



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

Функциональные характеристики

Санкт-Петербург, 2026

АННОТАЦИЯ

Настоящий документ содержит описание функциональных характеристик программного обеспечения «Платформа управления внешней поверхностью атаки CyberDef EASM» (далее: CyberDef EASM, программа).

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ	4
1.1. Наименование программы.....	4
1.2. Назначение программы.....	4
1.3. Варианты поставки.....	4
2. СОСТАВ ПРОГРАММЫ.....	5
2.1. Модули программы	5
2.2. Компоненты модуля VulnScan.....	5
2.3. Компоненты модуля CVEgggregator	6
3. ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ.....	7
3.1. Перечень функциональных возможностей.....	7
3.2. Обнаружение и инвентаризация активов.....	7
3.3. Выявление уязвимостей.....	8
3.4. База данных об уязвимостях	8
3.5. Управление сканированием	9
3.6. Представление результатов и отчётность.....	9
3.7. Интеграция с внешними системами	9
3.8. Разграничение доступа	9
3.9. Лицензирование.....	10
4. ТЕХНОЛОГИЧЕСКИЕ ХАРАКТЕРИСТИКИ.....	11
5. ОГРАНИЧЕНИЯ ТЕКУЩЕЙ ВЕРСИИ.....	12

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование программы

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

1.1.2. Сокращённое наименование программы: CyberDef EASM. В рамках настоящего документа также употребляются термины: программа, платформа.

1.2. Назначение программы

1.2.1. 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.

1.2.2. Основной функцией программы является автоматизированное выявление и анализ уязвимостей внешней поверхности атаки организации.

1.2.3. Программа применяется подразделениями информационной безопасности и информационных технологий для инвентаризации внешнего периметра организации, контроля состава доступных из сети интернет-сервисов и выявления уязвимостей в используемом программном обеспечении.

1.3. Варианты поставки

1.3.1. Программа распространяется в двух вариантах:

- в виде интернет-сервиса (облачного решения), доступного через сеть Интернет, с разделением на организации и ролевой моделью доступа участников;

- в виде программного обеспечения для установки и эксплуатации в информационной инфраструктуре заказчика, в том числе в закрытом контуре без доступа к сети Интернет.

1.3.2. Набор функциональных возможностей в обоих вариантах поставки одинаков. Различия относятся к среде исполнения. В облачном варианте компоненты программы работают под управлением Kubernetes, в варианте установки в инфраструктуре заказчика под управлением Podman.

1.3.3. В варианте установки в закрытом контуре актуальный снимок базы данных об уязвимостях входит в состав дистрибутива и восстанавливается при установке. Дальнейшая актуализация выполняется пакетами обновления, которые передаются на носителе; доступ в сеть Интернет для этого не требуется.

2. СОСТАВ ПРОГРАММЫ

2.1. Модули программы

2.1.1. В состав программы входят два модуля:

– VulnScan, модуль сканирования, выполняющий сценарии обнаружения активов и уязвимостей;

– CVEgggregator, модуль агрегации данных об уязвимостях из NIST NVD, банка данных угроз безопасности информации ФСТЭК России и бюллетеней НКЦКИ.

2.1.2. Модуль VulnScan обращается к модулю CVEgggregator по протоколу HTTP через программный интерфейс REST на этапе сопоставления обнаруженного программного обеспечения с базой данных об уязвимостях.

2.2. Компоненты модуля VulnScan

2.2.1. Состав компонентов модуля VulnScan приведён в таблице 1.

Таблица 1 — Компоненты модуля VulnScan

Компонент	Назначение
data-service	программный интерфейс, доступ к базе данных, разграничение доступа, формирование отчётов
web-ui-tenant	веб-интерфейс пользователя организации
web-ui-admin	веб-интерфейс администратора
pipeline-executor	запуск стадий сканирования
scenario-stage-runner	раскрытие сценария сканирования в стадии, обход дерева активов
entity-saver	сохранение разобранных сущностей в базу данных

Компонент	Назначение
pipeline-result-publisher	публикация результатов стадии, выгрузка артефактов в объектное хранилище
default-connector	разбор вывода инструментов сканирования по декларативной конфигурации
scan-gateway	шлюз между управляющим контуром и выносными раннерами

2.3. Компоненты модуля CVEggregator

2.3.1. Состав компонентов модуля CVEggregator приведён в таблице 2.

Таблица 2 — Компоненты модуля CVEggregator

Компонент	Назначение
api	программный интерфейс REST для чтения и записи данных об уязвимостях
cve_nist_source	загрузка сведений об уязвимостях из NIST NVD
cve_fstek_source	загрузка сведений из банка данных угроз ФСТЭК России
cve_nkcki_json_source	загрузка бюллетеней НКЦКИ в формате JSON
cve_nkcki_pdf_source	загрузка бюллетеней НКЦКИ в формате PDF
cpe_nist_dictionary	загрузка словаря идентификаторов CPE от NIST
cpe_nist_match	сопоставление идентификаторов CPE
dummy_report	веб-интерфейс отчётов модуля

3. ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

3.1. Перечень функциональных возможностей

3.1.1. Основная функция программы обеспечивается следующим набором функциональных возможностей:

- 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.

3.2. Обнаружение и инвентаризация активов

3.2.1. Обнаружение выполняется от единой точки входа, которой является доменное имя организации. Программа последовательно выполняет стадии конвейера сканирования:

- перебор поддоменов по словарю;
- проверка доступности обнаруженных хостов;
- определение IP-адресов;
- сканирование портов;
- определение типа и версии сервиса на открытых портах с формированием идентификатора CPE;
- обход веб-приложений со сбором адресов URL, скачиванием и хешированием обнаруженных файлов.

3.2.2. Результат каждой стадии автоматически передаётся на вход следующей стадии. Выбор стадии определяется типом обнаруженной сущности, ручное сопоставление результатов отдельных инструментов не требуется.

3.2.3. Обнаруженные данные связаны отношением «родитель — потомок». Порт принадлежит IP-адресу, уязвимость принадлежит идентификатору CVE, что обеспечивает формирование целостной картины внешнего периметра организации.

3.3. Выявление уязвимостей

3.3.1. Выявление уязвимостей выполняется сопоставлением идентификатора CVE обнаруженного программного обеспечения с базой данных об уязвимостях.

3.3.2. Каждая выявленная уязвимость дополняется сведениями из базы данных модуля CVEgggregator. Карточка уязвимости содержит описание, оценку и вектор атаки по методике CVSS, уровень критичности, класс слабости CWE, номер и описание из банка данных угроз ФСТЭК России. Приоритет отдаётся описанию ФСТЭК России, при его отсутствии используется описание NIST.

3.4. База данных об уязвимостях

3.4.1. База данных модуля CVEgggregator содержит две группы сведений:

- полную информацию по каждому идентификатору CVE, включая описание, оценку CVSS и вектор атаки, уровень критичности, класс слабости CWE, номер и описание из банка данных угроз ФСТЭК России;

- соответствие «программный продукт — уязвимости», то есть перечень уязвимостей для каждого идентификатора CVE с учётом версии продукта.

3.4.2. Источниками сведений являются NIST NVD, банк данных угроз безопасности информации ФСТЭК России и бюллетени НКЦКИ.

3.4.3. При установке в изолированном контуре модуль работает автономно. Сведения хранятся в базе данных на сервере заказчика, обращения в сеть Интернет при эксплуатации не выполняются.

3.5. Управление сканированием

3.5.1. Режим сканирования настраивается из личного кабинета. Пользователю доступны следующие параметры:

- задержка между отправляемыми пакетами;
- тип сканирования портов;
- строгий режим поиска уязвимостей по идентификатору CPE;
- предельное число адресов URL, собираемых при обходе веб-приложения.

3.5.2. Число одновременно выполняемых потоков сканирования определяется автоматически исходя из выделенных программе вычислительных ресурсов. Сканирование распараллеливается по активам, каждый хост и порт обрабатывается независимо.

3.6. Представление результатов и отчётность

3.6.1. Результаты сканирования отображаются в веб-интерфейсе на интерактивном дашборде.

3.6.2. Программа формирует отчёты по результатам сканирования, в том числе в формате PDF с графическим представлением данных. Состав отчёта задаётся в конструкторе отчётов.

3.6.3. Артефакты, полученные при сканировании, сохраняются в объектном хранилище, совместимом с протоколом.

3.7. Интеграция с внешними системами

3.7.1. Программа обеспечивает формирование инцидента в системе управления инцидентами.

3.7.2. Программа обеспечивает передачу информации о выявленных уязвимостях в системы управления событиями безопасности заказчика.

3.7.3. Сведения об уязвимостях предоставляются по программному интерфейсу REST, что позволяет использовать их в смежных системах заказчика.

3.8. Разграничение доступа

3.8.1. Данные разделяются по организациям. Доступ участников организации определяется ролевой моделью, разграничение данных выполняется на уровне строк базы данных.

3.8.2. Поддерживается двухфакторная аутентификация пользователей.

3.8.3. Интерфейс администратора и интерфейс пользователя организации разделены и работают как отдельные компоненты.

3.9. Лицензирование

3.9.1. В варианте установки в инфраструктуре заказчика работа программы определяется лицензией. Лицензия представляет собой текстовый файл, подписанный электронной подписью поставщика. В файле указываются лицензиат, срок действия, лимиты и разрешённые возможности.

3.9.2. Лицензия ограничивает:

- срок использования программы;
- число активных пользователей организации;
- число администраторов платформы;
- число целей сканирования.

3.9.3. Каждый домен или IP-адрес занимает одну единицу лимита целей сканирования. Повторный учёт одного хоста в разных сценариях не выполняется. Автоматически обнаруженные поддомены, порты, сервисы и уязвимости в лимит не входят. Нулевое значение лимита означает отсутствие ограничения.

3.9.4. Лицензия определяет доступность отдельных возможностей программы, таких как собственные стадии сканирования, сканирование по расписанию, API-токены, импорт конфигурации, собственные шаблоны отчётов и экспорт наборов данных. Право на получение обновлений базы данных об уязвимостях также определяется лицензией.

3.9.5. Лицензия может быть привязана к серверу установки. Привязка выполняется по коду установки, который формируется из отпечатков признаков сервера. Значения оборудования в код не включаются. Возможен выпуск лицензии без привязки.

3.9.6. Лицензия проверяется локально, без обращения к серверу активации, поэтому постоянное подключение к сети Интернет не требуется. Проверка выполняется при установке и в процессе работы, в том числе перед запуском сканирования.

3.9.7. При истечении срока действия или недействительной лицензии новые сканирования, включая запуск по расписанию, не запускаются. Уже запущенное сканирование может завершиться. Доступ к интерфейсу,

сохранённым данным, истории, отчётам и локальной базе данных об уязвимостях сохраняется.

3.9.8. За 30 дней до окончания срока действия лицензии интерфейс выводит предупреждение. Номер, лицензиат, срок действия, лимиты и состояние лицензии отображаются в настройках организации. Замена файла лицензии не требует переустановки программы.

4. ТЕХНОЛОГИЧЕСКИЕ ХАРАКТЕРИСТИКИ

4.1.1. Основные технологические характеристики программы приведены в таблице 3.

Таблица 3 — Технологические характеристики

Характеристика	Значение
Языки программирования	Python 3.13, Go, SQL, JavaScript
Система управления базами данных	PostgreSQL 17
Очередь задач	собственная реализация поверх PostgreSQL, отдельный брокер сообщений не используется
Кеширование и ограничение частоты запросов	Redis 7
Объектное хранилище	хранилище, совместимое с протоколом S3
Средства контейнеризации	Podman для установки в инфраструктуре заказчика, Kubernetes для облачного варианта
Операционная система сервера	Astra Linux 1.8
Веб-интерфейс	серверный рендеринг шаблонов, клиентский код без применения фреймворков

4.1.2. Для работы с веб-интерфейсом программы используется один из следующих браузеров: Яндекс.Браузер версии 20.3.0.1223 и выше, Chrome версии 45 и выше, Mozilla Firefox версии 115 ESR и выше, Safari версии 16.0 и выше.

5. ОГРАНИЧЕНИЯ ТЕКУЩЕЙ ВЕРСИИ

5.1.1. Обнаружение уязвимостей выполняется сопоставлением версии обнаруженного программного обеспечения с базами данных об уязвимостях, без активной эксплуатации и без отдельной проверки каждой уязвимости. Как следствие, возможны ложные срабатывания, а уязвимости, не отражённые в версии продукта, не выявляются.

5.1.2. Проверки выполняются без аутентификации на целевых ресурсах по методу «чёрного ящика». Передача учётных данных для сканирования в текущей версии не предусмотрена.

5.1.3. Точкой входа сканирования является доменное имя. Сканирование заданного диапазона IP-адресов в текущей версии не выполняется.