

ПРОТОКОЛ № 31127/2025

проведения совместных испытаний программного обеспечения "СекВарио Платформа" версии 1.0 и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8)

г. Ярославль

01.10.2025

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения совместных испытаний в период с 10.09.2025 по 24.09.2025 программного обеспечения "СекВарио Платформа" версии 1.0 (далее – ПО), разработанного ООО "НПФ ДНК-ТЕХНОЛОГИЯ", и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2025-0811SE18 (оперативное обновление 1.8.3) (далее – Astra Linux SE 1.8.3), разработанной ООО "РусБИТех-Астра".

2 Объект испытаний

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

Таблица 1 – Дистрибутив и документация ПО

Наименование файла	Контрольная сумма (SHA256)	Ссылка на эксплуатационную документацию
seqvario_platform.tar	13b23f07dd5490d77371c35339bf6f9e398b3a5c5c43ff86eda48c56a020088b	https://dna-tech.dev/platform
ngs-manager.tar	0f8a2cd3caeb10369597f974fa76c977ca122465788be842e2ee281874ed0ff1	https://dna-tech.dev/manager
hpjm.tar	0021d5df7610c26860d755894c74ff06a18b40c720c351942be02570766ff989	https://nextcloud.dna-tech.dev/s/wZ7SDKxWgwM5sWy

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки ПО в среде Astra Linux SE 1.8.3 в объеме, указанном в Приложении 1.

3.2 Перечень используемых репозиторий приведен в Приложении 2.

3.3 Для функционирования ПО в среде операционной системы с активным режимом ЗПС требуется внедрение электронной цифровой подписи.

3.4 Проверка корректности функционирования ПО с уровнем конфиденциальности 1-3 механизма мандатного разграничения доступа не проводилась по причине отсутствия поддержки ПО соответствующей функциональности ОС. Информация об отсутствии упомянутой поддержки была заявлена стороной разработчика ПО.

4 Вывод

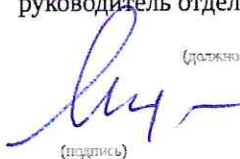
4.1 "СекВарио Платформа" версии 1.0 функционирует в среде операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8) уровень защищенности "Базовый" и признано совместимым, принимая во внимание информацию, содержащуюся в разделе 3.

5 Состав рабочей группы и подписи сторон

5.1 Данный протокол составлен участниками рабочей группы:

Широков Ю. В. – руководитель отдела разработки программного обеспечения, ООО «НПФ ДНК-ТЕХНОЛОГИЯ»;

Яковлев П. Д. – младший системный инженер, ООО «НПФ ДНК-ТЕХНОЛОГИЯ».

ООО «НПФ ДНК-ТЕХНОЛОГИЯ»	
руководитель отдела разработки ПО	
 (подпись)	(должность)
	Широков Ю. В. (фамилия, инициалы)

Перечень проверок совместимости ПО и Astra Linux SE 1.8.3

Таблица 1.1 - Результаты проверок ПО

Перечень проверок	Версия ядра		Статус механизмов безопасности в процессе выполнения проверки		
	6.1.141-1-generic	6.12.34-1-generic	ЗПС	МКЦ	МРД
Установка ПО	Успешно	Успешно	Неактивен	Активен	Неактивен
Эксплуатация ПО	Успешно	Успешно	Неактивен		
Удаление ПО	Успешно	Успешно	Неактивен		
Эксплуатация ПО. Уровень конфиденциальности 1-3	Не проводилась	Не проводилась	Неактивен		

Инструкция по установке и удалению ПО

1. Используемые репозитории в Astra Linux SE 1.8.3:

deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.3/main-repository/ 1.8_x86-64 main
contrib non-free non-free-firmware

2. Установка ПО:

2.1. ПО работает с системой оркестрации Kubernetes. Для тестирования использовалась версия – K3s.

2.1.1. Установка кластера K3s происходит одной bash командой:

```
curl -sL https://get.k3s.io | K3S_KUBECONFIG_MODE="644"  
INSTALL_K3S_VERSION="v1.29.15+k3s1" sh -s -
```

2.1.2. Для начала работы с кластером, необходимо внести переменную окружения следующей командой:

```
export KUBECONFIG=/etc/rancher/k3s/k3s.yaml
```

Для того, чтобы не вносить переменную при каждом запуске машины, рекомендуется внести строку с данной командой в файл .bashrc в домашней директории пользователя.

2.2. Установка Rancher.

Программное обеспечение для управления кластерами Kubernetes, которое упрощает развертывание, настройку и мониторинг. Данный шаг носит рекомендательный характер.

2.2.1. Установка платформы Rancher.

Установить Helm:

```
curl https://raw.githubusercontent.com/helm/helm/main/scripts/get-helm-3 | bash
```

2.2.2. Добавить необходимые репозитории:

```
helm repo add rancher-stable https://releases.rancher.com/server-charts/stable  
helm repo add jetstack https://charts.jetstack.io  
helm repo update
```

2.2.3. Установить CRDs и cert-manager:

```
kubectl create namespace cert-manager  
kubectl apply -f  
https://github.com/cert-manager/cert-manager/releases/download/v1.18.2/cert-  
manager.crds.yaml  
helm install cert-manager --namespace cert-manager --version v1.18.2  
jetstack/cert-manager
```

2.2.4. Установка Rancher:

```
helm install rancher rancher-stable/rancher --namespace cattle-system --create-namespace --set hostname=rancher.cluster --set bootstrapPassword=admin
```

2.2.5. Внести ссылку на Rancher в /etc/hosts для удобства

2.2.6. 127.0.0.1 rancher.cluster #домен должен совпадать с предоставленным выше, пункт 2.2.4 в переменной hostname.

2.3. Для установки ПО потребуется наличие нужных деплойментов и образов в локальном реестре docker.

2.3.1. Установить сервис HPJM, которое создаёт задачи для работы ПО с Kubernetes кластером:

```
kubectl apply -f local-registry.yaml
kubectl apply -f hpjm-pv.yaml
kubectl apply -f hpjm-pvc.yaml
kubectl apply -f hpjm-deployment.yaml
kubectl apply -f hpjm-service.yaml
kubectl apply -f hpjm-ingress.yaml
```

2.3.2. Установить ПО СекВарио Платформа и СекВарио Менеджер:

```
kubectl apply -f seqvario-pv.yaml
kubectl apply -f seqvario-pvc.yaml
kubectl apply -f manager-db-deployment.yaml
kubectl apply -f seqvario-db-deployment.yaml
kubectl apply -f seqvario-db-service.yaml
kubectl apply -f manager-db-service.yaml
kubectl apply -f manager-deployment.yaml
kubectl apply -f seqvario-deployment.yaml
kubectl apply -f seqvario-service.yaml
kubectl apply -f seqvario-ingress.yaml
kubectl apply -f manager-service.yaml
kubectl apply -f manager-ingress.yaml
kubectl apply -f role.yaml
kubectl apply -f rolebinding.yaml
```

2.3.3. При отсутствии нужных PriorityClasses, добавить следующие:

lowest: 1001

low: 1002

medium: 1003

high: 1004

highest: 1005

Пример создания:

apiVersion: scheduling.k8s.io/v1

description: high

kind: PriorityClass

metadata:

name: high

preemptionPolicy: Never

value: 1004

2.4. Установить на worker-ноду метку type=computation. На ней будут создаваться задачи для вычисления образцов.

3. Удаление ПО:

3.1. При условии, что кластер был запущен только для данного ПО и больше не нужен, достаточно удалить K3s, что понесёт удаление всех созданных ресурсов. Вызвать следующий скрипт:

```
k3s-uninstall.sh
```

3.2. Удалить helm. Для этого выполнить команды:

```
sudo rm /usr/local/bin/helm
```

```
sudo rm -rf ~/.cache/helm/
```

```
sudo rm -rf ~/.config/helm/
```

Перечень используемых сокращений

Astra Linux SE 1.8.3 - операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2025-0811SE18 (оперативное обновление 1.8.3);

РКСЗ - Документ из состава эксплуатационной документации Astra Linux SE 1.8.3, Руководство по КСЗ. Часть 1;

КСЗ - комплекс средств защиты;

ОС - операционная система;

ЗПС - замкнутая программная среда;

МКЦ - мандатный контроль целостности;

МРД - мандатное управление доступом;

ПО - программное обеспечение "СекВарио Платформа" версии 1.0.