Программное обеспечение для электронно-вычислительных машин
«Платформа управления внешними угрозами SENTRA»

Информация, необходимая для установки и эксплуатации

Листов 6

г. Москва, 2025 г.

СОДЕРЖАНИЕ

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ

Термин	Определение
ЭВМ	Электронно-вычислительная машина
ПО	Программное обеспечение
АРМ	Автоматизированное рабочее место

1. Введение

Настоящий документ содержит описание информацию, необходимую для установки и эксплуатации платформы управления внешними угрозами SENTRA (далее - Система). Система предназначена для отслеживания внешних угроз в реальном времени.

Исключительные права на Систему принадлежат Обществу с ограниченной ответственностью «ЗАЩИЩЕННЫЕ СИСТЕМЫ».

Система введена в эксплуатацию, поименована как программа для ЭВМ Платформа управления внешними угрозами SENTRA и поставлена на бухгалтерский учет согласно Акту о приеме объекта нематериальных активов №1 от 13.03.2025 г, Приказу о вводе в эксплуатацию нематериальных активов № 1 от 13.03.2025 г., Карточки учета НМА №00-000001 от 13.03.2025 г.

Краткое описание возможностей

Основными возможностями Системы являются:

- автоматизированный поиск корпоративных ресурсов, доступных из сети Интернет;
- регулярное обогащение списка ресурсов;
- регулярный мониторинг портов сервисов;
- выявление уязвимостей систем, сервисов и веб-приложений;
- классификацию уязвимостей по уровню критичности;
- автоматизированный подбор паролей для ssh, ftp, telnet, mssql, postgresql, imap, pop3, smtp, snmp, mysql, vmauthd, vnc, mongodb, asterisk, oracle, xmpp, rdp;
- подбор доменных учетных данных;
- анализ настроек доступа к файлам и папкам веб-серверов с целью предотвращения утечек конфиденциальных данных;
- управление и контроль процесса устранения уязвимостей при экспертной поддержке специалистов ООО «ЗАЩИЩЕННЫЕ СИСТЕМЫ».

2. Установка и эксплуатация Системы

2.1 Уровень подготовки пользователя

Все пользователи Системы должны иметь навыки работы с браузерами. Наличие профильного образования или сертификата о переподготовке позволит быстрее погрузиться в существующие процессы управления уязвимостями и оценки цифровых угроз.

Для получения доступа к ресурсам Системы пользователю необходимо использовать автоматизированное рабочее место (АРМ) в виде электронного вычислительного устройства, имеющего доступ в сеть Интернет, с установленным на него браузером.

2.2 Рекомендуемые требования

Для получения достоверных результатов работы сервиса необходимо внести адреса, предоставляемые ООО «ЗАЩИЩЕННЫЕ СИСТЕМЫ», в списки исключения на периметровых средствах защиты информации (WAF, antiDDoS, NGFW/UTM).

Веб-браузер должен поддерживать выполнение JavaScript-кода и быть совместимым с React 18. Поддерживается последними версиями браузеров:

- Edge 15 или новее,
- Firefox 59 или новее,
- Opera 12.10 или новее,
- Google Chrome 66 или новее.

Рекомендуется регулярно обновлять браузер для обеспечения стабильной работы ПО.

Неподдерживаемые веб-браузеры:

- Internet Explorer,
- Opera версий до версии 12.02,
- прочие браузеры.

Для удобства работы с техническими отчетами, выгружаемыми из интерфейса в формате CSV, рекомендуется установить офисный пакет (например, LibreOffice или Microsoft Office).

2.3 Установка Системы

Система является веб-приложением и не требует установки на АРМ. Доступ к Системе осуществляется через веб-браузер.

Для получения доступа к Системе профиль пользователя должен быть добавлен в Систему администратором после заключения договора. Запуск Системы происходит при открытии ссылки https://easm-dev.pt.singleton-security.ru/ в веб-браузере.

Для того, чтобы начать работу в Системе, следует выполнить следующие действия:

1. Открыть веб-браузер.
2. В адресной строке ввести ссылку на веб-приложение https://easm-dev.pt.singleton-security.ru/ и нажать «Enter» на клавиатуре.
3. Ввести адрес электронной почты и пароль на стартовой странице Системы в соответствующие поля формы авторизации.
4. Нажать на кнопку «Войти».

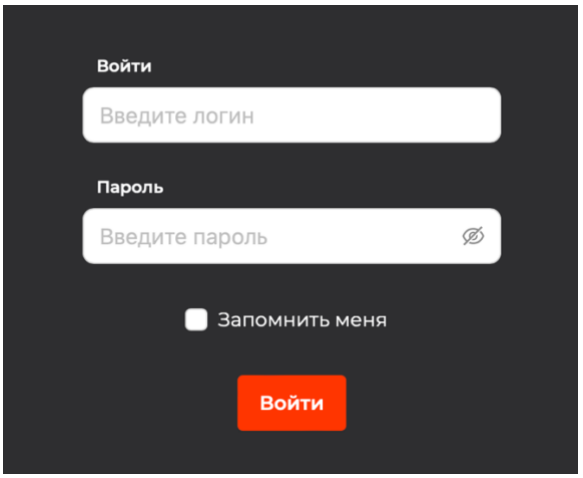

Рисунок 1. Форма авторизации на стартовой странице Системы

Все обновления Системы происходят на сервере. Система доступна только при наличии подключения к сети Интернет.

Для обновления Системы достаточно перезагрузить страницу или выйти, а потом снова зайти в учетную запись.

2.4 Эксплуатация Системы

Подробные инструкции по эксплуатации Системы приведены в документе «Программное обеспечение для электронно-вычислительных машин «Платформа управления внешними угрозами SENTRA». Руководство пользователя».

Пользователи Системы могут обратиться за технической поддержкой и направить обращение:

- на адрес электронной почты: sentra@singleton-security.ru,
- через Telegram-бота поддержки: https://t.me/singleton_easm_support_bot,
- через форму обратной связи, доступную в интерфейсе Системы.

Техническая поддержка направлена на решение следующих задач:

- устранение технических ошибок и неисправностей в работе Системы;
- консультация по функциональности Системы и помощь при возникновении сложностей в работе с Системой.