Программа, использующая описания уязвимостей на языке OVAL для автоматизированных проверок наличия уязвимостей программного обеспечения, работающего под управлением операционных систем Windows

ScanOVAL

Руководство оператора

Листов 13

2018

СОДЕРЖАНИЕ

АННОТАЦИЯ

Назначение документа

Настоящий документ представляет собой руководство пользователя по эксплуатации программы, использующей описания уязвимостей на языке OVAL для автоматизированных проверок наличия уязвимостей программного обеспечения, работающего под управлением операционных систем Microsoft Windows (далее – Программа или ScanOVAL).

Краткое изложение основной части документа

В разделе «Назначение программы» данного документа, приведены сведения о назначении программы и информация, необходимая для понимания функций программы и ее эксплуатации.

В разделе «Условия выполнения программы» указаны условия, необходимые для корректной работы программы (минимальный состав аппаратных и программных средств и т.п.).

Раздел «Выполнение программы» описывает последовательность действий оператора, обеспечивающих загрузку, запуск, выполнение и завершение программы. Приведено описание функций, формата, команд, с помощью которых оператор осуществляет загрузку и управляет выполнением программы, а также ответы программы на эти команды.

В разделе «Сообщения оператору» приведены тексты сообщений, выдаваемых в ходе выполнения программы и описание их содержания.

Настоящий документ «Руководство пользователя» оформлен с учетом требований ЕСПД (ГОСТ 19.101-77 [1)], ГОСТ 19.103-77 [2)], ГОСТ 19.104-78* [3)], ГОСТ 19.105-78* [4)], ГОСТ 19.106-78* [5)], ГОСТ 19.505-79* [6)], ГОСТ 19.604-78* [7)]).

[1)] ГОСТ 19.101-77 ЕСПД. Виды программ и программных документов
[2)] ГОСТ 19.103-77 ЕСПД. Обозначение программ и программных документов
[3)] ГОСТ 19.104-78* ЕСПД. Основные надписи
[4)] ГОСТ 19.105-78* ЕСПД. Общие требования к программным документам
[5)] ГОСТ 19.106-78* ЕСПД. Общие требования к программным документам, выполненным печатным способом
[6)] ГОСТ 19.505-79* ЕСПД. Руководство оператора. Требования к содержанию и оформлению
[7)] ГОСТ 19.604-78* ЕСПД. Правила внесения изменений в программные документы, выполненные печатным способом

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Программа ScanOVAL предназначена для оперативного автоматизированного обнаружения уязвимостей программного обеспечения на рабочих станциях и серверах, функционирующих под управлением операционных систем семейства Microsoft Windows.

Выявление уязвимостей производится на основании сравнения состояния системных параметров сканируемого программного обеспечения (или его компонентов) с базой уязвимостей, представленной в виде OVAL-описаний, разработанных в соответствии со спецификацией OVAL не ниже версии 5.10.1.

Программа позволяет выявлять одиночные и множественные уязвимости, в зависимости от количества поданных ей на вход OVAL-описаний.

Программа предназначена для специалистов в области информационной безопасности для проведения оценки защищенности информационных систем на наличие уязвимостей, сведения о которых содержатся в БДУ, а также других известных уязвимостей, описанных в формате OVAL.

Программа может использоваться для исследовательских целей, в частности, для поиска уязвимостей программного обеспечения, разработки и отладки описаний (определений) на языке OVAL проблем безопасности программных продуктов, функционирующих на платформе Microsoft Windows.

Перед применением Программы внимательно ознакомьтесь с условиями ее лицензирования!

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Полномочия для выполнения программы

Для работы программы требуются права локального администратора.

2.2. Минимальный состав аппаратных средств

Программа устанавливается на компьютеры, оснащенные процессорами семейства Intel (x32, x64) или совместимыми с ними. Конфигурации компьютеров должны соответствовать следующим минимальным требованиям:

- 32-разрядный (x32) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц или выше;
- 1 ГБ (для 32-разрядной системы) или 2 ГБ (для 64-разрядной системы) оперативной памяти;
- 0,5 ГБ свободного места на жестком диске;
- графическое устройство DirectX 9 с драйвером WDDM 1.0 или более поздней версии.

2.3. Среда функционирования программы

Программа функционирует под управлением клиентских операционных систем Microsoft Windows 7/8/8.1/10 или серверных операционных систем Microsoft Windows Server 2008/2008R2/2012/2012R2/2016.

Для обеспечения работы Программы необходимо следующее программное обеспечение:

- Microsoft .NET Framework версии 4.0 или выше;
- интерпретатор языка OVAL 5.10.1 или выше (поставляется совместно с дистрибутивом Программы).

2.4. Требования к персоналу (пользователю)

Пользователь программы (оператор) должен быть ознакомлен с настоящим Руководством и обладать практическими навыками работы с графическим пользовательским интерфейсом операционных систем Microsoft Windows.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Установка и запуск программы

Установка программы осуществляется с помощью инсталляционного пакета ScanOVAL.msi.

Запустите исполняемый файл ScanOVAL.msi. Дождитесь появления окна приветствия и нажмите кнопку «Далее». В случае, если на компьютере уже установлена программа ScanOVAL, инсталлятор предложит осуществить следующие операции выполнения: «Изменить», «Восстановить», «Удалить».

Далее в появившемся окне будет предложено ознакомиться с лицензионным соглашением. После ознакомления с содержимым выберете пункт «Я принимаю условия данного лицензионного соглашения» и нажмите кнопку «Далее».

Укажите каталог, в который будут установлены файлы программы. По умолчанию используются следующие каталоги:

для 32-х битных систем: «C:\Program Files\ScanOVAL»;

для 64-х битных систем: «C:\Program Files (x86)\ScanOVAL»;

В результате нажатия кнопки «Далее» появится окно «Все готово к установке ScanOVAL». В следующем окне необходимо нажать кнопку «Установить», в результате чего появится статусная строка установочного процесса. О завершении процесса установки будет свидетельствовать сообщение «Установка ScanOVAL завершена», при этом на рабочем столе появится ярлык программы.

ВАЖНО! Установка и запуск программы должны проводиться от имени учетной записи, имеющей административные привилегии на компьютере.

3.2. Интерфейс программы

Графический интерфейс программы ScanOVAL представляет собой окно, разделенное на четыре логических зоны (Главное окно):

- строка меню, расположена в верхней части окна, предназначена для доступа к сервисным функциям программы, настройке программы и справке;
- панель быстрого доступа, расположена ниже строки меню, содержит функциональные кнопки для работы с Программой;
- панель «Результаты», расположена в центральной части Главного окна, отображает список результатов проверок;
- панель «Подробности», расположена в нижней части программы, отображает детализированную информацию об уязвимости.

3.3. Работа с программой

3.3.1. Загрузка описаний уязвимостей

Для автоматического обнаружения уязвимостей необходимо в программу ScanOVAL загрузить соответствующие XML-файлы, содержащие OVAL-описания уязвимостей.

Программа работает с описаниями уязвимостей, разработанным в соответствии со спецификацией OVAL версии не ниже 5.10.1. OVAL-описания могут быть загружены с сайта банка данных угроз безопасности информации ФСТЭК России (БДУ ФСТЭК России).

Загружаемый XML-файл с OVAL-описаниями может содержать как описания одиночных уязвимостей, так и множественные (пакетные) описания, собранные в один файл.

Для загрузки описаний уязвимостей в «Главном окне программы» (Рисунок 1 – Главное окно программы) необходимо нажать на кнопку  («Открыть файл»). Открываемый XML-файл может быть загружен с локального диска компьютера, сетевого диска или иного места, доступного пользователю на данном компьютере.

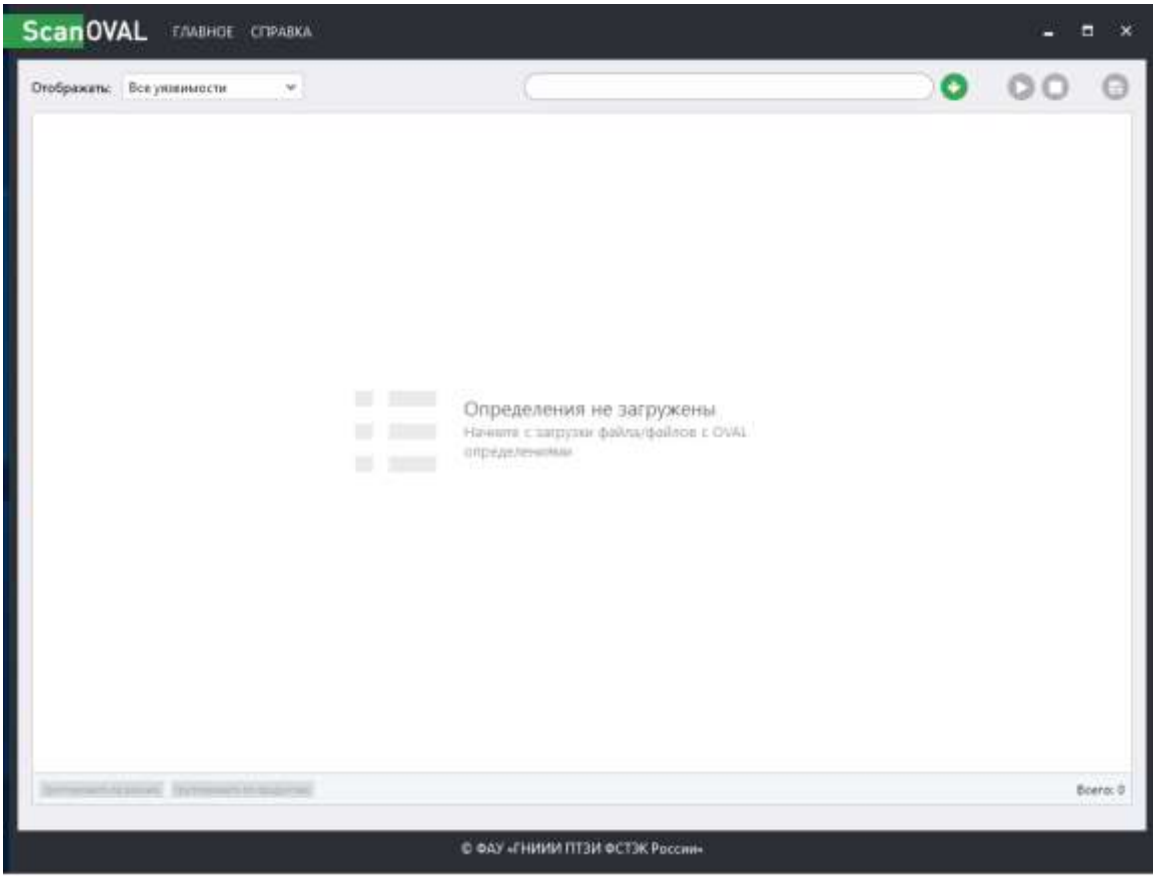

Рисунок 1 – Главное окно программы

В появившемся окне «Проводника». Выбрать необходимый файл и нажать кнопку «Открыть». В главном окне программы появится список выбранных описаний уязвимостей (Рисунок 2 – Список выбранных описаний уязвимостей).

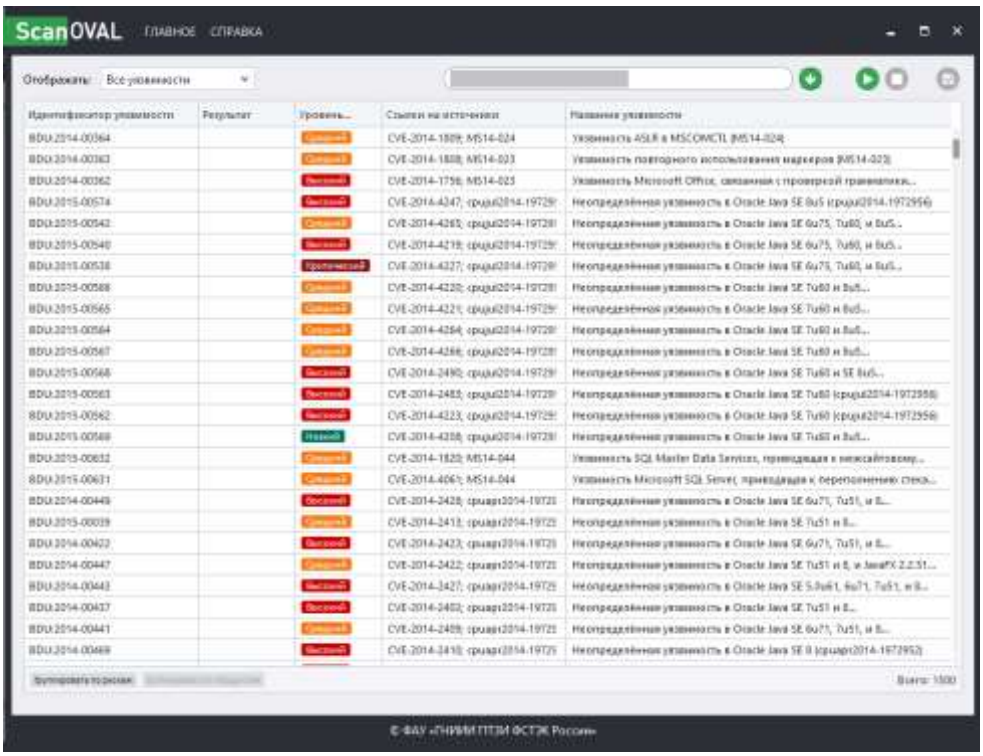

Рисунок 2 – Список выбранных описаний уязвимостей

В программе присутствует возможность добавления новых файлов и выгрузки уже используемых. Для этого необходимо воспользоваться диалогом выбора OVAL файлов (Рисунок 3).

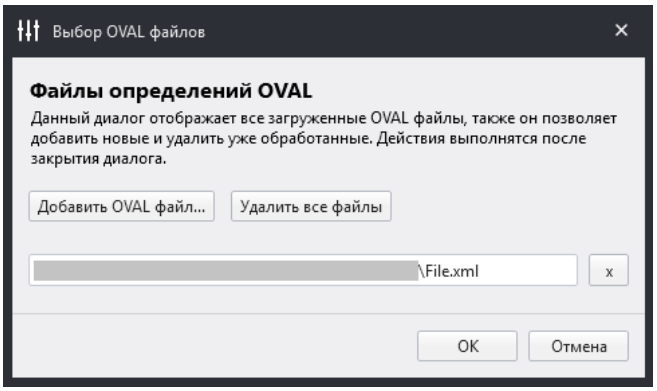

Рисунок 3 – Окно «Выбор OVAL файлов»

Данное окно вызывается автоматически по нажатию кнопки  («Открыть файл») повторно, при уже загруженном файле описании уязвимостей, то есть при первой загрузке пользователю отображается стандартное диалоговое окно Windows для выбора файла, все последующие нажатия открывают окно «Выбор OVAL файлов».

3.3.2. Обнаружение уязвимостей

Функция «Обнаружение уязвимостей» становится доступной при наличии загруженных в программу описаний уязвимостей.

Для обнаружения уязвимостей необходимо нажать на кнопку «Выполнить аудит»  . При этом в главном окне появится сообщение «Выполнение…» и на затемненном фоне окна будет наблюдаться динамика выполнения проверок.

Свидетельством окончания проверок является исчезновение сообщения «Выполнение…» и в главном окне появятся результаты проверок с подсвеченными маркерами сообщениями – «не обнаружено» / «обнаружено» (Рисунок 4).

Время сканирования проверок зависит от количества загруженных OVAL-описаний, а также от аппаратных ресурсов компьютера. Сканирование может занимать от нескольких секунд для одного или нескольких описаний до нескольких минут и более для сотен и тысяч загруженных описаний.

При работе со списком уязвимостей доступны группировки по рискам и по продуктам (Рисунок 4).

Группировка по рискам доступна после загрузки файлов OVAL-описаний. Группировка происходит после нажатия на кнопку «Группировать по рискам» в левой нижней части окна, в результате осуществляется группировка по столбцу «Уровень опасности уязвимости»;

Группировка по продуктам доступна только после проведения проверки обнаружения уязвимостей и происходит после нажатия на кнопку «Группировать по продуктам» в левой нижней части окна, в результате осуществляется группировка по классификатору CPE (Common Platform Enumeration).

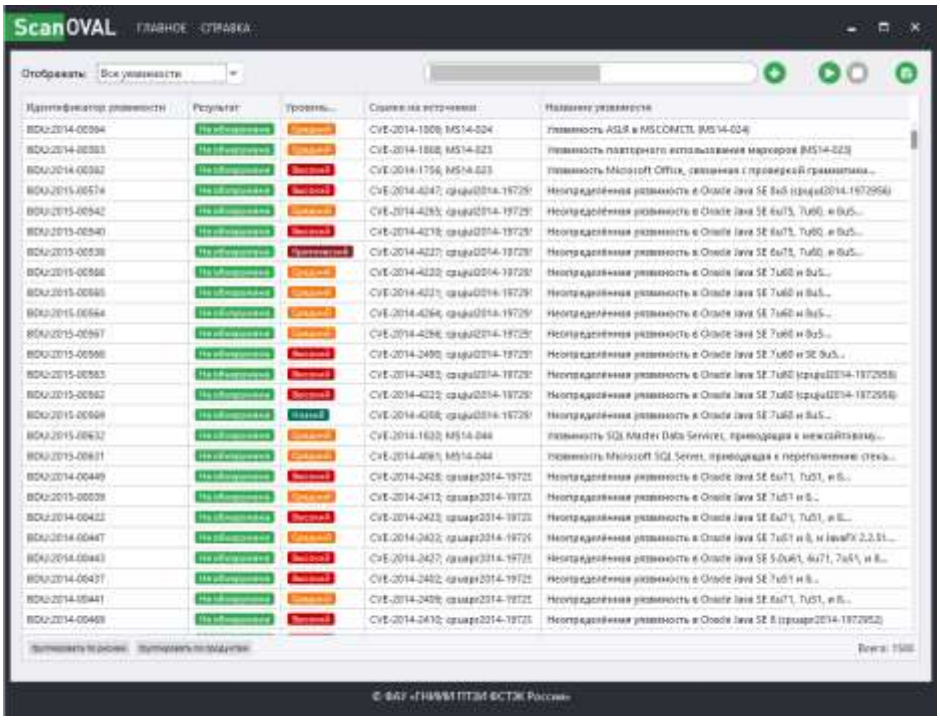

Рисунок 4 – Результат выполненной проверки

3.3.3. Просмотр результатов проверок

Результаты проверок отображаются в Главном окне программы на панелях «Результаты» и «Подробности».

Панель «Результаты» содержит общую информацию о результатах проверок. В строке результата отображается следующая информация:

- Идентификатор уязвимости – идентификатор уязвимости в БДУ ФСТЭК России;
- Результат – результат проверки («Обнаружено» / «Не обнаружено»);
- Уровень опасности уязвимости;
- Ссылки на источники описания уязвимости;
- Название уязвимости.

Панель «Подробности» расположена ниже панели «Результаты» и раскрывается кликом мыши по строке результата проверки или нажатием на кнопку «Подробности» (Рисунок 5 – Детализированная информация об уязвимости).

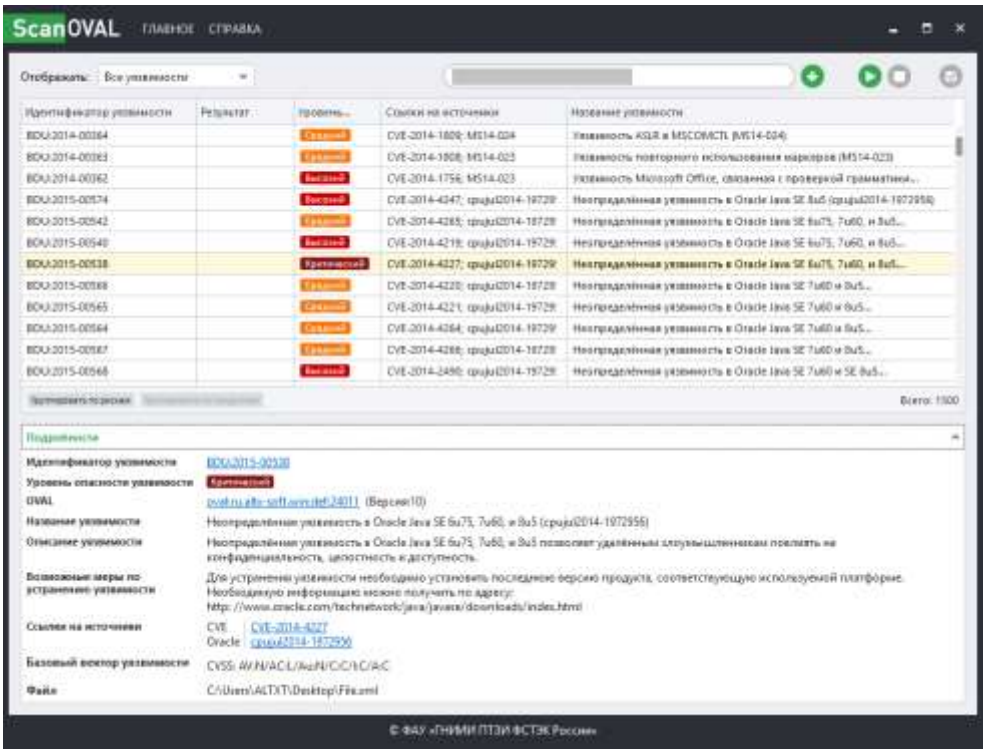

Рисунок 5 – Детализированная информация об уязвимости

В панели представлена детализированная информация об уязвимости:

- Идентификатор уязвимости в БДУ ФСТЭК России, содержащий гиперссылку на соответствующую страницу сайта БДУ ФСТЭК России;
- Результат – результат проверки: «Обнаружена» / «Не обнаружена»;
- Уровень опасности уязвимости;
- OVAL – путь к месту загрузки OVAL-описания;
- Название уязвимости;
- Описание уязвимости;

- Возможные меры по устранению уязвимости;
- Ссылки на источники;
- Базовый вектор уязвимости (CVSS);
- Программное обеспечение – обозначение уязвимого программного обеспечения в классификации CPE (Common Platform Enumeration);
- Детализация – объект для которого осуществлялась проверка;
- Файл – путь к расположению уязвимого ПО (файла). Данная строка появляется только при выявлении уязвимости.

3.3.4. Сохранение результатов проверок

Программа позволяет сохранять на локальном компьютере или любом доступном для компьютера месте результаты сканирования в формате HTML.

Для сохранения результатов проверок в Главном окне нажмите на кнопку «Создать отчет»  .

В появившемся окне «Проводника» укажите место для сохранения отчета и нажмите кнопку «Сохранить». После сохранения появится сообщение «Отчет сохранен». Для просмотра сохраненных отчетов можно воспользоваться произвольным веб-браузером.

3.3.5. Завершение выполнения программы

Работа Программы завершается нажатием на кнопку  в правом верхнем углу или через Меню: Главное -> Выйти из программы.

3.4. Настройка параметров программы

Для удобства работы с программой предусмотрен ряд настроек. По желанию пользователя некоторые настройки по умолчанию могут быть изменены.

Панель «Настройки» расположена в закладке «Главное». В данной панели можно произвести/просмотреть следующие настройки (Рисунок 6 – Панель настроек):

- «Сохранять файл результатов» – генерирует файл с отчётом о найденных уязвимостях в формате XML. Параметр включен по умолчанию;
- «Генерировать HTML файл» – генерирует файл с отчётом о найденных уязвимостях в формате HTML. Параметр включен по умолчанию;
- «Сохранять файл системных характеристик» – генерирует при каждом сканировании файл с основными параметрами системы. Параметр включен по умолчанию;
- «Выполнять проверку XSD входных данных» – проверяет входные данные на корректность с помощью XSD-схем;
- «Папка с данными» – задает путь к папке с OVAL-описаниями, к которой по умолчанию будет обращаться программа;

- «Папка с отчетами» – задает путь к папке, в которую по умолчанию будут сохраняться отчеты о результатах проверки;

- «Папка с временными файлами» – отображает путь к временным файлам, создаваемым при работе программы;

- «Папка с файлами XSD» – отображает путь к файлам XSD-схем;

- «Папка с логами» – отображает путь до каталога, в который осуществляется сохранение сведений о работе программы (журнал событий).

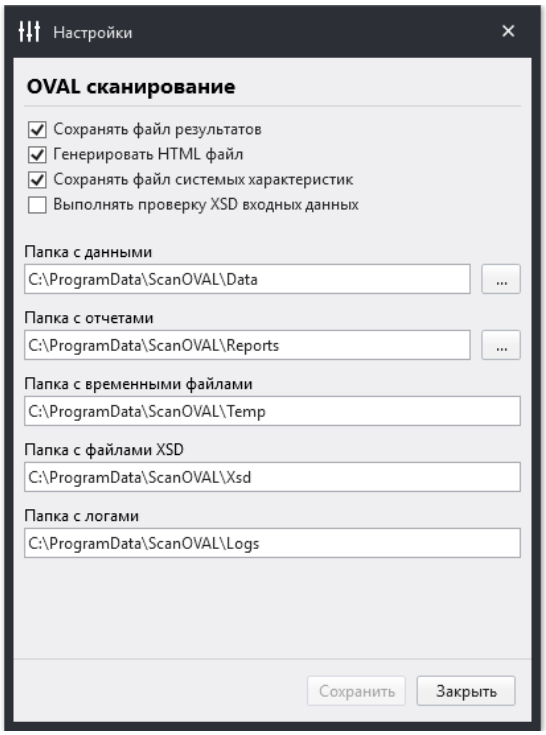

Рисунок 6 – Панель настроек

4. СООБЩЕНИЯ ОПЕРАТОРУ

4.1 Сообщения, свидетельствующие об ошибках при загрузке OVAL-описаний. Данные сообщения означают, что выбранные файлы не подходят для осуществления OVAL-сканирования. При этом конкретные причины ошибок отображаются в выпадающем меню «Подробные сведения» (рисунки 7 – 9).

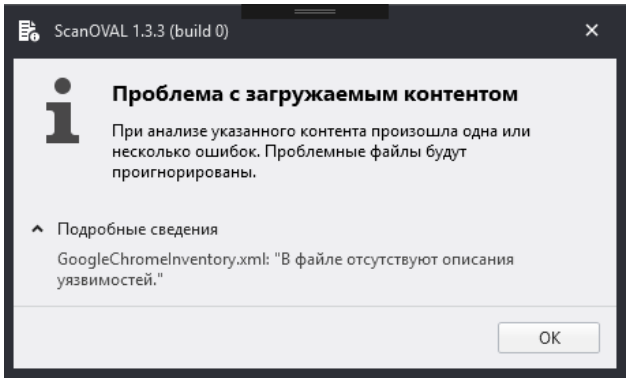

Рисунок 7 – В файле отсутствуют описания уязвимостей

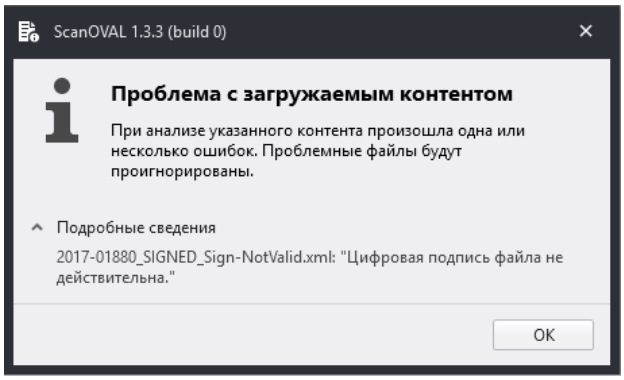

Рисунок 8 – Цифровая подпись не действительна

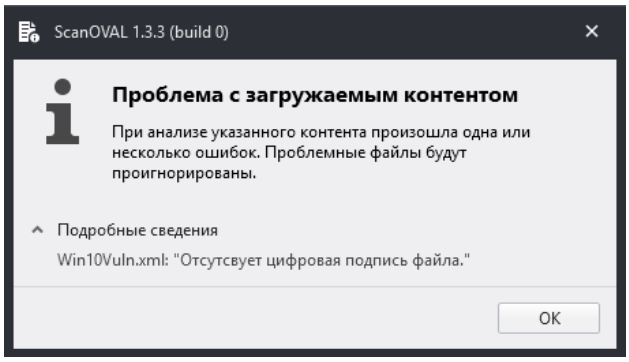

Рисунок 9 – Отсутствует цифровая подпись файла

4.2 Сообщение, возникающее при повторном запуске программы «ScanOVAL». Программа допускает запуск только одного экземпляра.

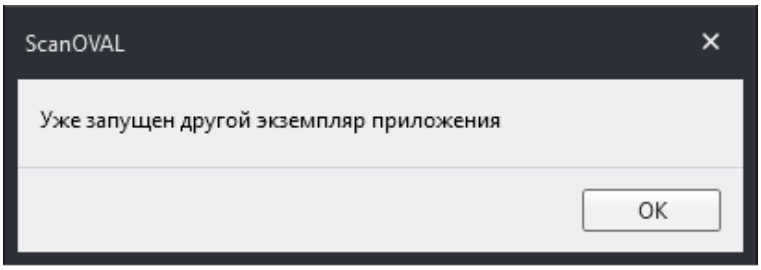

Рисунок 10 – Попытка повторного запуска программы «ScanOVAL»