

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

РОСА «КОБАЛЬТ»

Руководство оператора

Листов 17

СОДЕРЖАНИЕ

Обозначения и сокращения	3
1 Назначение программы.....	4
2 Условия выполнения программы	5
2.1 Полномочия для выполнения программы	5
2.2 Минимальный состав аппаратных средств	5
2.3 Среда функционирования программы	5
2.4 Требования к персоналу (пользователю).....	5
3 Выполнение программы	6
3.1 Установка и запуск программы	6
4 Интерфейс программы.....	8
5 Работа с программой.....	9
5.1 Загрузка описаний уязвимостей	9
5.2 Обнаружение уязвимостей.....	11
5.3 Просмотр результатов проверок.....	12
5.4 Сохранение результатов проверок	13
5.5 Завершение выполнения программы	14
6 Настройка параметров программы.....	15
7 Сообщения оператору.....	17
7.1 Сообщение при отсутствии файлов XSD-схем.....	17
7.2 Сообщение о неверной цифровой подписи загружаемых файлов.....	17

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 РОСА «КОБАЛЬТ» (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 Роса «Кобальт».

Для обеспечения работы Программы необходимо следующее ПО:

- графический интерфейс;
- qt 5.6.1;
- qt5-qtxmlpatterns;
- qt5-qtbase;
- qt5-qtbase-gui;
- openscap-scanner;
- 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.

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 cp /var/lib/scanoval/repo/PUBLIC-GPG-KEY-scanoval /etc/pki/rpm-gpg/
```

4. Создать конфигурационный файл репозитория:

```
sudo touch /etc/yum.repos.d/scanoval.repo
```

```
[scanoval]
```

```
name=ScanOVAL
```

```
baseurl=file:///var/lib/scanoval/repo/main/$basearch/release
```

```
enabled=1
```

```
gpgcheck=1
```

```
gpgkey=file:///etc/pki/rpm-gpg/PUBLIC-GPG-KEY-scanoval
```

```
[scanoval-content]
```

```
name=ScanOVAL OVAL content
```

```
baseurl=file:///var/lib/scanoval/repo/content/noarch/release
```

```
enabled=1
```

```
gpgcheck=1
```

```
gpgkey=file:///etc/pki/rpm-gpg/PUBLIC-GPG-KEY-scanoval
```

5. Обновить список репозитория:

```
sudo yum repolist
```

6. Установить Программу путем выполнения следующей команды:

sudo yum install openscap-scanner openssl scanoval scanoval-content-rel73

7. Запустить Программу путем выполнения следующей команды:

/usr/bin/scanoval.

Для удаления Программы необходимо выполнить команду:

sudo yum remove scanoval scanoval-content-rel73

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.

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;

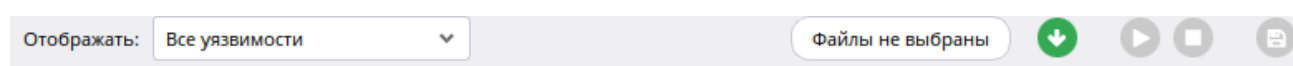


Рисунок 2 – Панель быстрого доступа

- 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:2019-03416	Обнаружено	Критический	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29....
BDU:2019-03308	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29....
BDU:2019-03309	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29....
BDU:2019-03310	Обнаружено	Высокий	ROSA-SA-18-05-29.005, C...	Rosa -- уязвимость в firefox (ROSA-SA-18-05-29.005)
BDU:2019-03311	Обнаружено	Высокий	ROSA-SA-18-05-29.005, C...	Rosa -- уязвимость в firefox (ROSA-SA-18-05-29.005)
BDU:2019-03312	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29....
BDU:2019-03510	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29....

Рисунок 3 – Панель «Результаты»

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

Подробности

Идентификатор уязвимости [BDU:2019-03416](#)

Результат Обнаружено

Уровень опасности уязвимости Критический

OVAL [oval.ru.albx-soft.nix:def:131989](#) (версия 3)

Название уязвимости Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29.005, ROSA-SA-18-05-29.006)

Описание уязвимости В продуктах firefox, thunderbird обнаружена уязвимость CVE-2018-5150.

Возможные меры по устранению уязвимости Использование рекомендаций: Для программных продуктов Mozilla Corp.: <https://www.mozilla.org/en-US/security/advisories/mfsa2018-11/> <https://www.mozilla.org/en-US/security/advisories/mfsa2018-12/> <https://www.mozilla.org/en-US/security/advisories/mfsa2018-13/> Для Ubuntu: <https://usn.ubuntu.com/3645-1/> <https://usn.ubuntu.com/3660-1/> <https://usn.ubuntu.com/3688-1/> Для программных продуктов Novell Inc.: <https://www.suse.com/security/cve/CVE-2018-5150/> Для Debian GNU/Linux: <https://lists.debian.org/debian-its-announce/2018/05/msg00013.html> Для программных продуктов Red Hat Inc.: <https://access.redhat.com/security/cve/cve-2018-5150>

Ссылки на источники VENDOR [ROSA-SA-18-05-29.005](#), VENDOR [ROSA-SA-18-05-29.006](#), CVE [CVE-2018-5150](#)

Базовый вектор уязвимости AV:N/AC:L/Au:N/C:C/I:C/A:C

Программное обеспечение cpe:/a:mozilla:firefox, cpe:/o:rosa:enterprise_linux:server:7.3

Детализация

Файл `/var/lib/scanoval/data/Rosa73VulnsOVAL.xml`

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.

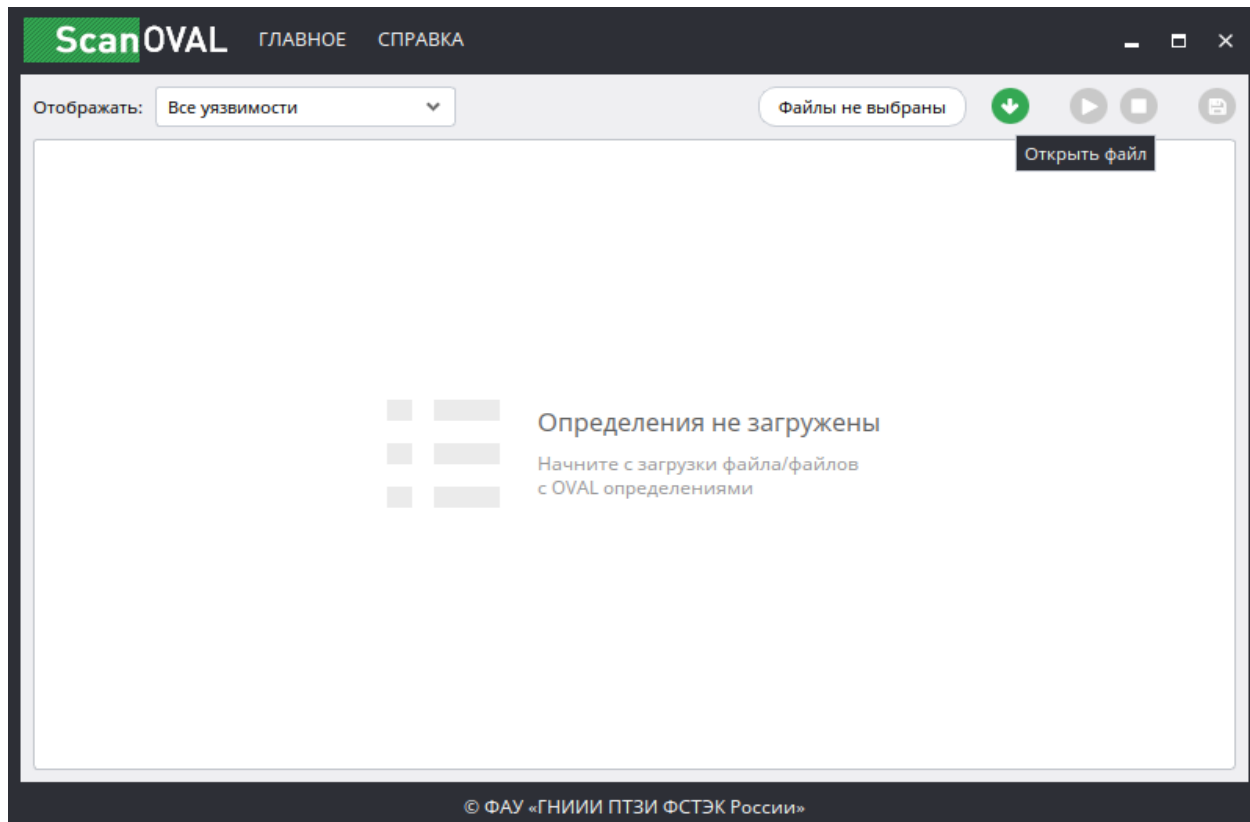



Рисунок 5 – Главное окно программы

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

Идентификатор уязвимости	Результат	Уровень опасности	Ссылки на источники	Название уязвимости
BDU:2019-03461		Высокий	ROSA-SA-18-07-04.002, C...	Rosa -- уязвимость в thunderbird (ROSA-SA-18-07-04.002)
BDU:2019-00511		Высокий	ROSA-SA-18-09-05.002, C...	Rosa -- уязвимость в Mutt (ROSA-SA-18-09-05.002)
BDU:2019-04576		Критический	ROSA-SA-18-09-05.002, C...	Rosa -- уязвимость в Mutt (ROSA-SA-18-09-05.002)
BDU:2019-04574		Критический	ROSA-SA-18-09-05.002, C...	Rosa -- уязвимость в Mutt (ROSA-SA-18-09-05.002)
BDU:2019-04293		Высокий	ROSA-SA-18-07-04.002, C...	Rosa -- уязвимость в thunderbird (ROSA-SA-18-07-04.002)
BDU:2019-04292		Высокий	ROSA-SA-18-07-04.002, C...	Rosa -- уязвимость в thunderbird (ROSA-SA-18-07-04.002)
BDU:2019-03466		Высокий	ROSA-SA-18-07-04.002, C...	Rosa -- уязвимость в thunderbird (ROSA-SA-18-07-04.002)
BDU:2019-03465		Высокий	ROSA-SA-18-07-04.002, C...	Rosa -- уязвимость в thunderbird (ROSA-SA-18-07-04.002)
BDU:2019-03464		Высокий	ROSA-SA-18-07-04.002, C...	Rosa -- уязвимость в thunderbird (ROSA-SA-18-07-04.002)
BDU:2019-03462		Высокий	ROSA-SA-18-07-04.002, C...	Rosa -- уязвимость в thunderbird (ROSA-SA-18-07-04.002)
BDU:2018-01494		Средний	ROSA-SA-18-03-20.001, C...	Rosa -- уязвимость в firefox (ROSA-SA-18-03-20.001)
BDU:2019-00237		Высокий	ROSA-SA-18-06-09.001, C...	Rosa -- уязвимость в gnupg2, gnupg2-smime (ROSA-SA-18-...
BDU:2019-00250		Высокий	ROSA-SA-18-05-24.001, C...	Rosa -- уязвимость в procps-ng (ROSA-SA-18-05-24.001)
BDU:2019-00182		Средний	ROSA-SA-18-05-24.001, C...	Rosa -- уязвимость в procps-ng (ROSA-SA-18-05-24.001)
BDU:2018-01268		Высокий	ROSA-SA-18-05-16.001, C...	Rosa -- уязвимость в DHCP, dhclient, dhcp-common, dhcp-li...
BDU:2019-00254		Высокий	ROSA-SA-18-08-02.001, C...	Rosa -- уязвимость в yum-utils (ROSA-SA-18-08-02.001)
BDU:2018-00368		Высокий	ROSA-SA-18-03-17.001, R...	Rosa -- уязвимость в samba (ROSA-SA-18-03-17.001, ROSA...
BDU:2018-00367		Высокий	ROSA-SA-18-04-02.004, C...	Rosa -- уязвимость в samba (ROSA-SA-18-04-02.004)
BDU:2018-00654		Высокий	ROSA-SA-18-05-22.004, C...	Rosa -- уязвимость в libreip, libreip-devel (ROSA-SA-18-05-...
BDU:2019-04024		Критический	ROSA-SA-18-07-04.002, C...	Rosa -- уязвимость в thunderbird (ROSA-SA-18-07-04.002)
BDU:2020-00048		Средний	ROSA-SA-18-05-22.018, C...	Rosa -- уязвимость в kernel (ROSA-SA-18-05-22.018)
BDU:2018-00491		Высокий	ROSA-SA-18-04-09.001, C...	Rosa -- уязвимость в kernel (ROSA-SA-18-04-09.001)
BDU:2018-00365		Высокий	ROSA-SA-18-04-05.002, C...	Rosa -- уязвимость в glibc (ROSA-SA-18-04-05.002)
BDU:2019-01628		Средний	ROSA-SA-18-08-10.001, C...	Rosa -- уязвимость в bind (ROSA-SA-18-08-10.001)
BDU:2018-00357		Средний	ROSA-SA-18-03-01.001, C...	Rosa -- уязвимость в dhcp-common, dhcp-libs (ROSA-SA-18-...
BDU:2018-00356		Высокий	ROSA-SA-18-03-01.002, C...	Rosa -- уязвимость в dhcp-common, dhcp-libs (ROSA-SA-18-...
BDU:2018-00979		Высокий	ROSA-SA-18-08-07.001, C...	Rosa -- уязвимость в kernel-nrj-desktop (ROSA-SA-18-08-07-...
BDU:2018-00412		Высокий	ROSA-SA-18-04-18.008, C...	Rosa -- уязвимость в kernel-lt (ROSA-SA-18-04-18.008)
BDU:2018-00414		Высокий	ROSA-SA-18-03-23.002, C...	Rosa -- уязвимость в kernel-lt (ROSA-SA-18-03-23.002)

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».

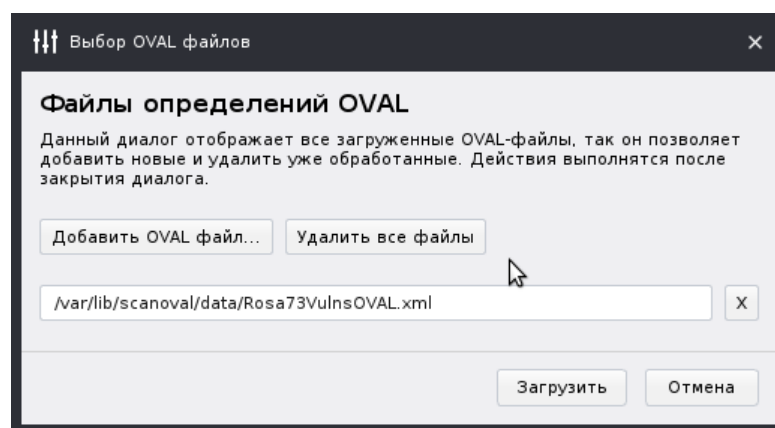



Рисунок 7 – Окно добавления/удаления OVAL-описаний

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:2019-03416	Обнаружено	Критический	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29...
BDU:2019-03308	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29...
BDU:2019-03309	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29...
BDU:2019-03310	Обнаружено	Высокий	ROSA-SA-18-05-29.005, C...	Rosa -- уязвимость в firefox (ROSA-SA-18-05-29.005)
BDU:2019-03311	Обнаружено	Высокий	ROSA-SA-18-05-29.005, C...	Rosa -- уязвимость в firefox (ROSA-SA-18-05-29.005)
BDU:2019-03312	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29...
BDU:2019-03510	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29...
BDU:2018-01426	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29...

Рисунок 8 – Результат выполненной проверки

5.3 Просмотр результатов проверок

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

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 «Подобности» расположена ниже панели «Результаты» и раскрывается кликом мыши по строке результата проверки или нажатием на кнопку «Подобности» (рисунок 9).

The screenshot shows the ScanOVAL application window. At the top, there is a header with the logo and navigation links. Below it is a search bar and a file selection dropdown. The main area contains a table with columns for vulnerability ID, result, severity, source links, and name. Below the table are buttons for grouping results and a summary of counts. A detailed view of a vulnerability is shown below the table, including its ID, result, severity, OVAL definition, name, description, remediation measures, source links, base vector, program protection, and the file path.

Идентификатор уязвимости	Результат	Уровень опасности	Ссылки на источники	Название уязвимости
BDU:2019-03416	Обнаружено	Критический	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в thunderbird (ROSA-SA-18-05-29....
BDU:2019-03308	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29....
BDU:2019-03309	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29....
BDU:2019-03310	Обнаружено	Высокий	ROSA-SA-18-05-29.005, C...	Rosa -- уязвимость в firefox (ROSA-SA-18-05-29.005)
BDU:2019-03311	Обнаружено	Высокий	ROSA-SA-18-05-29.005, C...	Rosa -- уязвимость в firefox (ROSA-SA-18-05-29.005)
BDU:2019-03312	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29....
BDU:2019-03510	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29....
BDU:2018-01426	Обнаружено	Высокий	ROSA-SA-18-05-29.005, R...	Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29....

Группировать по рискам Группировать по продуктам 7 1 Всего: 8

Подобности

Идентификатор уязвимости: [BDU:2019-03416](#)

Результат: **Обнаружено**

Уровень опасности уязвимости: **Критический**

OVAL: [oval:ru,albx-soft:nix:def:131989](#) (версия 3)

Название уязвимости: Rosa -- уязвимость в firefox, thunderbird (ROSA-SA-18-05-29.005, ROSA-SA-18-05-29.006)

Описание уязвимости: В продуктах firefox, thunderbird обнаружена уязвимость CVE-2018-5150.

Возможные меры по устранению уязвимости: Использование рекомендаций: Для программных продуктов Mozilla Corp.: <https://www.mozilla.org/en-US/security/advisories/mfsa2018-11/> <https://www.mozilla.org/en-US/security/advisories/mfsa2018-12/> <https://www.mozilla.org/en-US/security/advisories/mfsa2018-13/> Для Ubuntu: <https://usn.ubuntu.com/3645-1/> <https://usn.ubuntu.com/3660-1/> <https://usn.ubuntu.com/3688-1/> Для программных продуктов Novell Inc.: <https://www.suse.com/security/cve/CVE-2018-5150/> Для Debian GNU/Linux: <https://lists.debian.org/debian-its-announce/2018/05/msg00013.html> Для программных продуктов Red Hat Inc.: <https://access.redhat.com/security/cve/cve-2018-5150>

Ссылки на источники: VENDOR [ROSA-SA-18-05-29.005](#), VENDOR [ROSA-SA-18-05-29.006](#), CVE [CVE-2018-5150](#)

Базовый вектор уязвимости: AV:N/AC:L/Au:N/C:C/I:C/A:C

Программное обеспечение: cpe:/a:mozilla:firefox, cpe:/o:rosa:enterprise_linux:server:7.3

Детализация

Файл: /var/lib/scanoval/data/Rosa73VulnsOVAL.xml

© ФАУ «ГНИИИ ПТЗИ ФСТЭК России»


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):

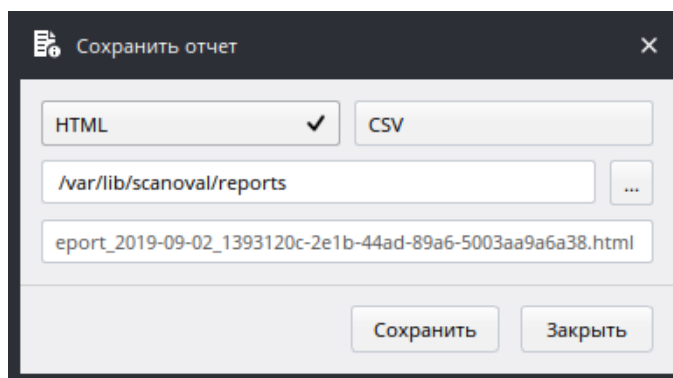


Рисунок 10 – Окно сохранения результатов проверок

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

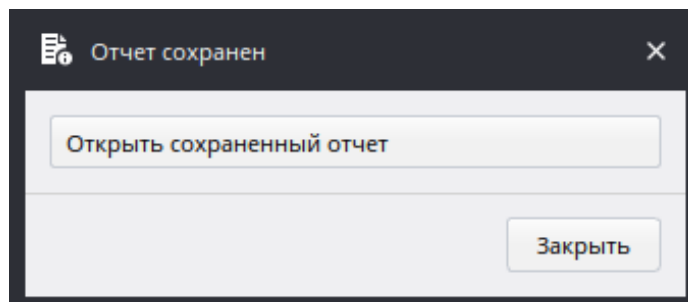



Рисунок 11 – Сообщение об успешном создании и сохранении отчета

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).

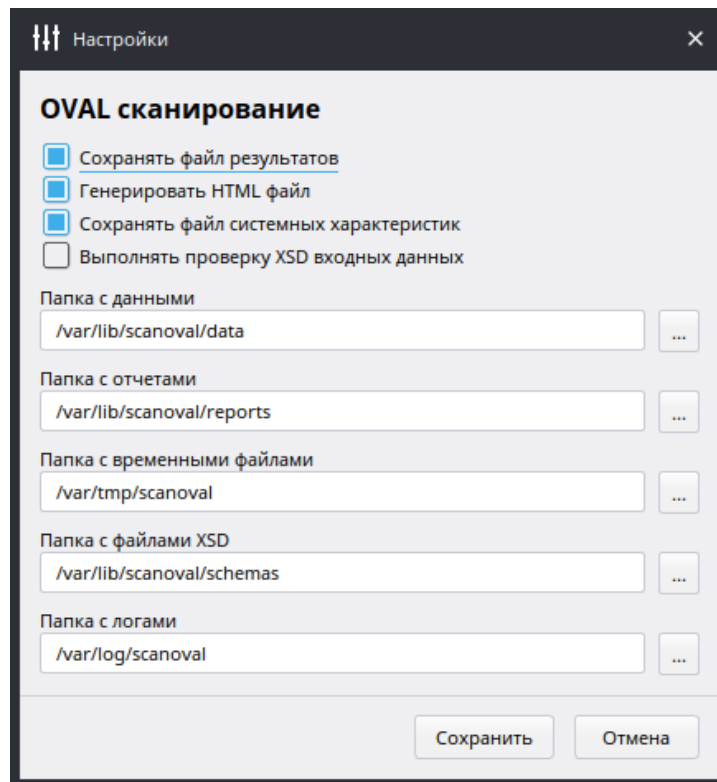


Рисунок 12 – Окно настроек

7 Сообщения оператору

7.1 Сообщение при отсутствии файлов XSD-схем

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

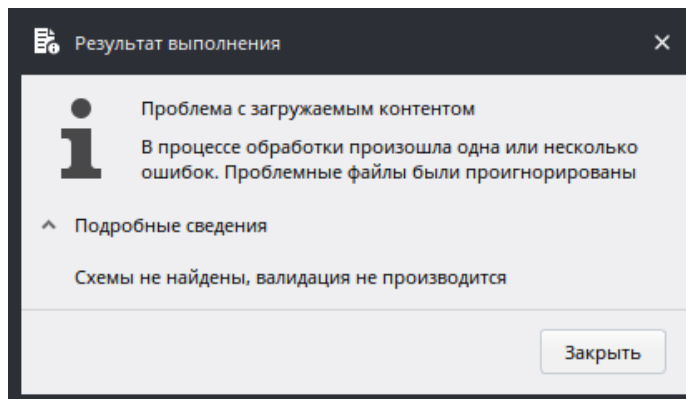


Рисунок 13 – Сообщение об отсутствии файлов XSD-схем

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.

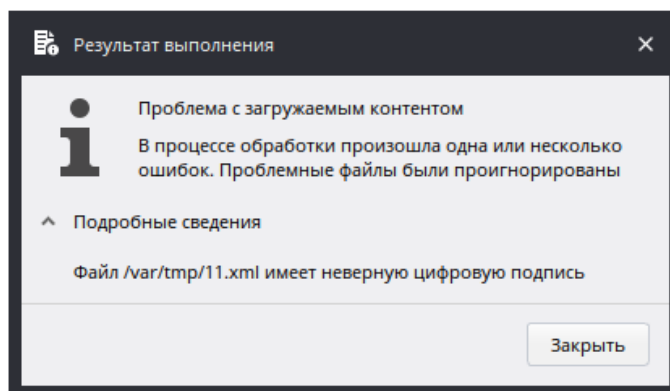


Рисунок 14 – Сообщение о неверной цифровой подписи загружаемых OVAL-описаний уязвимостей