ПРОГРАММА, ИСПОЛЬЗУЮЩАЯ ОПИСАНИЯ УЯЗВИМОСТЕЙ НА ЯЗЫКЕ OVAL ДЛЯ АВТОМАТИЗИРОВАННЫХ ПРОВЕРОК НАЛИЧИЯ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, РАБОТАЮЩАЯ ПОД УПРАВЛЕНИЕМ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА LINUX

Astra Linux Special Edition 1.7

Руководство оператора

Листов 18

2023

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящих отчетных материалах о научно-исследовательской работе применяют следующие обозначения и сокращения:

БДУ – банк данных угроз безопасности информации

ОС – операционная система

ПО – программное обеспечение

1 Назначение программы

Программное обеспечение Astra Linux Special Edition 1.7 (далее – Программа) предназначено для оперативного автоматизированного обнаружения уязвимостей программного обеспечения (ПО) на рабочих станциях и серверах, функционирующих под управлением операционных систем (ОС) семейства Linux.

Выявление уязвимостей производится на основании сравнения состояния системных параметров сканируемого ПО (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 банке данных угроз безопасности информации (далее – БДУ), а также других известных уязвимостей, описанных в формате OVAL.

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

2 Условия выполнения программы

2.1 Полномочия для выполнения программы

Для установки программы требуется учетная запись root или другая учетная запись с привилегиями суперпользователя.

2.2 Минимальный состав аппаратных средств

Конфигурация компьютера должна соответствовать следующим минимальным требованиям:

- процессор с тактовой частотой 1 ГГц или выше;
- не менее 512 Мб оперативной памяти;
- 0,5 Гб свободного места на жестком диске.

2.3 Среда функционирования программы

Программа функционирует под управлением ОС Astra Linux 1.7 SE.

Для обеспечения работы Программы необходимо следующее ПО:

- графический интерфейс пользователя Fly 2.0;
- Xorg версии 7.7;
- qt 5.11;
- libcurl3 (поставляется совместно с дистрибутивом Программы);
- openscap-scanner;
- openscap-common;
- openssl.

2.4 Требования к персоналу (пользователю)

Пользователь Программы (оператор) должен быть ознакомлен с настоящим Руководством оператора и обладать навыками администрирования и работы с ОС семейства Linux.

3 Выполнение программы

3.1 Установка и запуск программы

Программа представлена в виде архива, содержащего локальный репозиторий scanovalrepo. Репозиторий включает в себя пакет программы, описания уязвимостей в формате OVAL, а также необходимые зависимости для работы Программы.

ВАЖНО! Перед установкой Программы необходимо подключение ОС Astra Linux 1.7 SE к репозиторию base. Подробная информация приведена в официальной документации на ОС: https://wiki.astralinux.ru/pages/viewpage.action?pageId=149062354

Для инсталляции Программы необходимо выполнить следующие действия.

1. Скопировать на компьютер в домашнюю директорию пользователя архив локального репозитория.

2. Разархивировать репозиторий путем выполнения следующих команд:

cd ~

sudo tar -C /var/lib -xvf <scanovalrepo_name>.tar.gz

3. Установить открытый ключ:

sudo apt-key add /var/lib/scanoval/repo/PUBLIC-GPG-KEY-scanoval

4. Создать конфигурационный файл локального репозитория:

sudo touch /etc/apt/sources.list.d/scanoval.list

5. Добавить в файл /etc/apt/sources.list.d/scanoval.list следующую строку:

deb file:///var/lib/scanoval/repo 1.7_x86-64 main content

Сохранить изменения.

6. Обновить информацию о пакетах и их источниках командой:

sudo apt-get update

7. Установить Программу путем выполнения следующей команды:

sudo apt-get install openscap-scanner openscap-common openssl scanoval scanoval-content-alse17

8. Запустить Программу путем выполнения следующей команды:

/usr/bin/scanoval.

Для удаления Программы необходимо выполнить команды:

sudo apt-get remove openscap-scanner openscap-common scanoval scanoval-content-alse17

sudo apt-get autoremove

ВАЖНО! Установка Программы должна проводиться от имени учетной записи root или другой учетной записи с привилегиями суперпользователя.

Перед запуском Программы должен быть отключен режим Замкнутой программной среды.

3.2 Процедура обновления контента программы

Обновления контента поставляются в виде очередных версий пакета <scanovalcontentname_version>.deb, установка которого осуществляется следующим способом:

1. Удалить текущую версию контента:

sudo apt-get remove scanoval-content-alse17

2. Поместить в домашнюю директорию пользователя файл обновления контента <scanovalcontentname_version>.deb

3. Выполнить команды:

cd ~

sudo dpkg-deb –x <scanovalcontentname_version>.deb /

4. Запустить Программу путем выполнения следующей команды:

/usr/bin/scanoval

4 Интерфейс программы

Графический интерфейс Программы представляет собой Главное окно, которое разделено на четыре логических зоны:

- строка меню (рисунок 1), расположена в верхней части окна и предназначена для доступа к сервисным функциям Программы, настройке Программы и справке;

Рисунок 1 – Строка меню

- панель быстрого доступа (рисунок 2), расположена ниже строки меню и содержит функциональные кнопки для работы с Программой;

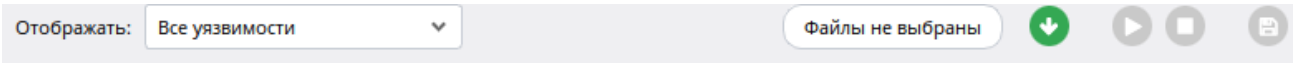


Рисунок 2 – Панель быстрого доступа

- панель «Результаты» (рисунок 3), расположена в центральной части Главного окна, отображает список результатов проверок;

Идентификатор уязвимости	Результат	Уровень опасности	Ссылки на источники	Название уязвимости
BDU:2020-05481		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в intel-microcode (2022-0819SE17)
BDU:2021-05257		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05230		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в python-urllib3 (2022-0819SE17)
BDU:2021-05198		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в bluez (2022-0819SE17)
BDU:2021-03430		Высокий	2022-0819SE17, ...	Astra Linux -- уязвимость в bluez (2022-0819SE17)
BDU:2021-05199		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05200		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-06406		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в glibc (2022-0819SE17)
BDU:2021-05312		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05250		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05249		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05306		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05305		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05304		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05293		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-03740		Высокий	2022-0819SE17, ...	Astra Linux -- уязвимость в python2.7 (2022-0819SE17)
BDU:2022-00004		Критический	2022-0819SE17, ...	Astra Linux -- уязвимость в samba (2022-0819SE17)
BDU:2020-03619		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в ia32-libs, sqlite3 (2022-0819SE17)

Группировать по рискам | Группировать по продуктам | Всего: 981

Рисунок 3 – Панель «Результаты»

- панель «Подробности» (рисунок 4), расположена в нижней части окна программы, отображает детализированную информацию об уязвимости.

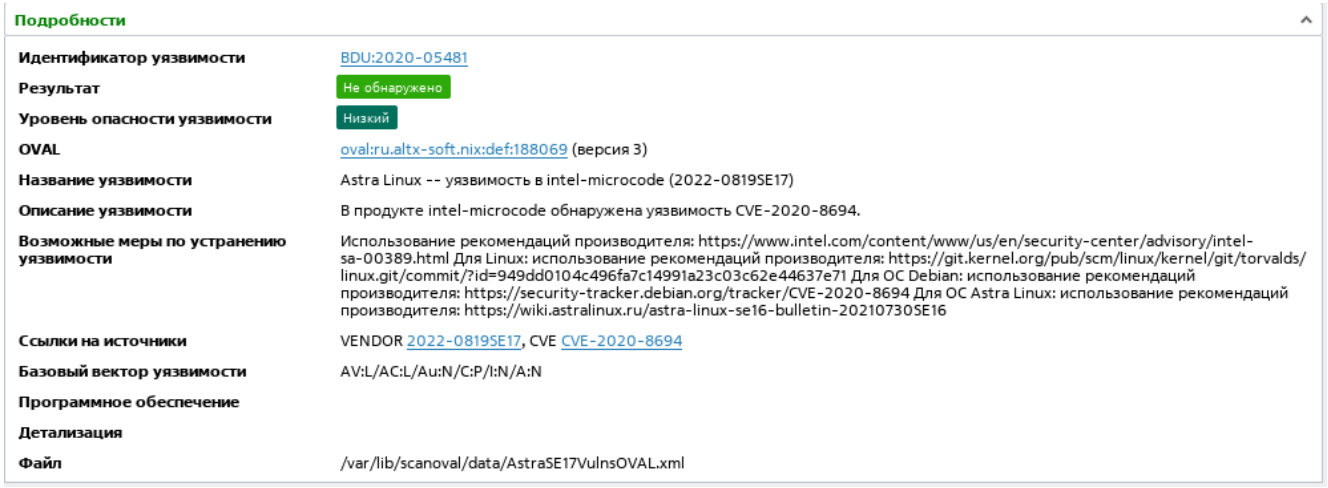


Рисунок 4 – Панель «Подробности»

5 Работа с программой

5.1 Загрузка описаний уязвимостей

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

Программа работает с произвольными описаниями уязвимостей, разработанным в соответствии со спецификацией OVAL версии не ниже 5.10.1.

Загружаемый XML-файл с OVAL-описанием может содержать:

- описания одиночных уязвимостей;
- множественные (пакетные) описания, собранные в один файл.

Для загрузки описаний уязвимостей в Главном окне программы необходимо нажать на кнопку  «Открыть файл» (рисунок 5). XML-файл может быть загружен с локального диска компьютера, сетевого диска или иного места, доступного пользователю на данном компьютере.

XML-файл с OVAL-описаниями уязвимостей, поставляемый вместе с Программой, находится в папке по умолчанию «/var/lib/scanoval/data».

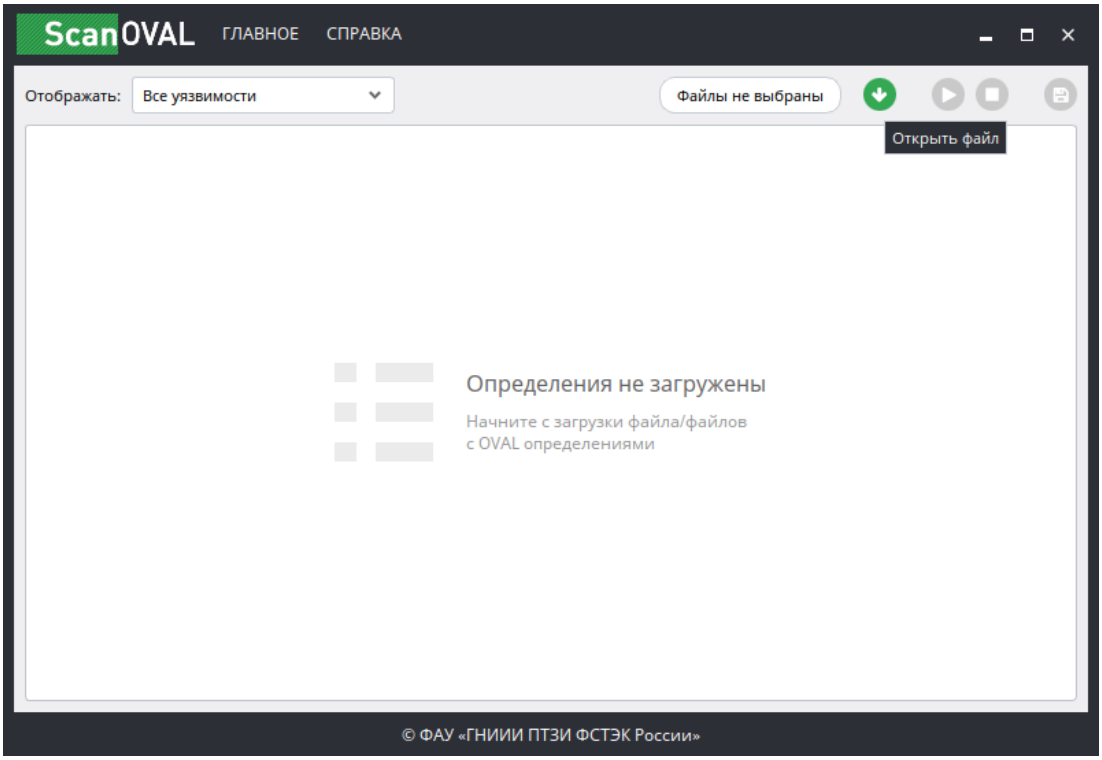


Рисунок 5 – Главное окно программы

В появившемся диалоговом окне выбрать необходимый файл и нажать кнопку «Открыть». В Главном окне программы появится список выбранных описаний уязвимостей (рисунок 6).

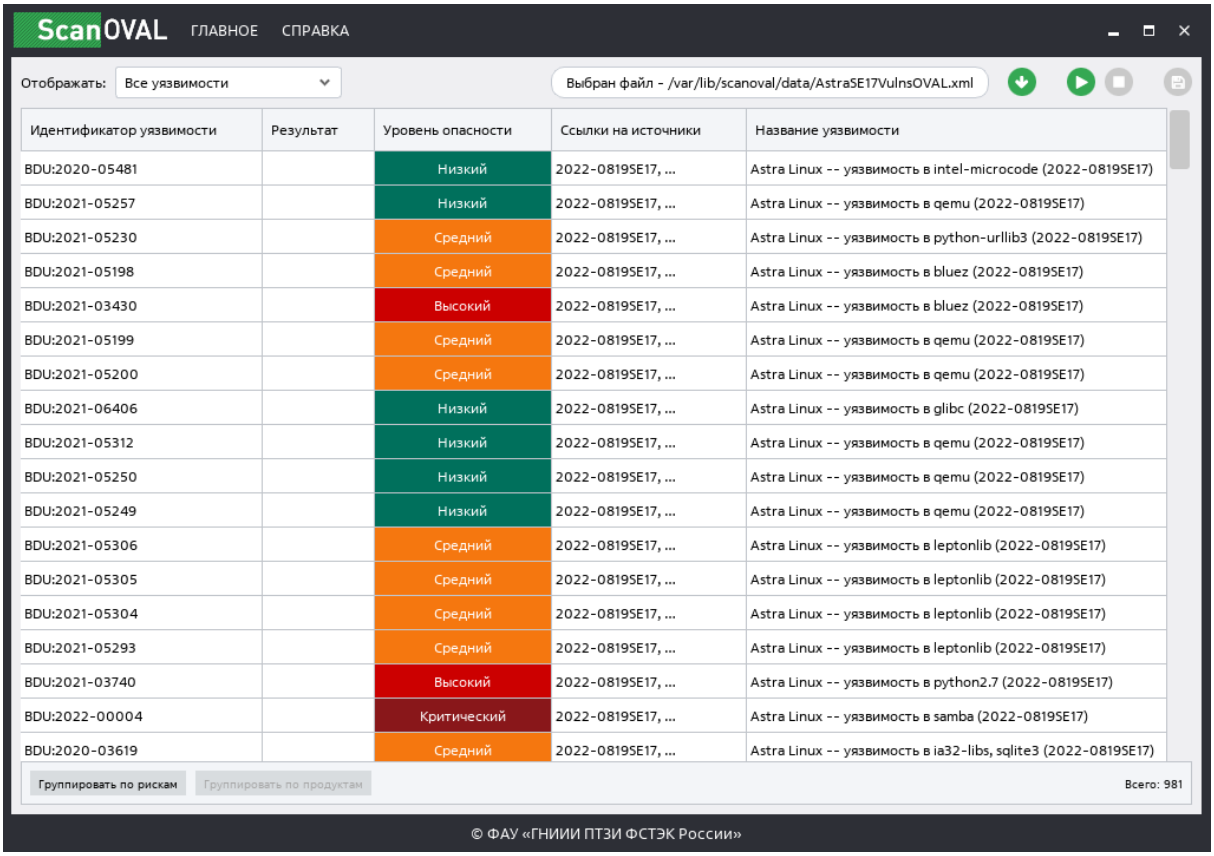


Рисунок 6 – Список выбранных описаний уязвимостей

Для добавления или удаления уже загруженных OVAL-описаний необходимо повторно нажать кнопку  и в появившемся окне (рисунок 7) выбрать требуемую операцию: «Добавить OVAL файл» или «Удалить все файлы». Добавление осуществляется в диалоговом режиме. Для подтверждения операции необходимо нажать кнопку «Загрузить».

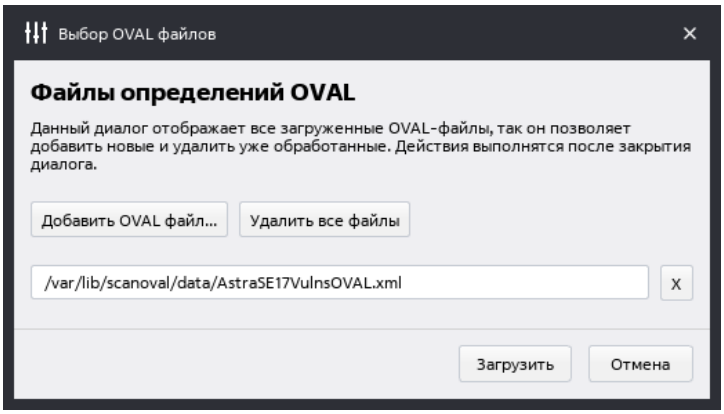


Рисунок 7 – Окно добавления/удаления OVAL-описаний

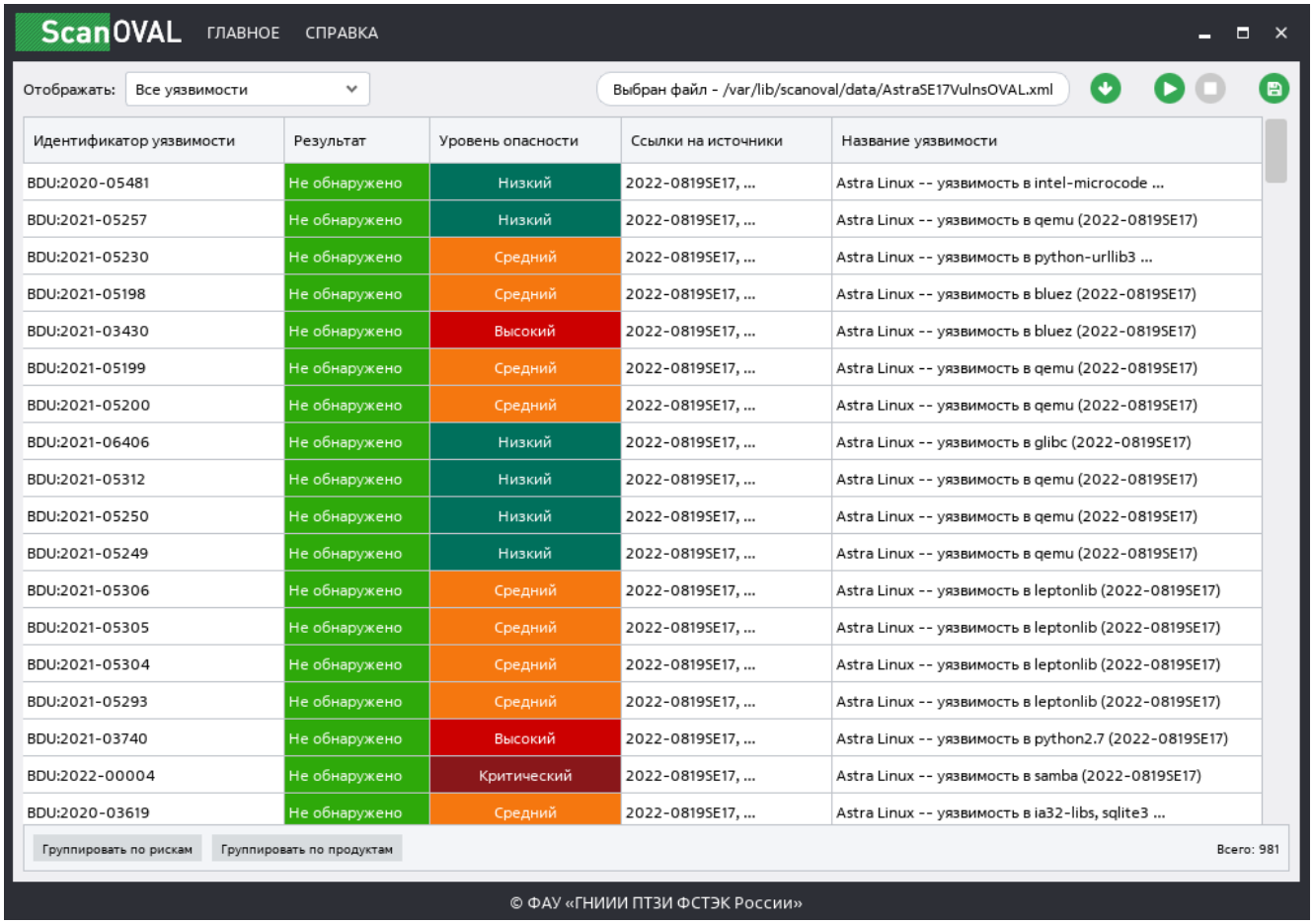
5.2 Обнаружение уязвимостей

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

Для обнаружения уязвимостей необходимо нажать на кнопку «Выполнить аудит»  , в результате чего в Главном окне появится сообщение «Выполнение…», а на затемненном фоне окна будет наблюдаться динамика выполнения проверок.

Время осуществления 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.

По окончании проверок сообщение «Выполнение…» исчезает, при этом в Главном окне появляются результаты проверок с сообщениями «обнаружено» / «не обнаружено» (рисунок 8).



Идентификатор уязвимости	Результат	Уровень опасности	Ссылки на источники	Название уязвимости
BDU:2020-05481	Не обнаружено	Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в intel-microcode ...
BDU:2021-05257	Не обнаружено	Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05230	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в python-urllib3 ...
BDU:2021-05198	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в bluez (2022-0819SE17)
BDU:2021-03430	Не обнаружено	Высокий	2022-0819SE17, ...	Astra Linux -- уязвимость в bluez (2022-0819SE17)
BDU:2021-05199	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05200	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-06406	Не обнаружено	Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в glibc (2022-0819SE17)
BDU:2021-05312	Не обнаружено	Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05250	Не обнаружено	Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05249	Не обнаружено	Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05306	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05305	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05304	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05293	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-03740	Не обнаружено	Высокий	2022-0819SE17, ...	Astra Linux -- уязвимость в python2.7 (2022-0819SE17)
BDU:2022-00004	Не обнаружено	Критический	2022-0819SE17, ...	Astra Linux -- уязвимость в samba (2022-0819SE17)
BDU:2020-03619	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в ia32-libs, sqlite3 ...

Рисунок 8 – Результат выполненной проверки

5.3 Просмотр результатов проверок

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

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

- Идентификатор уязвимости – идентификатор уязвимости в БДУ;
- 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 9).

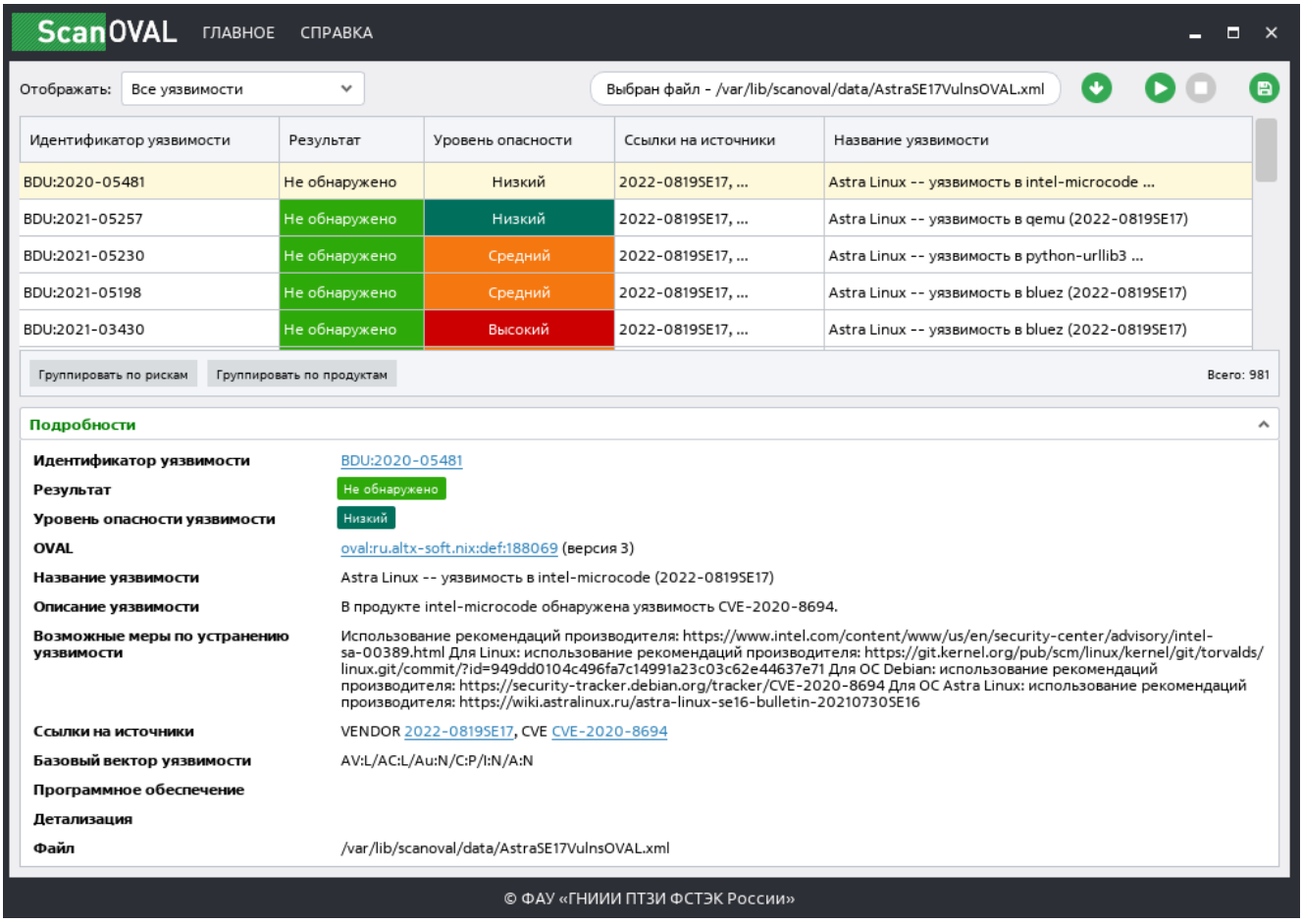


Рисунок 9 – Детализированная информация об уязвимости

В панели представлена детализированная информация об уязвимости:

- Идентификатор уязвимости в БДУ, содержащий гиперссылку на соответствующую страницу сайта БДУ;

- 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.

5.4 Сохранение результатов проверок

Программа позволяет сохранять на локальном компьютере или любом доступном для компьютера месте результаты сканирования в одном из выбранных форматов: HTML, CSV.

Для сохранения результатов проверок в Главном окне необходимо нажать на кнопку «Сохранить отчет»  и выбрать необходимый формат и путь сохранения файла (рисунок 10):

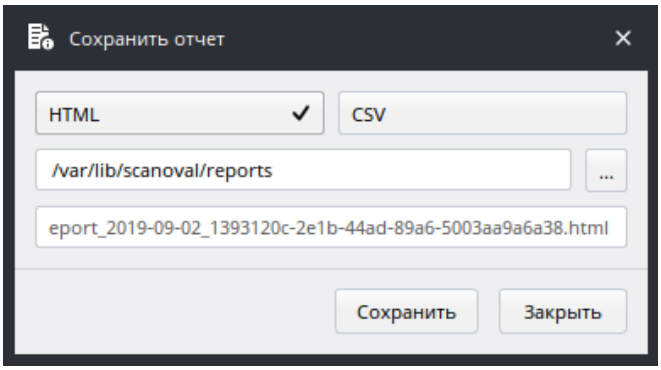


Рисунок 10 – Окно сохранения результатов проверок

В результате формирования и сохранения отчета появится сообщение «Отчет сохранен. Открыть сохраненный отчет» (рисунок 11).

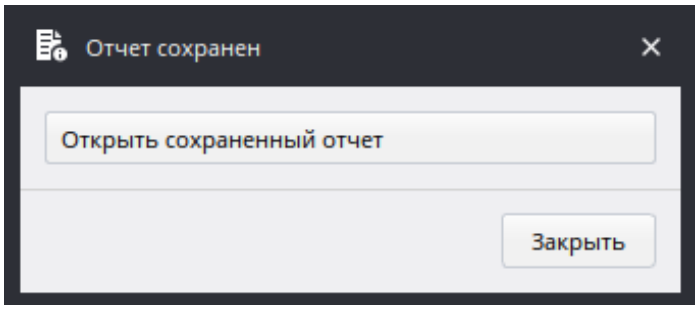


Рисунок 11 – Сообщение об успешном создании
и сохранении отчета

Для просмотра сохраненных отчетов в формате HTML может быть использован произвольный браузер. Просмотр отчетов в формате CSV осуществляется в программных средствах для работы с электронными таблицами.

5.5 Завершение выполнения программы

Работа Программы завершается нажатием на кнопку  в правом верхнем углу или через строку меню, путем перехода в закладку «Главное» и последующего выбора пункта «Выйти из программы».

6 Настройка параметров программы

Для удобства работы с Программой предусмотрен ряд настроек. Окно «Настройки» вызывается из закладки «Главное». В данном окне можно выполнить следующие настройки (рисунок 12):

- «Сохранять файл результатов» – применяется при необходимости генерации файла с отчётом о найденных уязвимостях в формате XML. Параметр включен при стандартных настройках;
- «Генерировать HTML файл» – применяется при необходимости генерации файла с отчётом о найденных уязвимостях в формате HTML. Параметр включен при стандартных настройках;
- «Сохранять файл системных характеристик» – применяется при необходимости генерации при каждом сканировании файла с основными параметрами системы. Параметр включен при стандартных настройках;
- «Выполнять проверку XSD входных данных» – применяется при необходимости проверки входных данных на корректность с применением XSD-схем;
- «Папка с данными» – применяется в случае необходимости задания пути к директории с OVAL-описаниями, к которой будет обращаться Программа при стандартных настройках;
- «Папка с отчетами» – применяется для задания пути к директории, в которую при стандартных настройках будут сохраняться отчеты о результатах проверки;
- «Папка с временными файлами» – применяется для задания пути к временным файлам, создаваемым при работе программы;
- «Папка с файлами XSD» – применяется для задания пути к файлам, содержащим XSD-схемы;
- «Папка с логами» – применяется для задания пути к директории для сохранения сведений о работе программы (журнала).

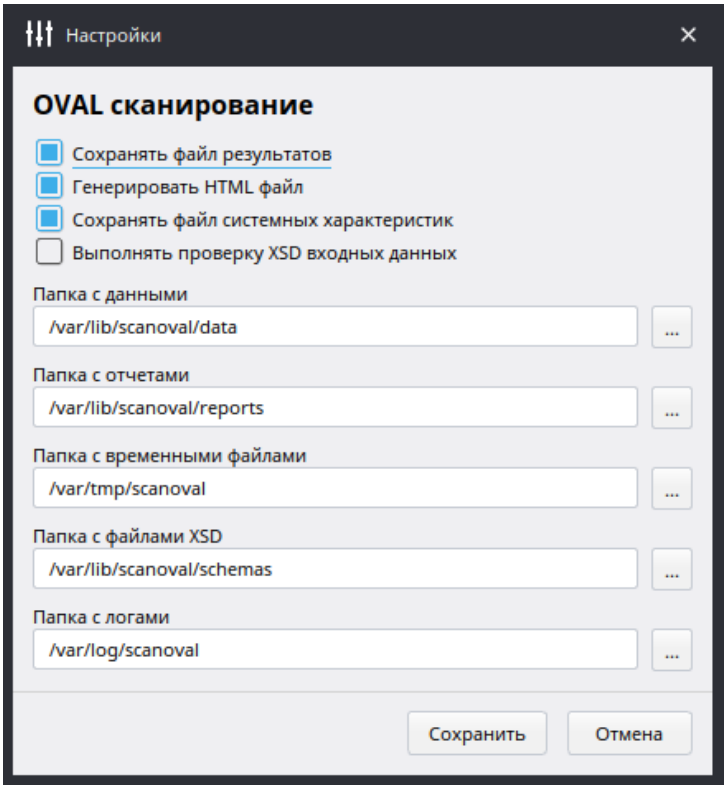


Рисунок 12 – Окно настроек

7 Сообщения оператору

7.1 Сообщение при отсутствии файлов XSD-схем

При отсутствии файлов, содержащих XSD-схемы, возникает сообщение, представленное на рисунке 13.

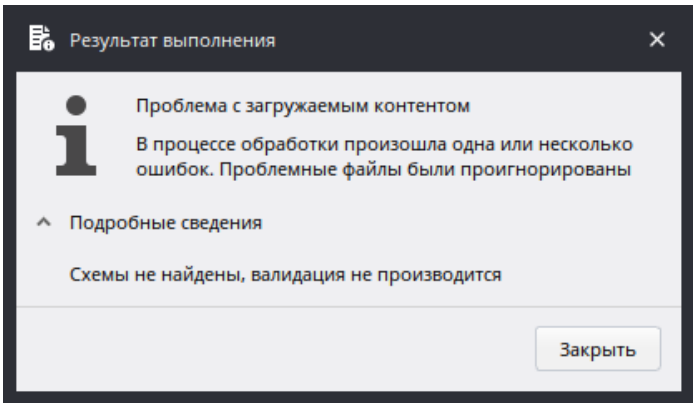


Рисунок 13 – Сообщение об отсутствии файлов XSD-схем

7.2 Сообщение о неверной цифровой подписи загружаемых файлов

В случае возникновения ошибок при проверке цифровой подписи загружаемых файлов с OVAL-описаниями уязвимостей возникает сообщение, представленное на рисунке 14.

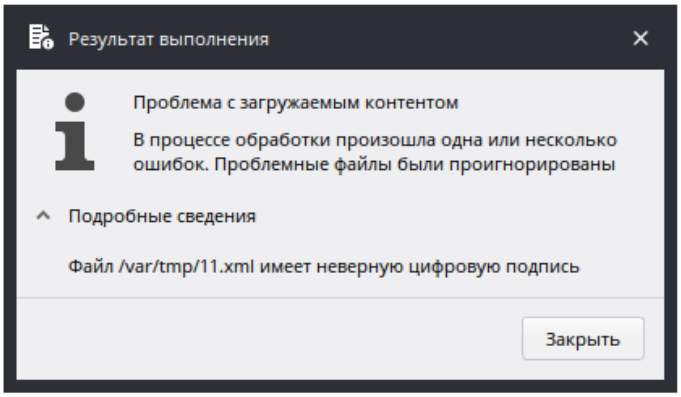


Рисунок 14 – Сообщение о неверной цифровой подписи загружаемых OVAL-описаний уязвимостей