



CyberDef EASM

**Платформа управления
внешней поверхностью атаки
(локальна версия)**

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ/ОПЕРАТОРА

Версия 1.0

2026

Содержание

1. Об этом документе	3
1.1. Термины и определения	3
2. О продукте CyberDef EASM	4
3. Требования к браузеру	4
4. Вход в систему	4
5. Первое сканирование	6
5.1. Создание сценария сканирования	6
5.2. Добавление активов	7
5.3. Запуск сканирования	7
5.4. Получение отчёта	8
6. Свои отчёты	9
6.1. Создание отчёта	9
6.2. Конструктор отчёта	9
6.3. Изменение поставляемого отчёта	10
6.4. Фиксация параметров отчёта	10
7. Наборы данных	11
7.1. Создание набора	11
7.2. Проверка набора	12
8. Двухфакторная аутентификация	12
8.1. Одноразовые коды из приложения	12
8.2. Аппаратные ключи	13
8.3. Если фактор потерян	13
9. Журнал действий	14
9.1. Что попадает в журнал	14
9.2. Что видно по каждой записи	14
9.3. Отбор и выгрузка	15
10. Что означают данные в отчёте	15
10.1. Какие данные доступны в отчётах	15

1. Об этом документе

Настоящее руководство предназначено для пользователя и оператора, осуществляющего настройку и выполнение сканирования в веб-интерфейсе организации программного обеспечения «Платформа управления внешней поверхностью атаки CyberDef EASM». Выполнение операций, описанных в руководстве, не требует доступа к серверу, на котором развёрнута платформа.

1.1. Термины и определения

Термин	Определение
CyberDef EASM	Платформа управления внешней поверхностью атаки.
VulnScan	Модуль сканирования в составе CyberDef EASM.
CVEgggregator	Модуль агрегатор данных об уязвимостях в составе CyberDef EASM.
Актив	Объект сканирования — IP-адрес или доменное имя.
Уровень критичности	Категория, отражающая степень опасности обнаруженной уязвимости.
CVE	Идентификатор уязвимости из базы данных известных уязвимостей (Common Vulnerabilities and Exposures).
CVSS	Числовая оценка критичности уязвимости и вектор атаки (Common Vulnerability Scoring System).
CWE	Идентификатор класса слабости/уязвимости программного обеспечения (Common Weakness Enumeration).
CPE	Идентификатор конкретного программного обеспечения и его версии, используемый для сопоставления с базой CVE (Common Platform Enumeration).
БДУ ФСТЭК	Банк данных угроз безопасности информации ФСТЭК России.
Второй фактор	Дополнительное подтверждение личности при входе помимо пароля - одноразовый код или аппаратный ключ.

2. О продукте CyberDef EASM

CyberDef EASM — платформа управления внешней поверхностью атаки. Программа обеспечивает автоматизированное обнаружение и инвентаризацию информационных активов организации, доступных из сети Интернет, анализ их защищённости, выявление уязвимостей и управление процессом их устранения.

Сканирование строит карту внешней поверхности атаки от указанных вами целей (IP-адресов или доменных имён) и доводит её до перечня обнаруженных уязвимостей с оценкой критичности — результат доступен в виде отчёта.

3. Требования к браузеру

Для доступа к веб-интерфейсу организации 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.

4. Вход в систему

Веб-интерфейс организации доступен по адресу вида `http://<организация>.<базовый-домен>:8080`, где вместо `<организация>` и `<базовый-домен>` указываются значения, присвоенные вашей организации при установке платформы (по умолчанию используется базовый домен `vulnscan.local`). Точный адрес и учётные данные для входа предоставляются администратором платформы.

Откройте полученный адрес в браузере — откроется рабочее пространство вашей организации.

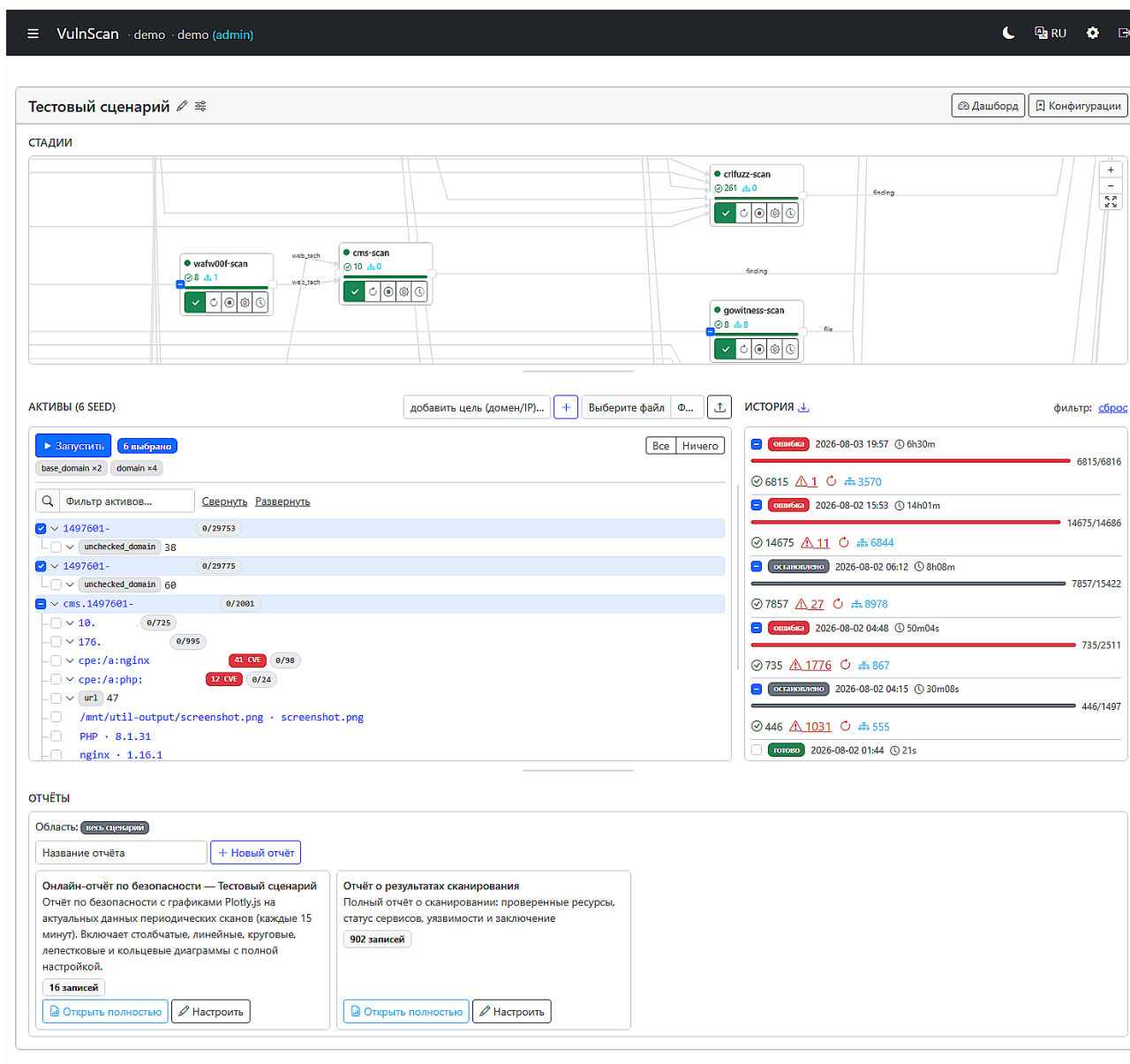


Рисунок 1 – Рабочее пространство организации в веб-интерфейсе CyberDef EASM

Если в вашей организации включён второй фактор, после ввода пароля откроется ещё один экран — с полем для одноразового кода, с кнопкой «Войти по аппаратному ключу» или с тем и другим сразу. Что делать на этом экране, описано в разделе «Двухфакторная аутентификация».

5. Первое сканирование

5.1. Создание сценария сканирования

Сканирование выполняется в рамках сценария — набора целей и настроек, объединённых для совместного запуска.

Для создания сценария нажмите кнопку меню ☰ в левом верхнем углу рабочего пространства.

В открывшемся списке сценариев нажмите кнопку «+ Новый сценарий».

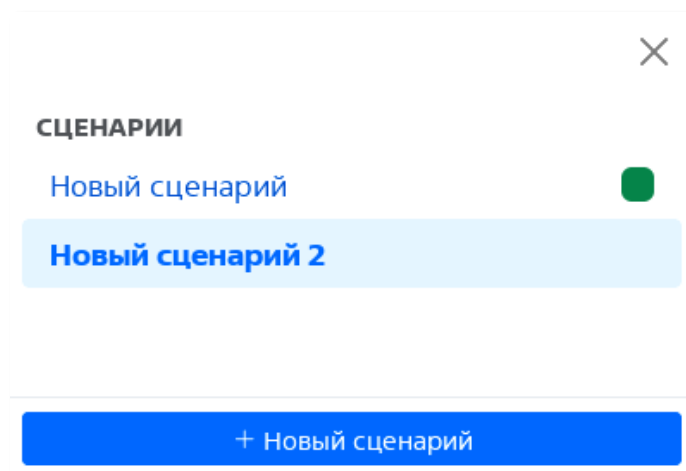


Рисунок 2 – Создание нового сценария сканирования

5.2. Добавление активов

Далее необходимо указать цели сканирования — активы.

В блоке «Активы» нажмите поле «добавить цель (домен/IP)» и укажите IP-адрес или доменное имя ресурса, который нужно проверить. Добавленные активы отображаются списком и остаются доступными для выбора перед каждым запуском.

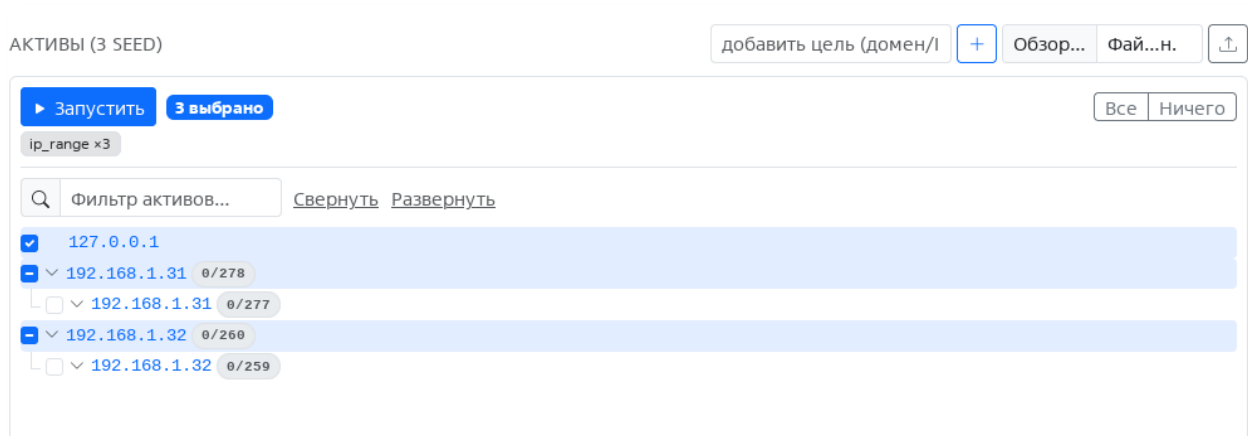


Рисунок 3 – Список добавленных активов

5.3. Запуск сканирования

Чтобы запустить сканирование, отметьте галочками активы, которые нужно проверить, и нажмите кнопку «Запустить». Ход выполнения отображается в блоке «История» справа: там указывается статус (например, «ВЫПОЛНЯЕТСЯ»), время запуска и продолжительность.

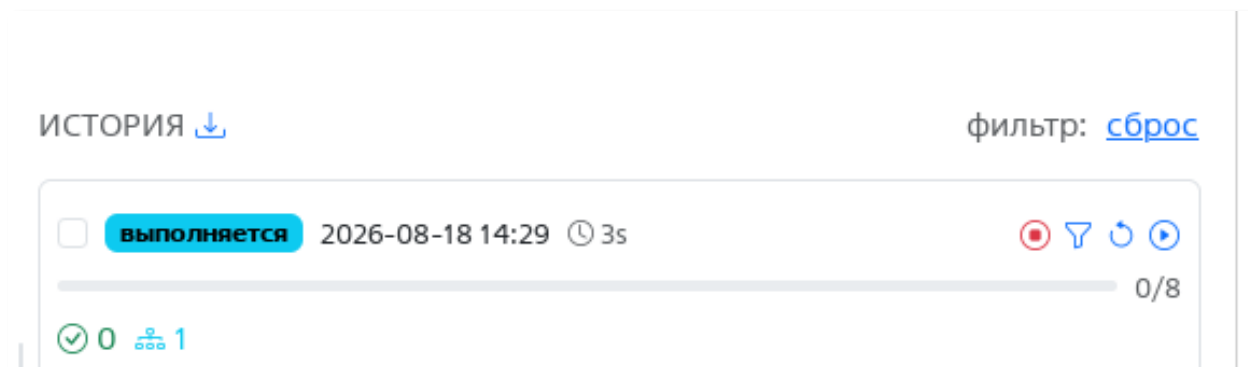


Рисунок 4 – Индикатор хода выполнения сканирования

5.4. Получение отчёта

После завершения сканирования в блоке «Отчёты» становится доступен отчёт о результатах: перечень проверенных ресурсов, статус сервисов, обнаруженные уязвимости и заключение. Чтобы просмотреть его полностью, нажмите кнопку «Открыть целиком».

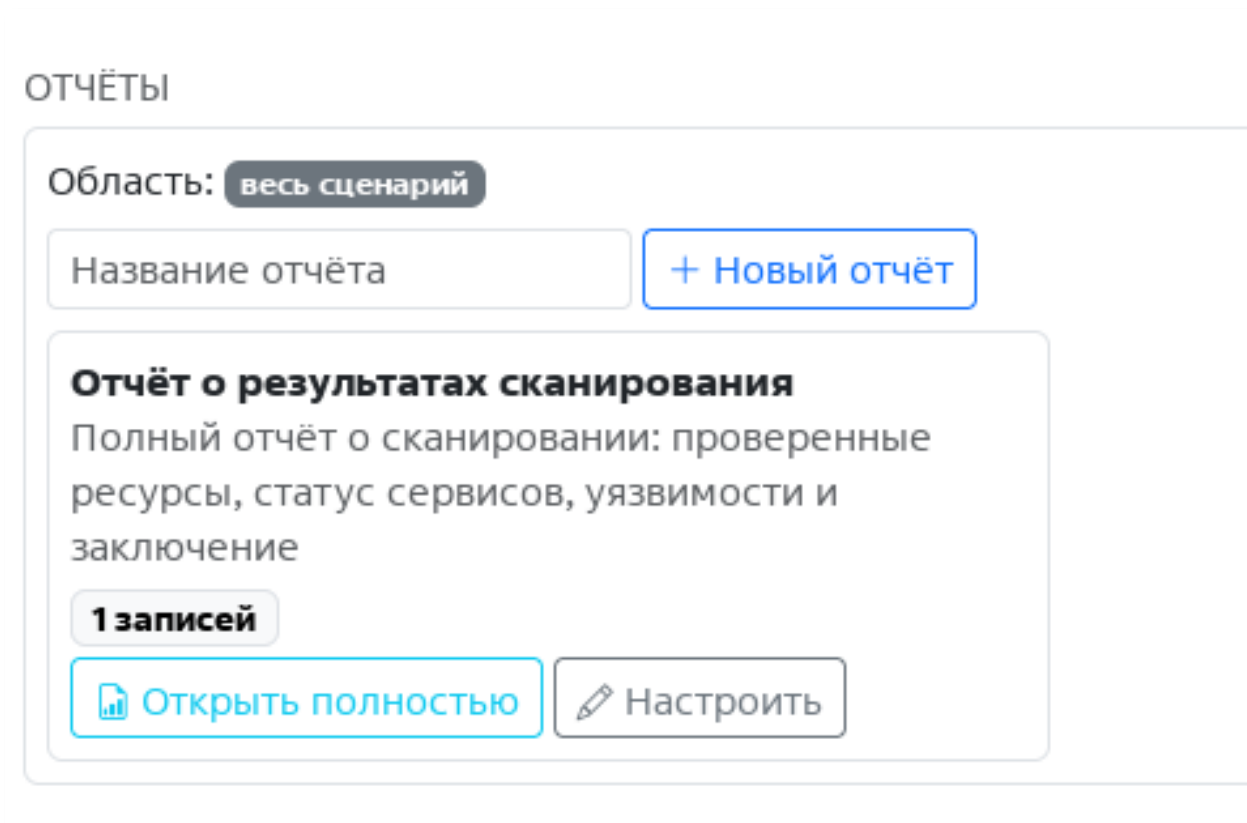


Рисунок 5 – Карточка отчёта о результатах сканирования

Отчёт открывается на отдельной странице. Над текстом отчёта расположены его параметры: сценарий, запуск сканирования и дополнительные условия отбора, если они предусмотрены. Измените значения и нажмите «Применить» — отчёт перестроится.

Кнопка «Экспортировать в PDF» сохраняет отчёт в файл ровно с теми параметрами, которые выбраны на экране.

Если запуск сканирования не выбран, отчёт строится по последнему сканированию выбранного сценария.

6. Свои отчёты

Кроме отчётов, поставляемых с платформой, можно собрать свои — в конструкторе, без программирования. Отчёт состоит из блоков: заголовков, текста, таблиц, показателей и графиков. Каждый блок с данными опирается на набор данных — описание того, что именно показывать (см. раздел «Наборы данных»).

6.1. Создание отчёта

Отчёты организации собраны на странице «Отчёты»: в рабочей области нажмите «Дашборд», затем «Отчёты». Отчёты, привязанные к сценарию, доступны и прямо в его рабочей области, в блоке «Отчёты».

Чтобы создать отчёт, введите название, выберите заготовку и нажмите «Новый отчёт».

Заготовка — это стартовый набор блоков, который дальше правится как обычно:

- «Обнаруженные уязвимости» — таблица уязвимостей с критичностью, оценкой CVSS и перечнем уязвимых активов;
- «Инвентаризация периметра» — счётчики проверенных адресов, портов и сервисов плюс таблица ресурсов;
- «Краткая сводка» — счётчики и статус по каждому обнаруженному сервису;
- «Пустой отчёт» — если удобнее собрать всё самостоятельно.

6.2. Конструктор отчёта

Конструктор открывается сразу после создания отчёта, а для существующего — кнопкой «Настроить» на его карточке.

Кнопка «Добавить блок» предлагает типы блоков:

Блок	Для чего
Заголовок	Название раздела отчёта.
Текст	Пояснение, вывод, сопроводительный абзац.
Таблица	Перечень записей из набора данных; колонки выбираются из списка.
Показатель	Одно число крупно (например, число уязвимых сервисов).
График	Столбчатая, линейная, круговая, кольцевая или лепестковая диаграмма.

Блок	Для чего
Отступ	Пустое пространство между блоками.
Разрыв страницы	Следующий блок начнётся с новой страницы при печати и в PDF.

У блока с данными сначала выбирается источник — набор данных, а затем поля: колонки таблицы, поле показателя, оси графика. Поля предлагаются списком, вводить их вручную не нужно.

Каждый блок можно переместить вверх или вниз, продублировать и удалить — кнопки в его правом верхнем углу.

Раздел «Оформление» задаёт вид документа целиком: акцентный цвет, цвет текста, шрифты заголовков и основного текста, логотип.

Кнопка «Сохранить» записывает изменения.

Под редактором находится панель «Предпросмотр» — тот же отчёт на реальных данных. Она обновляется после каждого сохранения, поэтому результат правки виден сразу.

Кнопка «Открыть целиком» показывает отчёт на отдельной странице — оттуда же он выгружается в PDF.

6.3. Изменение поставляемого отчёта

Отчёты из поставки помечены как общие и доступны только для чтения: их ведёт администратор платформы, и правка затронула бы все организации. Чтобы получить свою версию, откройте отчёт и нажмите «Клонировать для редактирования» — копия принадлежит вашей организации и правится без ограничений.

6.4. Фиксация параметров отчёта

Если отчёт готовит один сотрудник, а читает другой, часть параметров можно закрепить. В конструкторе раскройте «Заблокированные параметры» и укажите значение — оно станет постоянным для этого отчёта, а из формы параметров исчезнет. Так, например, фиксируют постоянное исключение служебных адресов из отчёта.

7. Наборы данных

Набор данных отвечает на вопрос «что показывать»: какие объекты сканирования брать, какие их свойства выводить и по какому условию отбирать. Блоки отчёта опираются на наборы, поэтому свой отчёт обычно начинается со своего набора.

Наборы собраны на странице «Наборы данных» — кнопка на странице «Отчёты» или в конструкторе отчёта. Наборы из поставки помечены: «общий» — принадлежит платформе, «SQL» — написан запросом вручную. И те, и другие доступны только для чтения; общий набор можно скопировать кнопкой «Клонировать для редактирования».

7.1. Создание набора

Нажмите «Новый набор» и заполните форму.

Что показываем — тип активов, которые станут строками: уязвимости, находки, порты, сервисы, URL, IP-адреса, домены и другие.

Область — «Выбранное сканирование» (набор покажет данные того запуска, который выбран в отчёте) или «Все сканирования».

Результат — «Строки» (перечень записей) или «Сводка» (группировка с подсчётом: например, количество уязвимостей по уровням критичности).

Колонки — что вывести по каждой записи. Источником колонки может быть:

- **«Своё поле»** — свойство самого актива (у уязвимости это идентификатор CVE, балл CVSS, уровень критичности, описание, номер БДУ ФСТЭК);
- **«Актив-предок»** — свойство объекта, на котором эта запись обнаружена. Данные сканирования связаны цепочкой «домен → IP-адрес → порт → сервис → программный продукт → уязвимость», поэтому к уязвимости можно вывести её IP-адрес или название сервиса, не сопоставляя ничего вручную;
- **«Служебное поле»** — например, дата обнаружения.

Фильтры — условия отбора: поле, условие (равно, содержит, не меньше и другие) и значение. Галочка «спросить у читателя» превращает фильтр в параметр отчёта: значение будет выбирать тот, кто открывает отчёт. Так делают, например, порог CVSS.

Сортировка и Не более строк задают порядок и предел выдачи.

7.2. Проверка набора

После сохранения под формой появляется панель «Проверка данных» — первые строки набора на реальных данных сканирования. Если строк нет, проверьте фильтры и область: возможно, в выбранном сканировании таких объектов не находили.

8. Двухфакторная аутентификация

Второй фактор — это подтверждение входа помимо пароля. Украденного пароля становится недостаточно: нужен ещё телефон с приложением или физический ключ.

Какие способы принимает ваша организация, решает её владелец. Поэтому на странице настроек вы увидите только разрешённые: одноразовые коды, аппаратные ключи или оба сразу.

Страница открывается так: меню учётной записи в правом верхнем углу → «Настройки» → «Двухфакторная аутентификация».

Если владелец организации сделал второй фактор обязательным, а вы его ещё не настроили, платформа откроет эту страницу сама и не пустит дальше, пока фактор не привязан.

8.1. Одноразовые коды из приложения

Понадобится приложение-аутентификатор на телефоне: Яндекс.Ключ, Aladdin 2FA, Google Authenticator или любое другое, работающее по стандарту TOTP.

- 1) Откройте страницу «Двухфакторная аутентификация».
- 2) Отсканируйте приложением показанный QR-код. Если камера недоступна, введите в приложении текстовый ключ, напечатанный под кодом.
- 3) Введите шестизначный код, который показало приложение, и нажмите кнопку подтверждения.

С этого момента при каждом входе после пароля будет запрашиваться текущий код из приложения.

Отключить коды можно на той же странице, подтвердив действие паролем. Если организация требует второй фактор, отключение недоступно.

8.2. Аппаратные ключи

Аппаратный ключ — устройство, которое вставляется в USB-порт или прикладывается к телефону по NFC. Подходят ключи стандарта FIDO2, в том числе **Рутокен MFA** и **JaCarta WebPass**.

Чтобы привязать ключ:

- 1) Откройте страницу «Двухфакторная аутентификация», блок «Аппаратные ключи».
- 2) При желании введите название ключа — например, «Рутокен на связке». Оно нужно, чтобы различать ключи в списке.
- 3) Нажмите «Привязать ключ», вставьте ключ и коснитесь его, когда браузер попросит.

Привязать можно несколько ключей — обычно заводят рабочий и запасной, чтобы потеря одного не отрезала доступ. Всего допускается до десяти ключей.

Чтобы войти по ключу: введите логин и пароль, затем на следующем экране нажмите «Войти по аппаратному ключу», вставьте ключ и коснитесь его.

Удалить ключ можно кнопкой «Удалить» в его строке. Последний ключ удалить не получится, если организация требует второй фактор и другого фактора у вас нет — иначе вы закрыли бы себе доступ.

Аппаратные ключи работают только при доступе к платформе по HTTPS и только по тому доменному имени, на котором ключ был привязан. Если адрес платформы изменится, ключи потребуется привязать заново.

8.3. Если фактор потерян

Обратитесь к владельцу вашей организации: он сбрасывает второй фактор в настройках организации. После сброса вы войдёте по паролю и сразу привяжете новый ключ или новое приложение.

9. Журнал действий

Журнал показывает, кто из сотрудников организации что сделал в платформе: входил, менял данные, запускал сканирование, выгружал отчёт. Он нужен, чтобы разобрать спорную ситуацию и подтвердить, что действие выполнял конкретный человек.

Журнал доступен в разделе «Безопасность» → «Журнал действий» бокового меню. Видеть его может владелец организации и сотрудники, которым выдана соответствующая роль, — обычный участник журнал не открывает.

9.1. Что попадает в журнал

Записываются действия, которые что-то меняют, и события входа:

- вход в систему, в том числе неудачные попытки и вход в отключённую учётную запись;
- выход, смена пароля, привязка и отключение второго фактора;
- добавление и удаление пользователей, смена ролей, изменение настроек организации;
- создание, изменение и удаление данных: сценариев, активов, отчётов, наборов данных;
- запуск сканирования, выгрузка отчёта в PDF.

Просмотр страниц и списков не записывается — иначе полезные записи утонули бы в обращениях к экранам.

9.2. Что видно по каждой записи

По каждому действию сохраняются дата и время, кто его выполнил (логин, ФИО и должность на момент действия), что именно сделано, над каким объектом, результат (успех, отказ, ошибка) и IP-адрес, с которого пришёл запрос.

ФИО и должность сохраняются снимком. Поэтому даже если сотрудник позже уволен и его учётная запись удалена, в журнале останется видно, кто выполнил действие.

9.3. Отбор и выгрузка

Над таблицей доступен отбор: период, сотрудник, вид действия, результат и поиск по тексту. Кнопка выгрузки сохраняет отобранные записи в файл CSV — он открывается в Excel и годится для передачи проверяющему.

За одну выгрузку сохраняется не более 100 000 записей. Если записей больше, сузьте период — иначе часть данных в файл не попадёт.

10. Что означают данные в отчёте

Каждая обнаруженная уязвимость представлена в отчёте как самодостаточная карточка и включает:

- оценку CVSS и вектор атаки;
- уровень критичности (например, CRITICAL, HIGH);
- описание из базы данных угроз ФСТЭК (приоритетно) либо NIST;
- идентификатор CWE (класс слабости/уязвимости);
- номер БДУ ФСТЭК.

Данные в отчёте связаны иерархией «родитель → потомок», обнаруженный порт принадлежит конкретному IP-адресу, а обнаруженная уязвимость (CVE) — конкретному сервису и его версии (CPE). Это позволяет проследить, на каком именно активе и сервисе обнаружена каждая уязвимость, без ручного сопоставления результатов.

10.1. Какие данные доступны в отчётах

Сканирование сохраняет объекты разных типов, и любой из них можно вывести в отчёт через набор данных. Ниже — что именно доступно по каждому типу.

Тип объекта	Что содержит
Домен, IP-адрес, порт, URL	Само значение.
Сервис	Название сервиса, продукт, версия.
Программный продукт (CPE)	Идентификатор вида cpe:/a:vendor:product:version

Тип объекта	Что содержит
Уязвимость (CVE)	Идентификатор, балл и версия CVSS, вектор атаки, уровень критичности, описание, класс слабости CWE, номер БДУ ФСТЭК, признак наличия описания ФСТЭК.
Приоритет уязвимости	Вероятность эксплуатации EPSS, процентиль, признак активной эксплуатации (KEV).
Эксплойт	Название, идентификатор Exploit-DB, тип, платформа.
Находка	Название проверки, уровень критичности, идентификатор проверки, место обнаружения.
Находка TLS	Проверка, уровень критичности, описание.
Веб-технология	Технология и её версия.
Файл, хеш файла	Имя файла, значение хеша.
Домен-двойник	Похожее доменное имя, найденное при проверке на фишинг.

Наполнение зависит от того, какие стадии включены в сценарий: если веб-приложения не обходились, URL и веб-технологий в отчёте не будет. Кроме свойств самого объекта, набор данных умеет выводить дату обнаружения и свойства объектов-предков по цепочке обнаружения.