



**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«ПЛАТФОРМА УПРАВЛЕНИЯ ВНЕШНЕЙ
ПОВЕРХНОСТЬЮ АТАКИ CYBERDEF EASM»**

Руководство по установке и проверке

Санкт-Петербург, 2026

АННОТАЦИЯ

Настоящая инструкция содержит указания по установке и проверке функционирования программного обеспечения «Платформа управления внешней поверхностью атаки CyberDef EASM» (далее CyberDef EASM, программа) в варианте развёртывания в информационной инфраструктуре заказчика.

Программа предназначена для автоматизированного обнаружения, инвентаризации и анализа защищённости информационных активов организации, доступных из сети Интернет, а также для выявления уязвимостей и управления процессом их устранения. Программа распространяется в виде интернет-сервиса (облачного решения), доступного через сеть Интернет, а также в виде программного обеспечения для установки и эксплуатации в информационной инфраструктуре заказчика.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ.....	4
1.1. Наименование программы	4
1.2. Назначение и область применения программы	4
1.3. Основные функции программы	4
1.4. Требования к составу и параметрам технических средств	5
1.5. Требования к установленному общесистемному программному обеспечению и версиям браузеров.....	5
1.6. Требования к квалификации персонала.....	6
2. УСТАНОВКА ПРОГРАММЫ.....	6
2.1. Шаги установки.....	6
1) Копирование и распаковка дистрибутива	6
2) Установка родman и зависимостей	7
3) Запуск скрипта установки.....	8
4) Завершение установки.....	9

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование программы

1.1.1. Полное наименование программы: программное обеспечение «Платформа управления внешней поверхностью атаки CyberDef EASM».

1.1.2. Сокращённое наименование программы: «CyberDef EASM».

1.2. Назначение и область применения программы

1.2.1. Программа «Платформа управления внешней поверхностью атаки CyberDef EASM» предназначена для использования в варианте развёртывания в информационной инфраструктуре заказчика.

1.2.2. Программа обеспечивает автоматизированное обнаружение и инвентаризацию информационных активов организации, доступных из сети Интернет, анализ их защищённости, выявление уязвимостей и управление процессом их устранения.

1.3. Основные функции программы

1.3.1. Функциональные возможности программы:

- аудит активов;
- обнаружение связанных активов;
- определение перечня сервисов на активах;
- выявление уязвимостей;
- отображение результатов сканирования уязвимостей на интерактивном дашборде;
- интеграция с отечественными и зарубежными базами уязвимостей;
- формирование инцидента в системе управления инцидентами;
- передача информации о выявленных уязвимостях в системы управления событиями безопасности заказчика;

- формирование отчётов;
- конструктор отчётов;
- проверка на использование простых паролей;
- гибкое управление режимом сканирования из личного кабинета.

1.4. Требования к составу и параметрам технических средств

1.4.1. Рекомендуемые технические требования к серверу, на который устанавливается программа, указаны в таблице №1.

Таблица №1 Рекомендуемые конфигурации хоста

Класс	CPU / ОЗУ / диск	Потоков (≈)	Для чего
Минимум	4 vCPU / 8 ГБ / 60 ГБ	2–4	демо/малый периметр, без CVE-базы на этом хосте
Рекомендуемо	8 vCPU / 16 ГБ / 120 ГБ	8–12	периметр + CVE-база на том же узле
Крупный	16+ vCPU / 32 ГБ / 250 ГБ	20–30	большой периметр, быстрые прогоны

1.4.2. Требования к пропускной способности сети, для корректной работы программы достаточно широкого LAN-канала (1 Гбит/с).

1.4.3. Операционная система сервера: Astra Linux 1.8. Для установки требуются права администратора (root).

1.5. Требования к установленному общесистемному программному обеспечению и версиям браузеров

1.5.1. На сервере должны быть установлены пакеты `podman` и `podman-compose` (порядок установки приведён в разделе 2 настоящей инструкции).

1.5.2. Для доступа к веб-интерфейсам тенанта и администратора на пользовательской платформе должен быть установлен один из следующих браузеров:

- Яндекс.Браузер версии 20.3.0.1223 и выше;
- Chrome версии 101 и выше;

- Mozilla Firefox версии 115 ESR и выше;
- Safari версии 16.0 и выше Mozilla.

1.6. Требования к квалификации персонала

1.6.1. Установку и настройку программы должен выполнять администратор Linux.

2. УСТАНОВКА ПРОГРАММЫ

Установка проводится на операционной системе Astra Linux 1.8. Для установки потребуются права администратора.

2.1. Шаги установки

1) Копирование и распаковка дистрибутива

Для установки используется учетная запись root.

Активируем её:

```
sudo passwd root
```

После назначения пароля войдем в систему под этой учетной записью.

Выставим значение umask:

```
umask 022
```

Создадим отдельную директорию в opt каталоге:

```
mkdir /opt/vulnscan
```

Скопируем в директорию архив vulnscan-offline-bundle.tar с дистрибутивом любым доступным способом.

Переходим в директорию с дистрибутивом:

```
cd /opt/vulnscan
```

Распакуем дистрибутив:

```
tar -xvf vulnscan-offline-bundle.tar
```

```
root@astra:/opt/vulnscan# tar -xvf vulnscan-offline-bundle-f356bbbf6b44baeb51be5215cc9ccd1892282b5a.tar
./
./podman/
./podman/scale-component.sh
./podman/rollback-image.sh
./podman/update-component.sh
./podman/images.list.sh
./podman/postgres-init/
./podman/postgres-init/01-roles.sh
./podman/install-component.sh
./podman/load-images.sh
./podman/.env.example
./podman/README.md
./podman/build-and-publish-incluster.sh
./podman/install-offline.sh
./podman/prepare-offline-bundle.sh
./podman/bundle-component.sh
./podman/publish-bundle.sh
./podman/worker/
./podman/worker/compose.yaml
./podman/worker/.env.example
./podman/worker/README.md
./podman/secrets.sh
./podman/bundle-images.sh
./podman/cve-snapshot-cronjob.yaml
./podman/sync-cve-db.sh
./podman/cvegggregator/
```

Рисунок 1 – Результат распаковки дистрибутива vulnscan-offline-bundle.tar

2) Установка podman и зависимостей

Проверим в редакторе nano source-лист, необходимо подключение базового репозитория Astra Linux:

```
nano /etc/apt/sources.list
```

Если репозиторий установлен в локальной сети организации, необходимо использовать строку подключения к нему. Если нет, то адрес базового репозитория Astra Linux 1.8 имеет вид:

```
https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-main/ 1.8_x86-64 main non-free non-free-firmware
```

строка должна быть раскомментирована (без символа # в начале строки).

```
GNU nano 7.2 /etc/apt/sources.list
#deb cdrom:[OS Astra Linux 1.8.6.39 1.8_x86-64 DVD ]/ 1.8_x86-64 contrib main non-free non-free-firmware
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-main/ 1.8_x86-64 main contrib non-free non-free-firmwa
#deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-extended/ 1.8_x86-64 main contrib non-free non-free-f
```

Рисунок 2 – Редактирование файла /etc/apt/sources.list в редакторе nano

Остальные строки могут быть закомментированы. Сохраним изменения в файле. Обновим список репозиторийев командой:

```
apt update
```

```
root@astra:/opt/vulnscan# apt update
Сущ:1 https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-main 1.8_x86-64 InRelease
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Все пакеты имеют последние версии.
```

Рисунок 3 – Результат выполнения команды apt update

Проведем установку podman и podman-compose:

```
apt install podman podman-compose
```

```
root@astra:/opt/vulnscan# apt install podman podman-compose
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Предлагаемые пакеты:
  containers-storage docker-compose
Следующие НОВЫЕ пакеты будут установлены:
  podman podman-compose
Обновлено 0 пакетов, установлено 2 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.
Необходимо скачать 26,2 MB архивов.
После данной операции объём занятого дискового пространства возрастёт на 93,2 MB.
Пол:1 https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-main 1.8_x86-64/main amd64 podman amd64 5.7.0.astra1+
ci32 [26,2 MB]
26% [1 podman 8 356 kB/26,2 MB 32%] 209 kB/s 1мин 25с
```

Рисунок 4 – Установка пакетов podman и podman-compose

После установки пакетов приступаем к установке самого дистрибутива.

3) Запуск скрипта установки

Запустим скрипт установки.

Переходим в директорию /opt/vulnscan:

```
cd /opt/vulnscan
```

Запускаем скрипт установки:

```
./podman/install-offline.sh
```

Ожидаем выполнения автоматизированной установки и настройки ПО.

```

root@astra:/opt/vulnscan# ./podman/install-offline.sh

► Проверка окружения и артефакта
  ✓ артефакт: /opt/vulnscan

► Сверка контрольных сумм
^C
root@astra:/opt/vulnscan# cd ..
root@astra:/opt# cd vulnscan/
root@astra:/opt/vulnscan# ./opt/vulnscan/
-bash: ./opt/vulnscan/: Нет такого файла или каталога
root@astra:/opt/vulnscan# ./podman/install-offline.sh

► Проверка окружения и артефакта
  ✓ артефакт: /opt/vulnscan

► Сверка контрольных сумм
vulnscan-images.tar: ЦЕЛ
cvegggregator-api.tar: ЦЕЛ
db.dump: ЦЕЛ
  ✓ суммы совпали

► Настройка .env под образы бандла
  ✓ .env: IMAGE_PREFIX=vulnscan-staging.registry.twcstorage.ru/ IMAGE_TAG=f356bbbf6b44baeb51be5215cc9ccd1892282b5a (из MANIFEST)

► Загрузка образов + модульная установка стека
Loading images from /opt/vulnscan/vulnscan-images.tar ...
Getting image source signatures
Copying blob a34284fcec52 skipped: already exists
Copying blob 256f393e029f skipped: already exists

```

Рисунок 5 — Начало выполнения скрипта install-offline.sh: проверка окружения, контрольных сумм и загрузка образов

4) Завершение установки

После завершения установки на экране отобразятся адреса веб-интерфейсов тенанта и администратора.

```

ожидание восстановления CVE-базы..... - готово
  ✓ CVE-база восстановлена
  проверка cvegggregator-api — ok
  ✓ cvegggregator-api работает

► Установка завершена
Веб-интерфейс тенанта: http://localhost:8080
Веб-интерфейс админа: http://localhost:8081
Логин администратора: admin (пароль — в /opt/vulnscan/podman/.env, ключ BOOTSTRAP_ADMIN_PASSWORD)

Проверка статуса: podman ps
Логи data-service: podman logs -f data-service
root@astra:/opt/vulnscan/podman# █

```

Рисунок 6 — Завершение установки: адреса веб-интерфейсов тенанта и администратора

Для доступа используем логин admin. Пароль можно прочесть в файле /opt/vulnscan/podman/.env

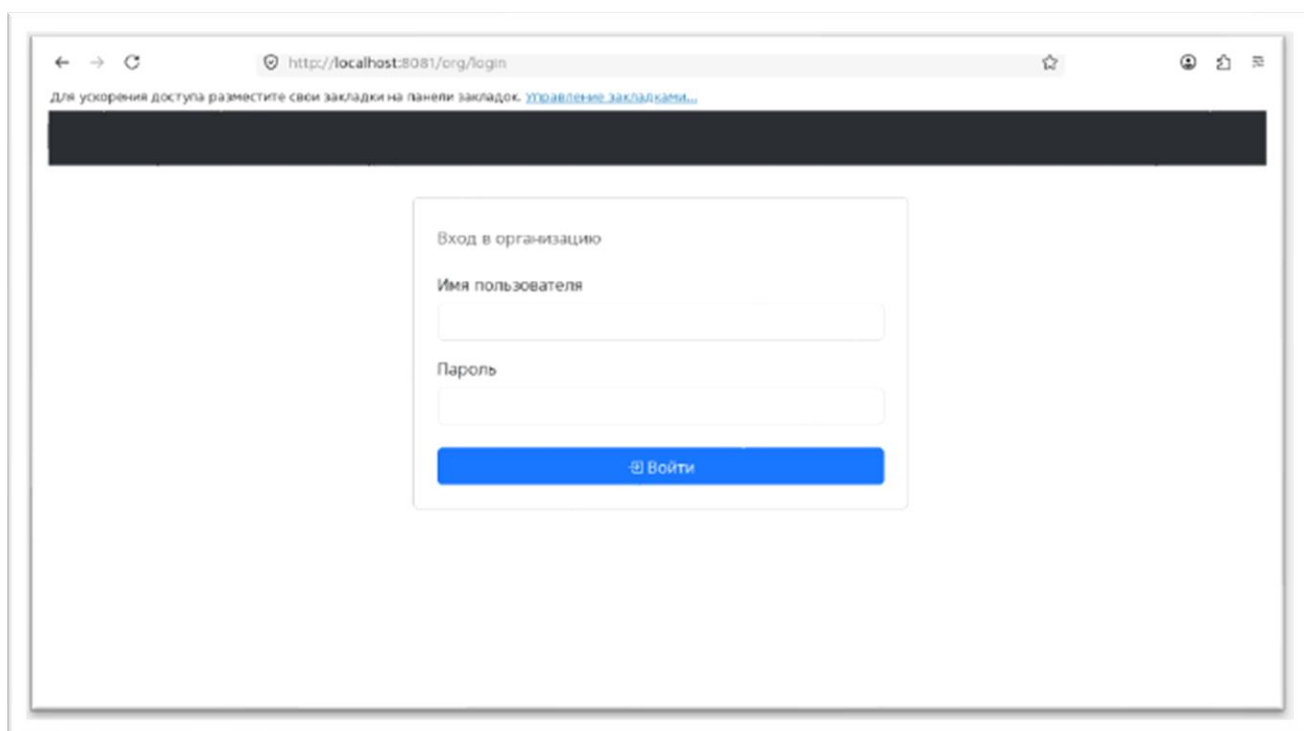


Рисунок 7 — Страница входа веб-интерфейса программы

Установка завершена.