SE 1.6.11

1 Установка ПО:

1.1 выполнить системные команды, действия:

Перед установкой ПО были установлены следующие пакеты: python3-pkg-resources, fly-admin-ald-server, ald-server-common, smolensk-security-ald, postgresql, apache2, libapache2-mod-auth-kerb. Также был изменен hostname, файл /etc/hosts, отключена служба NetworkManager и настроен сетевой интерфейс для службы networking.

Установка ПО: `sudo dpkg -i jahont_0.0.1-1_all.deb`

ПО представляет из себя python3 пакет, содержащий скрипт для настройки сервера ALD и веб-сервера apache2, а также файлы фронтенда и скомпилированные файлы бекенда на Go. После установки создается python3-скрипт /usr/bin/jahont для вызова ПО в одном из пяти режимов:

1. deploy — конфигурирование РМ;
2. user-add — добавление доменного пользователя;
3. user-rm — удаление доменного пользователя;
4. db-drop — удаление БД;
5. uninstall — удаление ПО.

Вызываем команду `sudo jahont deploy`

2 Удаление ПО:

2.1 выполнить системную команду:

`sudo jahont uninstall`

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 1.6.11 – операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ №20220829SE16 (оперативное обновление 11);

ДВиС – дирекция 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 «Яхонт-мини» версии 0.0.1.