



CyberDef EASM

Платформа управления
внешней поверхностью атаки
(локальна версия)

РУКОВОДСТВО АДМИНИСТРАТОРА

Версия 1.0

2026

Содержание

Содержание	2
1. Об этом документе	4
1.1. Термины и определения	4
2. О продукте CyberDef EASM	5
2.1. Назначение и область применения	5
2.2. Основные функции	5
2.3. Принцип работы модуля сканирования	6
2.4. Принцип работы модуля агрегации данных об уязвимостях	6
2.5. Ограничения текущей версии	7
3. Аппаратные и программные требования	8
3.1. Аппаратные требования	8
3.2. Программные требования	8
3.3. Требования к сетевой инфраструктуре	9
3.3.1. Сетевые транспорты	9
3.3.2. Сетевое взаимодействие с объектом сканирования	9
4. Подготовка к установке	10
5. Установка CyberDef EASM	12
5.1. Установка Podman и зависимостей	12
5.2. Запуск скрипта установки дистрибутива	13
5.3. Завершение установки	14
6. Первоначальная настройка	15
6.1. Создание учётной записи администратора	15
6.2. Настройка доступа по доменному имени	16
7. Аутентификация пользователей	17
7.1. Политика двухфакторной аутентификации	17
7.2. Требования для использования аппаратных ключей	18
7.3. Хранение данных и их защита	18
7.4. Восстановление доступа	18
7.5. Диагностика ошибок входа	19
7.6. Вход по электронной цифровой подписи (Рутокен ЭЦП, JaCarta PKI)	19

8. Журнал действий	21
8.1. Состав фиксируемых событий	21
8.2. Персонификация записей	21
8.3. Неизменяемость и изоляция данных журнала	21
8.4. Доступ к журналу	22
8.5. Срок хранения записей	22
8.6. Выгрузка журнала	22
9. Отчётность, шаблоны и наборы данных	23
9.1. Что доступно пользователю без администратора	23
9.2. Редактирование шаблона отчёта	23
9.2.1. Открытие шаблона отчёта	24
9.2.2. Клонирование шаблона.....	24
9.2.3. Возможности конструктора отчётов	24
9.2.4. Оформление	25
9.2.5. Заблокированные параметры.....	26
9.2.6. Блоки содержимого	26
9.2.7. Источники данных для блоков	27
9.2.8. Предварительный просмотр отчёта.....	27
9.2.9. Сохранение отчёта	28
9.3. Наборы данных на SQL.....	28
9.4. Диагностика.....	29

1. Об этом документе

Настоящее руководство предназначено для администратора, выполняющего установку, первоначальную настройку и эксплуатацию программного обеспечения «Платформа управления внешней поверхностью атаки CyberDef EASM» в информационной инфраструктуре заказчика.

1.1. Термины и определения

Термин	Определение
CyberDef EASM	Платформа управления внешней поверхностью атаки.
VulnScan	Модуль сканирования в составе CyberDef EASM.
CVEgggregator	Модуль агрегации данных об уязвимостях в составе CyberDef EASM.
Актив	Объект сканирования — IP-адрес или доменное имя.
root	Учётная запись с правами администратора операционной системы.
Podman	Средство контейнеризации, на котором развёртываются компоненты платформы.
БДУ ФСТЭК	Банк данных угроз безопасности информации ФСТЭК России.
Второй фактор	Дополнительное подтверждение личности при входе помимо пароля - одноразовый код или аппаратный ключ.
FIDO2	Стандарт входа по аппаратному ключу. По нему работают РутOKEN MFA и JaCarta WebPass.
ЭЦП	Электронная подпись на ГОСТ-сертификате.
Журнал действий	Неизменяемый перечень действий пользователей с указанием, кто и что сделал.

2. О продукте CyberDef EASM

2.1. Назначение и область применения

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.

Полное наименование программы: «Платформа управления внешней поверхностью атаки CyberDef EASM». Сокращённое наименование программы: «CyberDef EASM».

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.

В состав CyberDef EASM входят два модуля:

VulnScan — модуль сканирования, выполняющий сценарии обнаружения активов и уязвимостей.

CVEgggregator — модуль агрегации данных об уязвимостях из NIST NVD, БДУ ФСТЭК и НКЦКИ. На этапе сопоставления обнаруженного ПО с базой уязвимостей VulnScan обращается к API CVEgggregator.

2.2. Основные функции

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;
- строгая аутентификация: одноразовые коды и аппаратные ключи FIDO2 (включая Рутокен MFA и JaCarta WebPass) с выбором допустимых способов для каждой организации;
- журнал действий пользователей: неизменяемая фиксация с указанием исполнителя и выгрузкой для проверяющего.

2.3. Принцип работы модуля сканирования

VulnScan — модуль сканирования, обеспечивающий построение карты внешней поверхности атаки от единой точки входа доменного имени. Обнаружение выполняется последовательным конвейером стадий: перебор поддоменов, проверка доступности хостов, определение IP-адресов, полное сканирование портов, определение типа и версии сервиса (CPE), сопоставление с базой данных уязвимостей CVE/БДУ ФСТЭК. Результат каждой стадии автоматически передаётся на вход следующей. Параллельно выполняется обход веб-приложений со сбором URL-адресов, скачиванием и хешированием обнаруженных файлов.

Обнаруженные данные связаны отношением «родитель — потомок» (порт принадлежит IP-адресу, уязвимость CVE принадлежит CPE), что обеспечивает формирование целостной картины периметра без ручного сопоставления результатов отдельных инструментов.

2.4. Принцип работы модуля агрегации данных об уязвимостях

CVEgggregator — модуль агрегации данных об уязвимостях. В изолированной установке он работает автономно: все сведения хранятся в его собственной базе PostgreSQL на сервере заказчика, обращения в сеть Интернет при эксплуатации не выполняются. База модуля содержит две группы сведений:

- полную информацию по каждому идентификатору CVE — описание, оценку CVSS и вектор атаки, уровень критичности, класс слабости CWE, номер и описание из банка данных угроз ФСТЭК России;
- соответствие «программный продукт — уязвимости»: для каждого идентификатора CPE перечень CVE, которым подвержен этот продукт и его версия.

Актуальный снимок базы входит в состав дистрибутива и восстанавливается при установке, поэтому сразу после развёртывания модуль располагает полным набором данных. Дальнейшая актуализация выполняется пакетами обновления, которые передаются на носителе в изолированный контур; доступ в сеть Интернет для этого не требуется.

Пакеты обновления готовит поставщик на своей стороне на основе данных NIST NVD, банка данных угроз ФСТЭК России и бюллетеней НКЦКИ. В инфраструктуру заказчика передаётся только подготовленный пакет.

Данные предоставляются по REST API. Модуль VulnScan обращается к CVEgggregator на этапе сопоставления обнаруженного программного обеспечения (CPE) с базой уязвимостей (CVE) и обогащает найденные уязвимости оценкой CVSS, уровнем критичности, описанием ФСТЭК и номером БДУ.

2.5. Ограничения текущей версии

- Обнаружение уязвимостей выполняется путём сопоставления версии обнаруженного программного обеспечения с базами CVE и БДУ ФСТЭК (CPE → CVE), без активной эксплуатации и без отдельной проверки каждой уязвимости.
- Как следствие, возможны ложные срабатывания, а уязвимости, не отражённые в версии продукта (ошибки конфигурации, изменения после установки обновлений), не выявляются.
- Проверки выполняются без аутентификации на целевых ресурсах (по методу «чёрного ящика»); передача учётных данных для сканирования в текущей версии не предусмотрена.

3. Аппаратные и программные требования

3.1. Аппаратные требования

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

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

Таблица №1 — Рекомендуемые конфигурации хоста

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

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

Справка: управляющий контур платформы (база данных, API, веб-интерфейсы, очередь) в простое потребляет ориентировочно ~2 vCPU и 3–5 ГБ ОЗУ. Восстановление базы CVE (~12 млн строк) требует PostgreSQL 17 и 16 ГБ ОЗУ. Каждый дополнительный поток сканирования добавляет ориентировочно 0,5–1 vCPU и 250–500 МБ ОЗУ. Значения — инженерные оценки, а не гарантированные SLA; фактические показатели зависят от целевой сети.

3.2. Программные требования

На сервере должны быть установлены пакеты `podman` и `podman-compose` (порядок установки приведён в разделе 5 настоящего руководства).

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.

Установку и настройку программы должен выполнять администратор Linux.

3.3. Требования к сетевой инфраструктуре

3.3.1. Сетевые транспорты

Инструменты конвейера сканирования используют следующие сетевые протоколы: DNS-запросы (перебор поддоменов, резолвинг IP), HTTP/HTTPS (проверка «живости» хостов, обход веб-приложений, скачивание файлов, обращение к внутреннему сервису базы CVE) и TCP (полное сканирование всех 65535 портов и определение сервиса/версии ПО на открытых портах).

3.3.2. Сетевое взаимодействие с объектом сканирования

Основным источником сетевой нагрузки при сканировании является инструмент проверки портов: один поток TCP-сканирования создаёт пиковую нагрузку до ~2000 пакетов в секунду, при параллельном запуске нескольких потоков суммарная нагрузка на сеть растёт пропорционально.

Внимание. Высокая интенсивность сканирования может кратковременно повышать задержки и потери на слабых каналах связи, провоцировать срабатывание средств обнаружения и предотвращения вторжений (сканирование выглядит как сетевая разведка), приводить к нестабильной работе устройств — АСУ ТП, IoT-устройств, принтеров, медицинского оборудования.

Для первого запуска рекомендуется применить консервативные настройки (небольшое число потоков, увеличенная задержка между пакетами), заранее согласовать окно сканирования и IP-адрес сканера с ответственными за сетевую безопасность.

4. Подготовка к установке

Установка проводится на операционной системе Astra Linux 1.8.

Для установки используется учётная запись root.

1) Активируйте учётную запись root:

```
sudo passwd root
```

2) После назначения пароля войдите в систему под этой учётной записью.

Выставьте значение umask:

```
umask 022
```

3) Создайте отдельную директорию в opt каталоге:

```
mkdir /opt/vulnscan
```

4) Скопируйте в директорию архив vulnscan-offline-bundle.tar с дистрибутивом любым доступным способом.

5) Перейдите в директорию с дистрибутивом:

```
cd /opt/vulnscan
```

6) Распакуйте 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

7) Подготовка к установке завершена.

5. Установка CyberDef EASM

5.1. Установка Podman и зависимостей

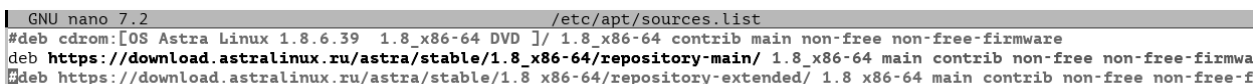
- 1) Откройте файл source-листа в редакторе nano и проверьте подключение базового репозитория Astra Linux:

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

- 2) Если репозиторий установлен в локальной сети организации, используйте строку подключения к нему. Если нет — используйте адрес базового репозитория Astra Linux 1.8:

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

- 3) Убедитесь, что эта строка 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-firmware  
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-extended/ 1.8_x86-64 main contrib non-free non-free-firmware
```

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

Остальные строки можно закомментировать.

- 4) Сохраните изменения в файле и обновите 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

- 5) Установите 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 HOBBIE 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

- 6) После установки пакетов переходите к установке самого дистрибутива.

5.2. Запуск скрипта установки дистрибутива

- 1) Перейдите в директорию /opt/vulnscan:

```
cd /opt/vulnscan
```

- 2) Запустите скрипт установки:

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

- 3) Дождитесь завершения 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

5.3. Завершение установки

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

```
ожидание восстановления CVE-базы..... - готово
✓ CVE-база восстановлена
✓ проверка sveggregator-api - ok
✓ sveggregator-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 используйте логин admin.

Пароль можно прочитать в файле: /opt/vulnscan/podman/.env

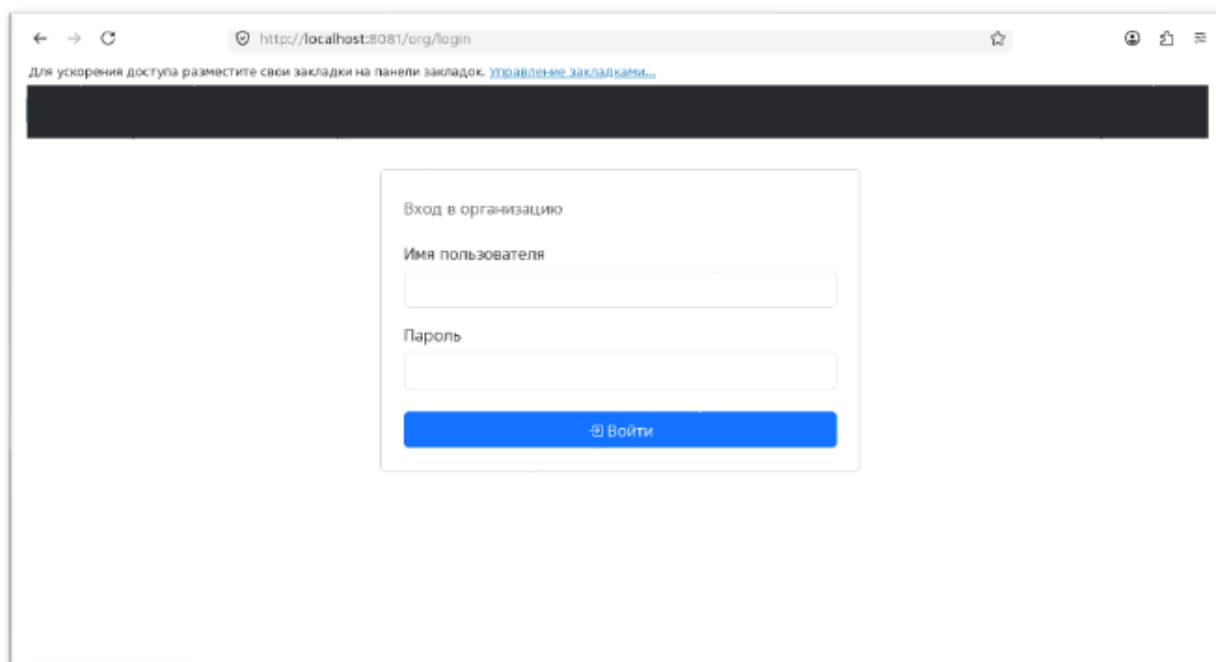


Рисунок 7 — Страница входа веб-интерфейса программы

Установка завершена.

6. Первоначальная настройка

6.1. Создание учётной записи администратора

Перед началом сканирования необходимо создать организацию и учётную запись администратора.

- 1) Выполните вход в контейнер vulnscan-data-service-1:

```
podman exec -it vulnscan-data-service-1 bash
```

```
root@astra:/home/localadm/vulnscan# podman exec -it vulnscan-data-service-1 bash
appuser@e6507c92e0db:/app$ █
```

Рисунок 8 – Вход в контейнер vulnscan-data-service-1

- 2) В открывшемся терминале выполните команду, указав вместо плейсхолдеров имя организации, имя учётной записи, адрес электронной почты и пароль (не менее 12 символов):

```
BOOTSTRAP_ORG_NAME=имя_организации \
BOOTSTRAP_ADMIN_USERNAME=имя_учетной_записи \
BOOTSTRAP_ADMIN_EMAIL=email@email.ru \
BOOTSTRAP_ADMIN_PASSWORD='Пароль_не_менее_12_символов' \
python scripts/bootstrap_single_tenant.py
```

После завершения работы скрипта на экране появится сообщение вида Provisioned organization 'имя_организации' with owner 'имя_учетной_записи', подтверждающее успешное создание организации.

```
appuser@e6507c92e0db:/app$ BOOTSTRAP_ORG_NAME=██████████ \
BOOTSTRAP_ADMIN_USERNAME=██████████ \
BOOTSTRAP_ADMIN_EMAIL=██████████@org.ru \
BOOTSTRAP_ADMIN_PASSWORD='██████████' \
python scripts/bootstrap_single_tenant.py
Provisioned organization 'Organization' with owner '██████████'.
appuser@e6507c92e0db:/app$ █
```

Рисунок 9 – Результат выполнения скрипта bootstrap_single_tenant.py

6.2. Настройка доступа по доменному имени

При установке создаётся базовый домен `vulnscan.local`. После создания организации адрес интерфейса будет иметь вид:

```
http://<организация>.<базовый-домен>:8080
```

1) Добавьте этот адрес на DNS-сервер организации.

Если эксплуатация будет происходить только на сервере, где установлен CyberDef EASM, вместо этого внесите изменения в файл `/etc/hosts`:

```
GNU nano 7.2
127.0.0.1      localhost
127.0.1.1      astra
192.168.1.31   vulnscan.local organization.vulnscan.local
# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
```

Рисунок 10 – Редактирование файла `/etc/hosts`

2) Первоначальная настройка завершена.

7. Аутентификация пользователей

7.1. Политика двухфакторной аутентификации

Способ входа в систему определяется отдельно для каждой организации, одной организации достаточно аутентификации по паролю, другой требуется аппаратный ключ. Платформа не устанавливает единый способ входа для всех организаций.

Настройка выполняется владельцем организации в разделе «Настройки организации», блок «Двухфакторная аутентификация». В рамках настройки задаются два параметра:

- обязательность второго фактора — при включении данного параметра участник, не имеющий привязанного фактора, при следующем входе перенаправляется на страницу привязки фактора и не получает доступа к системе до завершения настройки;
- перечень допустимых факторов — определяется установкой соответствующих флагов.

Фактор	Что это	Состояние
Одноразовый код (TOTP)	Приложение-аутентификатор на телефоне	Поддерживается
Аппаратный ключ (FIDO2)	USB- или NFC-ключ, в том числе Руткен MFA и JaCarta WebPass	Поддерживается
Внешний провайдер (OIDC)	Вход через систему единого входа организации	В разработке; отображается в списке, но недоступен для выбора

Отключение фактора прекращает его использование для всех участников организации, включая тех, кто уже привязал этот фактор: при переходе организации с одноразовых кодов на аппаратные ключи приём кодов действительно прекращается. Изменение настройки вступает в силу при следующем входе в систему или обновлении сессии; ранее открытые сессии продолжают действовать до истечения срока.

Платформа не допускает сохранения настройки, при которой второй фактор обязателен, а список допустимых факторов пуст: в этом случае все участники организации оказались бы на странице привязки без возможности привязать какой-либо фактор.

7.2. Требования для использования аппаратных ключей

Для использования аппаратных ключей необходимо выполнение следующих условий.

- Доступ по протоколу HTTPS. Без защищённого соединения браузер не предоставляет доступ к аппаратному ключу. Исключение составляет обращение к localhost при отладке.
- Постоянное доменное имя. Аппаратный ключ привязывается к домену платформы. При изменении адреса платформы ранее привязанные ключи перестают предлагаться браузером, и требуется их повторная привязка.

Домен задаётся переменной окружения WEBAUTHN_RP_ID. По умолчанию используется родительский домен, определяемый переменной SERVICE_DOMAIN: например, для data-service.vulnscan.example.com родительским доменом является vulnscan.example.com, что позволяет использовать один ключ на всех поддоменах организаций. При установке платформы на собственное доменное имя значение переменной WEBAUTHN_RP_ID следует задать явно и не изменять в дальнейшем.

7.3. Хранение данных и их защита

В базе данных хранится только открытая часть ключа; закрытая часть не покидает устройство пользователя, поэтому её хищение из базы данных исключено. Аппаратный ключ ведёт учёт количества собственных использований: если значение счётчика не увеличилось, предъявленные данные признаются копией, и попытка входа отклоняется. Обмен данными с ключом выполняется однократно и действителен в течение пяти минут.

Секрет одноразовых кодов хранится в зашифрованном виде; ключ шифрования формируется на основе параметра SECRET_KEY установки.

7.4. Восстановление доступа

Владелец организации выполняет сброс второго фактора участнику в настройках организации. После сброса участник входит в систему по паролю и повторно привязывает фактор.

Если второй фактор утрачен самим владельцем организации, сброс выполняется администратором платформы непосредственно в базе данных.

7.5. Диагностика ошибок входа

Симптом	Причина и порядок действий
Браузер не предлагает привязанный ключ	Изменился адрес платформы. Ключ привязан к домену; необходимо вернуть прежнее значение переменной WEBAUTHN_RP_ID либо привязать ключи заново
Кнопка привязки ключа сообщает, что браузер не поддерживает ключи	Платформа доступна по протоколу HTTP. Для работы аппаратных ключей требуется HTTPS
Участник не может привязать одноразовые коды, хотя второй фактор обязателен	Организация исключила коды из списка допустимых факторов. Необходимо проверить настройки организации
Владелец организации утратил второй фактор	Сброс выполняется администратором платформы в базе данных
Сотрудник входит по коду, хотя организация перешла на ключи	Изменение применяется при следующем входе в систему; ранее открытые сессии действуют до истечения срока

7.6. Вход по электронной цифровой подписи (Рутокен ЭЦП, JaCarta PKI)

Вход по сертификату ГОСТ в текущей версии платформы не поддерживается; данное ограничение не связано с планами доработки.

Указанные токены содержат не FIDO2-ключ, а сертификат ГОСТ. Проверка такого сертификата в соответствии с законодательством должна выполняться сертифицированным средством криптографической защиты информации (СКЗИ), а не программным кодом платформы, и выполняется на входном сервере — до поступления запроса в приложение. Для реализации такого способа входа потребуется:

- приобрести сертифицированное СКЗИ (КриптоПро CSP или аналог) — лицензия требуется на сервер, зачастую и на рабочие места пользователей;
- развернуть входной сервер, совместимый с ГОСТ, и получить для него сертификат в аккредитованном удостоверяющем центре (услуга платная, оформление занимает несколько недель);
- установить криптографический плагин на каждое рабочее место;

- согласовать перечень доверенных удостоверяющих центров и поле сертификата, по которому владелец сертификата сопоставляется с учётной записью пользователя.

Дополнительно необходимо учитывать, что для изолированной установки в контуре заказчика данный механизм разворачивается силами заказчика, а включение входа по ЭЦП означает, что вход в систему становится возможен только при наличии подключённого токена — пароль и одноразовый код перестают действовать.

Рекомендуемое практическое решение — организация входа через уже сертифицированную систему единого входа заказчика (фактор «Внешний провайдер (OIDC)», см. таблицу в разделе 1.1). В этом случае обработка ЭЦП выполняется на стороне системы единого входа заказчика, а платформа не обращается к криптографическим механизмам напрямую.

8. Журнал действий

Журнал фиксирует действия пользователей организации: кто выполнил действие, над каким объектом, когда, с какого адреса и с каким результатом. Журнал предназначен для разбора инцидентов и подтверждения того, что действие было выполнено конкретным сотрудником.

8.1. Состав фиксируемых событий

В журнале фиксируются изменяющие действия и события входа в систему: вход в систему (включая неуспешные попытки), выход из системы, смена пароля, привязка и отключение второго фактора, управление пользователями и ролями, изменение настроек организации, создание, изменение и удаление данных, запуск сканирования, выгрузка отчёта.

Просмотр страниц в журнал не записывается. Служебный обмен данными между компонентами платформы, не связанный с действиями пользователя, в журнал также не включается.

8.2. Персонафикация записей

Помимо ссылки на учётную запись, каждая запись журнала содержит снимок данных сотрудника на момент совершения действия: логин, фамилию, имя, отчество и должность. При удалении учётной записи ссылка на неё обнуляется, однако запись по-прежнему указывает исполнителя действия — удаление учётной записи пользователя не приводит к обезличиванию истории.

Каждая запись содержит идентификаторы запроса и трассировки, по которым событие сопоставляется с техническими журналами (логами) платформы.

8.3. Неизменяемость и изоляция данных журнала

Журнал реализован по принципу «только добавление»:

- изменение записи запрещено на уровне базы данных — попытка правки отклоняется, в том числе при прямом обращении к базе данных от имени владельца таблицы;
- через веб-интерфейс и API журнал доступен только для чтения — создание или удаление записи невозможно для любого пользователя, включая администратора платформы.

Удаление записей предусмотрено только для соблюдения установленного срока хранения и для каскадного удаления данных при удалении организации.

Организация имеет доступ исключительно к собственным записям журнала; действия администраторов платформы в журнал организации не включаются.

8.4. Доступ к журналу

Просмотр журнала требует отдельного права доступа. Данное право предоставлено владельцу организации, а также ролям, которым оно назначено явно. Общее правило «роль без явных ограничений имеет неограниченный доступ» на журнал не распространяется, поскольку журнал отображает действия всех сотрудников организации.

8.5. Срок хранения записей

Автоматическая очистка журнала не предусмотрена — платформа самостоятельно не удаляет его записи. Удаление устаревших записей выполняется администратором в соответствии с регламентом заказчика; значение по умолчанию, на которое рассчитан механизм хранения, составляет 365 дней.

8.6. Выгрузка журнала

Пользователь, имеющий право просмотра, может выгрузить отобранные записи журнала в файл формата CSV средствами веб-интерфейса. За одну выгрузку сохраняется не более 100 000 записей; при достижении этого предела результат выгрузки помечается признаком неполноты, что исключает возможность принять частичную выгрузку за полную.

9. Отчётность, шаблоны и наборы данных

Отчёт в платформе состоит из блоков, а данные для блоков даёт набор данных. И то, и другое существует в двух видах: общие объекты платформы и объекты организации.

Объект	Кто ведёт	Где правится
Общий отчёт и общий набор данных	Администратор платформы	Конфигурационный комплект поставки; веб-интерфейс администратора
Отчёт организации	Пользователь организации	Конструктор отчётов в веб-интерфейсе организации
Набор данных организации	Пользователь организации	Конструктор наборов данных в веб-интерфейсе организации
Набор данных на SQL	Администратор платформы	Веб-интерфейс администратора

Общие объекты поставляются вместе с платформой и доступны всем организациям только для чтения. Пользователь может скопировать общий отчёт или набор себе («Клонировать для редактирования») и дальше править копию — на исходный объект это не влияет.

9.1. Что доступно пользователю без администратора

Пользователь организации собирает отчёты и наборы данных самостоятельно, программирование не требуется. Набор данных описывается выбором из списков: тип объекта сканирования, колонки (включая свойства объектов-предков), условия отбора, группировка, сортировка и предел строк. Из этого описания платформа сама строит запрос к данным своей организации.

Обращение к чужим данным исключено на уровне базы, запросы выполняются от имени роли только для чтения и в контексте организации, поэтому набор физически не может вернуть строки другой организации.

9.2. Редактирование шаблона отчёта

Шаблоны отчётов сканирования редактируются в конструкторе отчётов. Ниже описано, как открыть шаблон для редактирования и какие возможности оформления доступны.

9.2.1. Открытие шаблона отчёта

Раздел «Отчёты» находится в рабочем пространстве сценария — ниже списка активов и истории запусков. У нужного шаблона нажмите кнопку «Настроить».

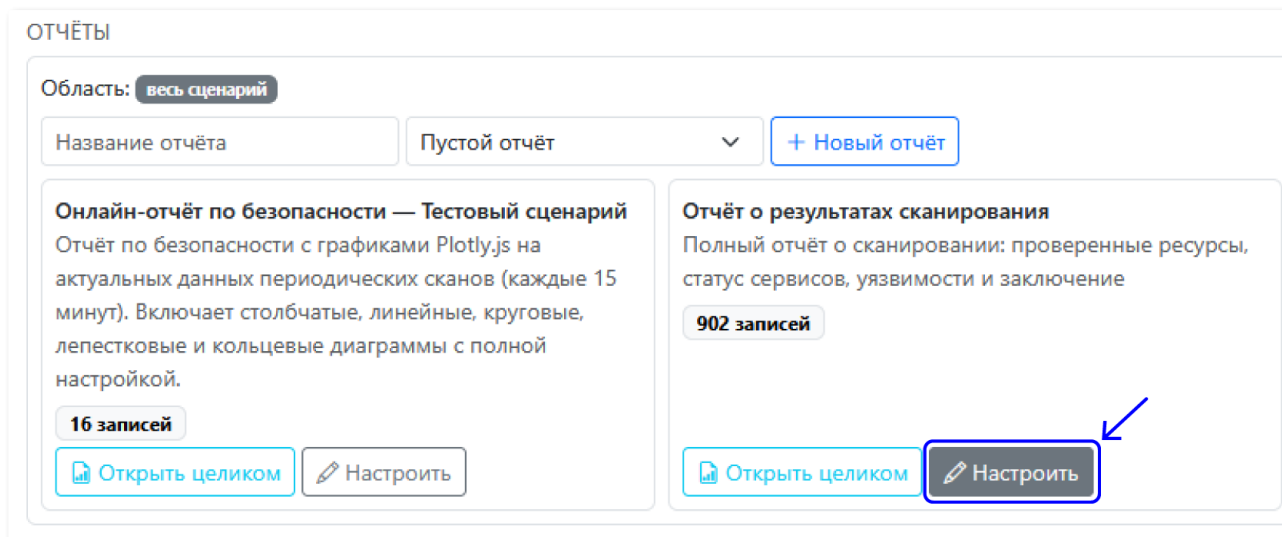


Рисунок 11 – Кнопка «Настроить» на карточке шаблона отчёта

9.2.2. Клонирование шаблона

Стандартные шаблоны — общие, редактировать их напрямую нельзя. Чтобы внести изменения, укажите название в поле справа и нажмите «Клонировать для редактирования»: на основе стандартного шаблона будет создана отдельная редактируемая копия.

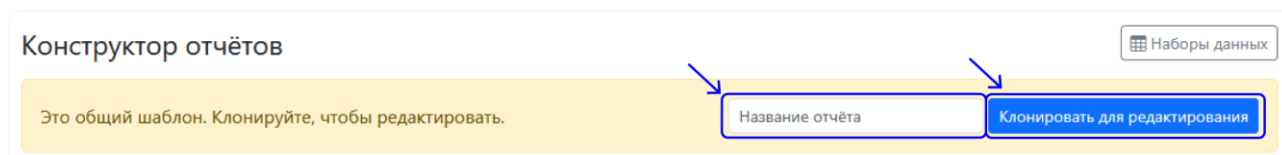


Рисунок 12 – Клонирование шаблона перед редактированием

9.2.3. Возможности конструктора отчётов

После клонирования открывается конструктор - название отчёта, акцентный цвет, кнопки «Сохранить» и «Открыть целиком», ниже — свёрнутые панели настроек и кнопки добавления блоков содержимого.

Конструктор отчётов

Название отчёта: Тест_2_ Акцентный цвет:

[Сохранить](#) [Открыть целиком](#)

► Оформление

► Заблокированные параметры

Пока нет блоков — добавьте ниже.

+ Заголовок + Текст + Таблица + Показатель + График + Отступ + Разрыв страницы

Рисунок 13 – Общий вид конструктора отчётов

9.2.4. Оформление

В панели «Оформление» настраиваются цвет текста, шрифт заголовков, основной шрифт отчёта и логотип (по ссылке на изображение).

Конструктор отчётов

Название отчёта: Тест_2_ Акцентный цвет:

[Сохранить](#) [Открыть целиком](#)

▼ Оформление

Цвет текста: Шрифт заголовков: Georgia (serif) Основной шрифт: System (sans) URL логотипа: https://...

Рисунок 14 – Панель «Оформление»

9.2.5. Заблокированные параметры

В этой панели можно жёстко зафиксировать значение отдельного параметра отчёта.

Рисунок 15 – Панель «Заблокированные параметры»

9.2.6. Блоки содержимого

Содержимое отчёта собирается из блоков: Заголовок, Текст, Таблица, Показатель, График, Отступ, Разрыв страницы. У каждого добавленного блока есть своя панель управления: переместить вверх или вниз, продублировать либо удалить.

Рисунок 15 – Панель управления добавленным блоком

9.2.7. Источники данных для блоков

Блокам «Показатель», «Таблица» и «График» нужно указать источник данных. Готовые источники можно посмотреть, а также создать новые в разделе «Наборы данных» — кнопка в правом верхнем углу конструктора. Подробнее о наборах данных — в следующем разделе.

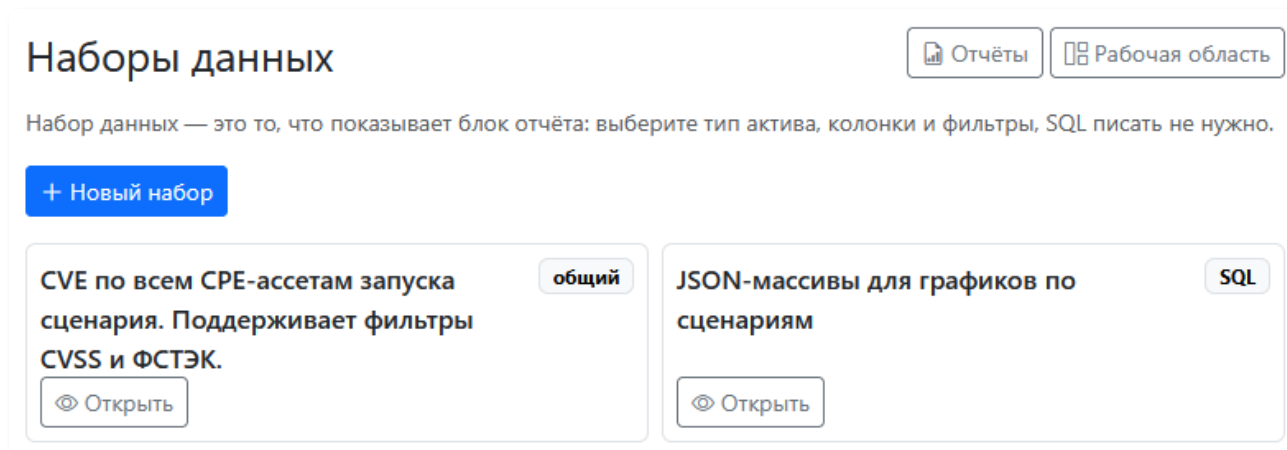


Рисунок 16 – Раздел «Наборы данных» — источники данных для блоков отчёта

9.2.8. Предварительный просмотр отчёта

Внизу страницы конструктора расположен блок «Предпросмотр» — там отображается, как будет выглядеть итоговый отчёт с учётом всех добавленных блоков и настроек оформления. После изменений нажмите «Обновить», чтобы увидеть актуальный результат, не покидая страницу конструктора.

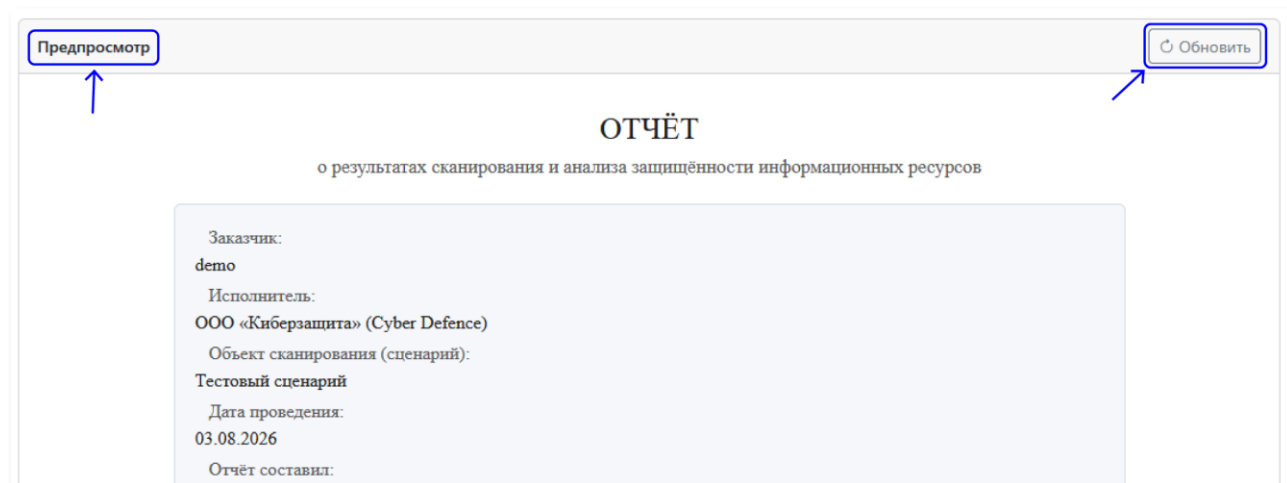


Рисунок 17 – Блок «Предпросмотр» внизу страницы конструктора

9.2.9. Сохранение отчёта

Чтобы сохранить отчёт, нажмите «Сохранить» — рядом появится отметка «Сохранено».

Конструктор отчётов

Название отчёта: Тест_2_ Акцентный цвет: [dropdown]

[Сохранить] [Открыть целиком]

► Оформление

► Заблокированные параметры

Сохранено ←

Рисунок 18 – Сохранение отчёта

9.3. Наборы данных на SQL

Часть поставляемых наборов написана запросом вручную — они помечены «SQL» и конструктором не редактируются: у них нет описания, из которого можно перестроить запрос. Такие наборы ведёт администратор через веб-интерфейс администратора либо через конфигурационный комплект.

Если пользователю нужен набор, который не собирается конструктором (нестандартная агрегация, объединение разных типов объектов), заведите его как SQL-набор и объявите список колонок — тогда колонки появятся в конструкторе отчётов как варианты выбора, и пользователь сможет строить по такому набору блоки.

9.4. Диагностика

Симптом	Причина и решение
Отчёт открывается с пустыми таблицами	Не выбран сценарий или запуск сканирования. Если запуск не выбран, отчёт строится по последнему сканированию сценария; если сканирований не было, данных нет
В наборе данных нет ни одной строки	В выбранном сканировании объектов такого типа не находили. Проверьте, включены ли в сценарий стадии, которые их создают
При сохранении набора — сообщение о неизвестном наборе данных	В инсталляции нет поставляемого набора, на который ссылается заготовка отчёта. Примените конфигурационный комплект отчётов
Пользователь не может изменить отчёт или набор	Объект общий, он ведётся платформой. Пользователю следует сделать копию кнопкой «Клонировать для редактирования»