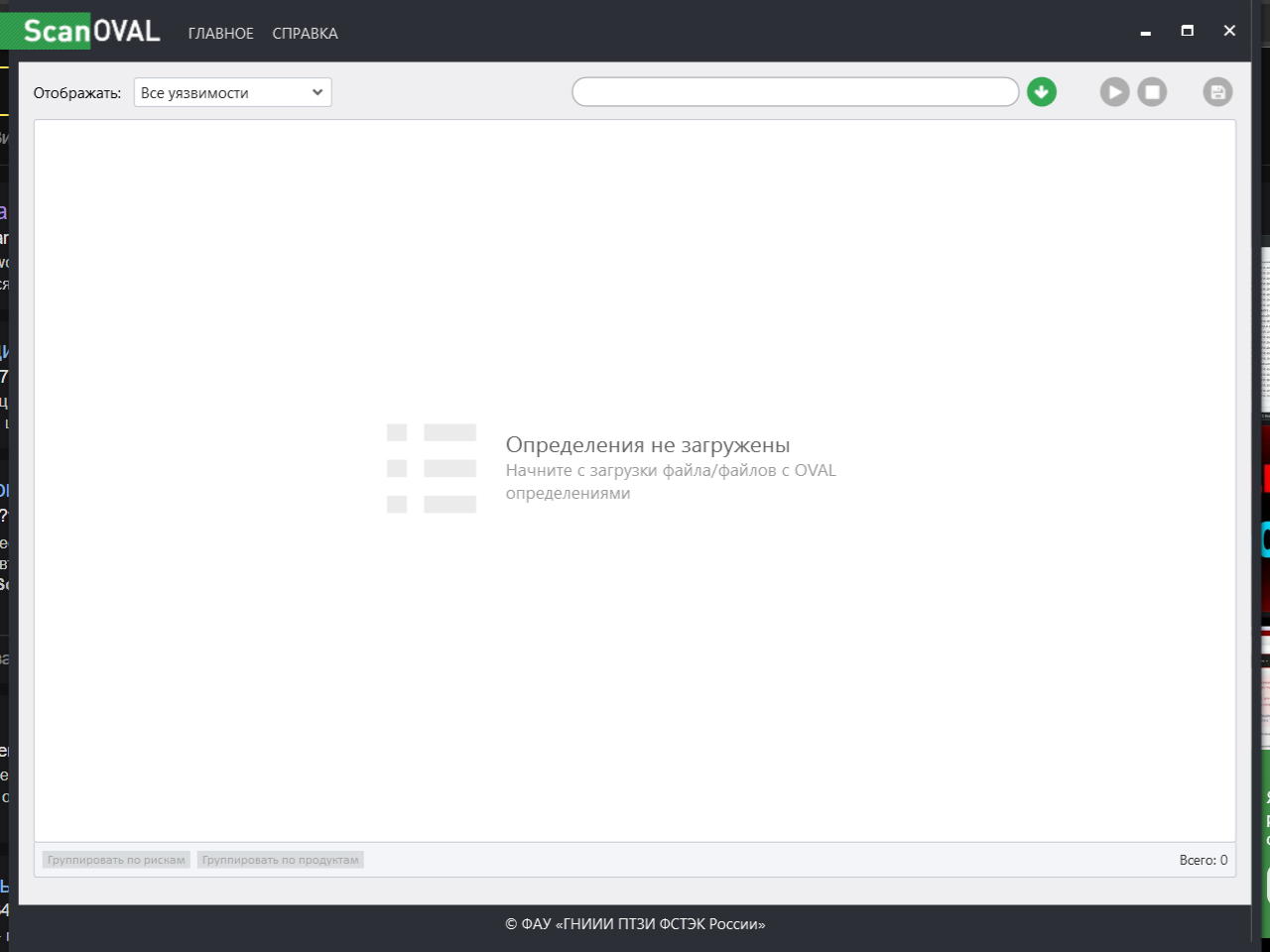
Практическая работа

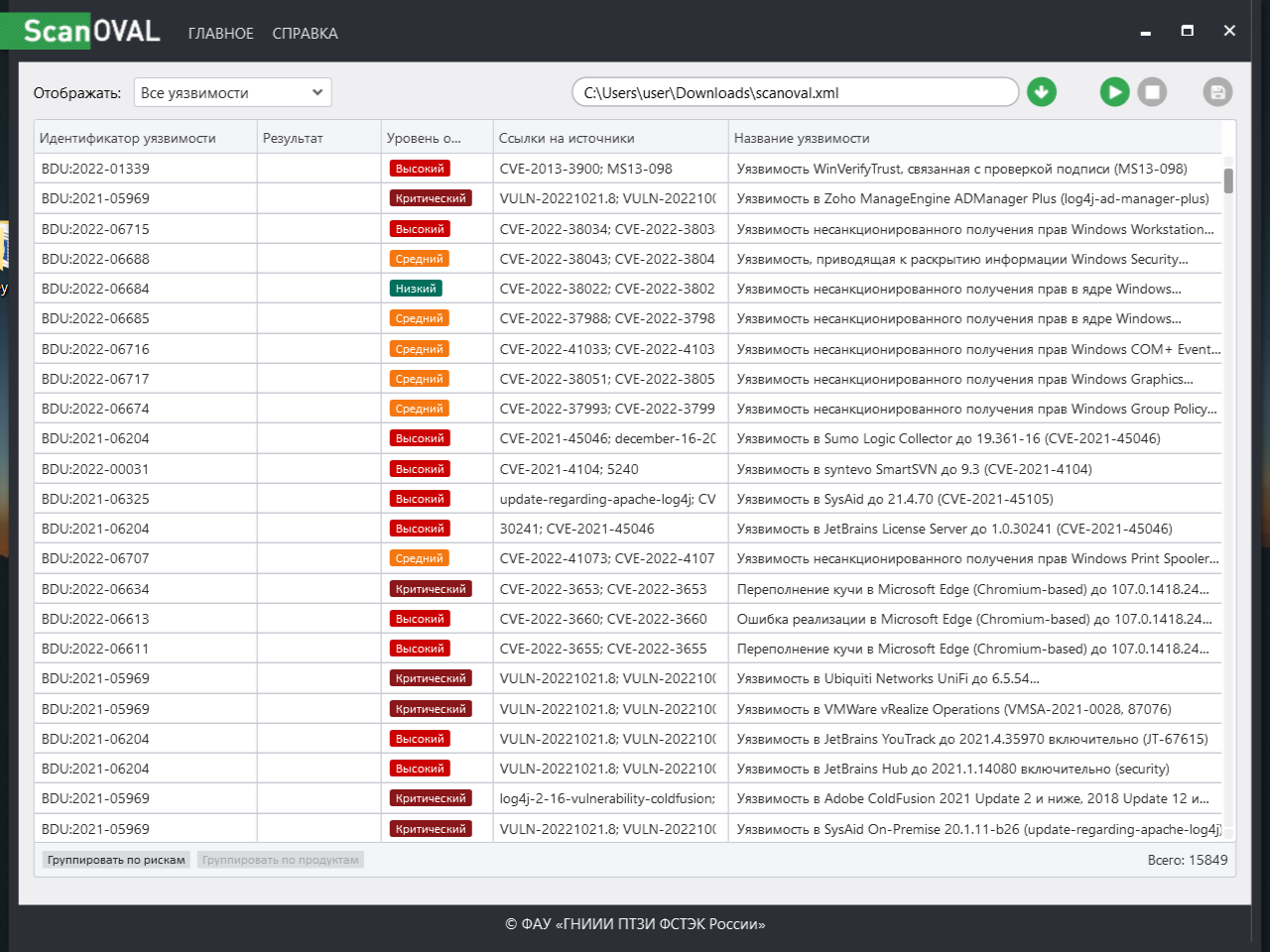
Автоматизация проверки наличия уязвимостейпрограммного обеспечения, работающего под управлениемоперационных систем Windows

Тестирование на наличие уязвимостей производилось на ноутбуке HP на базе операционной системы Microsoft Windows 10 x64ю

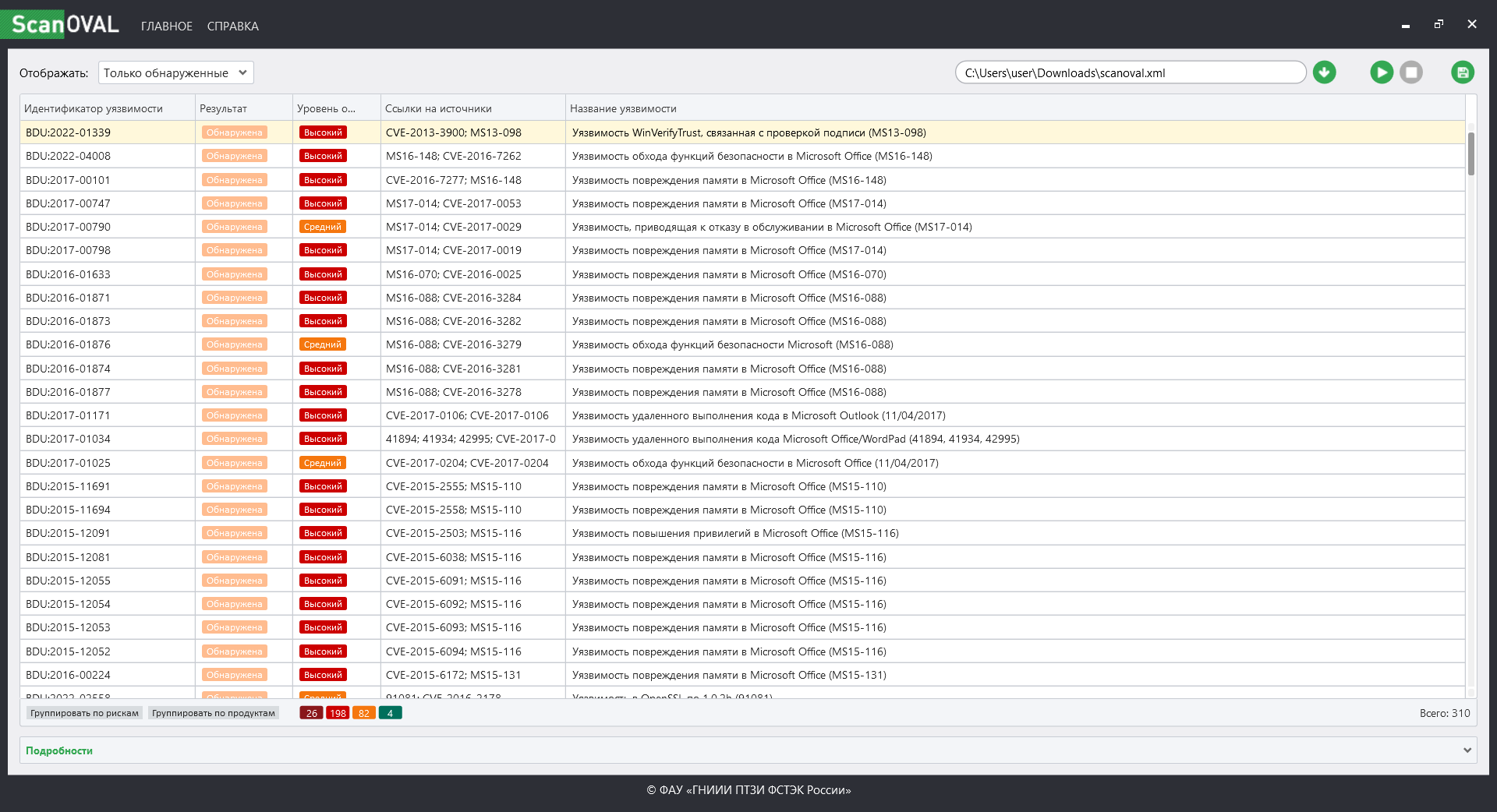
1. С сайта БДУ ФСТЭК была скачана и установлена программа ScanOval:



1. Помимо этого, с того же сайта были скачаны и загружены в программу определения для обнаружения уязвимостей:



1. После чего был произведен первоначальный анализ системы на наличие уязвимостей:



Представим более подробно:



Выделим нескольких критических угроз, найденных в ОС:

1. *BDU:2019-02891*

Уязвимость пакетов программ Microsoft SharePoint, Microsoft Office, Office 365 и текстового редактора Microsoft Word связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код в целевой системе с привилегиями текущего пользователя в результате открытия пользователем специально созданного вредоносного файла.

Тип ошибки: Выход операции за границы буфера в памяти.

Уровень опасности уязвимости:

* Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10)
* Высокий уровень опасности (базовая оценка CVSS 3.0 составляет 8,8)

1. *BDU:2021-05392*

Уязвимость пакетов программ Microsoft Office, Microsoft Office Online Server, Microsoft Office Web Apps Server, службы Word Automation Services и текстового редактора Microsoft Word связана с выходом операции за границы буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код с помощью специально созданного файла с расширением RTF.

Тип ошибки: Выход операции за границы буфера в памяти.

Уровень опасности уязвимости:

* Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10)
* Высокий уровень опасности (базовая оценка CVSS 3.0 составляет 8,8)

Уязвимость была устранена.

1. *BDU:2020-05901*

Уязвимость редактора электронных таблиц Microsoft Excel, пакетов программ Microsoft Office Web Apps, Microsoft 365 Apps, Microsoft Office, Office Online Server связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код

Тип ошибки: Код

Уровень опасности уязвимости:

* Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10)
* Высокий уровень опасности (базовая оценка CVSS 3.0 составляет 7,8)

Уязвимость была устранена.

1. Для уменьшения числа уязвимостей были произведены такие действия, как обновление системы и обновление пакета программ Microsoft Office 2016. В итоге был получен следующий результат:



Общее число уязвимостей уменьшилось, однако основные уязвимости Microsoft Office 2016, в том числе те, которые были приведены выше, остались.

В связи с вышесказанным было принято решение удалить данный офисный пакет. После проведения таких действий получили следующий результат:



Как видно, это положительно повлияло на итоговый результат анализа системы на наличие уязвимостей.