МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «Белорусский государственный технологический университет»

Кафедра информационных технологий

**Практическое занятие №13**

**Тема «** **Настройка антивирусов»**

Выполнила:

Студентка 2 курса, 7 группы

Курносенко Софья Андреевна

Проверил:

Барковский Евгений Валерьевич

**Практическое занятие №13**

**Тема «Настройка антивирусов»**

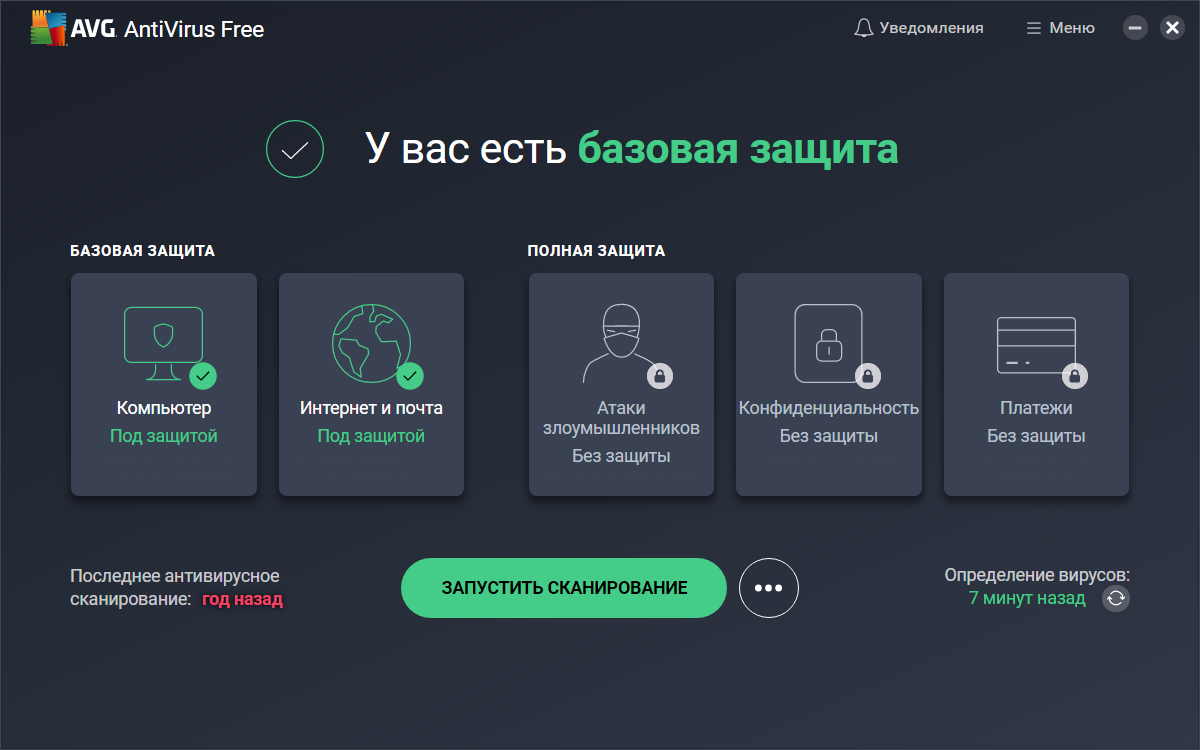
**Цель**: Овладение навыками настройки и использования различных антивирусов.

**Задание к выполнению**

1. **Установить и настроить антивирусную программу по варианту.**

Был установлен антивирус AVG AntiVirus Free.



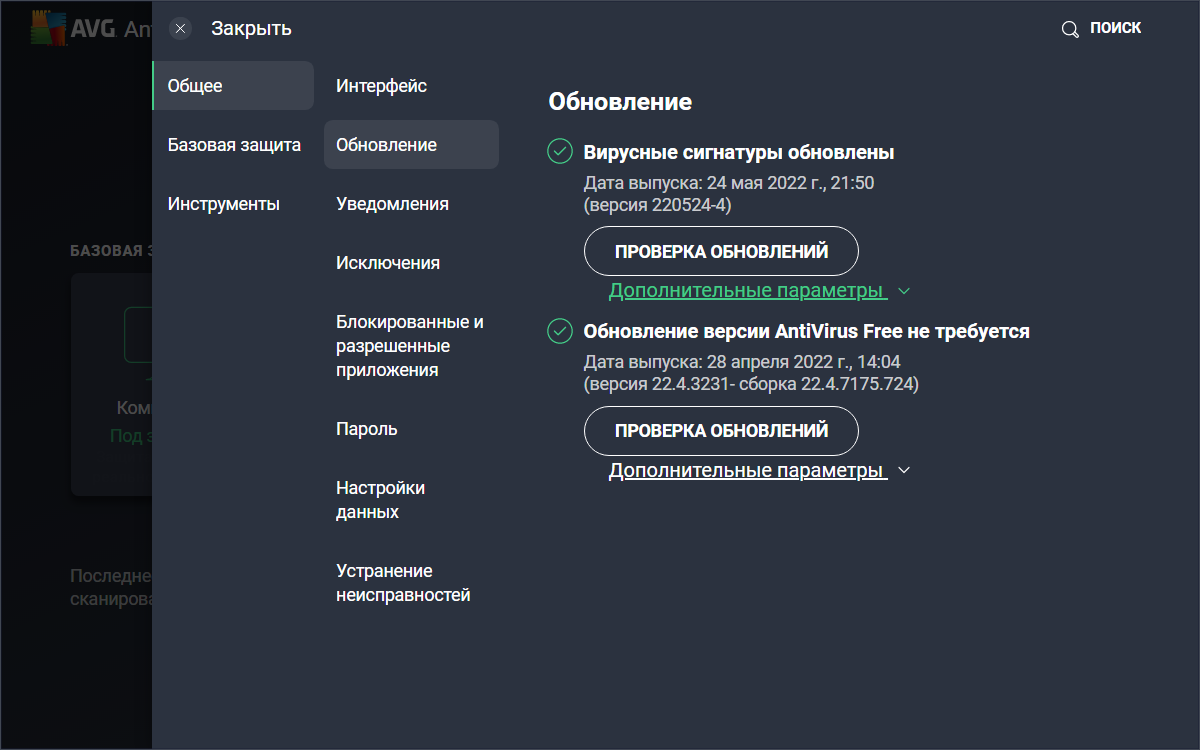


1. **Обновить базу данных сигнатур вирусов.**

**База данных сигнатур вирусов** – это словарь с известными вирусами, составленный авторами программы.

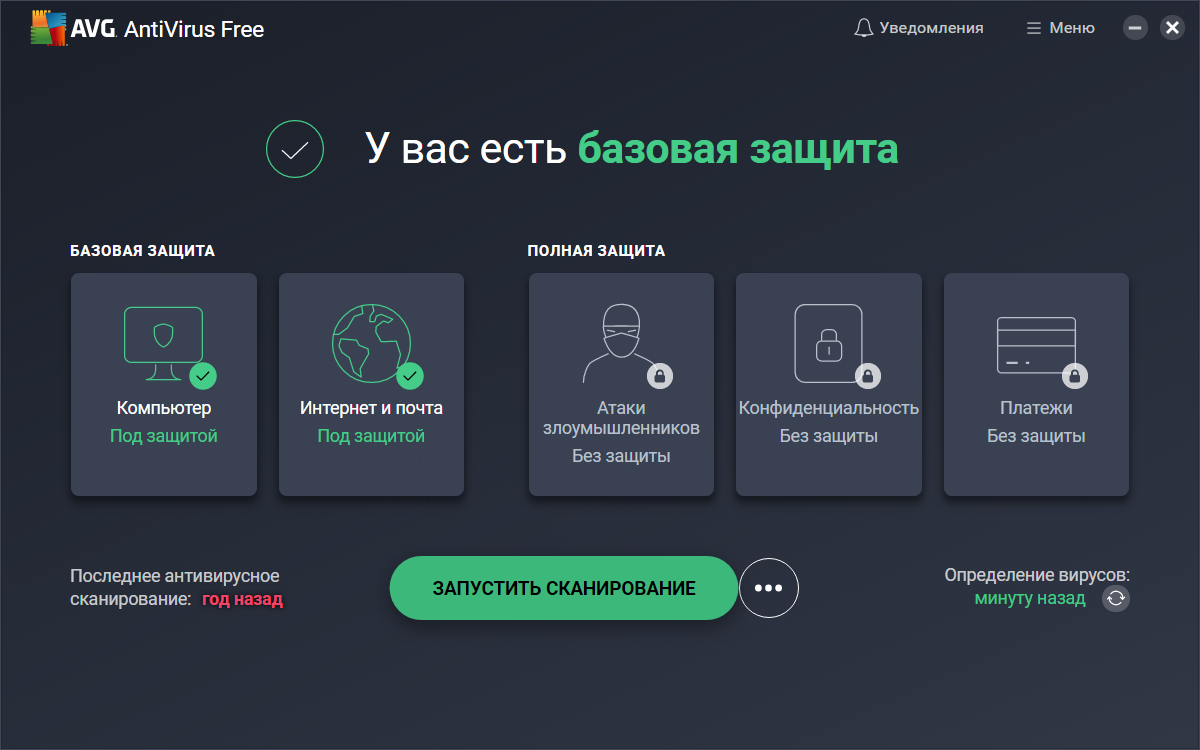
**Сигнату́ра вируса** — характерные признаки компьютерного вируса, используемые для их обнаружения.

Меню → Настройки → Общее → Обновления:

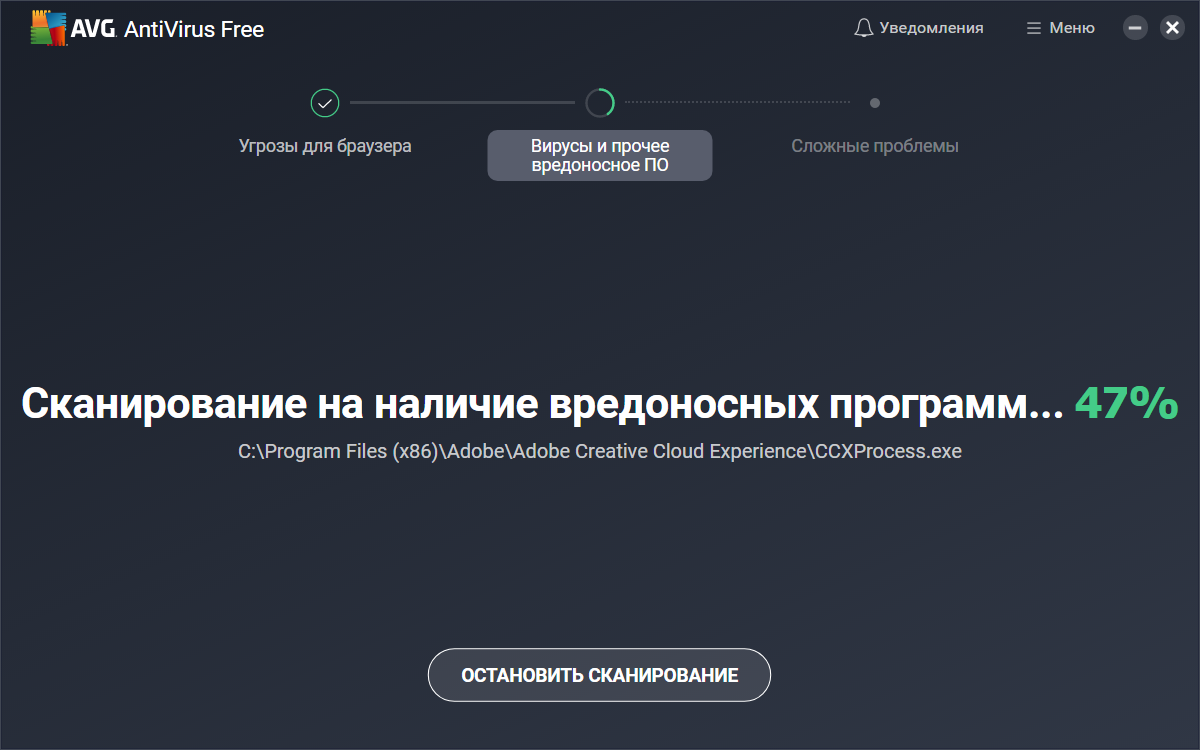


1. **Выполнить сканирование дисков.**

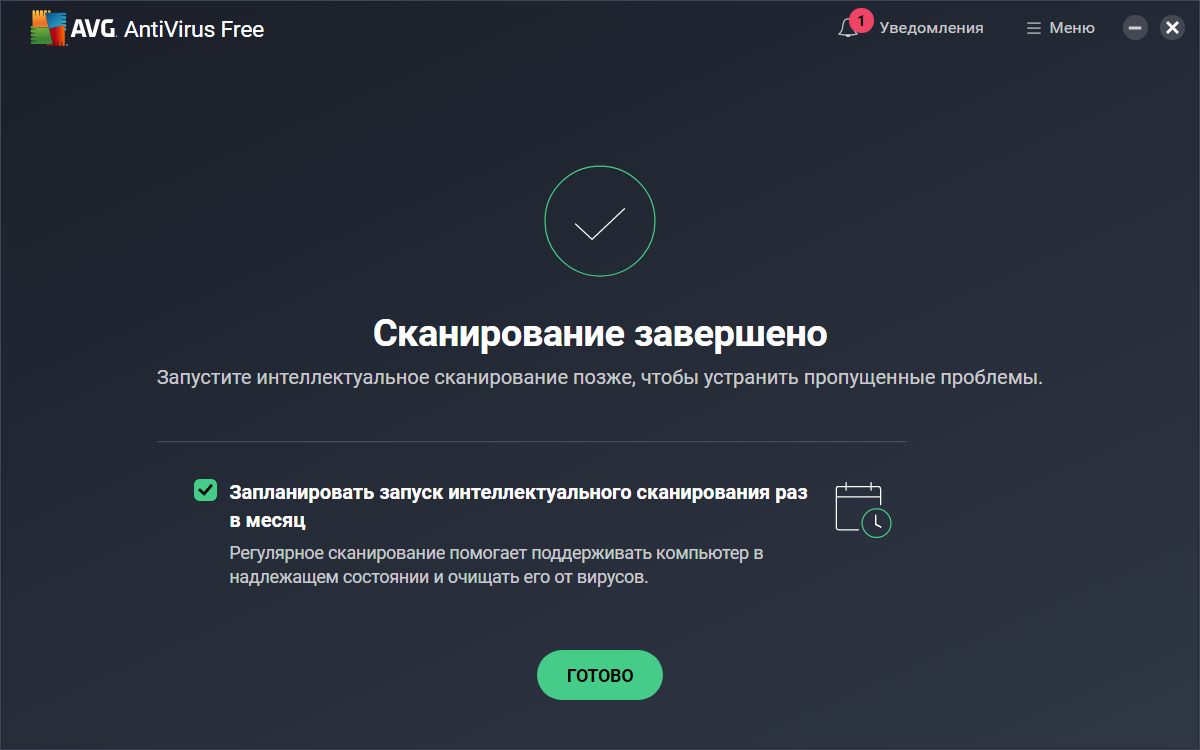
Нажимаю кнопку «Запустить сканирование»:



В процессе сканирования:



После завершения:



Варианты заданий находятся в презентации 6.2 (на последнем слайде).

**Компьютерный вирус** – это специально написанная программа, способная самопроизвольно присоединяться к другим программам (заражать их), создавать свои копии и внедрять их в файлы, системные области компьютера и другие объединенные с ним компьютеры в целях нарушения нормальной работы программ, порчи файлов и каталогов, а также создания разных помех при работе на компьютере.

**Появление вирусов в компьютере. Признаки:**

* уменьшение производительности работы компьютера;
* невозможность и замедление загрузки ОС;
* повышение числа файлов на диске;
* замена размеров файлов;
* периодическое появление на экране монитора неуместных сообщений;
* уменьшение объема свободной ОП;
* резкое возрастание времени доступа к жесткому диску;
* разрушение файловой структуры;
* загорание сигнальной лампочки дисковода, когда к нему нет обращения;
* изменение даты и времени модификации файлов;
* исчезновение файла и каталога или искажение их содержимого;
* прекращение работы или неправильная работа ранее успешно функционировавших программ.

**Антивирусная программа** — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных программ и восстановления заражённых такими программами файлов и профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом.

**Как работает антивирус**

В зависимости от того, числится ли вирус в базе данных сигнатур вируса, различают два способа:

‣ **Сигнатурный метод или реактивная защита.** В основе данного механизма лежит **сигнатура** — набор уникальных характеристик вируса или семейства однотипных вирусов. Сигнатуры создаются вирусными аналитиками на основе анализа уже известных вредоносных программ и формируются в постоянно обновляемую антивирусную базу. Антивирусное ПО автоматически загружает свежие базы и сравнивает содержимое локальных и внешних файлов с данными из сигнатур. Принцип работы антивируса с сигнатурами позволят точно определить тип угрозы и понять как с ней бороться. Недостаток сигнатурного метода в том, что он бессилен против неизвестных и модифицированных вирусов, а также не способен анализировать подозрительную активность приложений.

‣ **Эвристический анализ или проактивная защита.** Используется для предупреждения потенциальных угроз и решения задач, с которыми сигнатурный метод не справляется. Возможностей много:

◦ анализ работы программ на предмет подозрительных действий. Например, программе для скачивания видео с видеохостингов явно не нужно без вашего согласия прописываться в ветке автозагрузки системного реестра, произвольно открывать порты и обмениваться данными с неизвестными серверами. Если таких подозрительных активностей становится слишком много, антивирус сигнализирует об этом. Конечно то, как работают антивирусы с эвристическим анализом пока нельзя назвать совершенством. Случаются ложные срабатывания на доверенные программы. Впрочем, это решается настройкой;

◦ безопасный запуск и поведенческий анализ подозрительных программ в «песочнице» — эмуляторе ОС;

◦ обнаружение (но не лечение) незнакомого вредоносного ПО, на основе похожих сигнатур и по косвенным признакам.

Антивирусные программы проверяют файлы компьютера на наличие вирусов. При обнаружении вируса антивирусная программа либо отправляет его в карантин, либо полностью удаляет его до нанесения ущерба компьютеру и файлам.

**Вывод**: в данной лабораторной работе овладела навыками настройки и использования антивируса.