CYBERDEFENCE

CyberDef EASM

Платформа управления внешней поверхностью атаки
(облачная версия)

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ/ОПЕРАТОРА

Версия 4.0

2026

Содержание

Содержание 2
1. Введение 4
1.1. Область применения 4
1.2. Назначение документа 4
1.3. Термины и определения 4
2. Назначение программы 5
2.1. Функции программы 5
2.2. Роли пользователей 6
3. Условия выполнения программы 6
3.1. Требования к браузеру 6
3.2. Доступ к программе 6
4. Начало работы 7
4.1. Вход в систему 7
4.2. Вход с двухфакторной аутентификацией 7
4.3. Выход из системы 8
4.4. Верхняя панель 8
4.5. Главная страница проекта 9
4.6. Профиль и смена пароля 11
4.7. Настройка двухфакторной аутентификации 12
5. Работа с проектами и активами 14
5.1. Проекты 14
5.2. Настройки проекта и архивирование 15
5.3. Активы проекта 16
6. Сканирование 17
6.1. Принцип работы 17
6.2. Наборы проверок 18
6.3. Создание набора проверок 19
6.4. Запуск сканирования 21
6.5. Ход выполнения запуска 22
6.6. Остановка и повторный запуск 24
6.7. Результаты запуска 24

6.8. Задания 26
6.9. Расписание сканирования 27
6.10. История запусков 29
7. Работа с отчётами 30
7.1. Виды отчётов 30
7.2. Уязвимости (CVE) 31
7.3. Отчёт о результатах сканирования 32
7.4. Сводка по сценарию 34
7.5. Что изменилось 35
7.6. Дополнительные отчёты 37
7.7. Шаблоны отчётов 42
7.8. Подробные отчёты 44
7.9. Наборы данных 46
8. Администрирование организации 49
8.1. Настройки организации 49
8.2. Безопасность 50
8.3. Добавление пользователя 51
8.4. Роли и права доступа 51
9. Сообщения оператору 52
10. Справочная информация 53
10.1. Типы активов и каталог проверок 53
10.2. Шкала критичности уязвимостей 54

1. Введение

1.1. Область применения

Руководство предназначено для пользователей и операторов облачной версии программного обеспечения «Платформа управления внешней поверхностью атаки CyberDef EASM» (далее программа). Пользователем и оператором в документе называется сотрудник организации, который работает с программой через веб-интерфейс. Действия администратора организации вынесены в отдельный раздел.

1.2. Назначение документа

Документ описывает назначение программы, условия её применения, порядок выполнения основных операций и сообщения, которые получает пользователь. Каждый раздел с инструкциями содержит порядок действий, ожидаемый результат и вид соответствующего экрана. Элементы интерфейса, с которыми выполняются действия, выделены на рисунках рамкой.

1.3. Термины и определения

Термин	Определение
CyberDef EASM	Платформа управления внешней поверхностью атаки.
Проект	Рабочее пространство, которое объединяет активы, наборы проверок, задания, историю запусков и отчёты.
Актив	Объект, известный программе или обнаруженный при сканировании: домен, IP-адрес, порт, сервис, CPE, уязвимость и другие.
Исходный актив	Актив, с которого начинается сканирование, например доменное имя или IP-адрес организации.
Группа активов	Сохранённый перечень активов для повторного выбора при запуске сканирования.
Проверка	Отдельный шаг сканирования, например сканирование IP-адреса на открытые порты. Получает на вход активы одного типа и формирует активы другого типа.
Набор проверок	Сохранённый перечень проверок, которые выполняются при сканировании.
Задание	Сохранённое сочетание активов и набора проверок для повторного запуска, в том числе по расписанию.

Термин	Определение
Запуск	Однократное выполнение сканирования.
CVE	Идентификатор уязвимости в базе данных известных уязвимостей.
CVSS	Числовая оценка критичности уязвимости и вектор атаки.
CWE	Идентификатор класса слабости программного обеспечения.
CPE	Идентификатор программного продукта и его версии.
EPSS	Оценка вероятности эксплуатации уязвимости.
CISA KEV	Каталог известных эксплуатируемых уязвимостей.
БДУ ФСТЭК	Банк данных угроз безопасности информации ФСТЭК России.

2. Назначение программы

2.1. Функции программы

CyberDef EASM предназначен для автоматизированного обнаружения, инвентаризации и анализа защищённости информационных активов организации, доступных из сети Интернет, а также для выявления уязвимостей и управления процессом их устранения.

Основные функции программы:

- аудит активов и обнаружение связанных активов;
- определение перечня сервисов на активах;
- выявление уязвимостей сопоставлением обнаруженного программного обеспечения с базой данных об уязвимостях;
- использование отечественных и зарубежных баз уязвимостей: NIST NVD, БДУ ФСТЭК России, бюллетени НКЦКИ;
- отображение результатов сканирования и управление их обработкой;
- формирование отчётов и экспорт отчётов в PDF;
- управление режимом сканирования из личного кабинета;
- разграничение доступа пользователей и журнал действий.

2.2. Роли пользователей

Набор доступных функций определяется ролью пользователя в организации. Готовые роли приведены в таблице. Подробнее о ролях и правах доступа сказано в разделе «Администрирование организации».

Роль	Назначение
Аналитик	Работа со сценариями: цели, запуск сканирований, отчёты.
Администратор организации	Все возможности, включая управление пользователями, ролями и журнал действий.
Только просмотр	Только чтение результатов и отчётов.

3. Условия выполнения программы

3.1. Требования к браузеру

Для работы с веб-интерфейсом используется 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.

3.2. Доступ к программе

Адрес веб-интерфейса, логин и пароль пользователя сообщает администратор организации. Учётные записи создаются в настройках организации. Исходные активы, то есть домены и IP-адреса организации, добавляет администратор платформы.

Если для организации включена обязательная двухфакторная аутентификация, для входа потребуется приложение-аутентификатор на телефоне. Порядок настройки описан в разделе «Настройка двухфакторной аутентификации».

4. Начало работы

4.1. Вход в систему

1) Откройте в браузере адрес веб-интерфейса, полученный от администратора организации.
2) Введите логин в поле «Имя пользователя» и пароль в поле «Пароль».
3) Нажмите кнопку **«Войти»**.

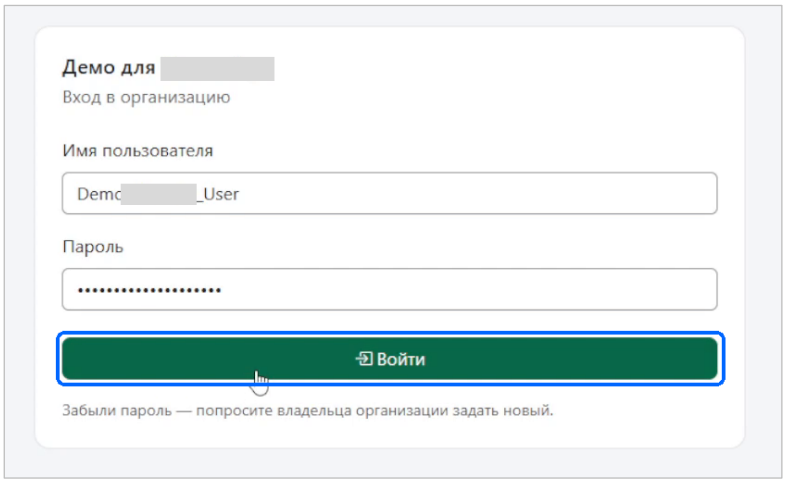


Рисунок 1 – Страница входа в организацию

Результат. Открывается главная страница проекта.

4.2. Вход с двухфакторной аутентификацией

Применяется, если для учётной записи включена двухфакторная аутентификация.

1) Введите логин и пароль и нажмите **«Войти»**.
2) В окне «Код подтверждения» введите шестизначный код из приложения-аутентификатора в поле **«Код из приложения»**.
3) Нажмите **«Подтвердить»**.

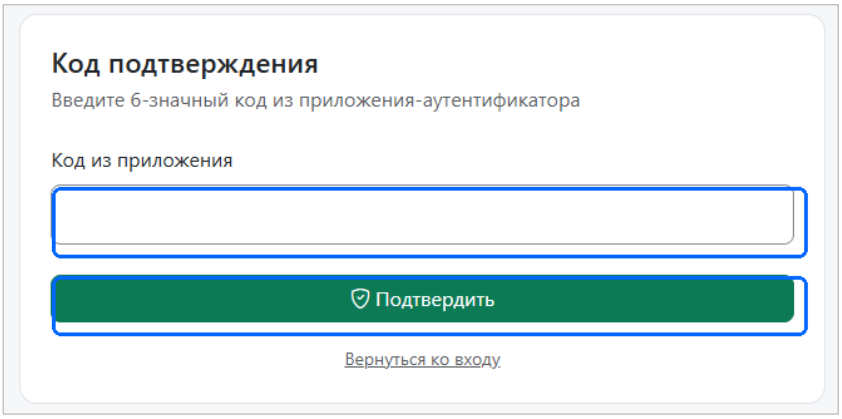


Рисунок 2 – Ввод кода подтверждения при входе

Ссылка «Вернуться ко входу» возвращает на страницу ввода логина и пароля.

Результат. Открывается главная страница проекта.

4.3. Выход из системы

1) Нажмите на имя учётной записи в правом верхнем углу экрана.
2) В открывшемся меню выберите **«Выйти»**.

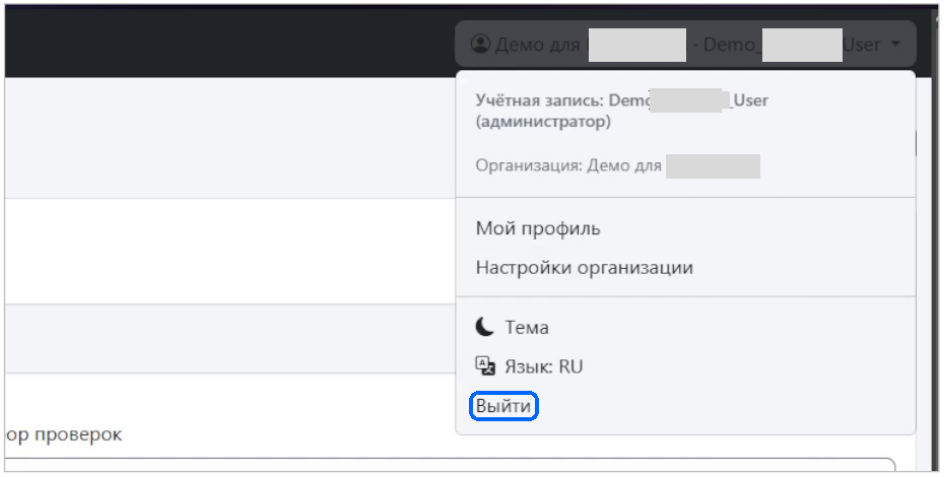


Рисунок 3 – Выход из системы

Результат. Открывается страница входа в организацию.

4.4. Верхняя панель

Веб-интерфейс состоит из верхней панели и рабочей области. Работа с активами, сканированием и отчётами ведётся внутри проекта.

В левой части верхней панели отображается название текущего проекта. Нажатие на название открывает меню проектов. В меню доступны поиск проекта, список проектов организации и пункт **«Управление проектами»**, который открывает страницу «Проекты».

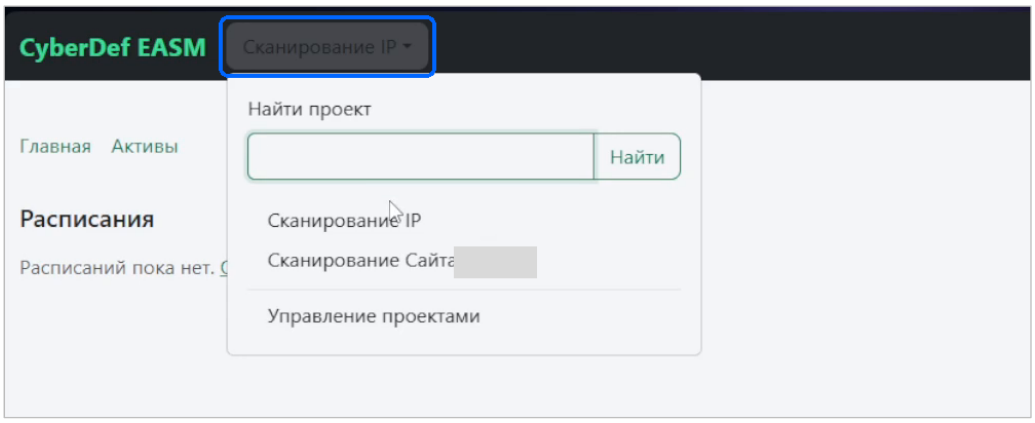


Рисунок 4 – Меню проектов

В правой части верхней панели отображаются название организации и имя пользователя. Нажатие на имя открывает меню учётной записи. В меню указаны учётная запись, роль и организация, а также доступны пункты:

- «Мой профиль» – настройки пользователя, смена пароля и двухфакторная аутентификация;
- «Настройки организации» – администрирование организации;
- «Тема» – переключение светлого и тёмного оформления;
- «Язык» – выбор языка интерфейса;
- «Выйти» – завершение работы.

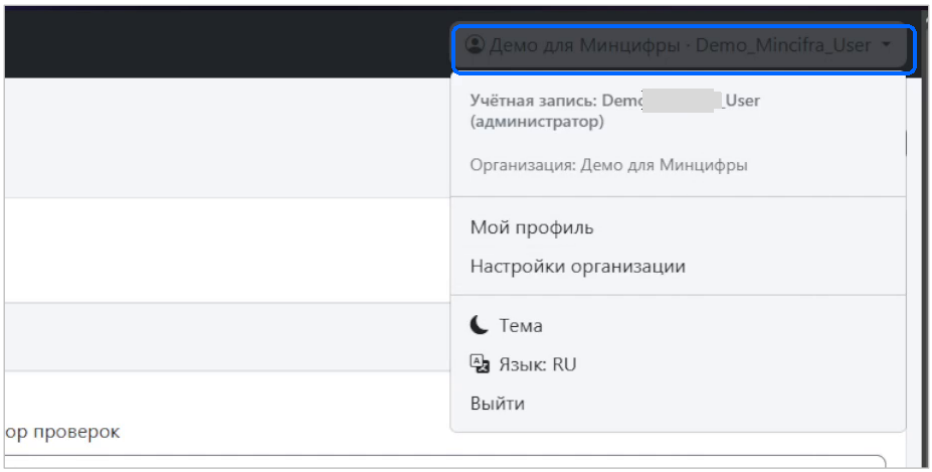


Рисунок 5 – Меню учётной записи

4.5. Главная страница проекта

В верхней части страницы расположены вкладки **«Главная»** и **«Активы»**, справа кнопка **«Ещё»** для перехода к расписаниям, наборам проверок и настройкам проекта. Главная страница содержит четыре блока.

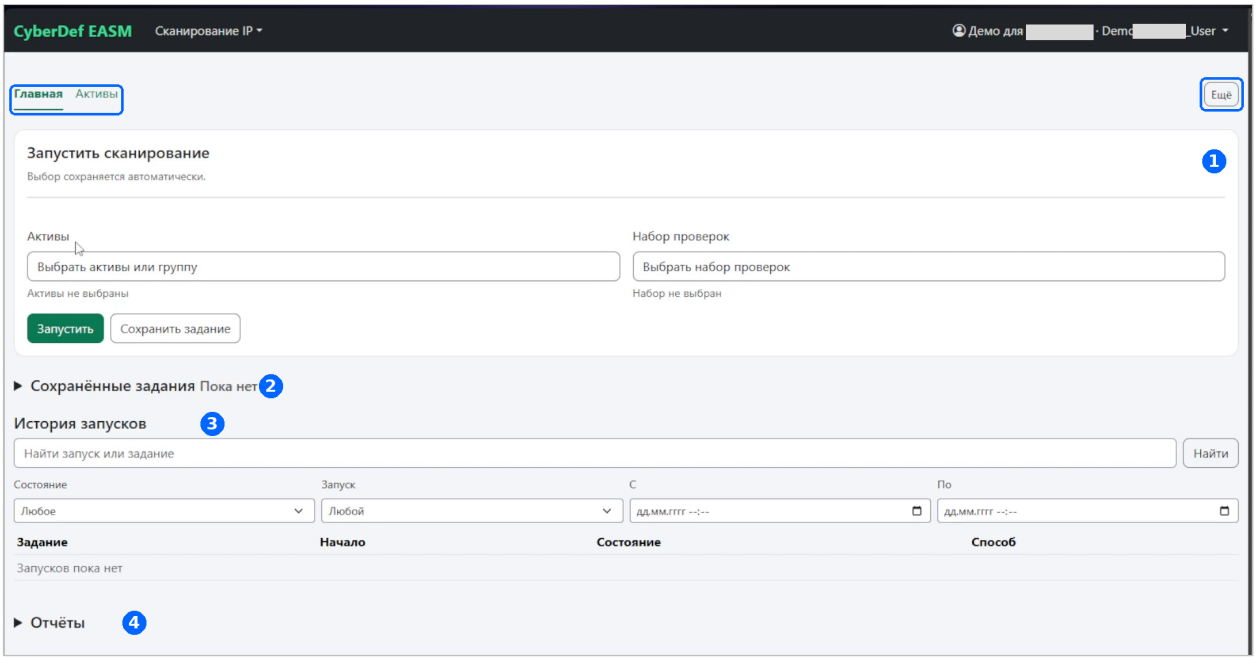


Рисунок 6 – Главная страница проекта

№	Блок и назначение
1	«Запустить сканирование». Выбор активов и набора проверок, запуск сканирования и сохранение задания. Выбор сохраняется автоматически как черновик. Незавершённые черновики отображаются строками «Продолжить: Задание без названия», лишний черновик удаляется кнопкой «Удалить».
2	«Сохранённые задания». Список сохранённых заданий с поиском и кнопкой «Запустить».
3	«История запусков». Таблица запусков проекта с поиском и фильтрами по состоянию, способу запуска и периоду.
4	«Отчёты». Переход к отчётам по результатам сканирования.

4.6. Профиль и смена пароля

1) Нажмите на имя учётной записи в правом верхнем углу экрана.
2) Выберите **«Мой профиль»**.

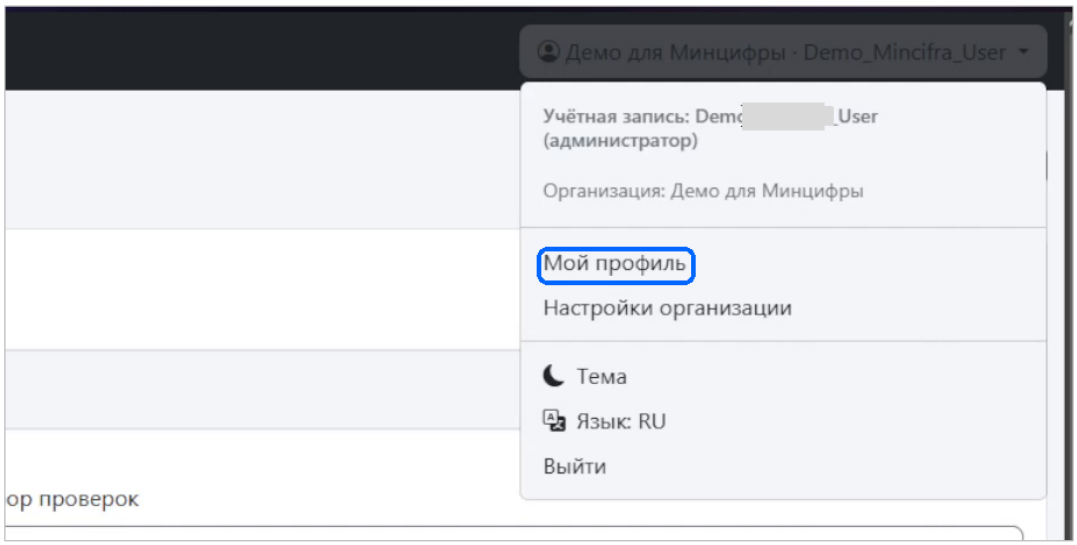


Рисунок 7 – Переход к настройкам пользователя

На странице «Настройки пользователя» доступны смена пароля и заполнение профиля.

Чтобы сменить пароль, введите текущий пароль, новый пароль и повтор нового пароля, затем нажмите **«Сохранить»**. Пароль должен содержать не менее 12 знаков, включая заглавную и строчную букву, цифру и спецзнак, и не входить в список частых паролей.

В блоке «Профиль» заполняются фамилия, имя, отчество и должность. Изменения сохраняются кнопкой **«Сохранить профиль»**.

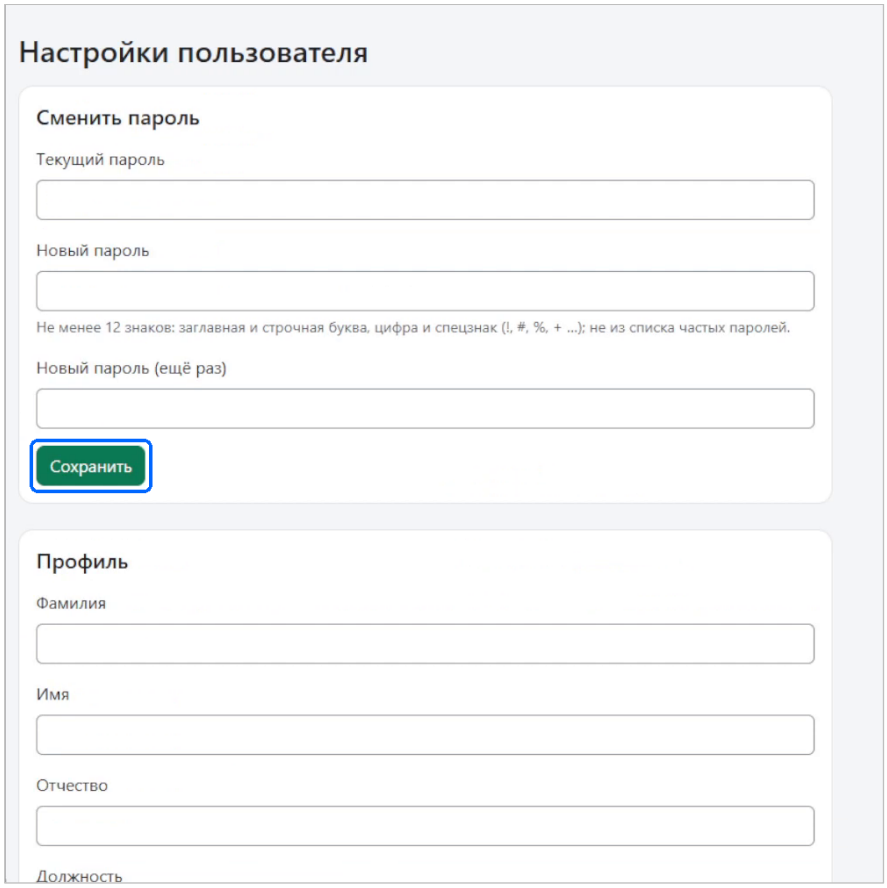


Рисунок 8 – Настройки пользователя

4.7. Настройка двухфакторной аутентификации

Для работы понадобится приложение-аутентификатор на телефоне, например Яндекс ID (Цифровой ключ), Microsoft Authenticator, Google Authenticator или Aegis Authenticator. Если приложения ещё нет, установите его из магазина приложений.

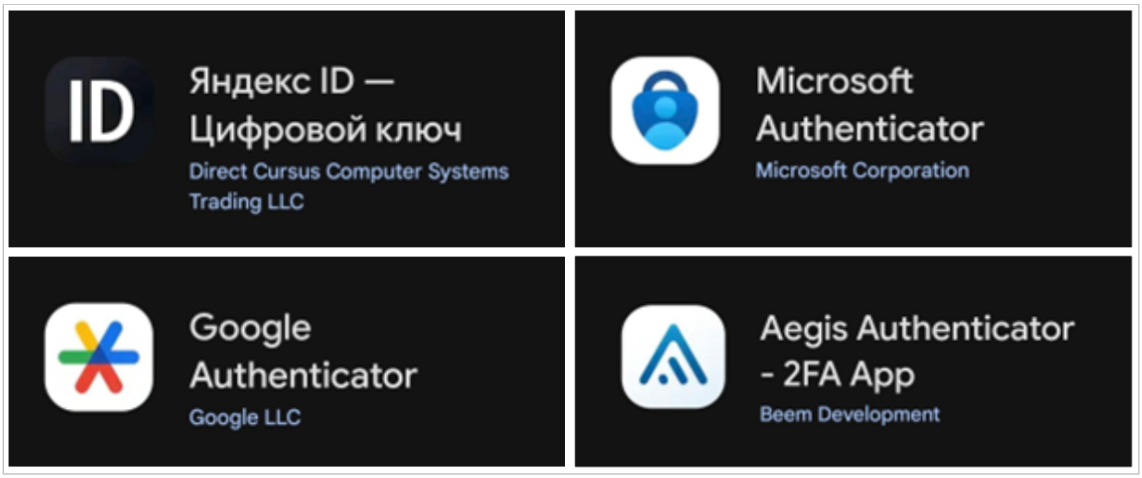


Рисунок 9 – Приложения-аутентификаторы в магазине приложений

> В магазинах много похожих приложений. Проверьте, что название и разработчик совпадают с указанными на рисунке.

1) На странице «Настройки пользователя» в блоке «Двухфакторная аутентификация» нажмите **«Настроить двухфакторную аутентификацию»**.

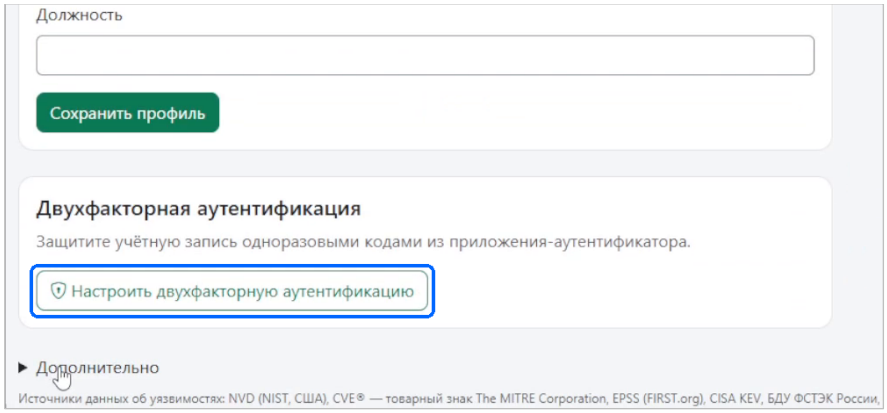


Рисунок 10 – Блок «Двухфакторная аутентификация»

2) Откройте приложение на телефоне и добавьте новый аккаунт, например кнопкой «Сканировать QR-код» в Яндекс ID. Наведите камеру на QR-код на экране. Если сканирование не получается, введите в приложении ключ из строки «Ключ для ручного ввода».
3) Введите шестизначный код из приложения в поле **«Код из приложения»**.
4) Нажмите **«Включить 2FA»**.

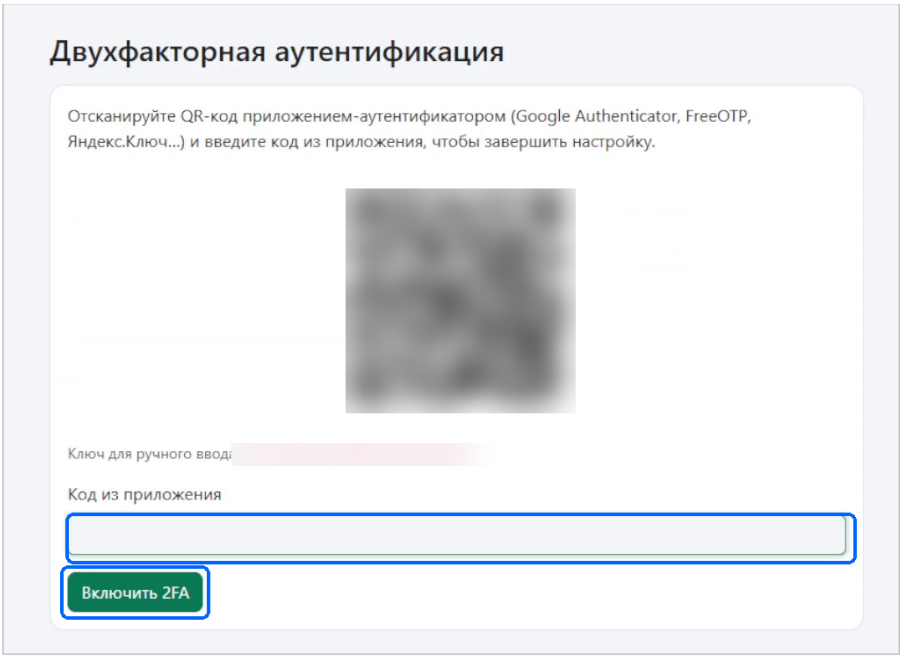


Рисунок 11 – Страница настройки двухфакторной аутентификации

Результат. На странице появляется надпись «Двухфакторная аутентификация включена». При следующем входе после пароля запрашивается код из приложения.

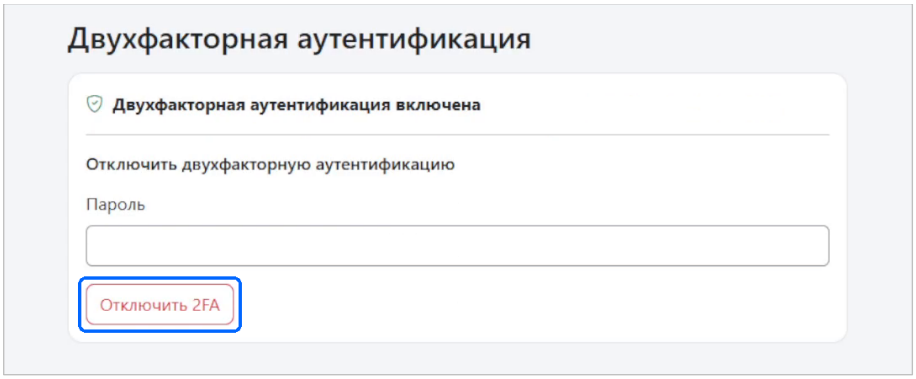


Рисунок 12 – Двухфакторная аутентификация включена

Чтобы отключить двухфакторную аутентификацию, введите пароль в поле «Пароль» и нажмите **«Отключить 2FA»**.

5. Работа с проектами и активами

5.1. Проекты

Проект объединяет активы, наборы проверок, задания, историю запусков и отчёты. На странице «Проекты» отображаются карточки проектов организации с количеством заданий и запусков. Для перехода в проект нажмите на его название. Ссылка **«Архив»** открывает список архивных проектов.

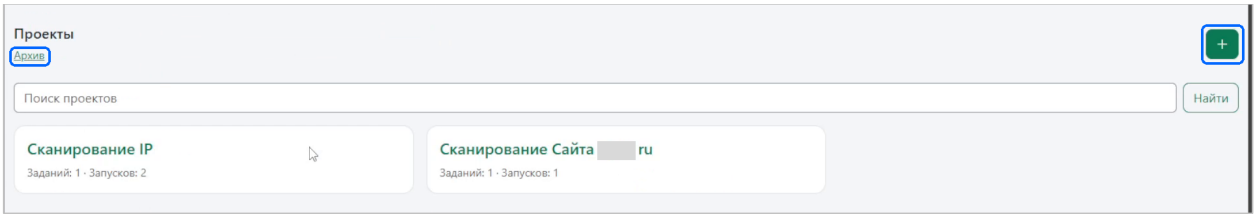


Рисунок 13 – Страница «Проекты»

Чтобы создать проект:

1) Нажмите кнопку **«+»** в правом верхнем углу страницы «Проекты».
2) Введите название в поле «Название проекта». Название не должно совпадать с названием существующего проекта.
3) Нажмите **«Создать»**.

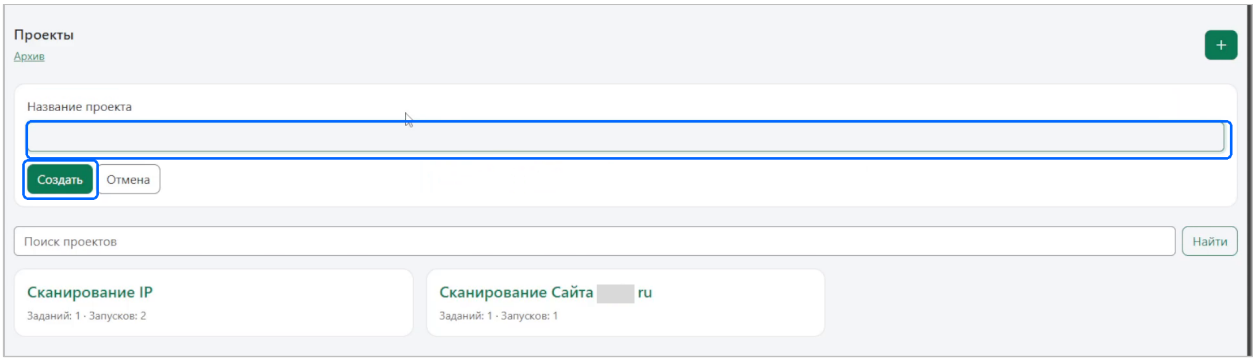


Рисунок 14 – Создание проекта

Результат. Открывается главная страница нового проекта.

5.2. Настройки проекта и архивирование

1) Нажмите кнопку **«Ещё»** в правом верхнем углу страницы проекта.
2) Выберите **«Настройки проекта»**.

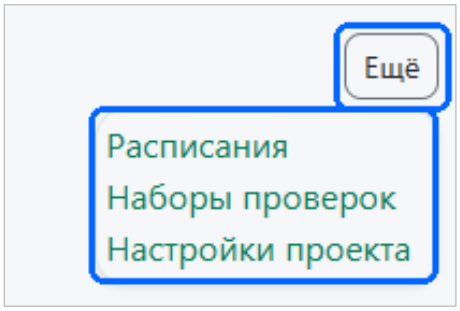


Рисунок 15 – Меню «Ещё»

На странице «Настройки проекта» доступны следующие действия:

- изменение названия и описания проекта с сохранением кнопкой **«Сохранить изменения»**;
- настройка доступа участников организации к проекту в блоке **«Настроить доступ»**;
- перенос проекта в архив в блоке **«Архивировать проект»**.

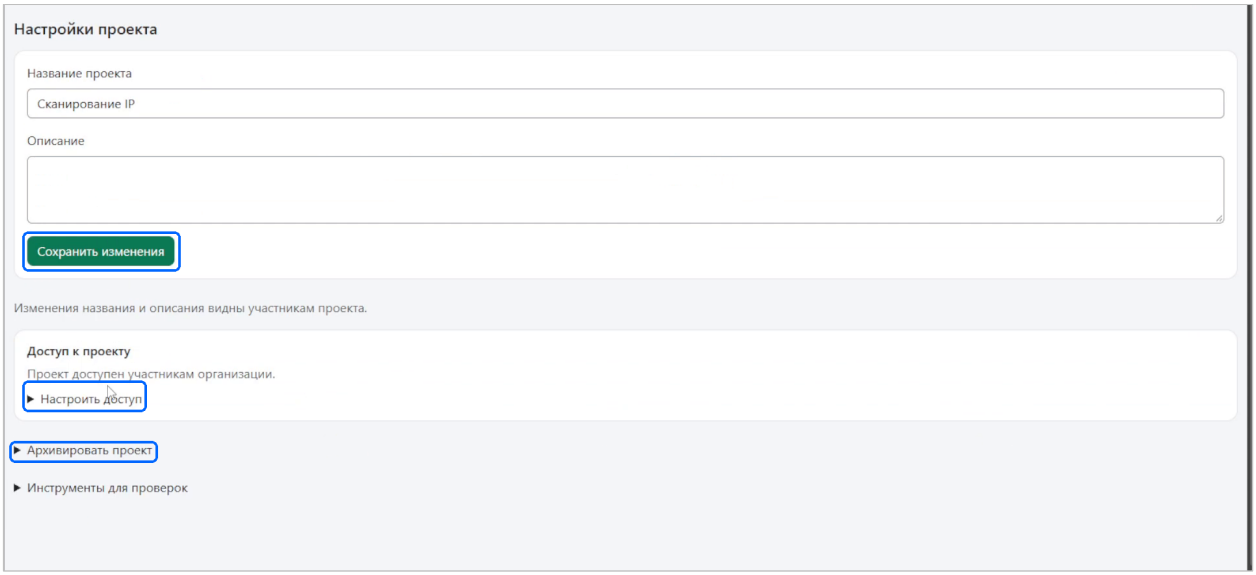


Рисунок 16 – Настройки проекта

Кнопка **«Архивировать проект»** также расположена в нижней части страниц проекта. Архивный проект пропадает из рабочего списка, история и результаты сохраняются, расписания останавливаются. Проект можно вернуть из архива на странице «Проекты» по ссылке «Архив».

5.3. Активы проекта

Вкладка **«Активы»** содержит все активы проекта, исходные и обнаруженные при сканировании. Каждая строка списка содержит значение актива, его тип и статус. Список разбит на страницы, для перехода используются кнопки «Назад» и «Далее».

Для поиска служат строка «Поиск по всем активам» и фильтры:

- «Тип» – тип актива, перечень типов приведён в разделе «Справочная информация»;
- «Объекты» – активы и группы, только активы или только группы;
- «Происхождение» – источник появления актива;
- «Задание» – активы, полученные в рамках выбранного задания.

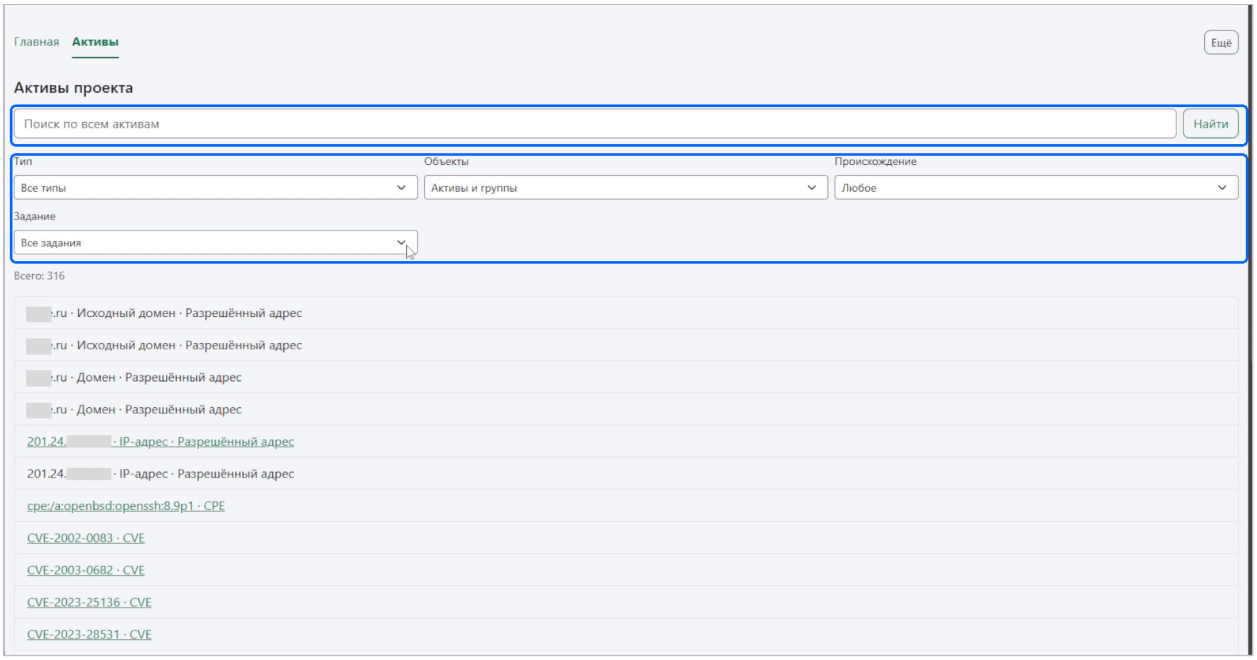


Рисунок 17 – Активы проекта

6. Сканирование

6.1. Принцип работы

Сканирование выполняется по набору проверок. Каждая проверка получает на вход активы определённого типа и формирует новые активы. Например, проверка «Сканирование IP на открытые порты» получает IP-адрес и находит открытые порты, проверка «Определение сервиса, версии и CPE на порту» определяет программное обеспечение на порту, а проверка «Поиск уязвимостей (CVE) по версии ПО в базе уязвимостей» сопоставляет CPE с базой данных об уязвимостях.

Результат каждой проверки автоматически передаётся проверкам, которые принимают активы этого типа. Так от одного исходного актива строится цепочка до сервисов, уязвимостей и эксплойтов. Связи проверок отображаются в виде графа в редакторе набора проверок и на странице запуска.

Для запуска сканирования выбираются активы и набор проверок. Это сочетание можно сохранить как задание и запускать повторно вручную или по расписанию.

6.2. Наборы проверок

Для перехода к наборам нажмите **«Ещё»** и выберите **«Наборы проверок»**. На странице отображаются наборы проекта с описанием. Готовые наборы «Быстрая проверка домена» и «Полная пассивная проверка» не изменяются, на их основе создаётся копия кнопкой **«Сделать копию»**. Собственные наборы редактируются кнопкой **«Изменить»** и переносятся в другой проект кнопкой **«В другой проект»**. Новый набор создаётся кнопкой **«Создать набор»**.

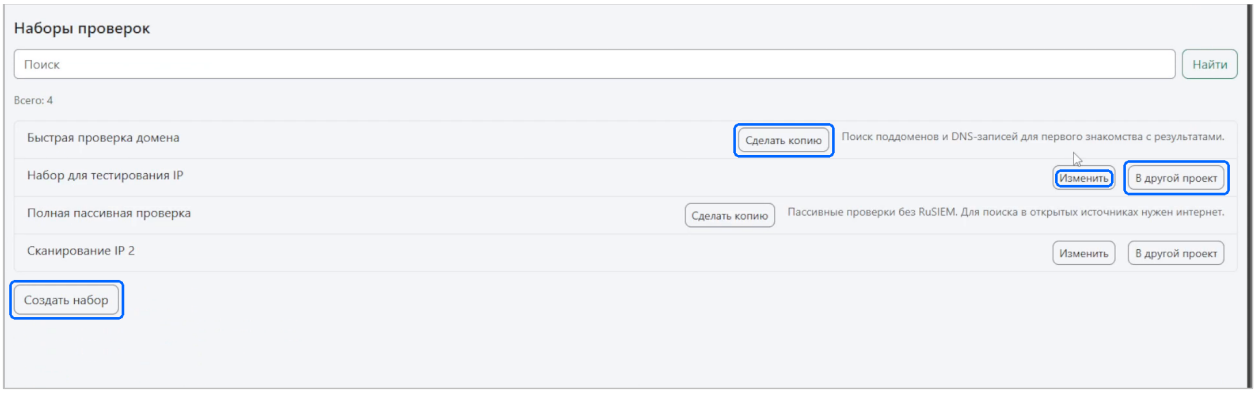


Рисунок 18 – Наборы проверок

Каталог проверок приведён в разделе «Справочная информация». Для каждой проверки указан тип: пассивная, обычная или активная.

6.3. Создание набора проверок

Состав набора настраивается в окне «Редактор набора проверок». Переключатель **«Граф»** и **«Список»** меняет вид отображения, кнопки «–» и «+» меняют масштаб графа. На графе показано, какие активы получает и формирует каждая проверка.

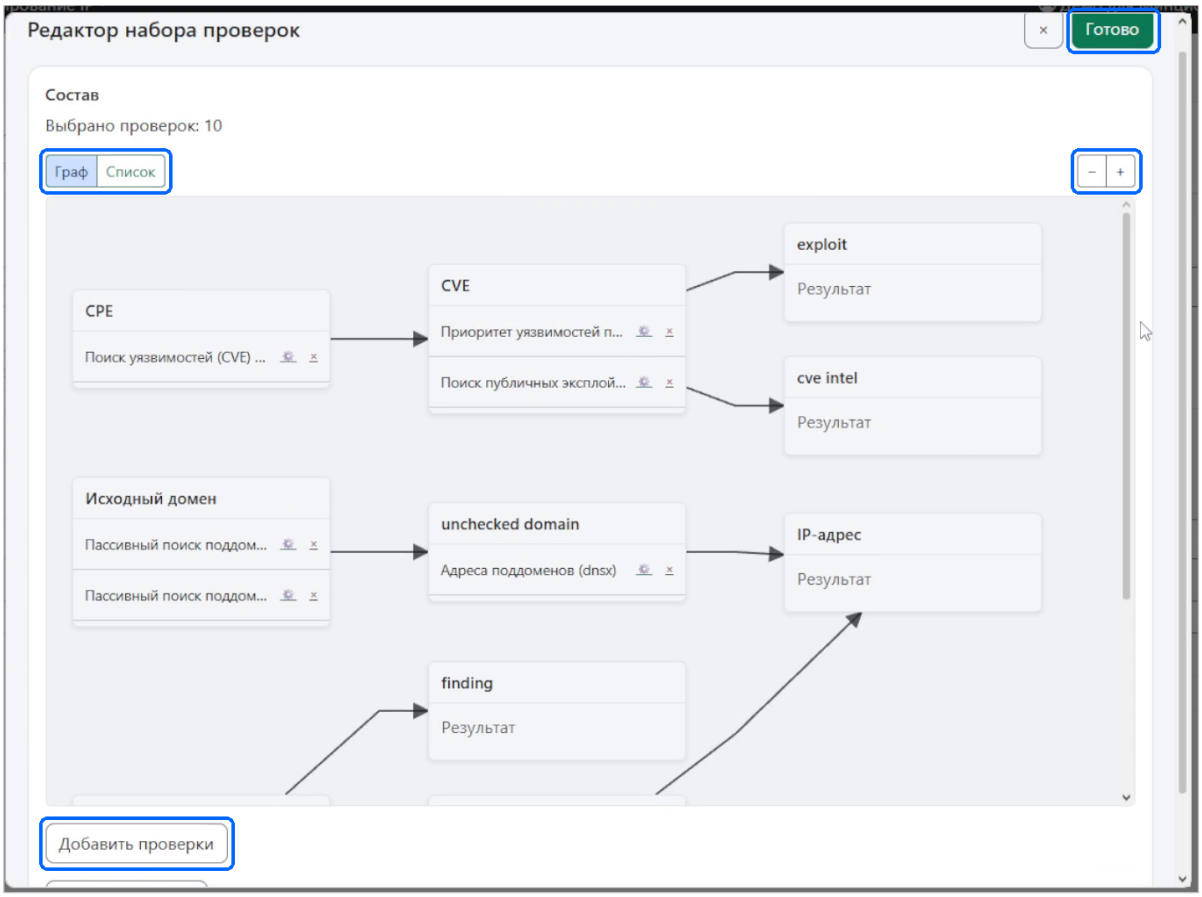


Рисунок 19 – Редактор набора проверок, вид «Граф»

1) Нажмите **«Создать набор»** на странице «Наборы проверок» или в окне «Наборы проверок» при запуске сканирования.
2) В редакторе нажмите **«Добавить проверки»**.
3) В каталоге нажмите **«+»** слева от каждой нужной проверки. Для перехода к следующей странице каталога нажмите «Далее».

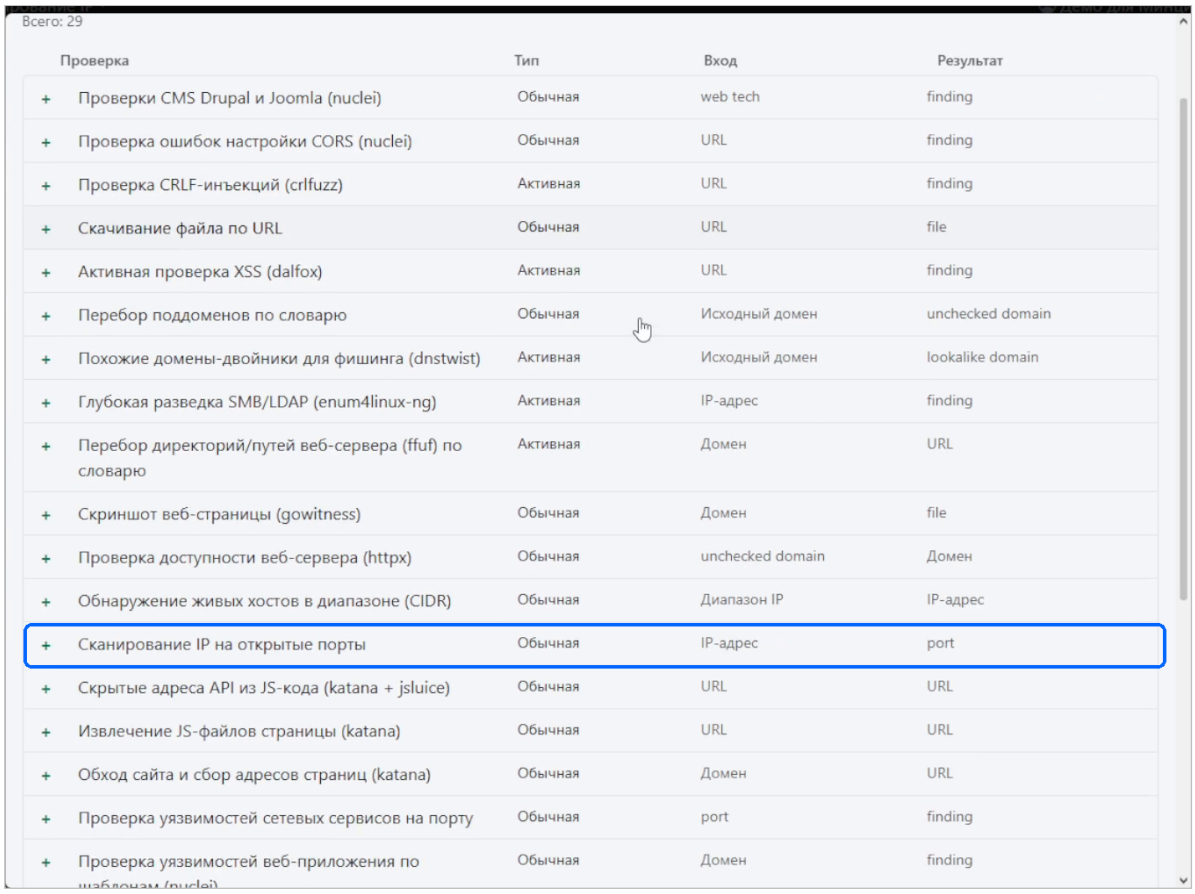


Рисунок 20 – Каталог проверок

4) Нажмите **«Готово»**. Состав набора отображается на графе или в списке. В виде «Список» для каждой проверки доступны «Параметры проверки» и кнопка «Убрать», которая исключает проверку из набора.
5) Нажмите **«Сохранить набор»**, введите название в поле **«Название набора проверок»**.
6) Нажмите **«Сохранить набор и вернуться»**.



Рисунок 21 – Сохранение набора проверок

Если набор нужен только для текущего задания, название не требуется, достаточно нажать **«Готово»**.

Результат. Набор появляется в списке наборов проекта.

6.4. Запуск сканирования

Запуск выполняется на главной странице проекта в блоке «Запустить сканирование».

1) Нажмите на поле **«Выбрать активы или группу»**.

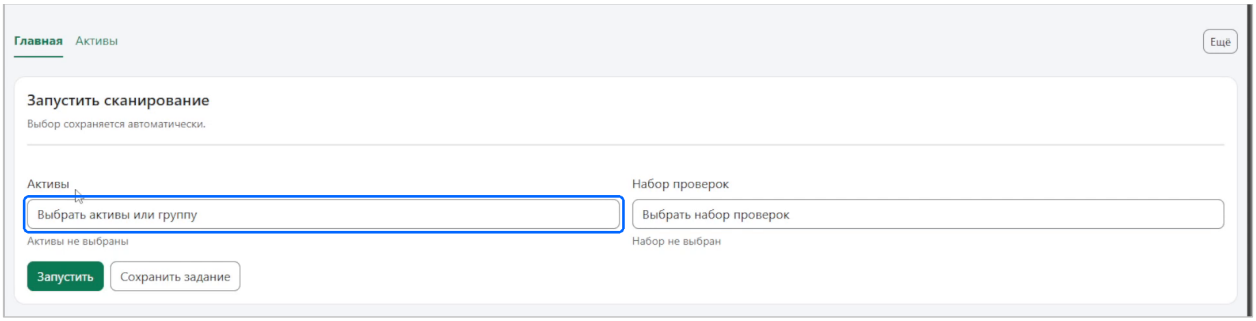


Рисунок 22 – Поле выбора активов

2) В окне «Выберите активы» отметьте нужные активы. Для поиска используйте строку поиска и фильтры «Тип», «Объекты», «Происхождение», «Задание». Нажмите **«Готово»**.

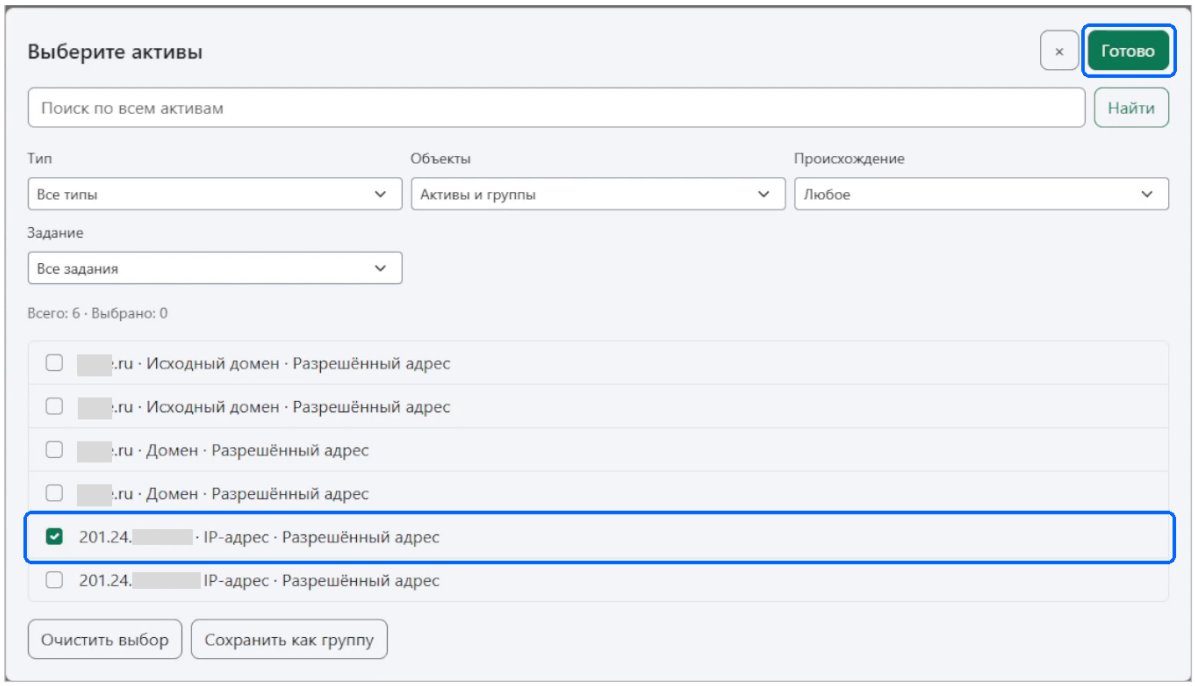


Рисунок 23 – Выбор активов для сканирования

3) Нажмите на поле **«Выбрать набор проверок»**, отметьте набор и нажмите **«Готово»**.

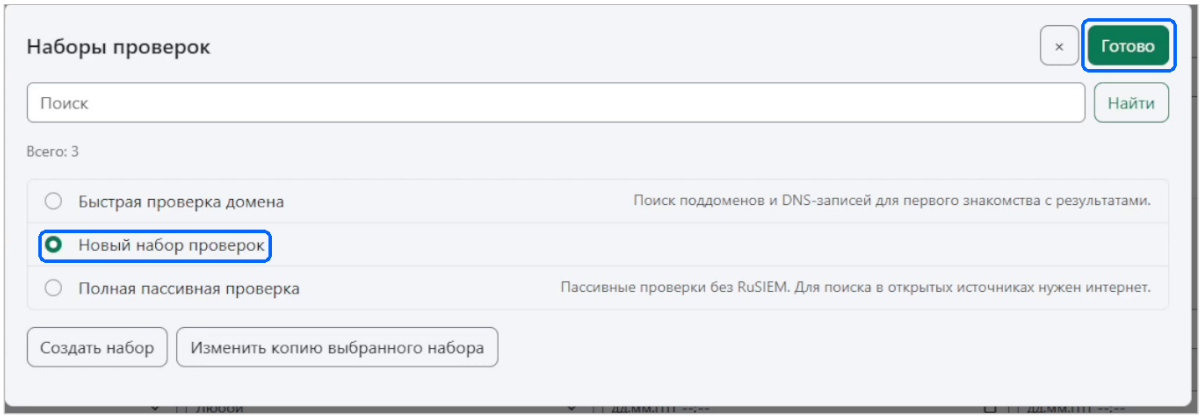


Рисунок 24 – Выбор набора проверок

4) Нажмите **«Запустить»**.

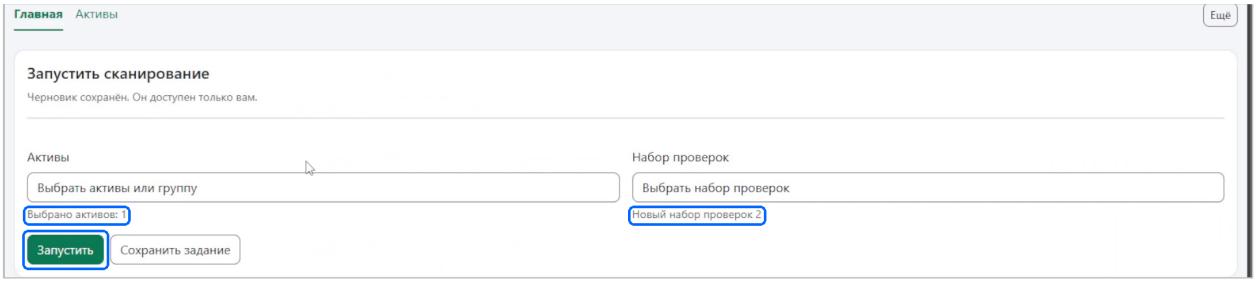


Рисунок 25 – Запуск сканирования

Кнопка «Очистить выбор» в окне выбора активов снимает все отметки. Кнопка «Сохранить как группу» сохраняет выбранные активы как группу для следующих запусков. Кнопка «Изменить копию выбранного набора» в окне «Наборы проверок» открывает копию отмеченного набора в редакторе.

Результат. Под полями «Активы» и «Набор проверок» отображаются выбранные активы и название набора. После нажатия «Запустить» открывается страница запуска.

6.5. Ход выполнения запуска

В верхней части страницы запуска указаны название задания, состояние, время запуска, количество исходных активов, выполненных проверок и ошибок. В блоке **«Ход запуска»** отображаются индикатор выполнения и счётчики «Выполнено», «Ошибок» и «Найдено активов».

В блоке «Проверки на графе» показана цепочка проверок набора. Для каждой проверки выводится состояние «Ожидает», «Выполняется» или «Завершена». Длительность сканирования зависит от состава проверок и количества обнаруженных активов.

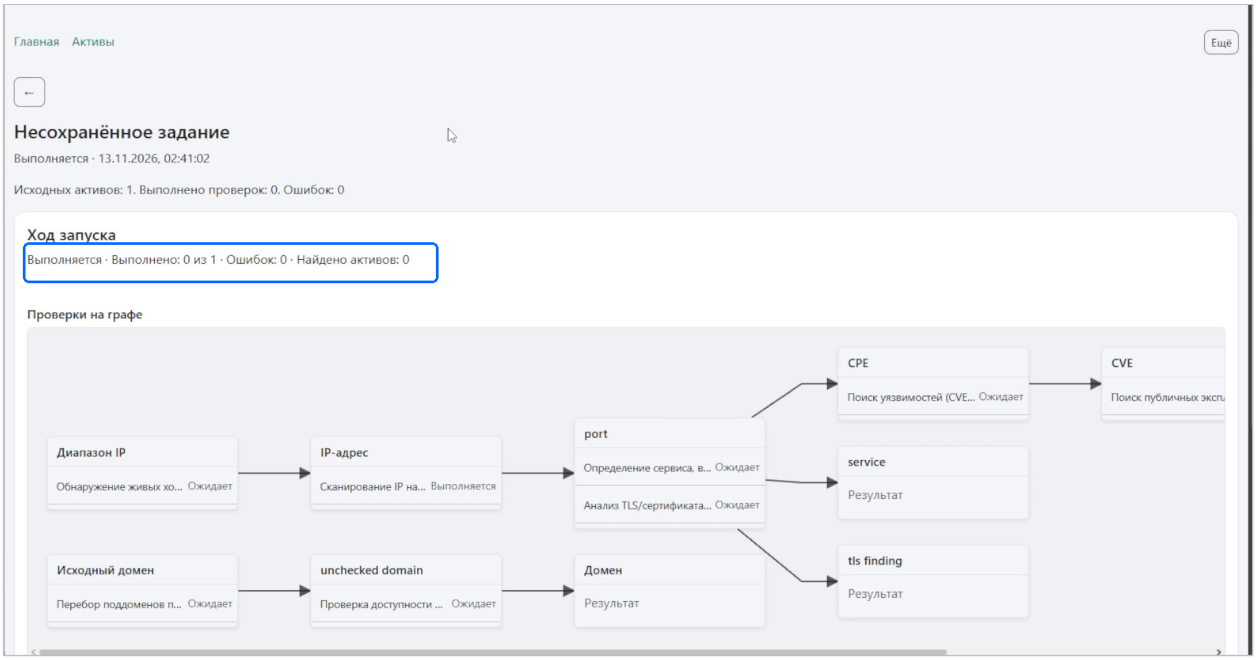


Рисунок 26 – Страница запуска в процессе выполнения

Результат. После завершения сканирования состояние меняется на «Завершён», индикатор показывает 100 %.

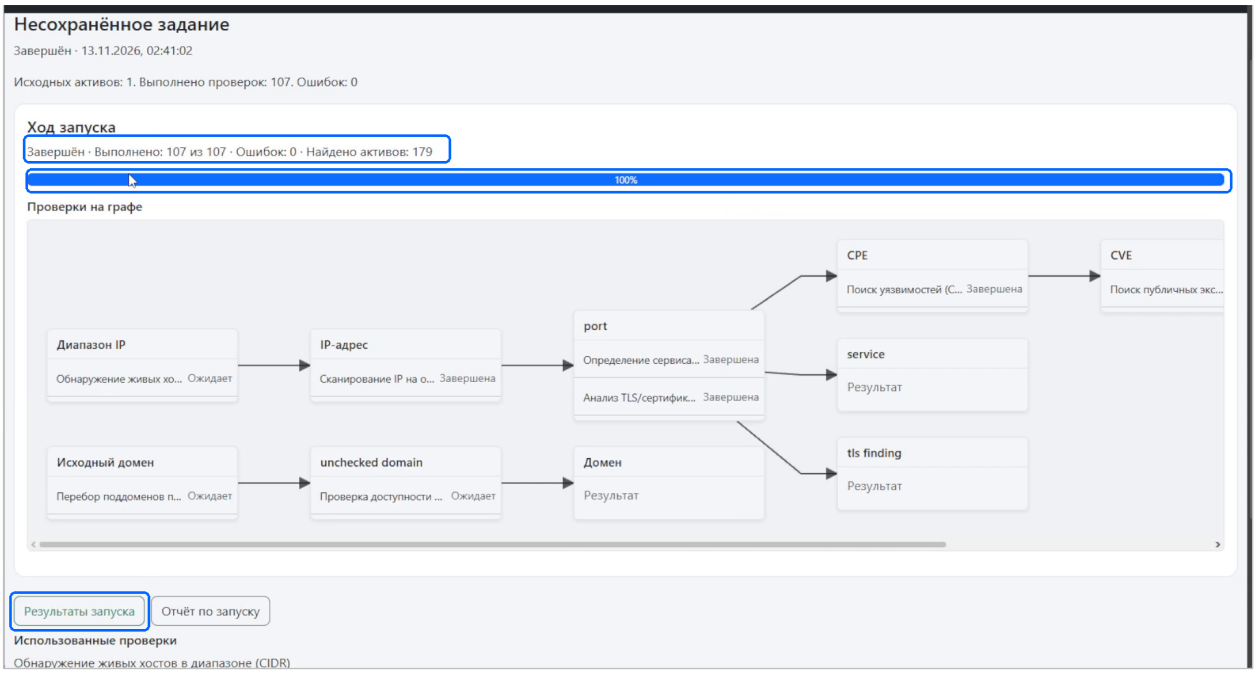


Рисунок 27 – Завершённый запуск

Страницу запуска можно открыть позднее из блока «История запусков» на главной странице проекта.

6.6. Остановка и повторный запуск

Под графом на странице запуска расположены кнопки **«Результаты запуска»** и **«Отчёт по запуску»**, перечень использованных проверок и кнопки управления запуском:

- «Сохранить задание» – сохранение активов и набора проверок как задания;
- «Повторить запуск» – новый запуск с теми же активами и набором проверок;
- «Остановить» – прерывание выполняемого сканирования.

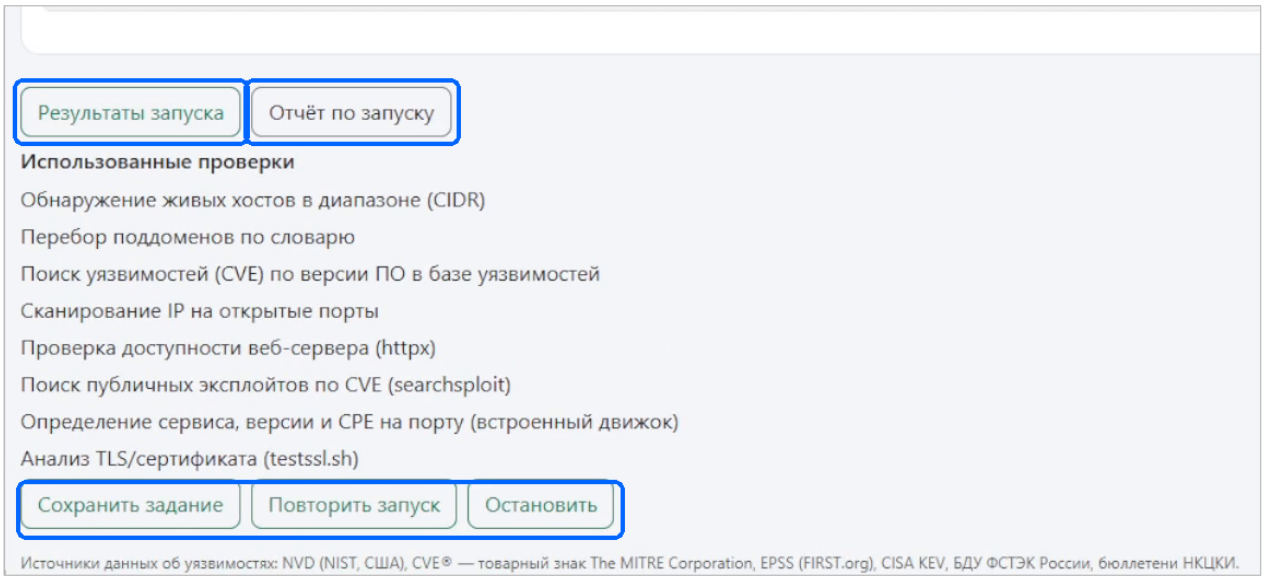


Рисунок 28 – Кнопки управления запуском

6.7. Результаты запуска

1) На странице запуска нажмите **«Результаты запуска»**.

Открывается вкладка «Активы» с панелью «Результаты запуска». В панели указан идентификатор запуска, ссылка **«Открыть запуск»** возвращает на страницу запуска. Для отбора служат строка «Поиск в результатах запуска» и фильтр «Тип актива», рядом с каждым типом указано количество найденных активов. Кнопка «Выбрать все результаты фильтра» отмечает все активы выбранного типа, счётчик «Всего / Выбрано» показывает число найденных и отмеченных активов. Панель закрывается кнопкой «Готово».

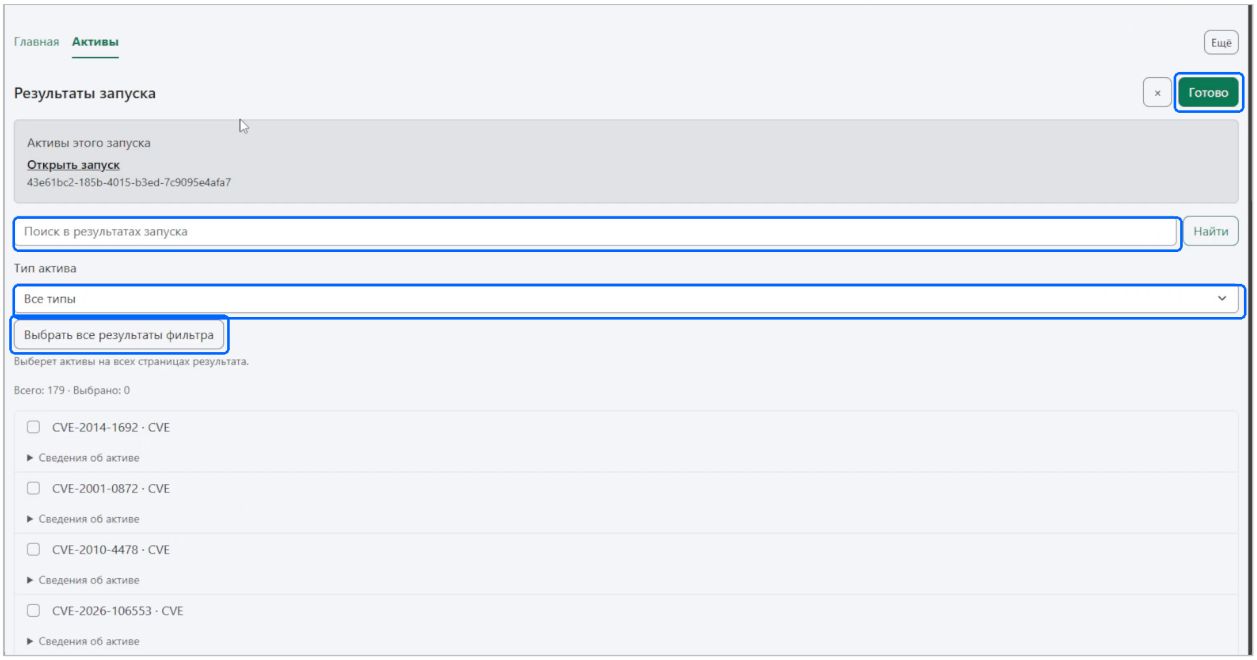


Рисунок 29 – Результаты запуска

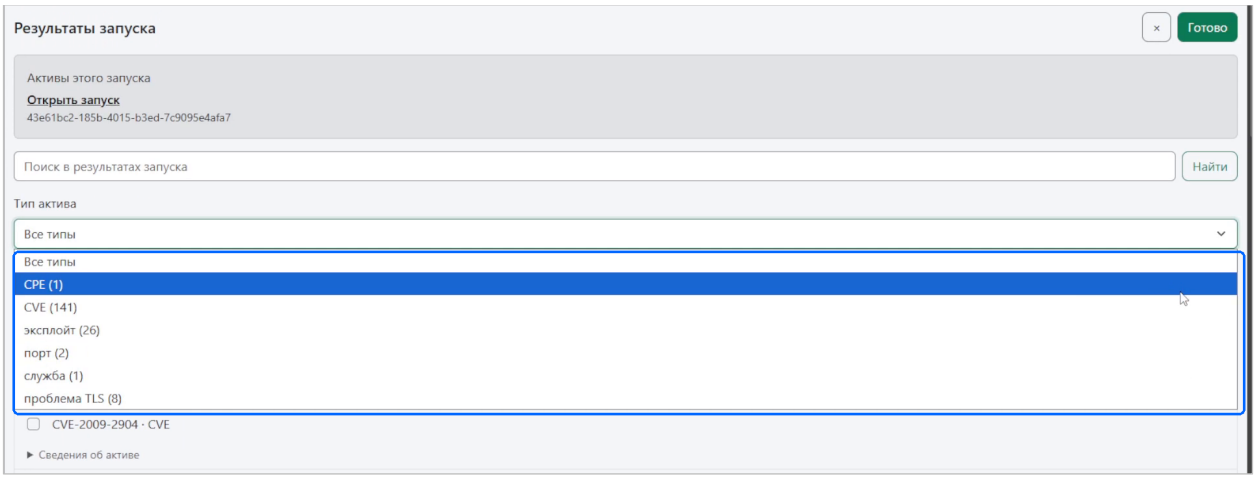


Рисунок 30 – Фильтр по типу актива

Подробные сведения об активе открываются нажатием на строку **«Сведения об активе»** под названием актива. Для уязвимости выводятся:

- cve_name – идентификатор CVE;
- base_score – оценка CVSS;
- cvss_version – версия методики CVSS;
- vector – вектор атаки;
- severity – уровень критичности;
- cwe – класс слабости;
- bdu – идентификатор в БДУ ФСТЭК России;

- has_fstec – наличие описания в БДУ ФСТЭК России;
- description – описание уязвимости.

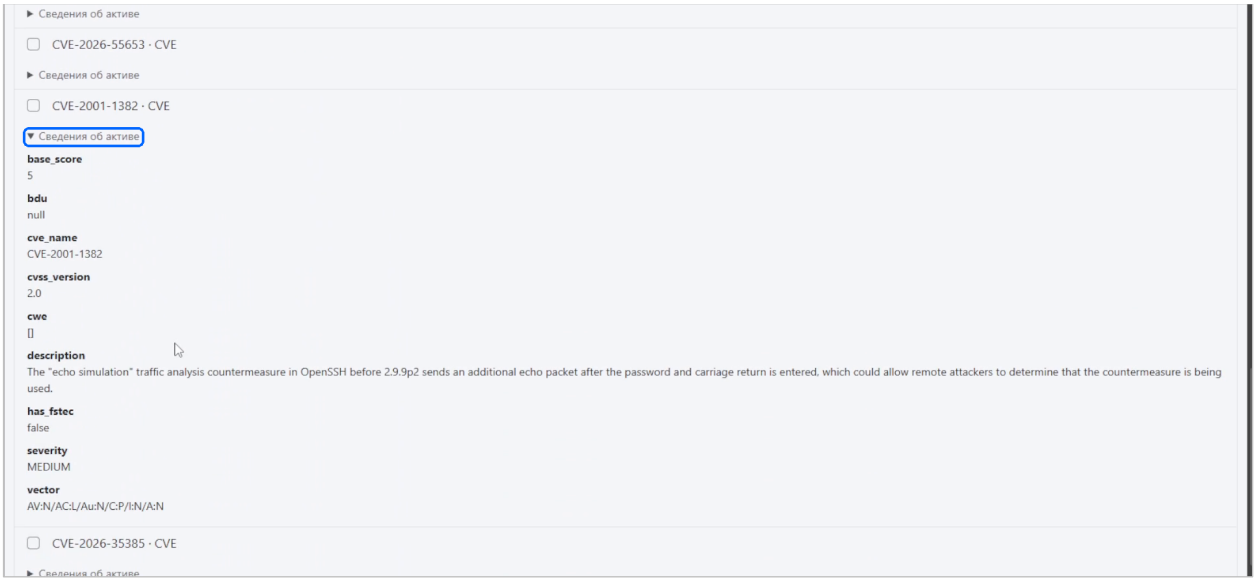


Рисунок 31 – Сведения об уязвимости

6.8. Задания

Задание сохраняется кнопкой **«Сохранить задание»** на главной странице проекта или на странице запуска.

1) На главной странице проекта нажмите **«Сохранить задание»**.
2) Введите название в поле **«Название задания»**.
3) Нажмите **«Сохранить»**.

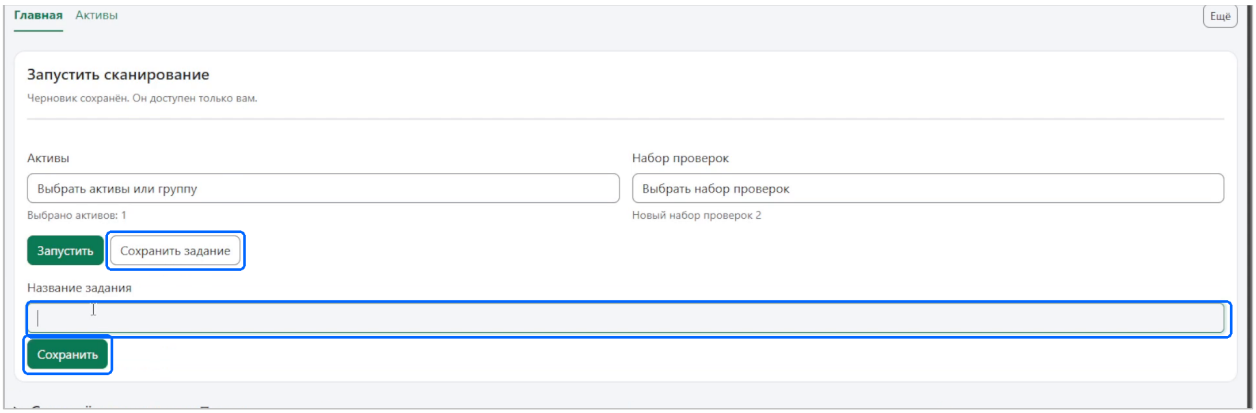


Рисунок 32 – Сохранение задания

Результат. Задание появляется в блоке «Сохранённые задания».

В блоке «Сохранённые задания» задания можно найти по названию и запустить кнопкой **«Запустить»**. Полный список заданий проекта с поиском находится на странице «Все задания».

Нажатие на название задания открывает его карточку. В карточке указаны количество исходных активов и состав проверок, доступны кнопки **«Запустить»**, **«История задания»** и **«Показать динамику»**. Кнопка **«Ещё»** открывает меню с пунктами «Изменить», «Сохранить копию», «В другой проект», «Расписание» и «Архивировать задание».

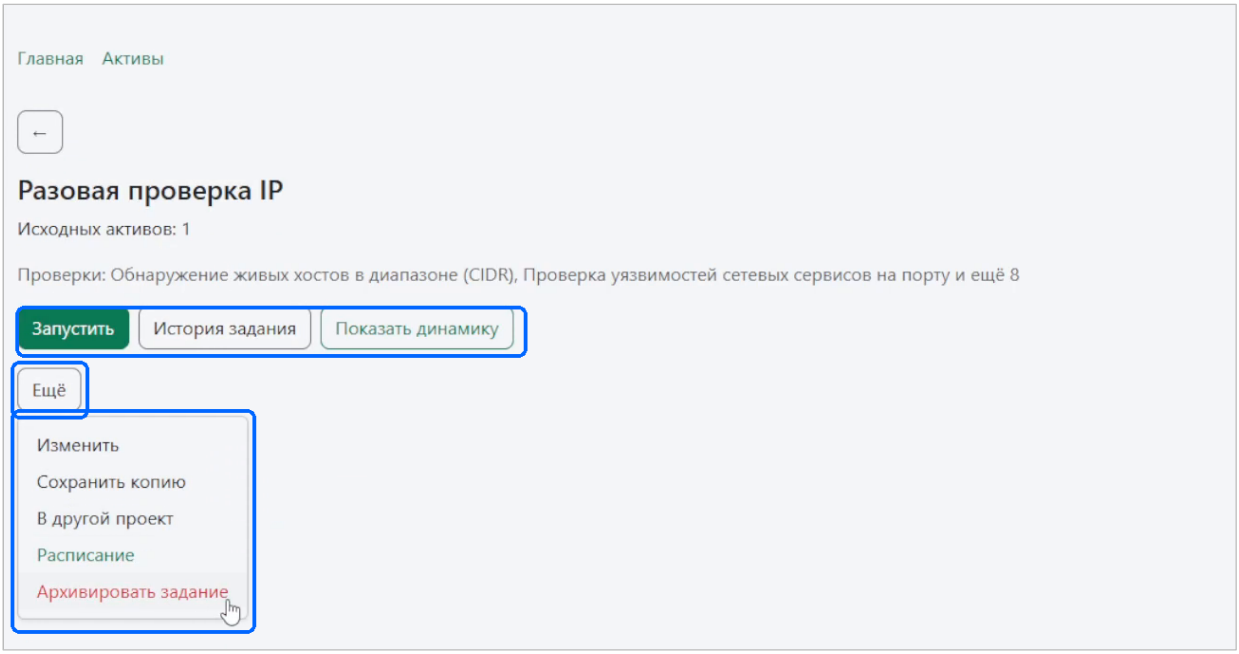


Рисунок 33 – Карточка задания

6.9. Расписание сканирования

Расписание задаётся для сохранённого задания. Все расписания проекта отображаются на странице «Расписания», которая открывается через **«Ещё»** → **«Расписания»**. Чтобы настроить расписание:

1) На странице «Расписания» нажмите ссылку **«Открыть сохранённые задания»**.

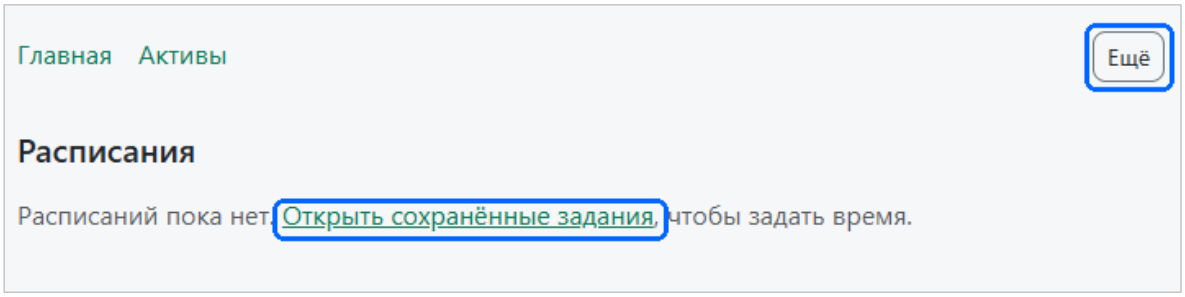


Рисунок 34 – Страница «Расписания» без настроенных расписаний

2) На странице «Все задания» выберите задание. Для поиска служат строка «Поиск» и кнопка «Найти».

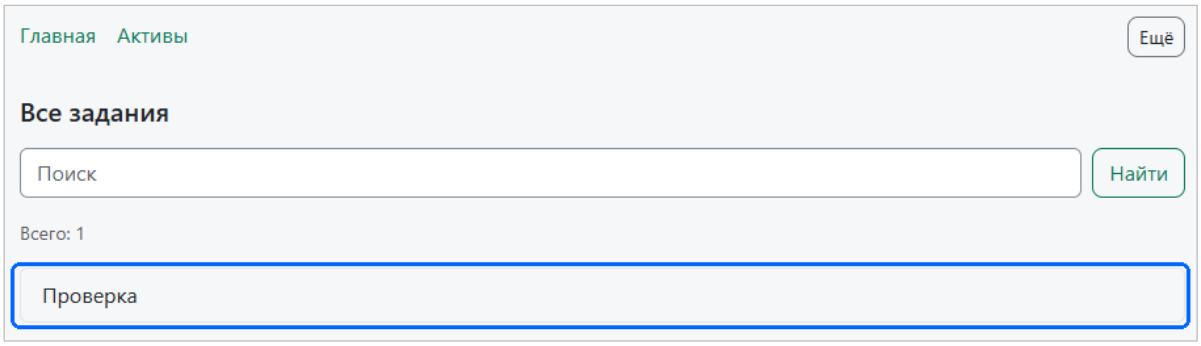


Рисунок 35 – Страница «Все задания»

3) В карточке задания нажмите **«Ещё»** и выберите **«Расписание»**.
4) В форме «Расписание» выберите частоту запуска в поле **«Как часто»**: «Каждый день», «По рабочим дням», «Раз в неделю» или «Другое расписание». При выборе «Раз в неделю» появляется поле «День недели».
5) Укажите время запуска в поле **«Время»** и при необходимости часовой пояс в поле «Часовой пояс».
6) При необходимости ограничьте длительность сканирования в поле «Остановить через, часов (необязательно)».
7) Оставьте отметку «Расписание включено» и нажмите **«Сохранить расписание»**.

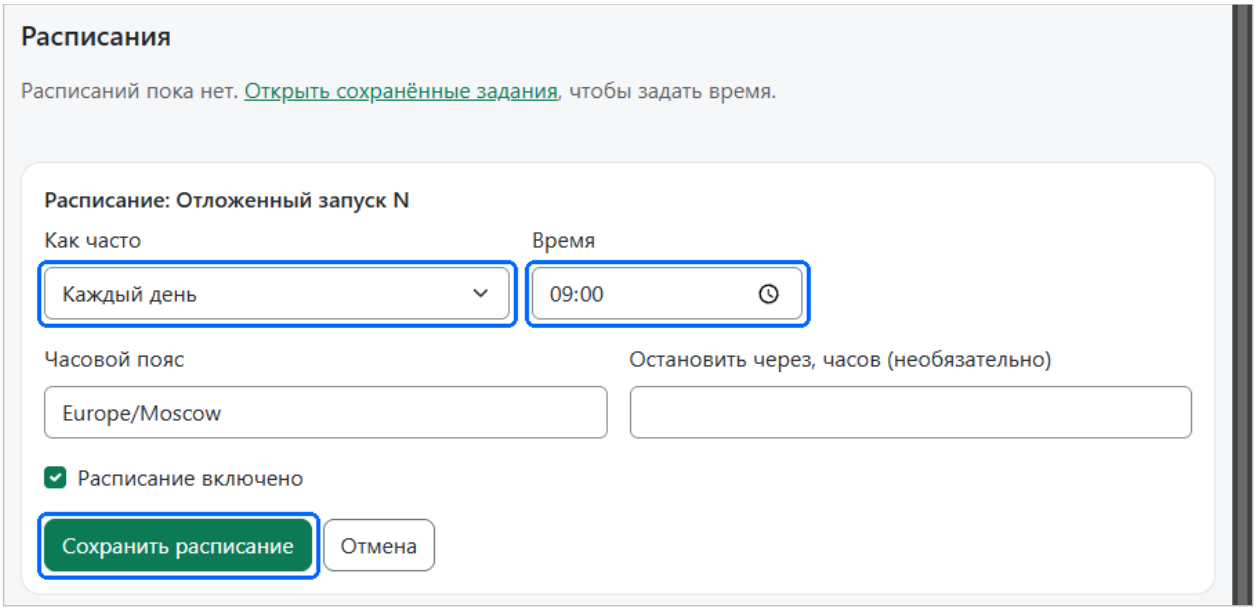


Рисунок 36 – Настройка расписания

Результат. Задание появляется на странице «Расписания» с состоянием «Включено» и датой следующего выполнения.

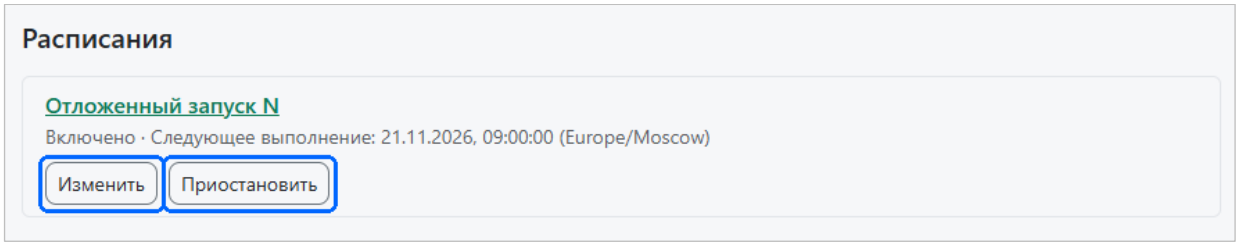


Рисунок 37 – Настроенное расписание

Кнопка **«Изменить»** открывает форму расписания для редактирования, кнопка **«Приостановить»** временно отключает запуск по расписанию.

6.10. История запусков

История запусков проекта отображается на главной странице в блоке «История запусков». В таблице указаны задание, время начала, состояние и способ запуска. Для отбора служат строка поиска и фильтры «Состояние», «Запуск», «С» и «По». Ссылка «Показать все запуски» открывает полный список.

История отдельного задания открывается кнопкой **«История задания»** в карточке задания. Дополнительные условия отбора находятся в блоке **«Фильтры истории»**.

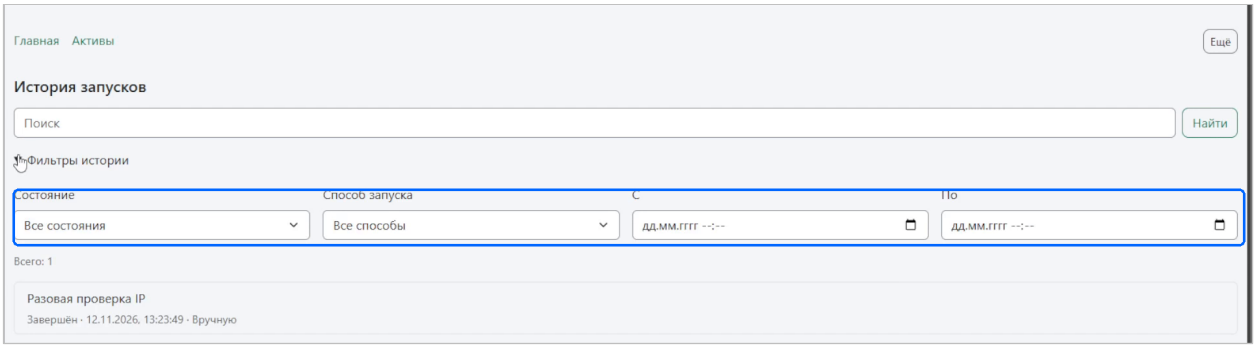


Рисунок 38 – История запусков задания

7. Работа с отчётами

7.1. Виды отчётов

Отчёты доступны на главной странице проекта в блоке **«Отчёты»**. Нажмите на название блока, чтобы развернуть его.

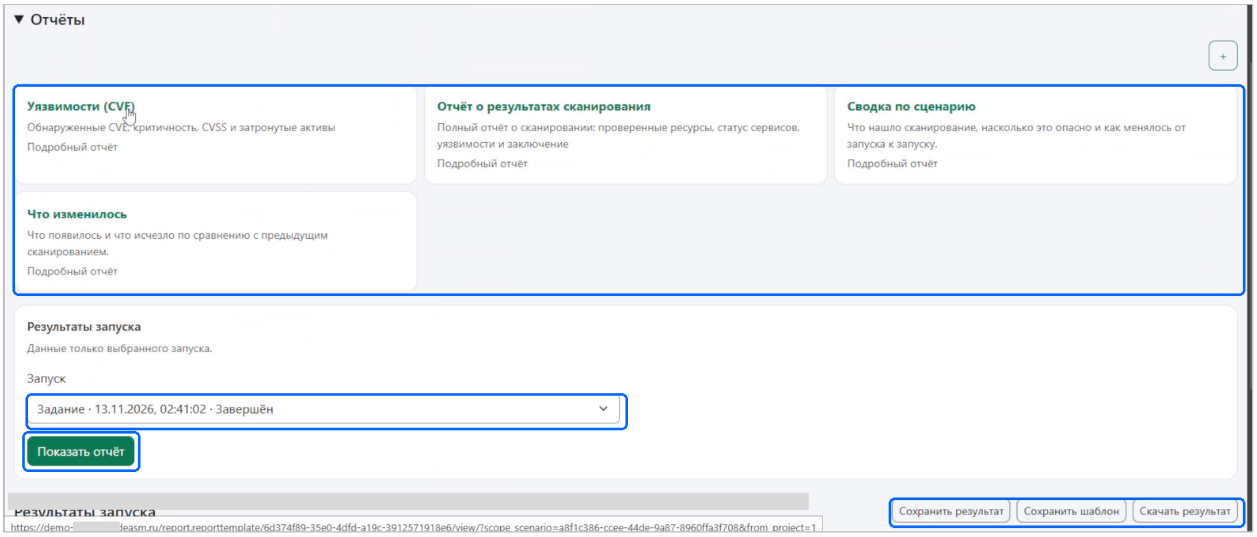


Рисунок 39 – Блок «Отчёты»

Отчёт	Содержание
Уязвимости (CVE)	Обнаруженные CVE, критичность, CVSS и затронутые активы.
Отчёт о результатах сканирования	Полный отчёт о сканировании: проверенные ресурсы, статус сервисов, уязвимости и заключение.
Сводка по сценарию	Что нашло сканирование, насколько это опасно и как менялось от запуска к запуску.
Что изменилось	Что появилось и что исчезло по сравнению с предыдущим сканированием.

Отчёт открывается нажатием на его название. Страницы отчётов устроены одинаково:

- в верхней части расположены параметры отчёта и кнопка **«Применить»**, которая обновляет данные по выбранным параметрам;
- в поле «Запуск» выбирается запуск, по которому строится отчёт. Пункт «Все запуски проекта» объединяет данные всех запусков;

- кнопка **«Экспортировать в PDF»** сохраняет отчёт на компьютер в формате PDF;
- кнопка с изображением луны переключает светлое и тёмное оформление отчёта;
- кнопка **«К отчётам проекта»** возвращает к списку отчётов.

7.2. Уязвимости (CVE)

Отчёт содержит таблицу «Обнаруженные уязвимости» с колонками «Уязвимость», «Критичность», «CVSS», «Уязвимые активы» и «Программное обеспечение». Уязвимости упорядочены по убыванию оценки CVSS.

Параметры отчёта:

- «Запуск»;
- «Минимальный балл CVSS (0–10)» – в отчёт попадают уязвимости с оценкой не ниже указанной;
- «Только CVE с описанием из ФСТЭК» – значения «Не задано», «Да», «Нет».

1) В блоке «Отчёты» нажмите **«Уязвимости (CVE)»**.
2) Выберите запуск в поле **«Запуск»** и при необходимости задайте остальные параметры.
3) Нажмите **«Применить»**.
4) Для сохранения отчёта нажмите **«Экспортировать в PDF»**.

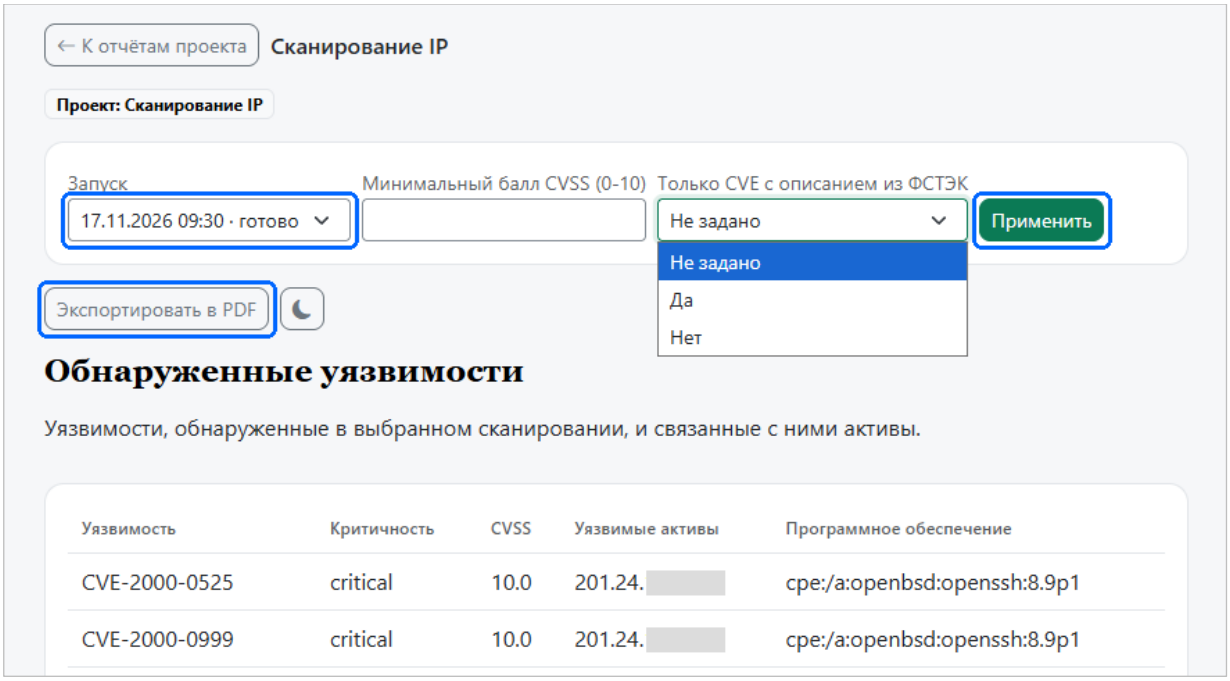


Рисунок 40 – Отчёт «Уязвимости (CVE)»

Результат. Отчёт сохраняется на компьютер в формате PDF.

7.3. Отчёт о результатах сканирования

Отчёт оформлен как официальный документ о результатах сканирования и анализа защищённости информационных ресурсов. В титульной части указаны заказчик, исполнитель, объект сканирования и дата проведения. Отчёт содержит разделы:

- «Введение»;
- «Общие положения»;
- «Этапы проведения работ» – время начала и окончания сканирования;
- «Описание методики оценки» – уровни критичности по базовой оценке CVSS;
- «Результаты анализа» – сетевые и веб-ресурсы, сведения об уязвимостях сервисов и карточки обнаруженных уязвимостей с описанием, оценкой CVSS, идентификаторами CVE и БДУ ФСТЭК России, уязвимыми активами и CWE;
- «Заключение» – количество учтённых ресурсов и сводная оценка критичности по сервисам.

Кроме параметров «Запуск», «Минимальный балл CVSS (0–10)» и «Только CVE с описанием из ФСТЭК», в отчёте доступно поле **«Исключить IP-адреса из отчёта»**. В нём через запятую указываются IP-адреса, которые не должны попасть в отчёт. Если поле пустое, в отчёт включаются все адреса.

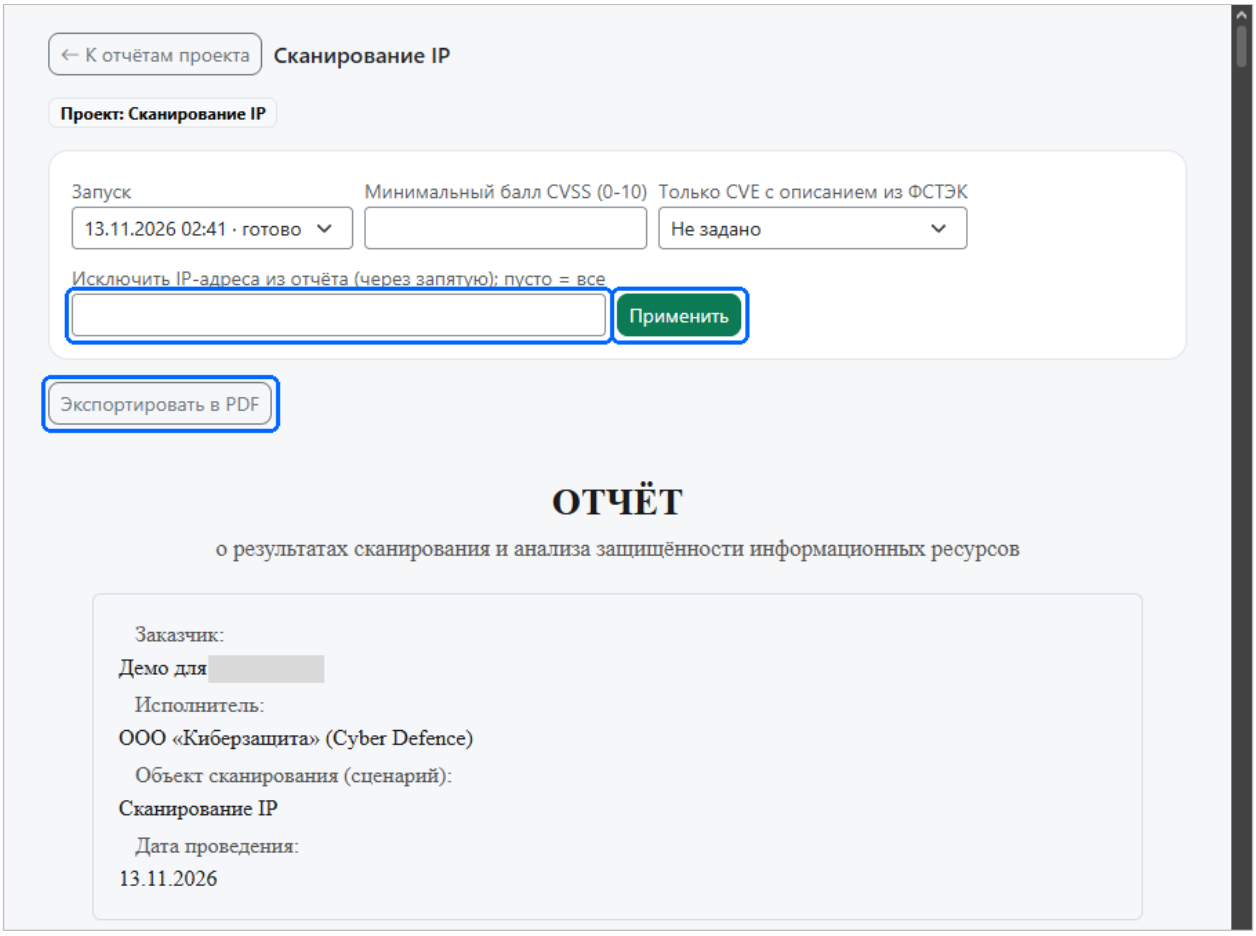
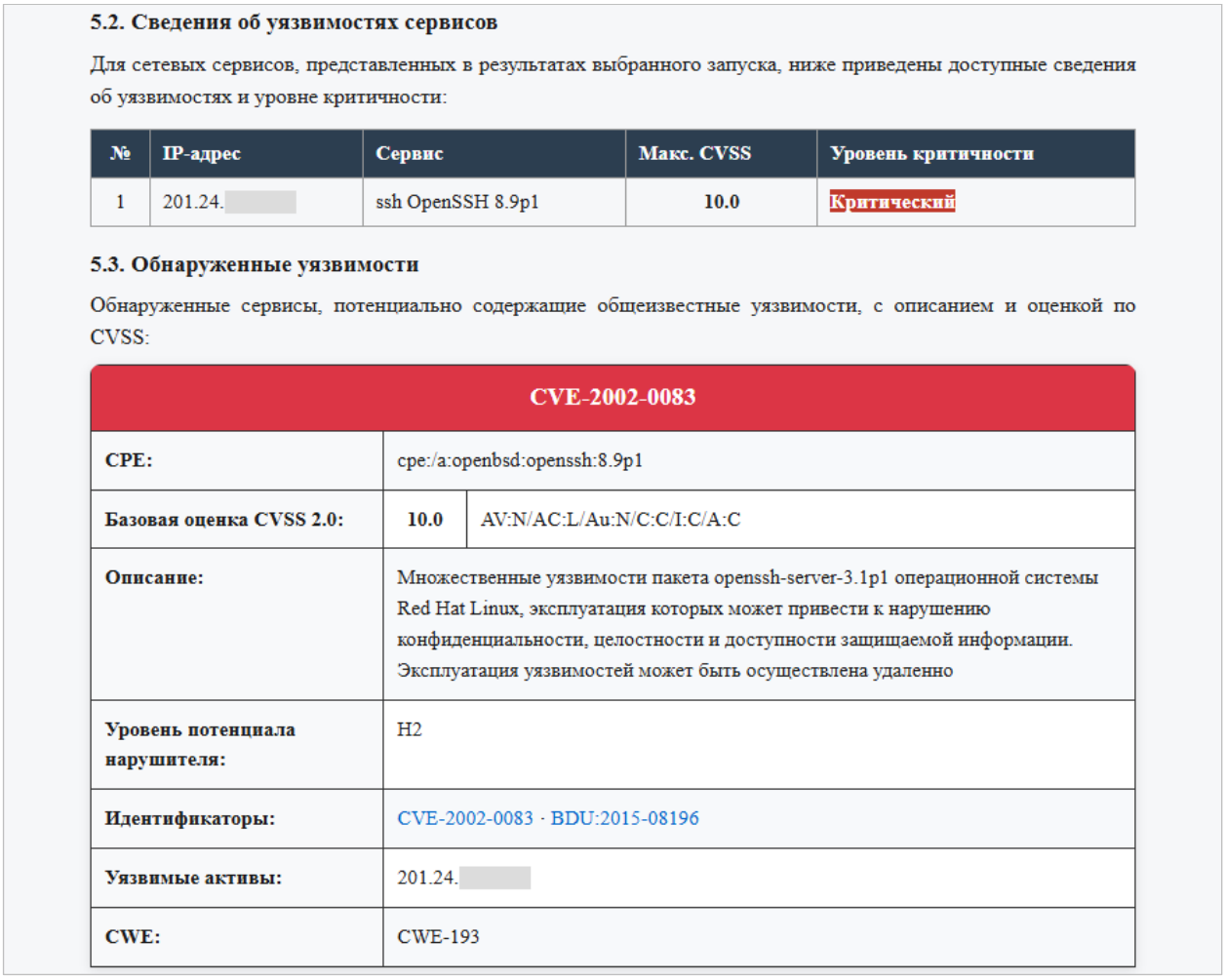


Рисунок 41 – Отчёт о результатах сканирования



5.2. Сведения об уязвимостях сервисов

Для сетевых сервисов, представленных в результатах выбранного запуска, ниже приведены доступные сведения об уязвимостях и уровне критичности:

№	IP-адрес	Сервис	Макс. CVSS	Уровень критичности
1	201.24.	ssh OpenSSH 8.9p1	10.0	Критический

5.3. Обнаруженные уязвимости

Обнаруженные сервисы, потенциально содержащие общеизвестные уязвимости, с описанием и оценкой по CVSS:

CVE-2002-0083		
CPE:	cpe:/a:openbsd:openssh:8.9p1	
Базовая оценка CVSS 2.0:	10.0	AV:N/AC:L/Au:N/C:C/I:C/A:C
Описание:	Множественные уязвимости пакета openssh-server-3.1p1 операционной системы Red Hat Linux, эксплуатация которых может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации. Эксплуатация уязвимостей может быть осуществлена удаленно	
Уровень потенциала нарушителя:	H2	
Идентификаторы:	CVE-2002-0083 · BDU:2015-08196	
Уязвимые активы:	201.24.	
CWE:	CWE-193	

Рисунок 42 – Сведения об уязвимостях в отчёте о результатах сканирования

7.4. Сводка по сценарию

Отчёт показывает общую картину по сканированию. В верхней части выводятся показатели: число уникальных уязвимостей, число критических уязвимостей, требующих реакции в первую очередь, число узлов в результатах и оценка риска с учётом эксплуатируемости.

Ниже расположены диаграммы «Уязвимости на активах по критичности» и «Уязвимости по уровню критичности», график «Динамика за период» и таблица «Список угроз» с колонками «Проблема», «Где», «Тип», «Дата», «Критичность» и «Состояние».

Параметры отчёта:

- «Запуск»;
- «Сколько строк показывать» – число строк в таблице «Список угроз», по умолчанию 50;
- «Только нерешённые проблемы»;

- «Показывать последние N сканирований» – число сканирований на диаграммах и графике, по умолчанию 30.

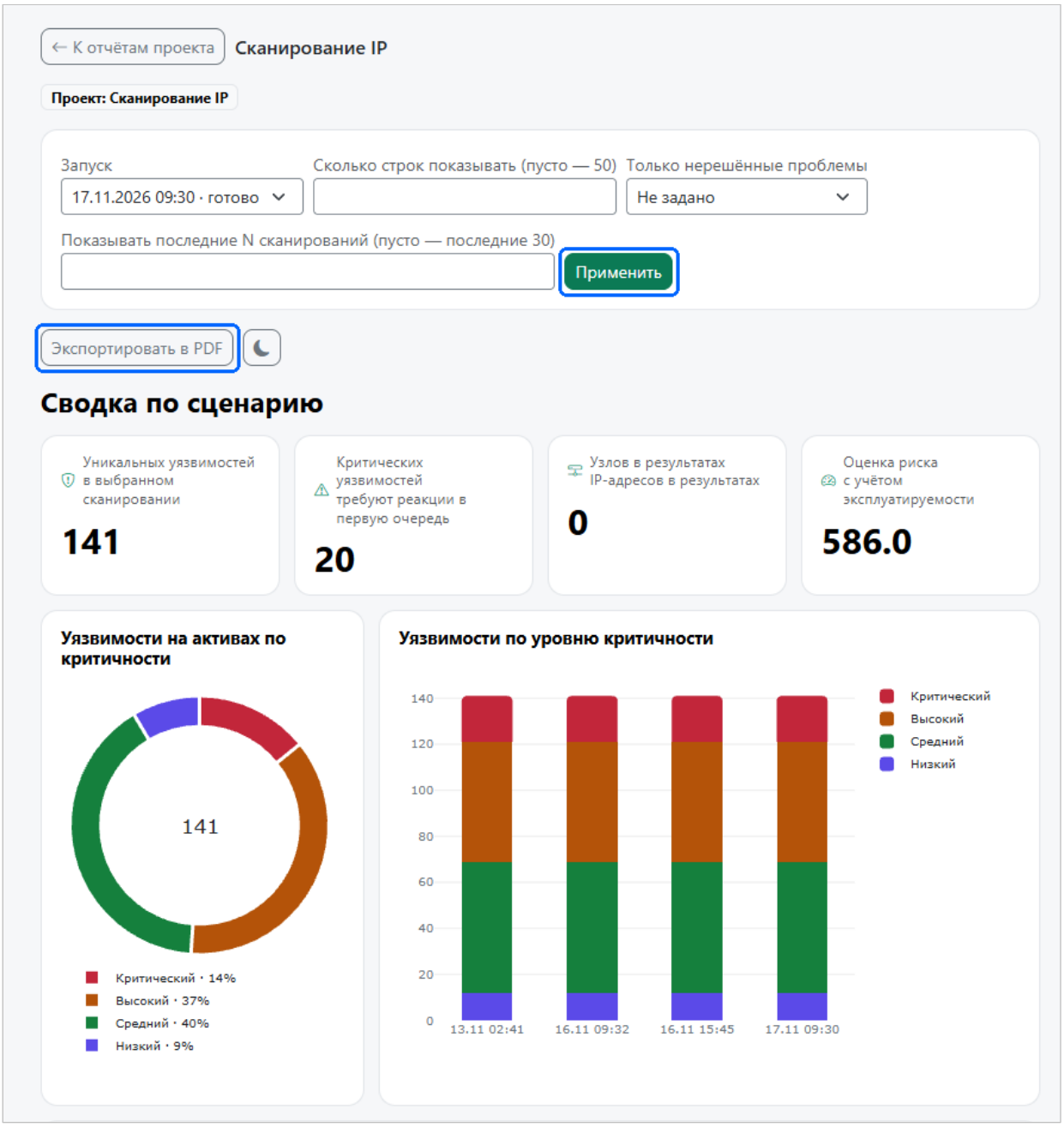


Рисунок 43 – Отчёт «Сводка по сценарию»

7.5. Что изменилось

Отчёт сравнивает выбранный запуск с предыдущим сканированием. Показатели «Появилось», «Исчезло» и «Осталось» показывают число активов, которые появились, пропали или были найдены в обоих сканированиях. В таблице «Изменения» перечислены изменение, тип и значение каждого актива.

Параметры отчёта:

- «Запуск»;
- «Только изменения (без того, что осталось как было)»;
- «Ограничить одним типом активов» – если поле пустое, в отчёт включаются все типы.

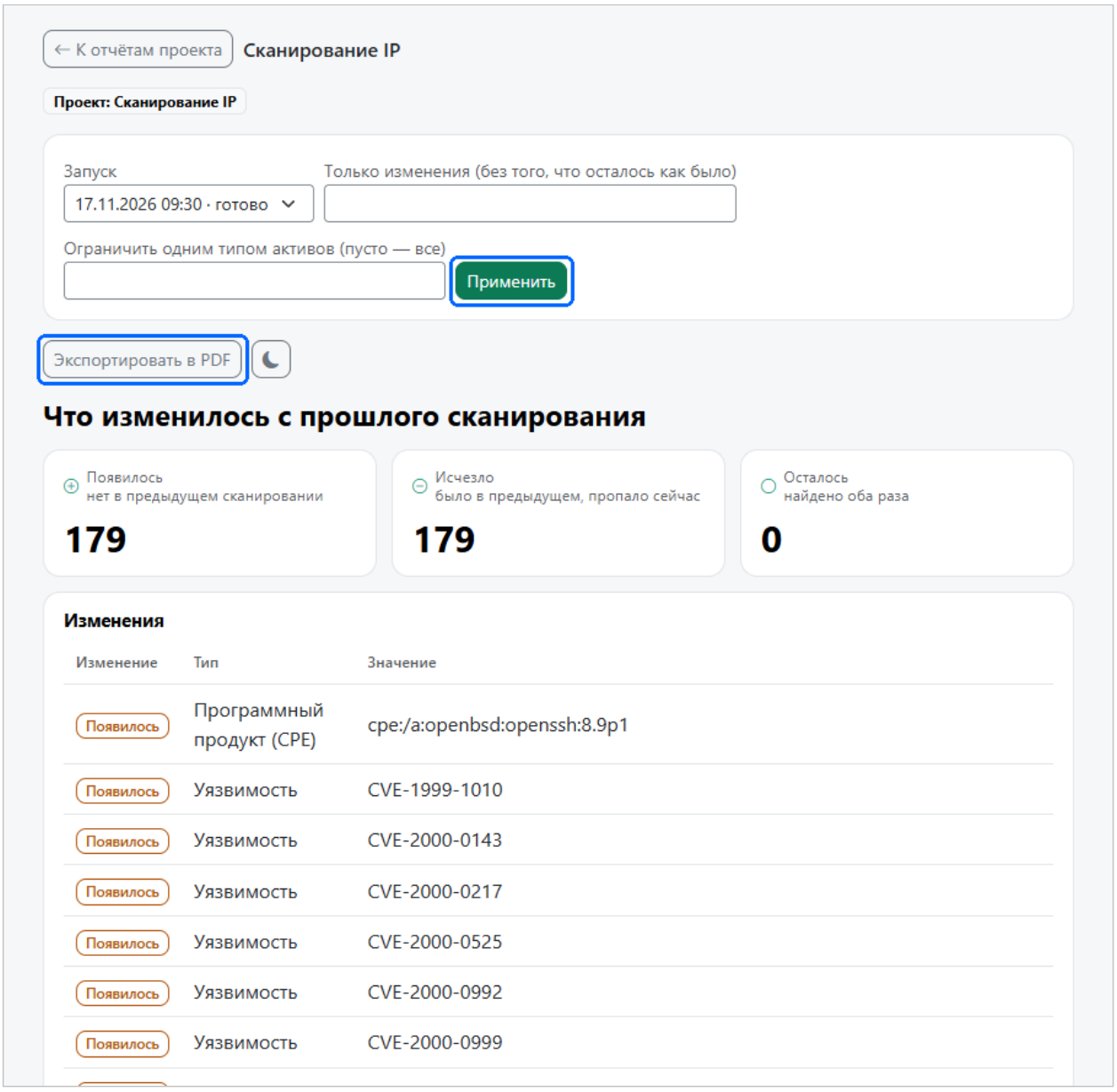


Рисунок 44 – Отчёт «Что изменилось»

7.6. Дополнительные отчёты

Кроме четырёх основных отчётов, в блок «Отчёты» можно добавить готовые отчёты «Результаты запуска», «Краткое сравнение запусков», «Динамика задания» и «Обзор заданий». Для этого нажмите кнопку **«+»** в правом верхнем углу блока и выберите нужный отчёт в разделе «Готовые отчёты».

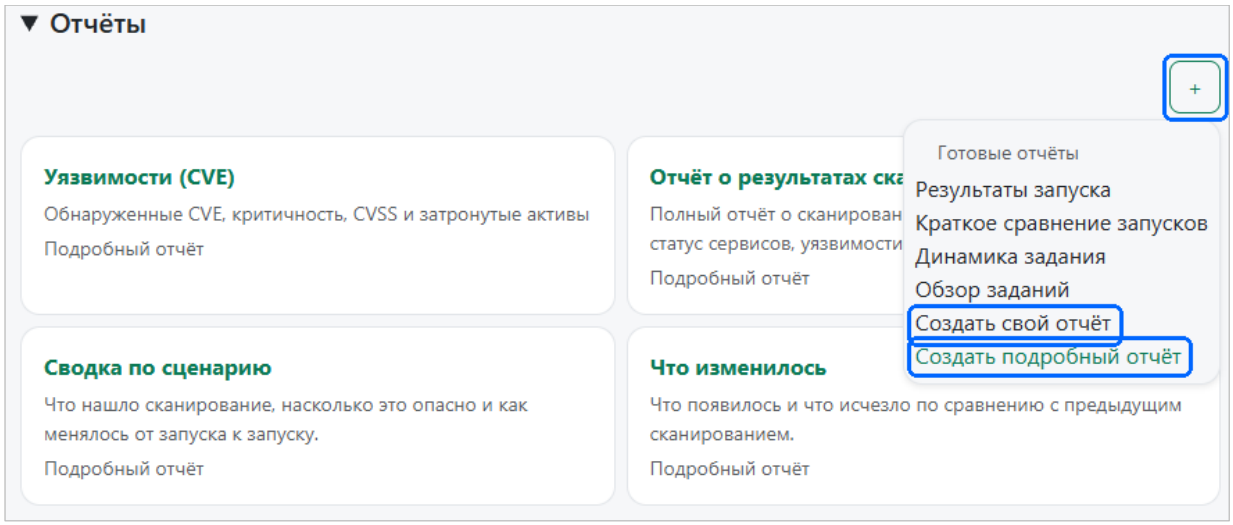


Рисунок 45 – Меню кнопки «+» в блоке «Отчёты»

Добавленный отчёт отображается в блоке «Отчёты» отдельной карточкой. Нажатие на название карточки открывает параметры отчёта. Чтобы убрать отчёт из блока, нажмите **«Ещё»** на карточке и выберите **«Убрать со страницы»**.

Результаты запуска

Отчёт показывает данные только выбранного запуска.

1) Выберите запуск в поле **«Запуск»**.
2) Нажмите **«Показать отчёт»**.

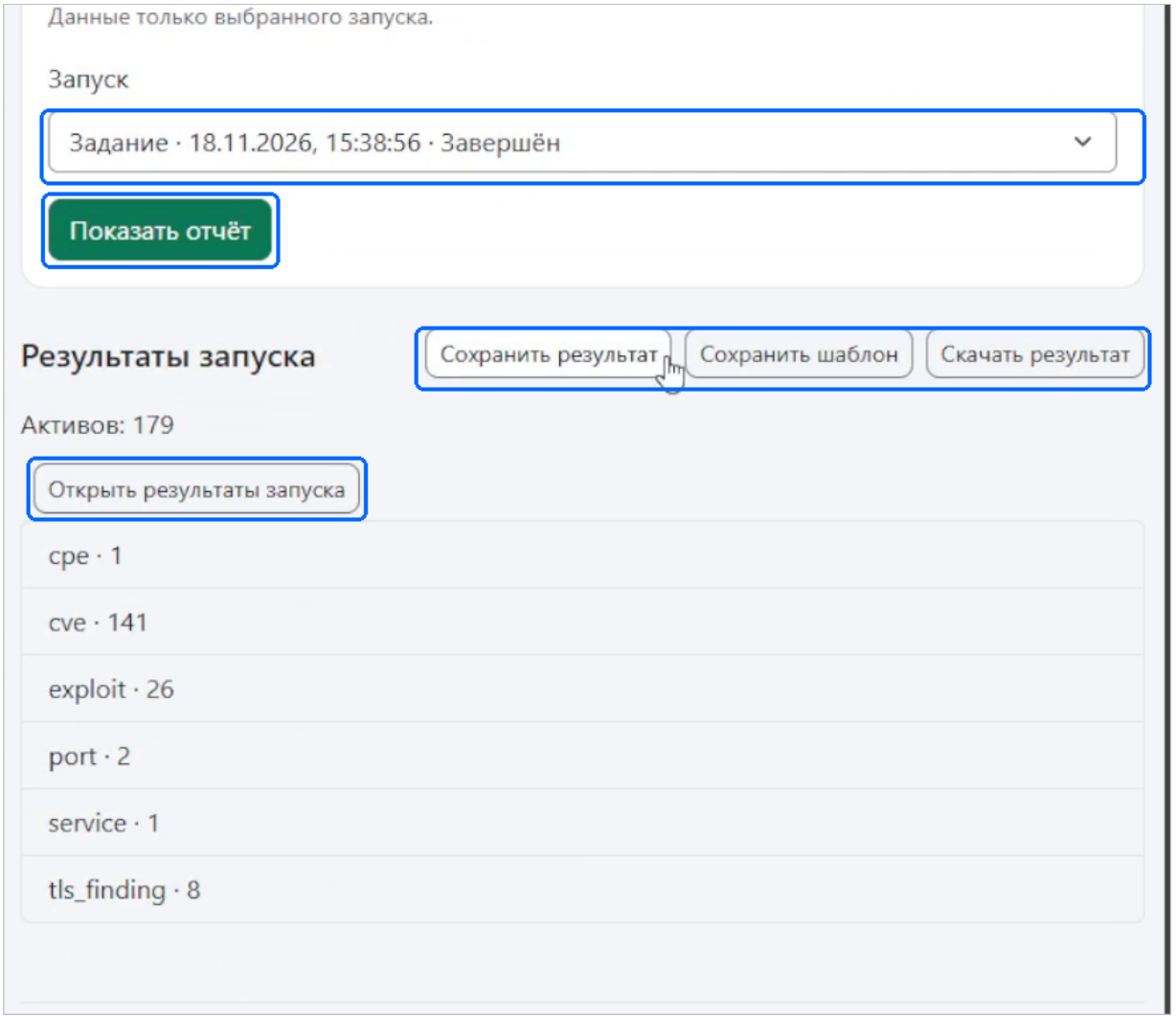


Рисунок 46 – Отчёт «Результаты запуска»

Выводится количество активов каждого типа, найденных при запуске. Кнопка «Открыть результаты запуска» открывает перечень активов. Для работы с результатом доступны кнопки:

- «Сохранить результат» – сохранение результата под заданным названием;
- «Сохранить шаблон» – создание собственного отчёта на основе результатов, описано в разделе «Шаблоны отчётов»;
- «Скачать результат» – выгрузка результата в файл формата JSON.

Чтобы сохранить результат, нажмите **«Сохранить результат»**, введите название в поле «Название сохранённого результата» и нажмите **«Сохранить»**.

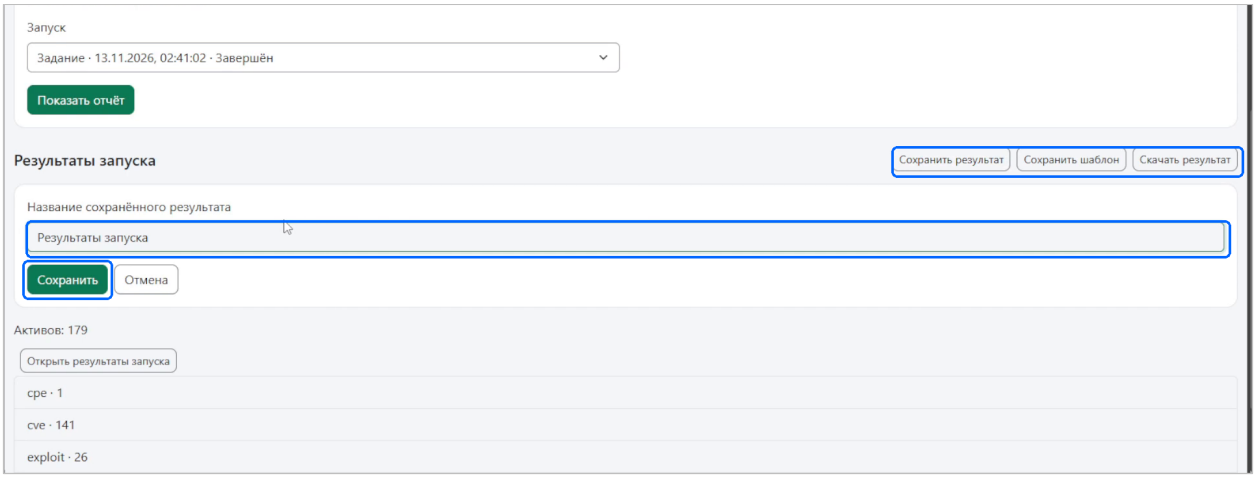


Рисунок 47 – Сохранение результата запуска

Результат. Результат появляется в списке «Сохранённые результаты». Сохранённый результат удаляется кнопкой «Удалить» с подтверждением.

Краткое сравнение запусков

Отчёт сравнивает два завершённых запуска. При разном охвате запусков отсутствие объекта не считается устранением.

1) Выберите запуск в поле **«Базовый запуск»**.
2) Выберите запуск для сравнения в поле **«Новый запуск»**.
3) Нажмите **«Показать отчёт»**.

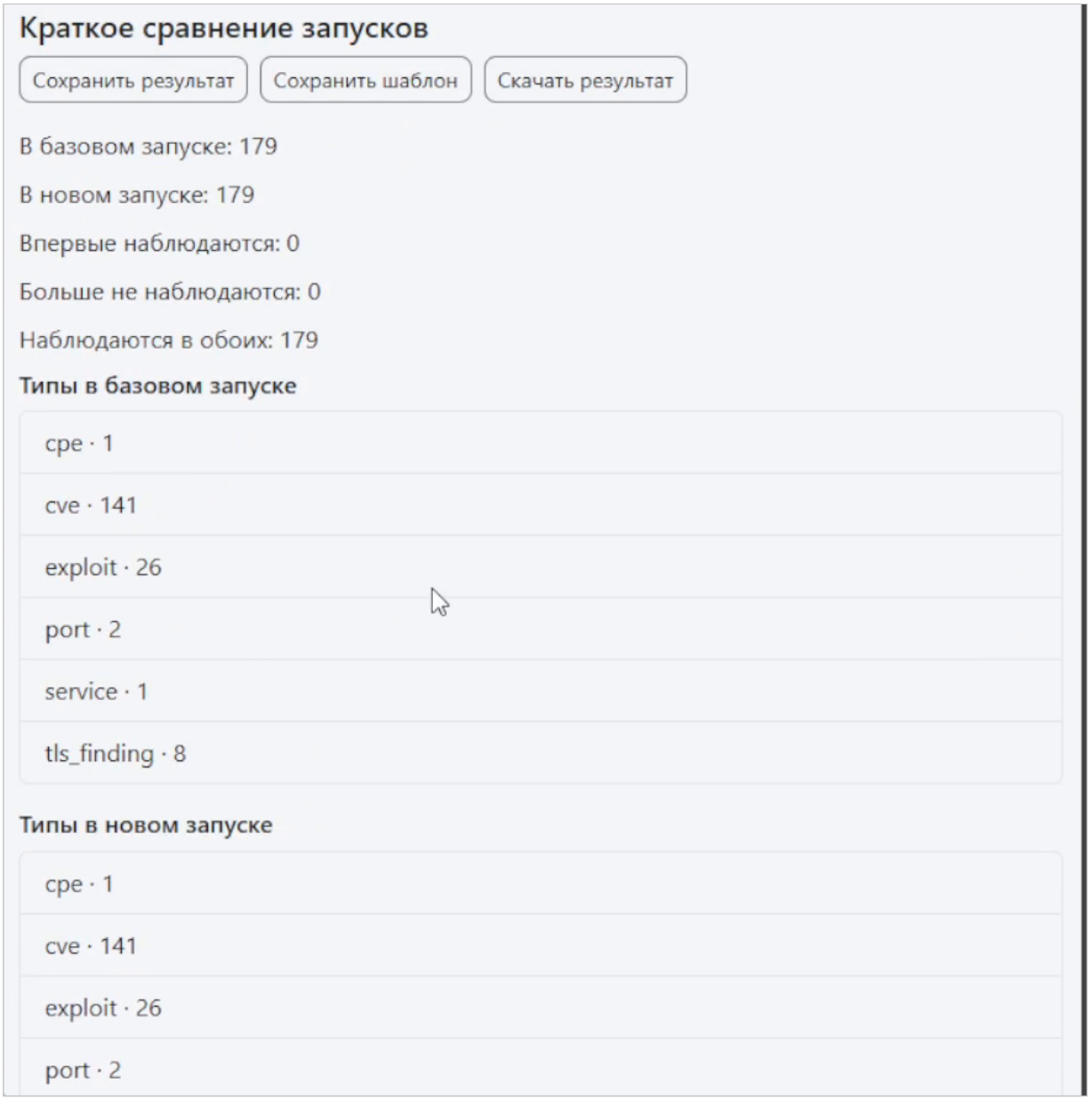


Рисунок 48 – Отчёт «Краткое сравнение запусков»

В отчёте указаны количество активов в базовом и новом запуске, число активов, которые наблюдаются впервые, больше не наблюдаются и наблюдаются в обоих запусках, а также количество активов каждого типа в обоих запусках. Кнопки «Сохранить результат», «Сохранить шаблон» и «Скачать результат» работают так же, как в отчёте «Результаты запуска».

Динамика задания

Отчёт показывает завершённые запуски выбранного задания.

1) Выберите задание в поле **«Задание»**.
2) При необходимости ограничьте период в полях «С» и «По».
3) Нажмите **«Показать отчёт»**.

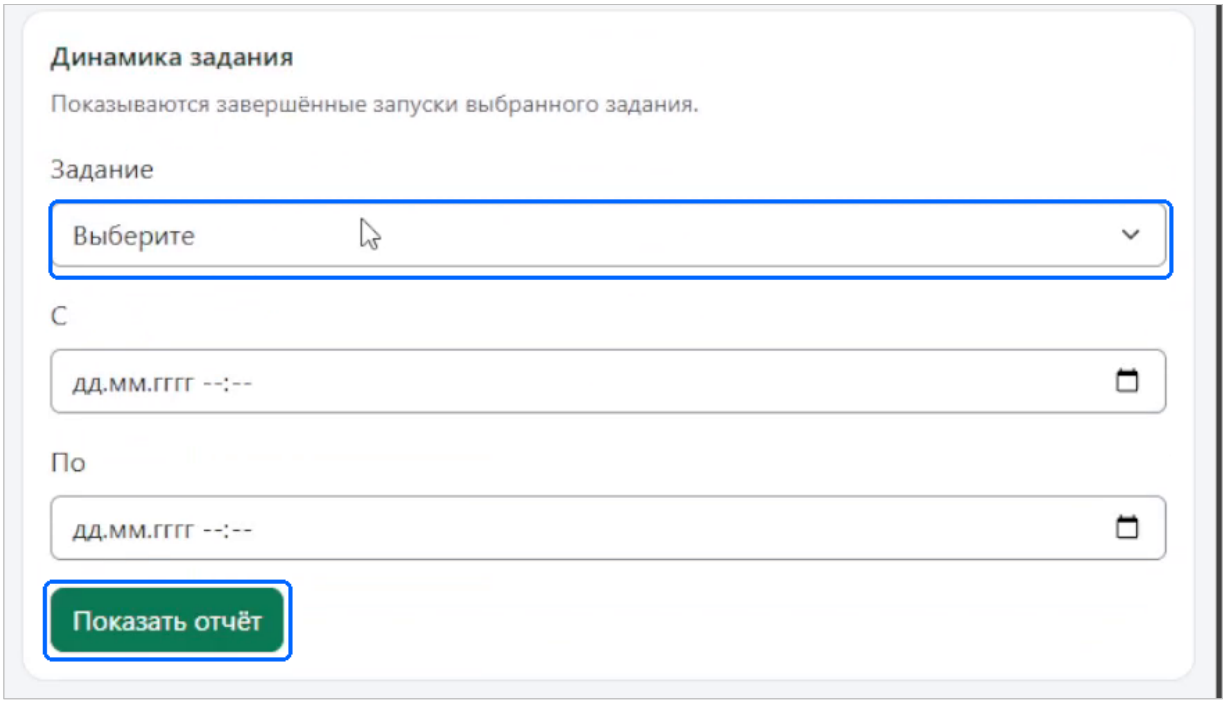


Рисунок 49 – Параметры отчёта «Динамика задания»

Обзор заданий

Отчёт объединяет результаты нескольких заданий. Можно взять последний завершённый запуск каждого задания или выбрать конкретные запуски.

1) Отметьте задания в списке «Задания».
2) Выберите вариант в поле «Какие запуски включить», например «Последний завершённый запуск каждого задания».
3) Нажмите **«Показать отчёт»**.

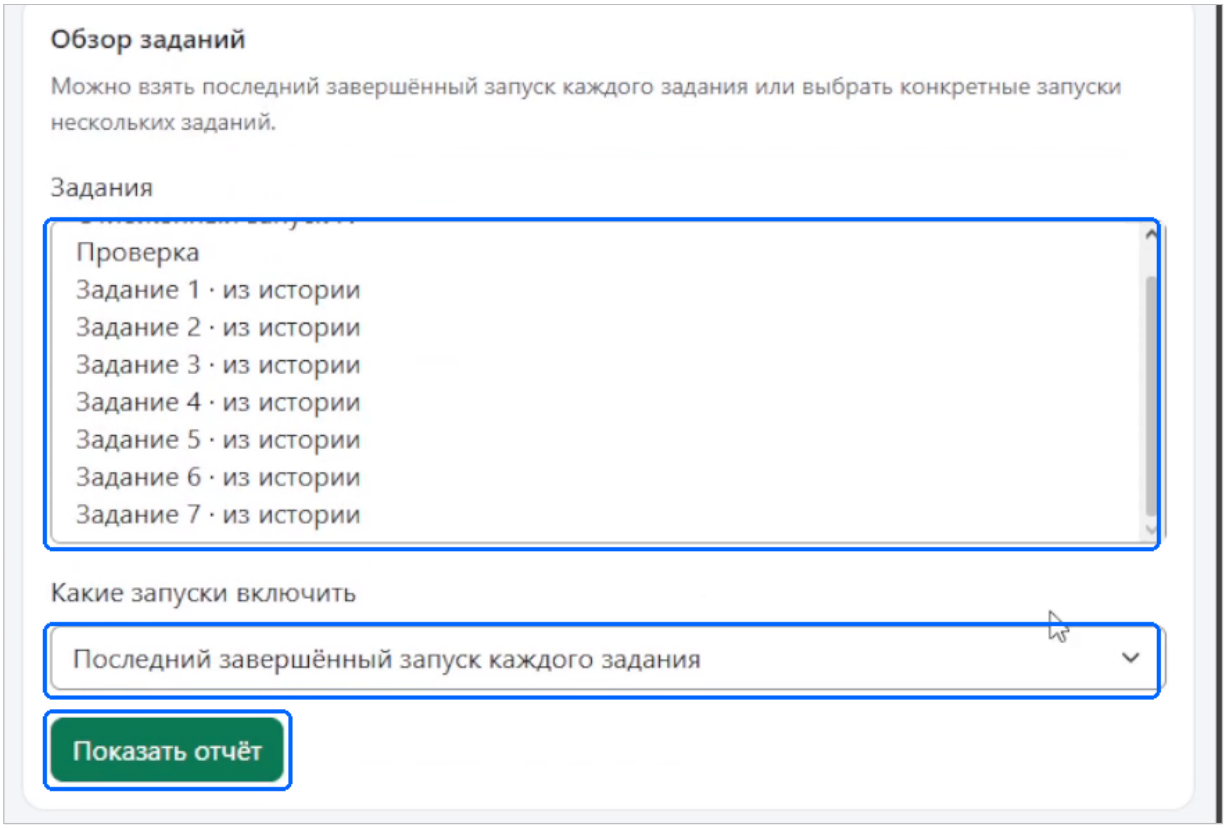


Рисунок 50 – Параметры отчёта «Обзор заданий»

7.7. Шаблоны отчётов

Шаблон позволяет создать собственный отчёт, который отображается в блоке «Отчёты» рядом со стандартными отчётами. Форма «Новый шаблон» открывается кнопкой «Сохранить шаблон» в дополнительных отчётах или через кнопку **«+»** в правом верхнем углу блока «Отчёты» и пункт **«Создать свой отчёт»**.

Чтобы создать шаблон:

1) Введите название в поле «Название» и при необходимости пояснение.
2) Выберите «Источник данных»: «Результаты запуска», «Краткое сравнение запусков», «Динамика задания» или «Обзор заданий».
3) Отметьте разделы отчёта: «Итог», «Типы активов», «Ссылка на результаты». Если нужна только собственная таблица, снимите все отметки.
4) При необходимости раскройте блок «Таблица по своему SQL-запросу» и введите запрос.
5) Оставьте отметку «Показывать на странице отчётов» и нажмите **«Сохранить шаблон»**.

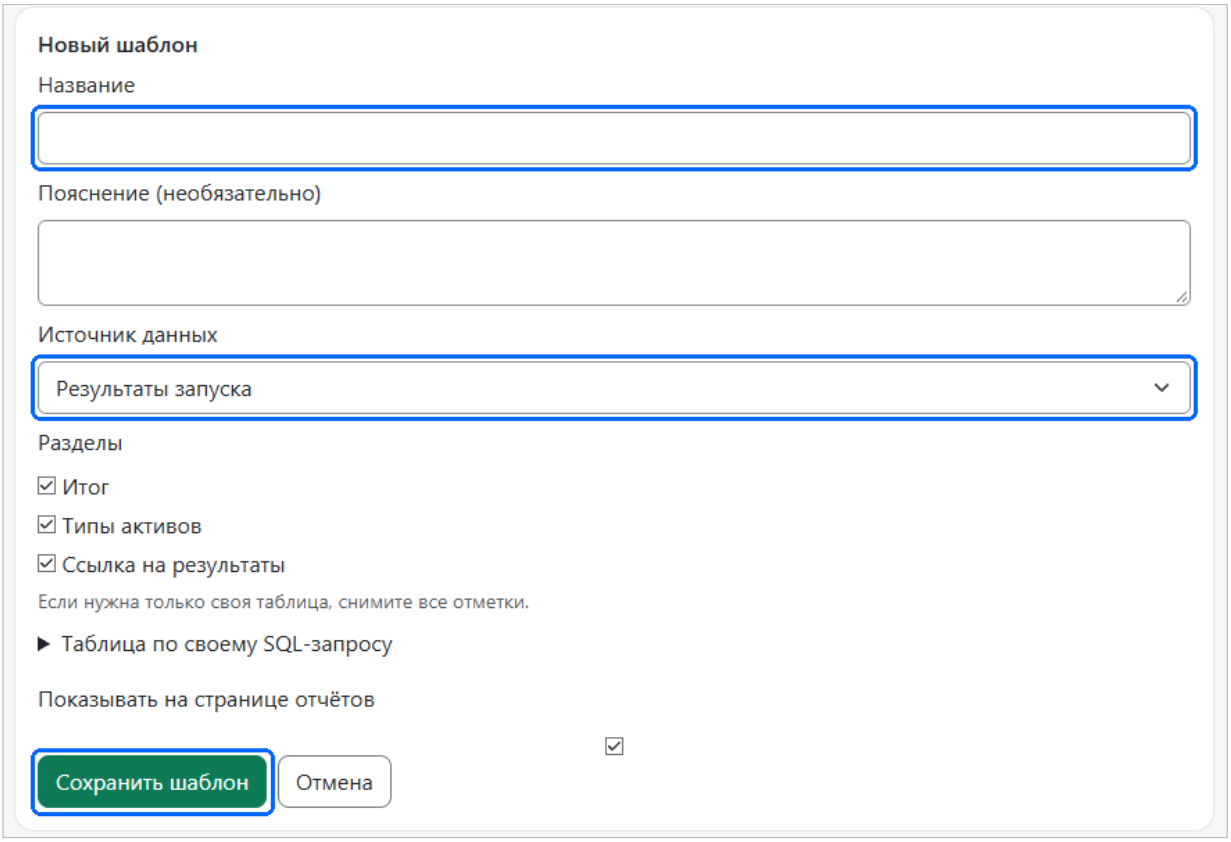


Рисунок 51 – Форма «Новый шаблон»

SQL-запрос работает только с данными выбранных запусков проекта. Доступны таблицы runs (поля run_id, task_id, status, created) и observations (поля run_id, task_id, asset_id, asset_type, value). Результат ограничен 500 строками, значения активов обрезаются до 2000 символов. Пример запроса: SELECT asset_type, COUNT(*) AS total FROM observations GROUP BY asset_type ORDER BY total DESC.

Результат. Шаблон появляется в блоке «Отчёты».

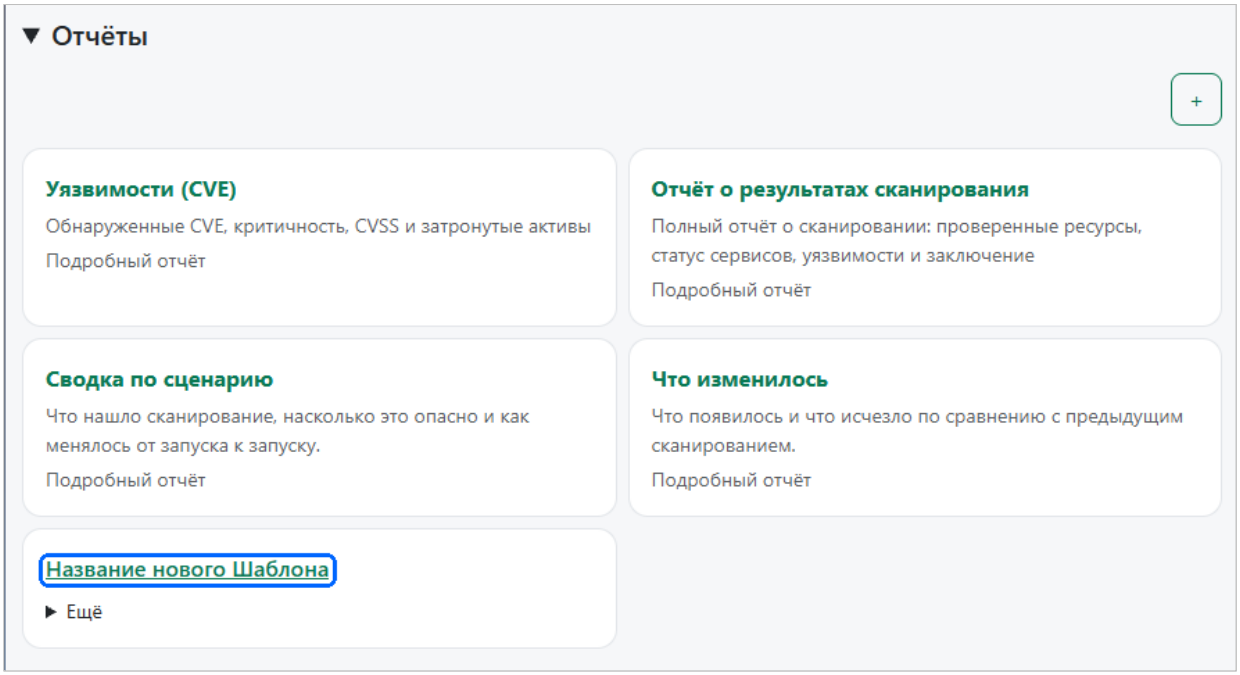


Рисунок 52 – Новый шаблон в блоке «Отчёты»

Меню «Ещё» на карточке шаблона содержит пункты «Изменить», «Копировать», «В другой проект», «Убрать со страницы» и «Удалить».

7.8. Подробные отчёты

Пункт «Создать подробный отчёт» в меню кнопки **«+»** открывает страницу «Отчёты проекта». На странице перечислены общие отчёты организации с поиском по названию. Каждый отчёт можно скопировать для настройки кнопкой **«Скопировать и настроить»**.

Чтобы создать новый отчёт, раскройте блок «Новый отчёт», введите название в поле «Название отчёта», выберите вид отчёта («Пустой отчёт», «Обнаруженные уязвимости», «Инвентаризация периметра», «Краткая сводка») и нажмите **«Создать»**.

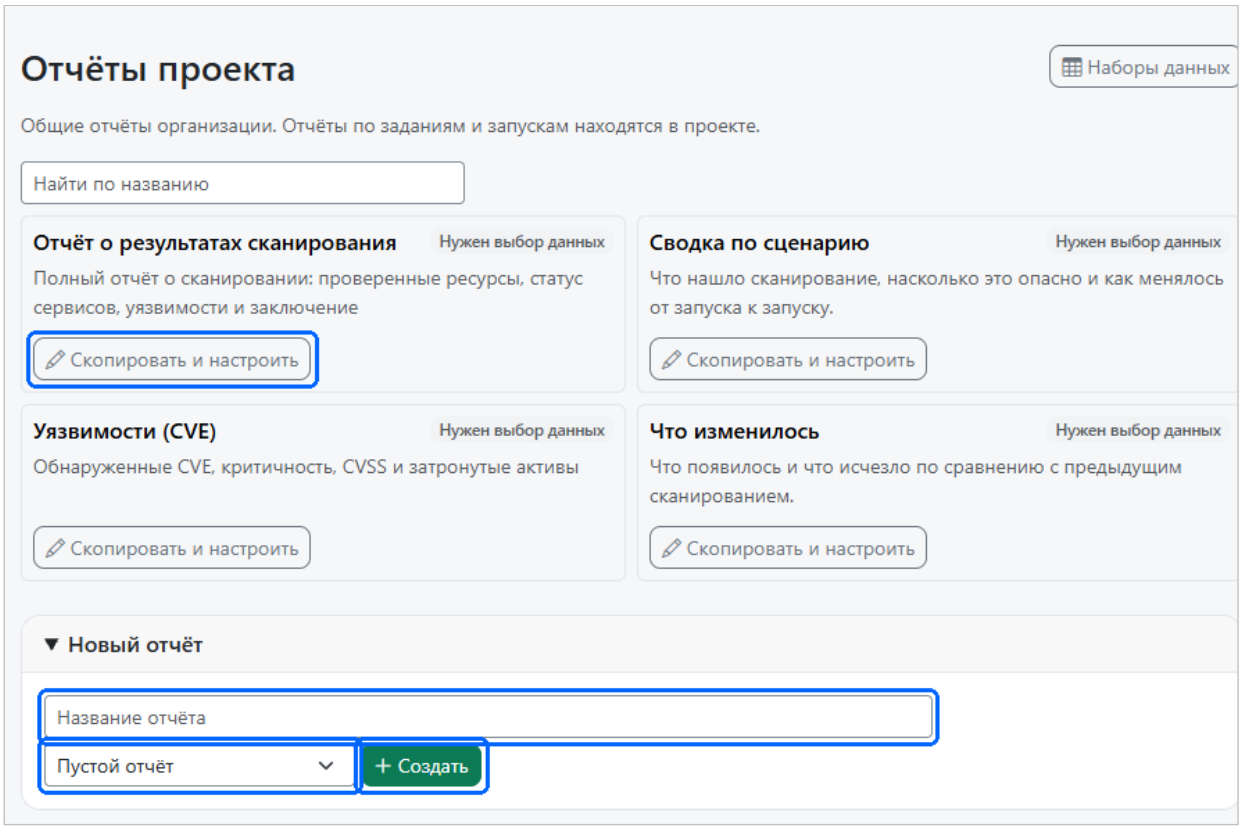


Рисунок 53 – Страница «Отчёты проекта»

Кнопка «Скопировать и настроить» на карточке отчёта открывает страницу «Конструктор отчётов». Общий шаблон организации не изменяется. Чтобы получить свою копию для редактирования, введите название в поле «Название новой копии» и нажмите **«Скопировать и настроить»**.

В блоке «История шаблона» перечислены сохранённые версии шаблона, версию можно открыть кнопкой «Посмотреть». Восстановление версии создаёт новую версию шаблона, данные сканирования при этом не копируются. В блоке «Предпросмотр» выбираются область данных, запуск и параметры отчёта, данные загружаются кнопкой «Выбрать данные». Ссылка «Открыть текущую сохранённую версию / PDF» открывает отчёт в последней сохранённой версии, а не с правками, которые ещё не сохранены.

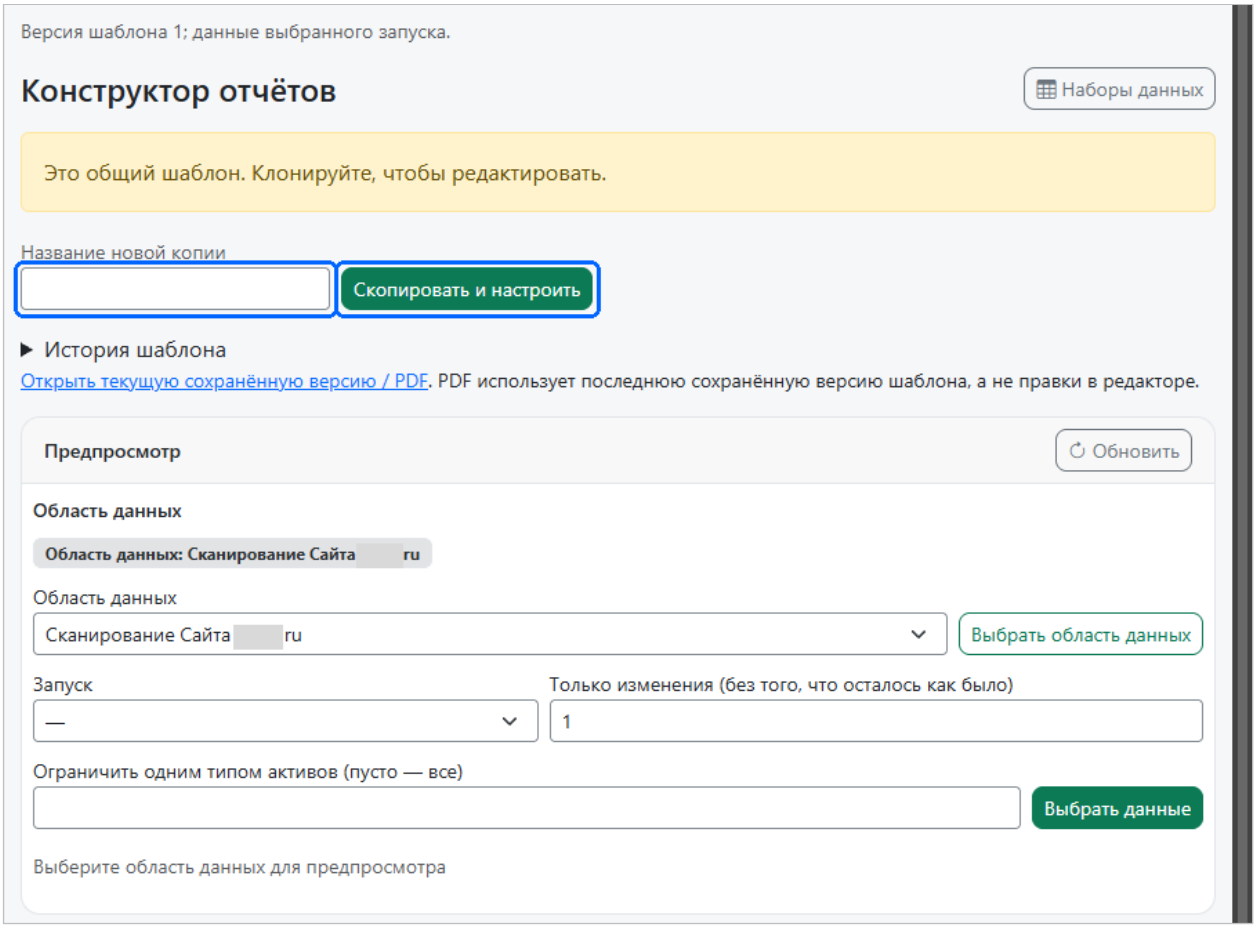


Рисунок 54 – Конструктор отчётов

7.9. Наборы данных

Набор данных определяет, что показывает блок отчёта: тип актива, колонки и фильтры. Для создания набора не требуется писать SQL-запросы. Страница «Наборы данных» открывается кнопкой **«Наборы данных»** на странице «Отчёты проекта» или в конструкторе отчётов.

Наборы с отметкой «общий» подготовлены администратором и открываются кнопкой «Открыть» для просмотра. Собственные наборы редактируются кнопкой «Изменить» и удаляются кнопкой с изображением корзины. Для поиска набора служит строка «Найти по названию».

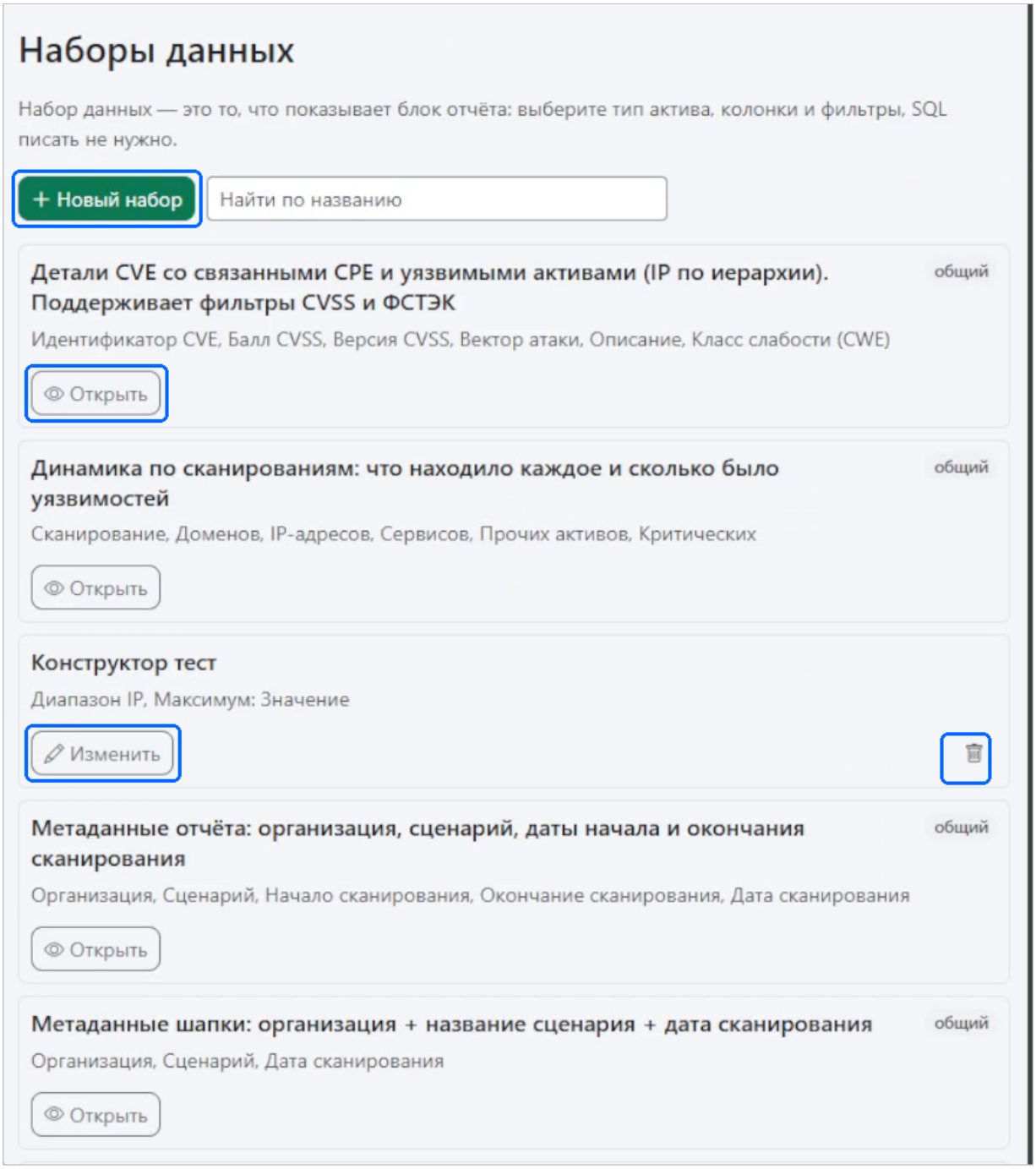


Рисунок 55 – Страница «Наборы данных»

Чтобы создать набор данных:

1) Нажмите **«Новый набор»**. Откроется страница «Конструктор набора данных».
2) Введите название в поле «Название набора».
3) Выберите тип активов в поле «Что показываем» и источник данных в поле «Область», например «Выбранное сканирование».
4) Выберите вид результата в поле «Результат». «Строки» выводит таблицу, колонки которой добавляются кнопкой «Добавить колонку». «Сводка»

группирует данные: в строке «Разрез» задаётся, по чему группировать, в строке «Показатель» что считать, например «Количество» или «Максимум» по выбранному полю.

5) При необходимости нажмите «Добавить фильтр» и задайте источник, поле, условие («равно», «содержит» и другие) и значение. Отметка «спросить у читателя» оставляет значение фильтра для ввода при просмотре отчёта. Фильтр удаляется красной кнопкой справа.
6) Задайте сортировку и ограничение в поле «Не более строк», по умолчанию 500.
7) Нажмите **«Сохранить»**.

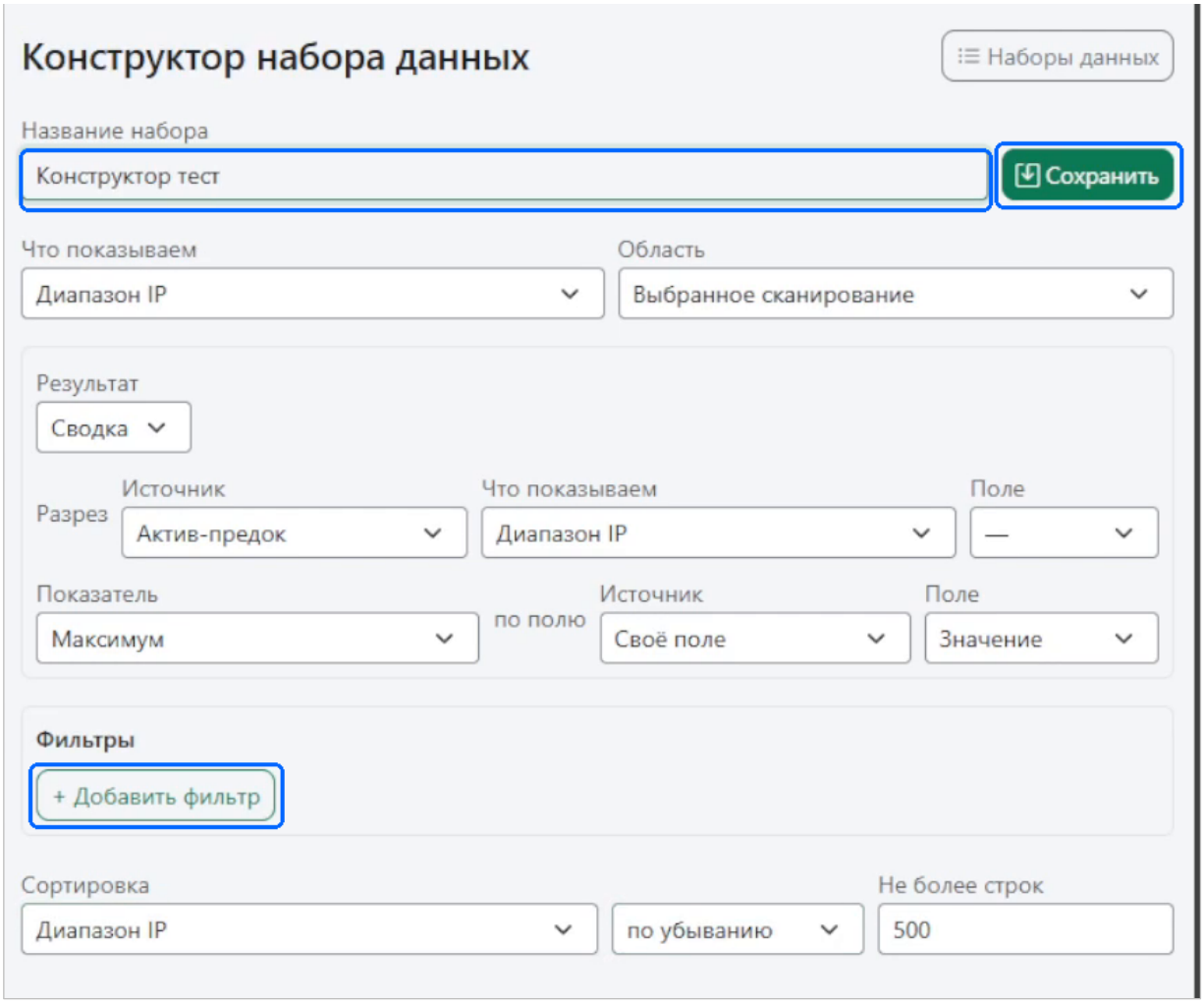


Рисунок 56 – Конструктор набора данных

Результат. Набор появляется на странице «Наборы данных». В блоке «Проверка данных» конструктора отображается результат набора, он обновляется кнопкой «Обновить».

8. Администрирование организации

Раздел предназначен для пользователя с ролью «Администратор организации».

8.1. Настройки организации

1) Нажмите на имя учётной записи в правом верхнем углу экрана.
2) Выберите **«Настройки организации»**.

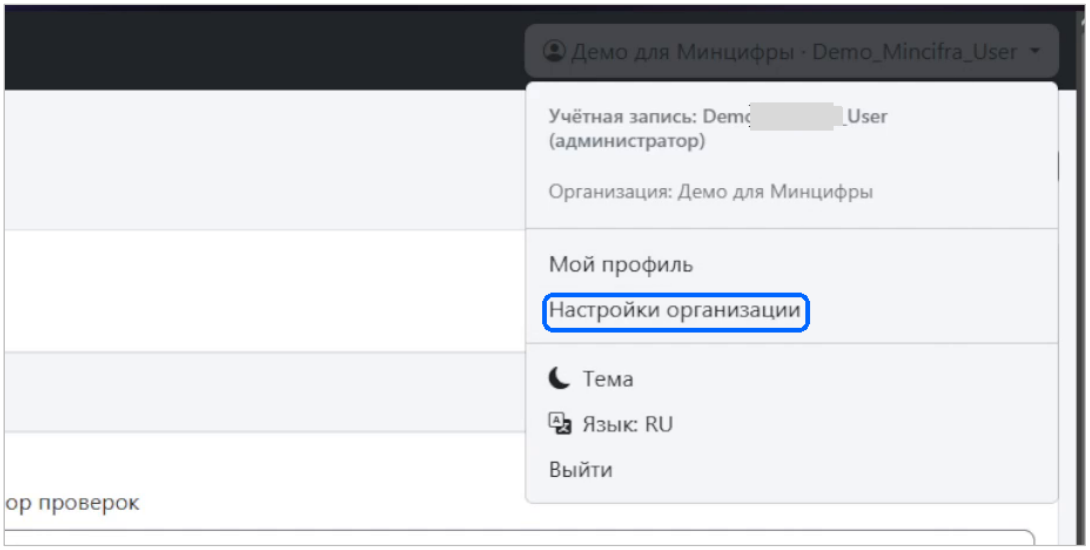


Рисунок 57 – Переход к настройкам организации

На странице «Настройки организации» доступны следующие блоки:

- «Название организации» – название в интерфейсе, сохраняется кнопкой «Сохранить название». Адрес входа при этом не меняется;
- «Тариф» – название тарифа, срок действия, ограничения по числу пользователей и целей сканирования;
- «Пользователи» – список пользователей организации и их состояние.

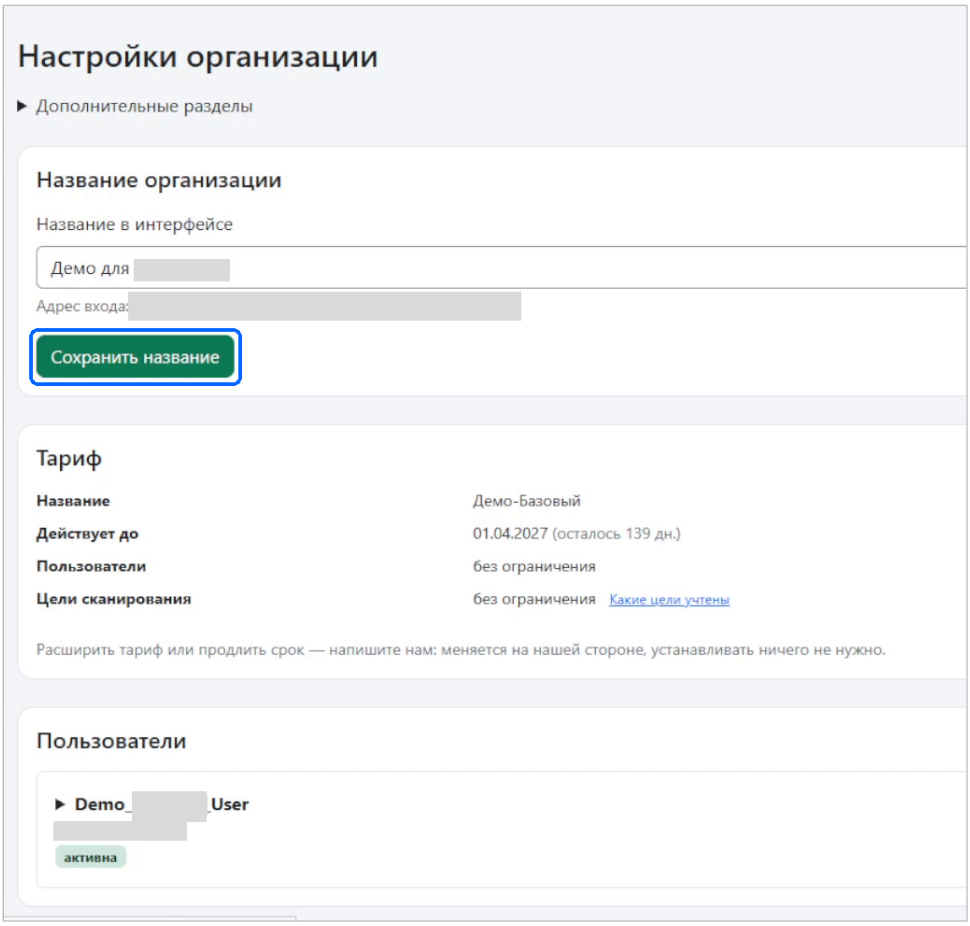


Рисунок 58 – Настройки организации

8.2. Безопасность

В блоке «Безопасность» включается обязательная двухфакторная аутентификация для всех участников и выбираются допустимые вторые факторы: одноразовый код (TOTP) и аппаратный ключ (FIDO2/WebAuthn). Изменения сохраняются кнопкой **«Сохранить»**.

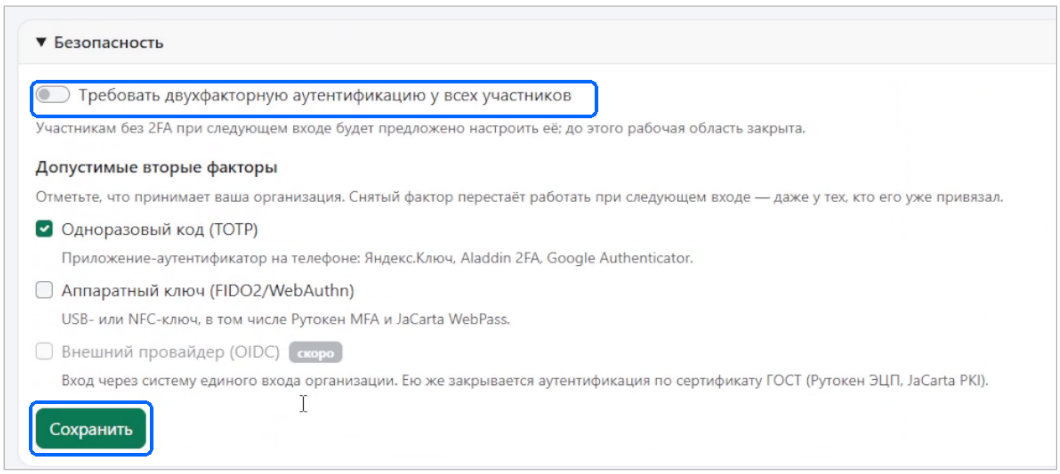


Рисунок 59 – Блок «Безопасность»

8.3. Добавление пользователя

1) На странице «Настройки организации» разверните блок «Добавить пользователя».
2) Введите логин в поле «Логин» и адрес электронной почты в поле «Email».
3) Пароль в поле «Пароль» формируется автоматически. Его можно сформировать заново или скопировать кнопками справа от поля.
4) Выберите роль в поле «Роль».
5) Нажмите **«Добавить»**.

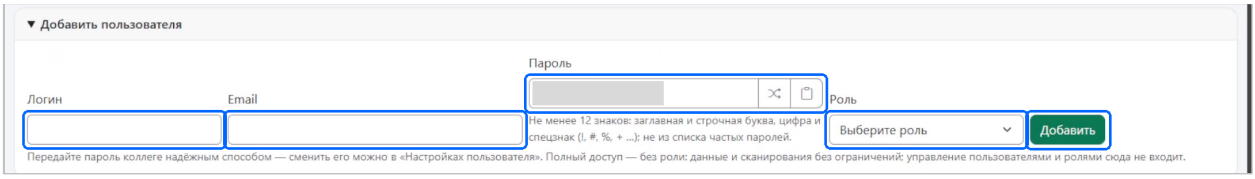


Рисунок 60 – Добавление пользователя

Результат. Пользователь появляется в списке «Пользователи». Передайте пароль коллеге надёжным способом. Сменить пароль пользователь может в настройках пользователя.

8.4. Роли и права доступа

В блоке «Роли» приведены готовые роли и их права. Состав прав готовых ролей настраивается в организации. Описание готовых ролей приведено в разделе «Роли пользователей».

Чтобы создать роль:

1) Введите название в поле «Название роли».
2) Отметьте права: просмотр данных, изменение данных, удаление данных, запуск сканирований, импорт конфигурации, выгрузка конфигурации, управление пользователями, управление ролями, журнал действий.
3) Нажмите **«Создать роль»**.

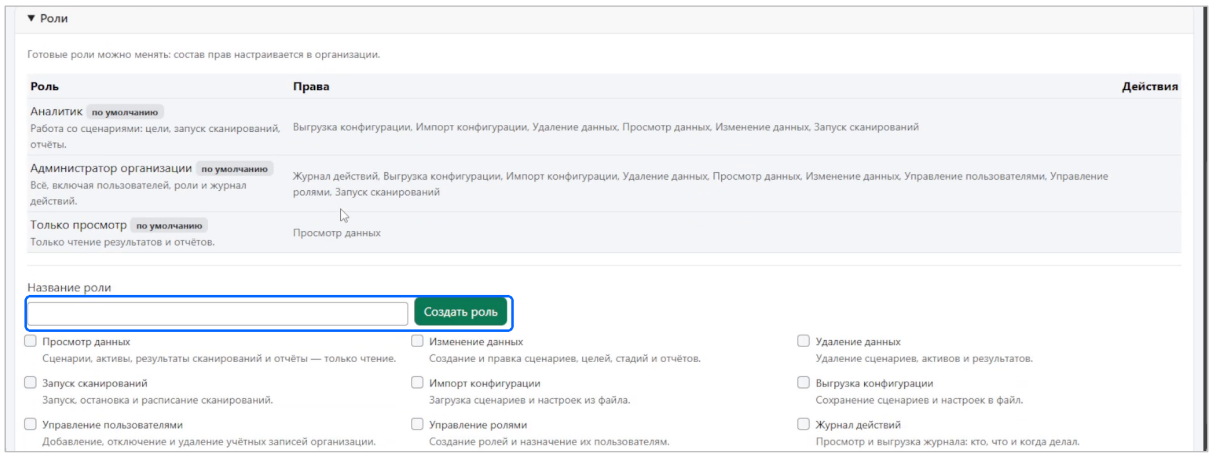


Рисунок 61 – Роли и создание роли

Результат. Новая роль появляется в списке ролей и становится доступной при добавлении пользователя.

9. Сообщения оператору

В таблице приведены сообщения и состояния, на которые следует обратить внимание при работе с программой, и действия пользователя.

Сообщение или состояние	Причина	Действие пользователя
Сообщение об ошибке при создании проекта	Проект с таким названием уже существует.	Введите название, которого нет в списке проектов, и нажмите «Создать».
«Сканирование ещё не запускалось»	В проекте нет запусков, по которым можно построить отчёт.	Запустите сканирование, как описано в разделе «Запуск сканирования».
«Выберите задания»	В отчёте «Обзор заданий» не отмечено ни одного задания.	Отметьте задания в списке «Задания» и нажмите «Показать отчёт».
«Расписаний пока нет»	В проекте не настроено ни одного расписания.	Нажмите ссылку «Открыть сохранённые задания» и задайте расписание для задания.
«Нужен выбор данных» на карточке отчёта	Для отчёта не выбрана область данных.	Нажмите «Скопировать и настроить» и выберите область данных в блоке «Предпросмотр».
«Это общий шаблон. Клонируйте, чтобы редактировать»	Общий шаблон организации изменить нельзя.	Введите название в поле «Название новой копии» и нажмите «Скопировать и настроить».

10. Справочная информация

10.1. Типы активов и каталог проверок

В программе используются следующие типы активов: CPE, CVE, приоритет CVE, эксплойт, IP-адрес, порт, служба, проблема TLS, исходный домен, домен, маска домена, диапазон IP и группа.

Проверки каталога, их входные данные и результат приведены в таблице.

Проверка	Вход	Результат
Обнаружение живых хостов в диапазоне (CIDR)	Диапазон IP	IP-адрес
Перебор поддоменов по словарю	Исходный домен	unchecked domain
Проверка доступности веб-сервера (httpx)	unchecked domain	Домен
Сканирование IP на открытые порты	IP-адрес	port
Определение сервиса, версии и CPE на порту (встроенный движок)	port	CPE, service
Анализ TLS/сертификата (testssl.sh)	port	tls finding
Поиск уязвимостей (CVE) по версии ПО в базе уязвимостей	CPE	CVE
Поиск публичных эксплойтов по CVE (searchsploit)	CVE	exploit
Адреса домена по записям A (домен → IP)	Домен	IP
Пассивный поиск поддоменов (subfinder)	Домен	Поддомены

10.2. Шкала критичности уязвимостей

Критичность уязвимости определяется по базовой оценке CVSS. Сведения об уязвимостях программа получает из баз NVD (NIST, США), CVE, EPSS (FIRST.org), CISA KEV, БДУ ФСТЭК России и бюллетеней НКЦКИ.

Уровень критичности	Базовая оценка CVSS
Информационный	0,0
Низкий	0,1–3,9
Средний	4,0–6,9
Высокий	7,0–8,9
Критический	9,0–10,0