**Содержание:**

# Введение

Информация является результатом отображения и обработки в человеческом сознании многообразия окружающего мира, представляет собой сведения об окружающих человека предметах, явлениях природы, деятельности других людей. информационный безопасность угроза

Защита информации - область науки и техники, которая включает совокупность средств, методов и способов человеческой деятельности, направленных на обеспечение защиты всех видов информации в организациях и предприятиях различных направлений деятельности и различных форм собственности.

Информационная безопасность - это состояние защищенности информации среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств.

Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности. [1]

Информацию, которую можно защитить, представлена на любых носителях, может храниться, обрабатываться и передаваться различными способами.

Цель защиты информации предотвратить разглашения, утечки и несанкционированного доступа; предотвратить противоправные действий по уничтожению, копированию, блокированию информации; предотвратить другие формы незаконного вмешательства.

Данная тема актуальна, так как каждый пользователь персонального компьютера желает, чтобы информация которая хранится у него на компьютере, или внешнем накопителе оставалась доступна только ему. В наше время защитить информацию от нежелательного программного обеспечения практически невозможно. Сейчас вредоносные программы создаются лучше, чем защита от этих программ. Но если знать, как правильно пользоваться антивирусной защитой и применять эти знания на практике, то защитить свою информацию можно на долгие годы.

Цель данной работы состоит в определении видов угроз информационной безопасности и их состава.

Задачи:

1. Что такое информационная безопасность
2. Разобрать какие существуют виды и состав угроз информационной безопасности
3. Виды вредоносных программ и способы защиты от вредоносных программ.
4. Наиболее популярные антивирусные программы.

# Глава 1. Информационная безопасность

## 1.1 Понятие определения информационной безопасности

Информационная безопасность— это процесс обеспечения конфиденциальности, целостности и доступности информации. Схема. 1. «Влияние угроз информации на критерии информационной безопасности»

Конфиденциальность — необходимость предотвращения разглашения какой-либо информации, чего-либо.

Целостность информации — термин в информатике означающий, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение.

Доступность информации — состояние информации при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно. К правам доступа относятся: право на чтение, изменение, хранение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов. [2]

**Достоверность** – данный принцип выражается в строгой принадлежности информации субъекту, который является ее источником или от которого она принята. [3]

Схема. 1. «Влияние угроз информации на критерии информационной безопасности» [6]

Проявляются в нарушениях

Конфиденциальность

Целостность

Доступность

1. Разглашение
2. Утечка
3. Несанкционированный доступ
4. Искажение
5. Ошибки
6. Потери

Нарушение связи

Вывод:

Информация – сведения об окружающем нас мире.

Информационная безопасность – информация, которая безопасна и доступна для окружающих. Также есть информация, которая секретна и не безопасна.

## 1.2 Виды угроз информационной безопасности

Под угрозой информационной безопасности принято понимать потенциально возможные действия, явления или процессы, способные оказать нежелательное воздействие на систему или на хранящуюся в ней информацию.

Такие угрозы, воздействуя на ресурсы, могут привести к искажению данных, копированию, несанкционированному распространению, ограничению или блокированию к ним доступа. В настоящее время известно достаточно большое количество угроз, которые классифицируют по различным признакам.

По природе возникновения различают **естественные** и **искусственные** угрозы. К первой группе относятся те, что вызваны воздействием на компьютерную систему объективных физических процессов или стихийных природных явлений. Вторая

группа – те угрозы, которые обусловлены деятельностью человека.

По степени преднамеренности проявления**,** угрозы разделяют на **случайные** и **преднамеренные.**

Также есть разделение в **зависимости от их непосредственного источника**, в качестве которого может выступать природная среда (например, стихийные бедствия), человек (разглашение конфиденциальных данных), программно-аппаратные средства: санкционированные (ошибка в работе операционной системы) и несанкционированные (заражение системы вирусами).

Источник угроз может иметь разное положение. В зависимости от этого фактора также выделяют **три группы:**

1. Угрозы, источник которых находятся вне контролируемой группы компьютерной системы (пример – перехват данных, передаваемых по каналам связи)
2. Угрозы, источник которых – в пределах контролируемой зоны системы (это может быть хищение носителей информации)
3. Угрозы, находящиеся непосредственно в самой системе (например, некорректное использование ресурсов).
4. Угрозы способны по-разному воздействовать на компьютерную систему.  Это могут быть **пассивные воздействия,** реализация которых не влечет за собой изменение структуры данных (например, копирование).

**Активные угрозы** — это такие, которые, наоборот, меняют структуру и содержание компьютерной системы (внедрение специальных программ).

Классификация **по месту расположения в системе** подразумевает деление на три группы: угрозы доступа к информации, находящейся на внешних запоминающих устройствах, в оперативной памяти и к той, что циркулирует в линиях связи.

Угрозы могут использовать прямой стандартный путь к ресурсам с помощью незаконно полученных паролей или посредством неправомерного применения терминалов законных пользователей, а могут «обойти» существующие средства защиты иным путем.

Такие действия, как хищение информации, относят к угрозам, проявляющимся независимо от активности системы. А, например, распространение вирусов может

быть обнаружено исключительно в процессе обработки данных.

Случайными, или **непреднамеренными** называются такие угрозы, которые не связаны с действиями злоумышленников. Механизм их реализации изучен достаточно хорошо, поэтому существуют разработанные методы противодействия.

Аварии и стихийные бедствия представляют особую опасность для компьютерных систем, так как они влекут за собой наиболее негативные последствия. Вследствие физического разрушения систем информация становится недоступной, либо утрачивается.  Кроме того, невозможно полностью избежать или предупредить сбои и отказы в сложных системах, в результате которых, как правило, хранящаяся на них информация искажается или уничтожается, нарушается алгоритм работы технических устройств.

Для проникновения в компьютерную систему с целью дальнейшего хищения или уничтожения информации используются такие методы и средства шпионажа, как прослушивание, хищение программ, атрибутов защиты, документов и носителей информации, визуальное наблюдение и другие.

При несанкционированном доступе к данным обычно используют штатные аппаратные и программные средства компьютерных систем, вследствие чего нарушаются установленные правила разграничения доступа пользователей или процессов к информационным ресурсам. Самые распространенные нарушения – это перехват паролей (производится с помощью специально разработанных программ), выполнение каких-либо действий под именем другого человека, а также использование злоумышленником привилегий законных пользователей. [3]

# Глава 2. Программное обеспечение

## 2.1 Специальные вредоносные программы

Вредоносные программы – это любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, или владельцу ЭВМ, или владельцу сети ЭВМ, путём копирования, искажения, удаления или подмены информации. [4]

Компьютерный вирус – это небольшая вредоносная программа, которая самостоятельно может создавать свои копии и внедрять их в программы (исполняемые файлы), документы, загрузочные сектора носителей данных.

Известно много различных способов классификации компьютерных вирусов. Одним из способов классификации компьютерных вирусов – это разделение их по следующим основным признакам. Схема. 2. «Классификация программных вирусов и сетевых червей»

- среда обитания;
- особенности алгоритма;
- способы заражения;
- степень воздействия (безвредные, опасные, очень опасные).

В зависимости от среды обитания основными типами компьютерных вирусов являются:

- Программные (поражают файлы с расширением. COM и .EXE) вирусы.
- Загрузочные вирусы.
- Макровирусы.
- Сетевые вирусы.

**Программные вирусы** – это вредоносный программный код, который внедрен внутрь исполняемых файлов (программ). Вирусный код может воспроизводить себя в теле других программ – этот процесс называется размножением.

По прошествии определенного времени, создав достаточное количество копий, программный вирус может перейти к разрушительным действиям – нарушению работы программ и операционной системы, удаляя информации, хранящиеся на жестком диске. Этот процесс называется вирусной атакой.

**Загрузочные вирусы** – поражают не программные файлы, а загрузочный сектор магнитных носителей (гибких и жестких дисков).

**Макровирусы** – поражают документы, которые созданы в прикладных программах, имеющих средства для исполнения макрокоманд. К таким документам относятся документы текстового процессора WORD, табличного процессора Excel. Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд.

**Сетевые вирусы** пересылаются с компьютера на компьютер, используя для своего распространения компьютерные сети, электронную почту и другие каналы.

По алгоритмам работы различают компьютерные вирусы:

- черви (пересылаются с компьютера на компьютер через компьютерные сети, электронную почту и другие каналы);
- вирусы-невидимки (Стелс-вирусы);
- троянские программы;
- программы – мутанты;
- логические бомбы;

В настоящее время к наиболее распространенным видам вредоносных программ, относятся: черви, вирусы, троянские программы. [5]

- черви – утилиты, которые активируются при каждой загрузке компьютера. Они обладают способностью перемещаться в пределах системы или сети и размножаться аналогично вирусам.  Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти, а затем к блокировке работы;
- троянские кони — такие программы «скрываются» под видом полезного приложения, а, на самом деле, наносят вред компьютеру: разрушают программное обеспечение, копируют и пересылают злоумышленнику файлы с конфиденциальной информацией. [3]

Схема. 2. «Классификация программных вирусов и сетевых червей»

Программные вирусы и сетевые черви

По среде обитания

По деструктивным возможностям

По методу маскировки

Файловые

Загрузочные

Сетевые

Безвредные

Малоопасные

Опасные

Очень опасные

Шифрованный

Метаморфный

Полиморфный

Желательно не допускать появление вирусов в ПК, но при заражении компьютера вирусом очень важно его обнаружить.

Основные признаки появления вируса в ПК:

- медленная работа компьютера;
- зависания и сбои в работе компьютера;
- изменение размеров файлов;
- уменьшение размера свободной оперативной памяти;
- значительное увеличение количества файлов на диске;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов. [5]

Вывод:

Вредоносные программы создаются по разным причинам. Например, личная неприязнь сотрудников. На крупной фирме один сотрудник менее успешней чем другой иными словами зависть. Если сотрудник, который менее успешней обладает знаниями по созданию вредоносных программ, вполне легко может нанести непоправимый вред другому сотруднику, а то и фирме.

Даже если человек не обладает нужными знаниями по созданию вредоносных программ, есть много других людей, которые умеют это делать, достаточно иметь финансовую обеспеченность.

Вредоносные программы создаются не только для умышленного нанесения вреда, но и в качестве невинной шутки (напугать).

## 2.2 Способы защиты от вредоносных программ

Одним из основных способов борьбы с вирусами является своевременная профилактика. Существует достаточно много программных средств антивирусной защиты. Современные антивирусные программы состоят из модулей:

- Эвристический модуль – для выявления неизвестных вирусов.
- Монитор – программа, которая постоянно находится в оперативной памяти ПК
- Устройство управления, которое осуществляет запуск антивирусных программ и обновление вирусной базы данных и компонентов
- Почтовая программа (проверяет электронную почту)
- Программа сканер – проверяет, обнаруживает и удаляет фиксированный набор известных вирусов в памяти, файлах и системных областях дисков
- Сетевой экран – защита от хакерских атак

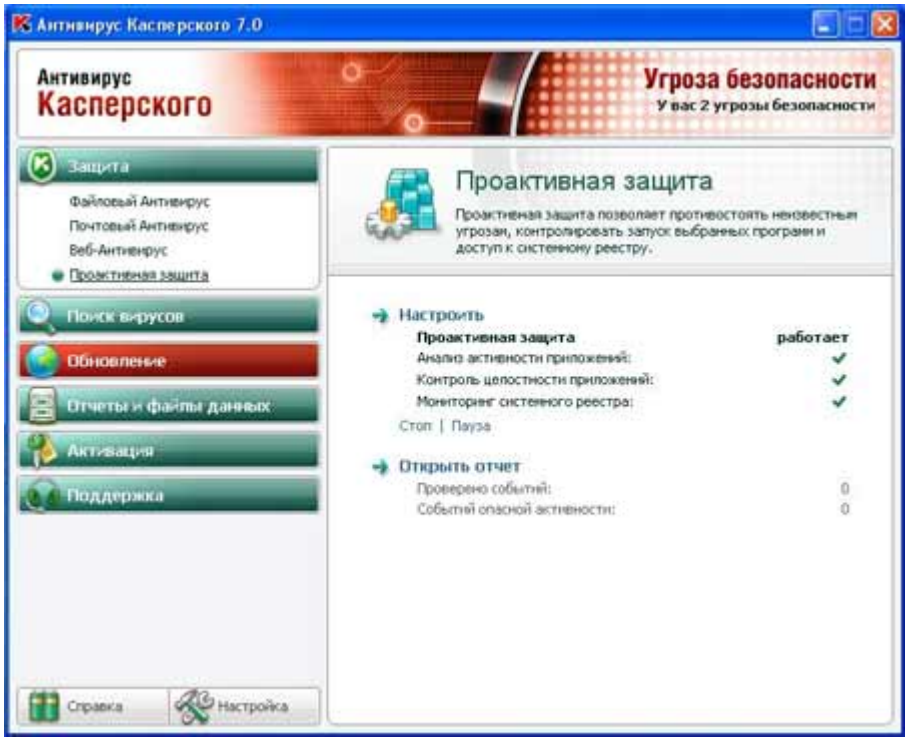
К наиболее эффективным и популярным антивирусным программам относятся: Антивирус Касперского 7.0, AVAST, Norton AntiVirus и многие другие.

К более подробному рассмотрению отнесем Антивирус Касперского 7.0, так как на мой взгляд это лучший из лучших антивирусных защит.

Программа состоит из следующих компонентов:

- Файловый Антивирус - компонент, контролирующий файловую систему компьютера. Он проверяет все открываемые, запускаемые и сохраняемые файлы на компьютере.
- Почтовый Антивирус- компонент проверки всех входящих и исходящих почтовых сообщений компьютера.
- Веб-Антивирус – компонент, который перехватывает и блокирует выполнение скрипта, расположенного на веб-сайте, если он представляет угрозу.
- На рисунке 1. «Проактивная защита» - компонент, который позволяет обнаружить новую вредоносную программу еще до того, как она успеет нанести вред. Таким образом, компьютер защищен не только от уже известных вирусов, но и от новых, еще не исследованных. [5]

Рис. 1. «Проактивная защита»




**Антивирус Касперского 7.0** – это классическая защита компьютера от вирусов, троянских и шпионских программ, а также от любого другого вредоносного ПО. [5]

Вывод:

Для того чтобы защитить свой компьютер от нежелательных программ:

- 1. Не запускайте программы из Интернета или в виде вложения в сообщение электронной почты без проверки на вирус.
  2. Проверяйте все внешние накопители на наличие вирусов, прежде чем копировать или открывать содержимое.
  3. Необходимо установить антивирусную программу и регулярно проверять на наличие вирусов. Настроить антивирусную программу на еженедельную проверку на вирусы (например, воскресенье в 3.00 каждую неделю компьютер будет проверять на наличие вирусов)
  4. Необходимо регулярно сканировать жесткие диски в поисках вирусов. Сканирование обычно выполняется автоматически при каждом включении ПК и при размещении внешнего диска в считывающем устройстве.
  5. Создавать надежные пароли, чтобы вирусы не могли легко подобрать пароль и получить разрешения администратора.
  6. Основным средством защиты информации – это резервное копирование ценных данных, которые хранятся на жестких дисках. Нельзя чтобы важная информация хранилась только в одном единственном месте.

Например, студентка колледжа написала диплом и сохранила только на внешний накопитель. В итоге внешний накопитель был утерян и диплом пришлось писать с самого начала.

Если вы будете соблюдать рекомендации, изложенные выше, то вирусные программы будут встречаться вам значительно реже.

## 2.3 Выбор антивирусной защиты

На сегодняшний день выбор надежного антивируса самое главное для любого пользователя, что может защитить компьютер лучше, чем полноценное комплексное решение, направленное на сохранность данных и стабильную работу. Результаты этой проверки находятся в таблице 1. «Анализ антивирусных программ».

Для своего анализа я взяла бесплатные и одну пробную версии программ – это Avast, Anti-Virus, Kaspersky Free, Eset Nod32

Таблица 1. «Анализ антивирусных программ»

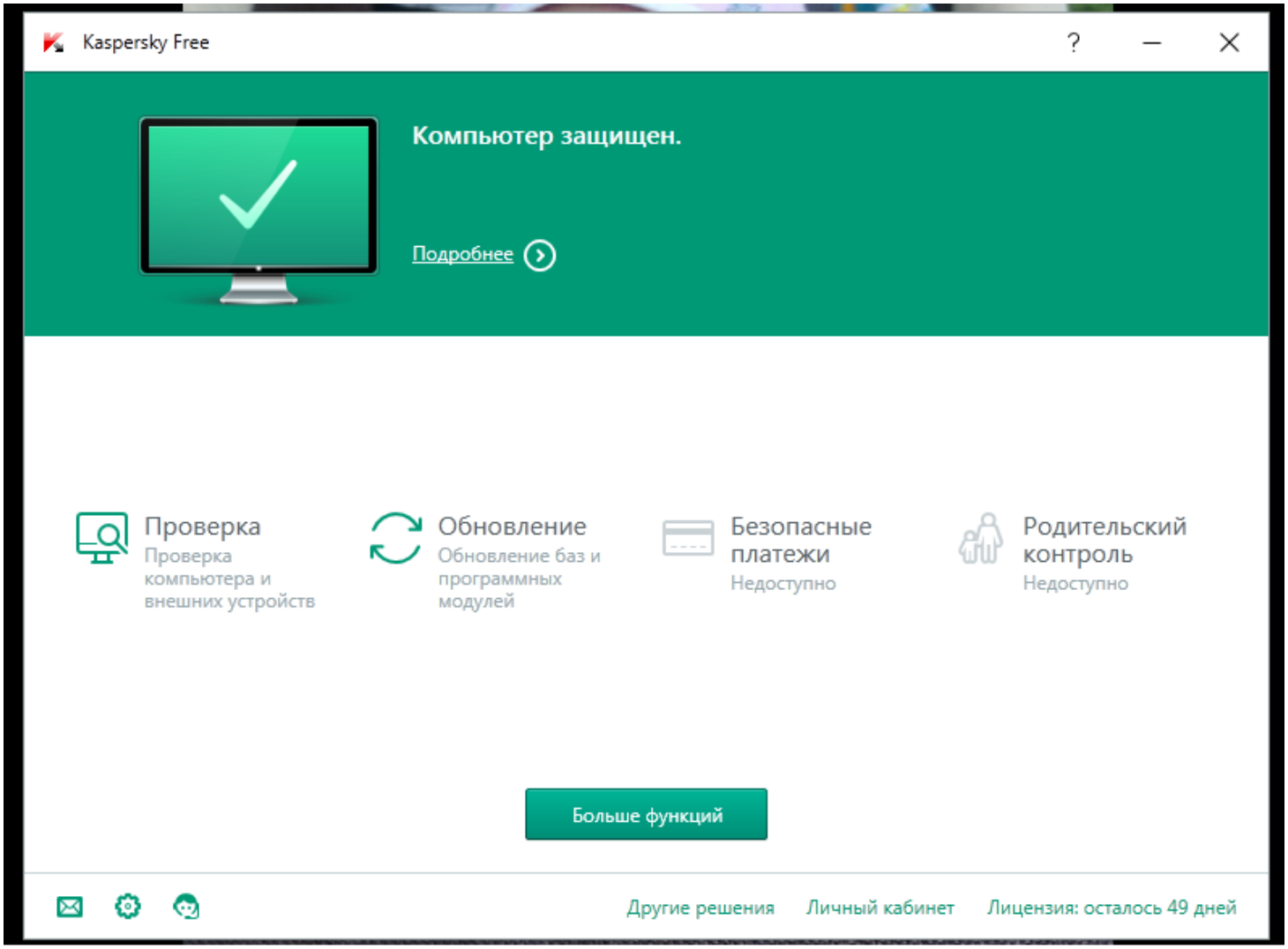
| | Kaspersky Free | Avast Free Antivirus | Eset Nod32 Smart Security Family | AVG Free |
|---|---|---|---|---|
| Лицензия | бесплатная | Бесплатная (есть платная) | пробная | Бесплатная (есть платная) |
| Русский язык | + | + | + | + |
| Поддержка | + | + | + | + |
| Сканирование по запросу | + | + | + | + |

| | | | | |
|---|---|---|---|---|
| Постоянная защита | + | + | + | + |
| Сканирование во время загрузки | + | + | + | + |
| e-mail защита | - | + | + | - |
| Антиспам | - | + | + | - |
| Веб-защита | - | + | + | + |
| Онлайн-обновление | + | + | + | + |
| Время загрузки системы с антивирусом | >1мин | <1мин | >1мин | >1мин |
| Время сканирования системных папок | >10мин | >10мин | >10мин | >10мин |

Kaspersky Free

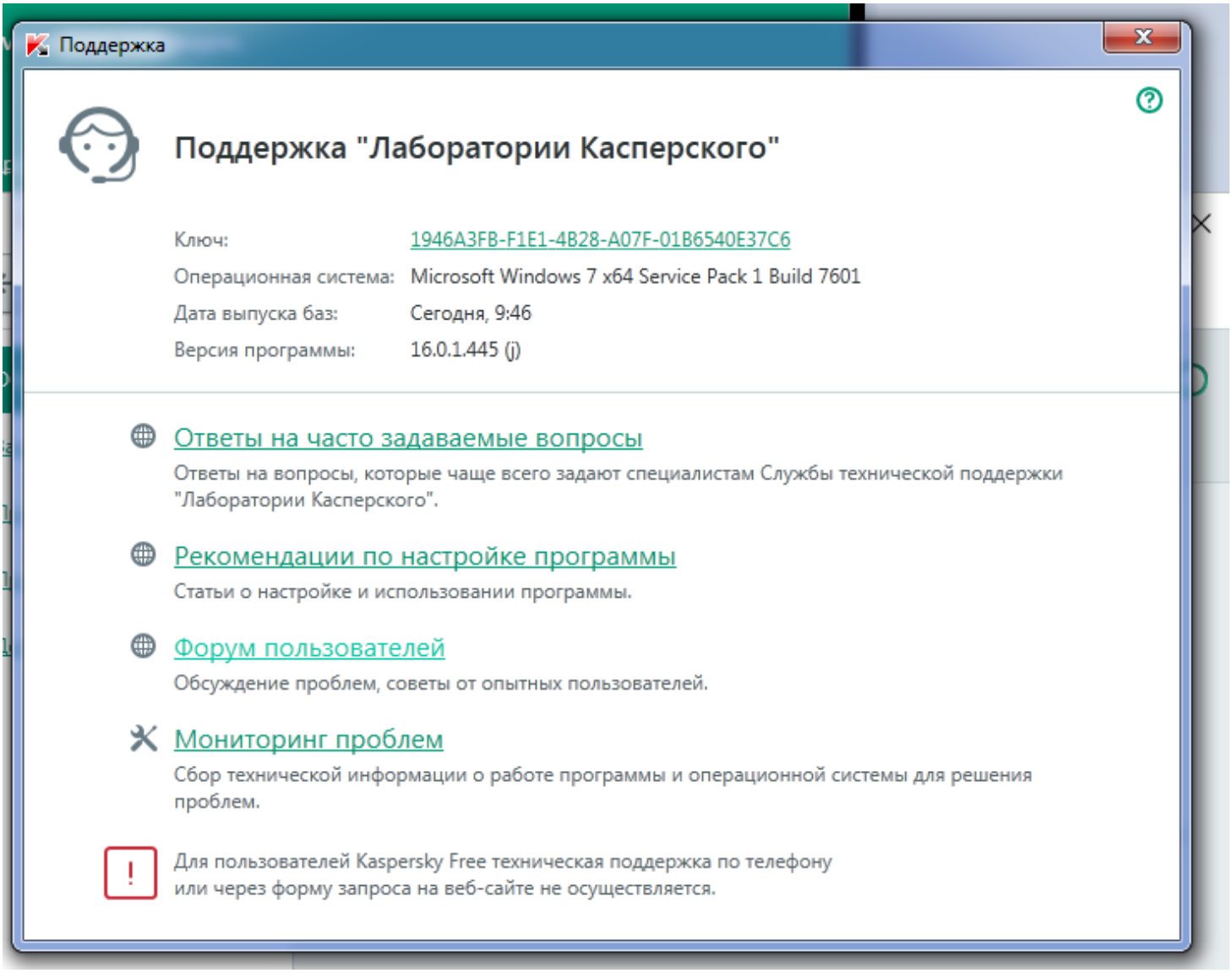
На рисунке 2. «Главное меню Kaspersky Free» видно, что лицензия есть. Идет лицензия на 365 дней. По истечению срока лицензии, можно будет переустановить программу и отсчет будет сначала на 365 дней. Также внизу рисунка есть значки для перехода в службу поддержки.

Рисунок 2. «Главное меню Kaspersky Free»



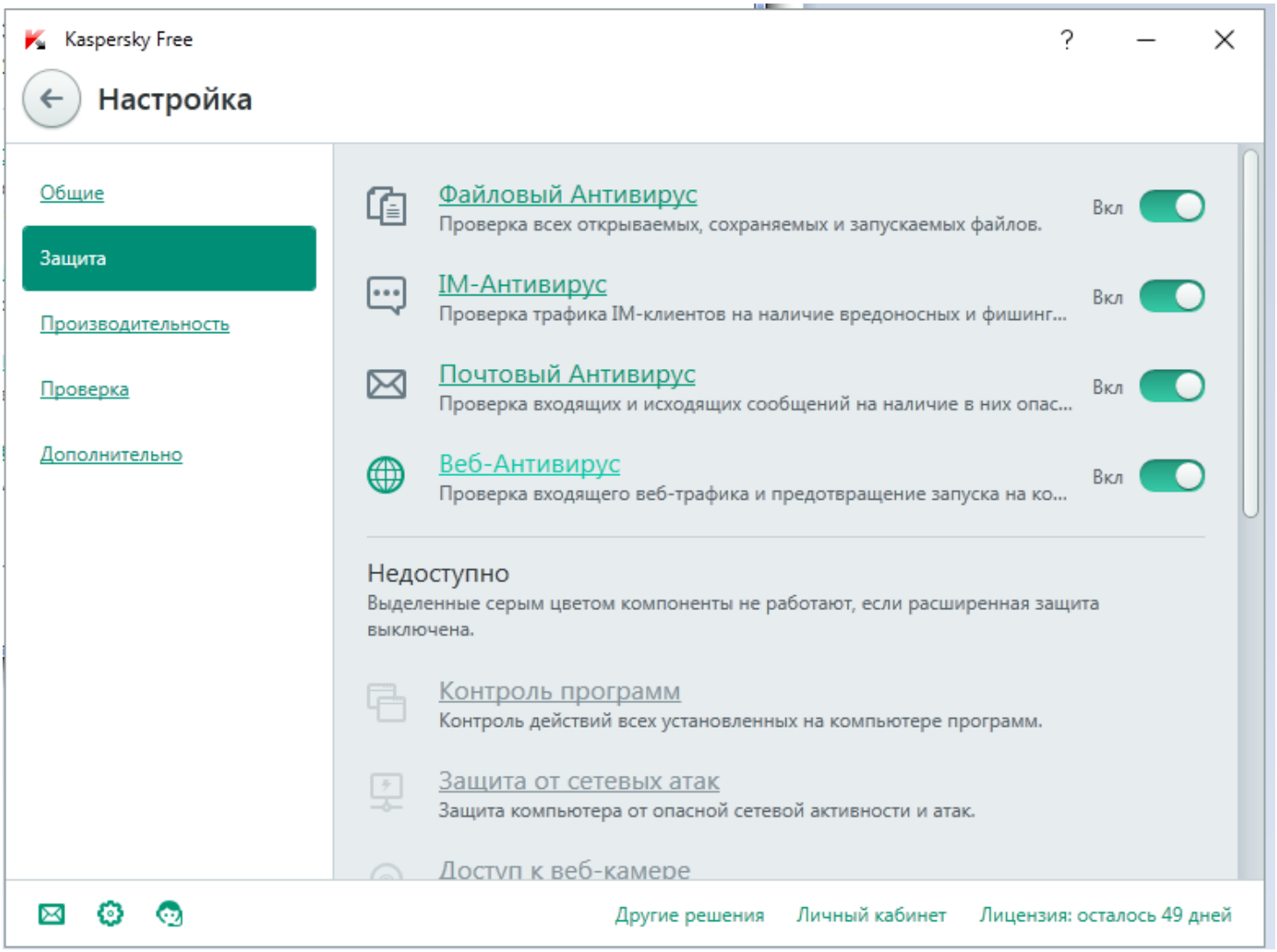

На рисунке 3. «Служба поддержки» внизу есть предупреждение о том, что в бесплатной версии антивируса служба поддержки не осуществляется по телефону и через форму запроса на веб-сайте

Рисунок 3. «Служба поддержки»




На рисунке 4. «Настройка Kaspersky Free» Доступны для защиты Файловый Антивирус, IM-Антивирус, Почтовый Антивирус, Веб-Антивирус. Все остальное доступно в более расширенной версии Касперского.

Рисунок 4. «Настройка Kaspersky Free»

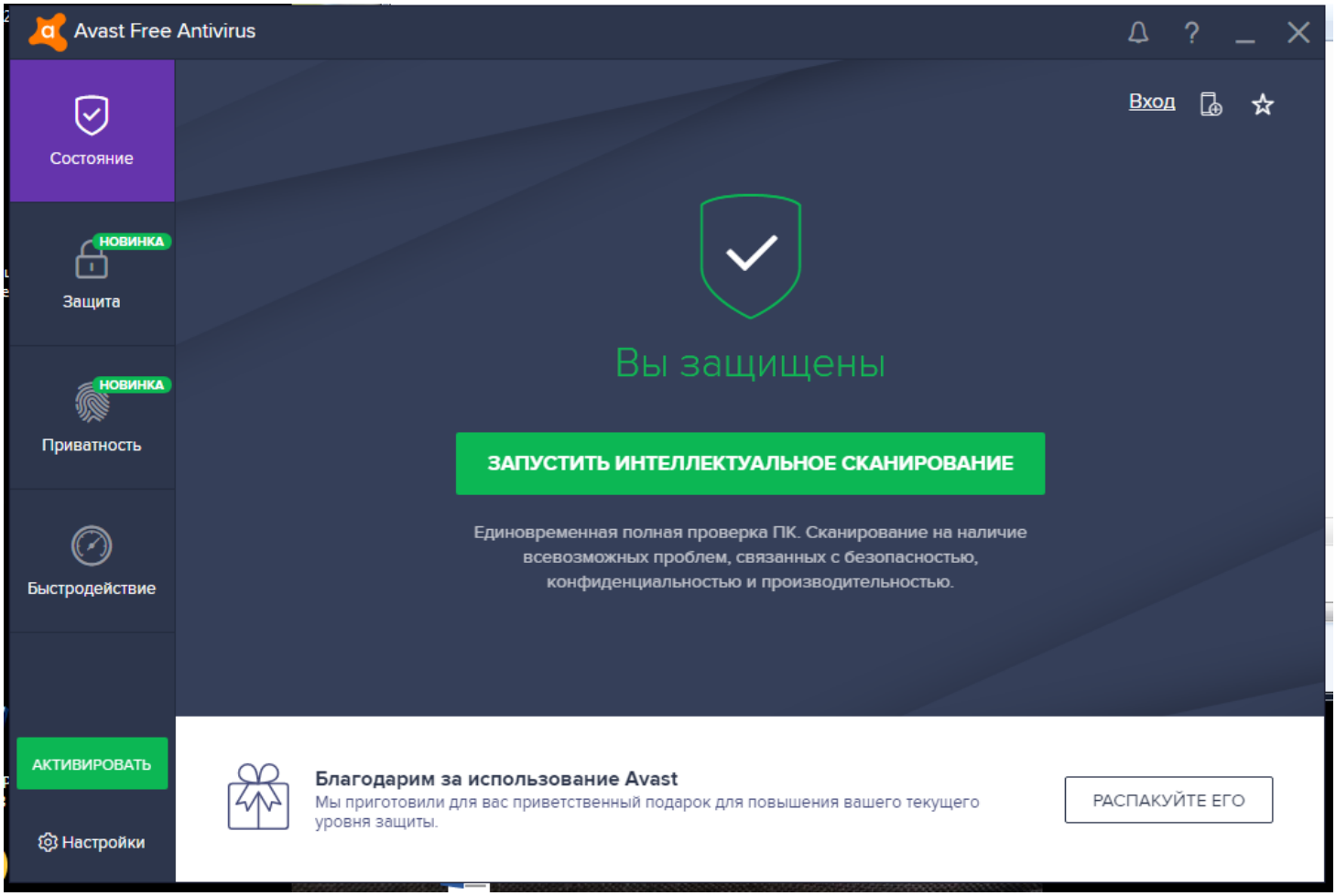



Вывод: Kaspersky Free вполне достаточно для домашнего пользования. Не требует никаких затрат. Прост и удобен в использовании обычному юзеру.

Avast Free Antivirus

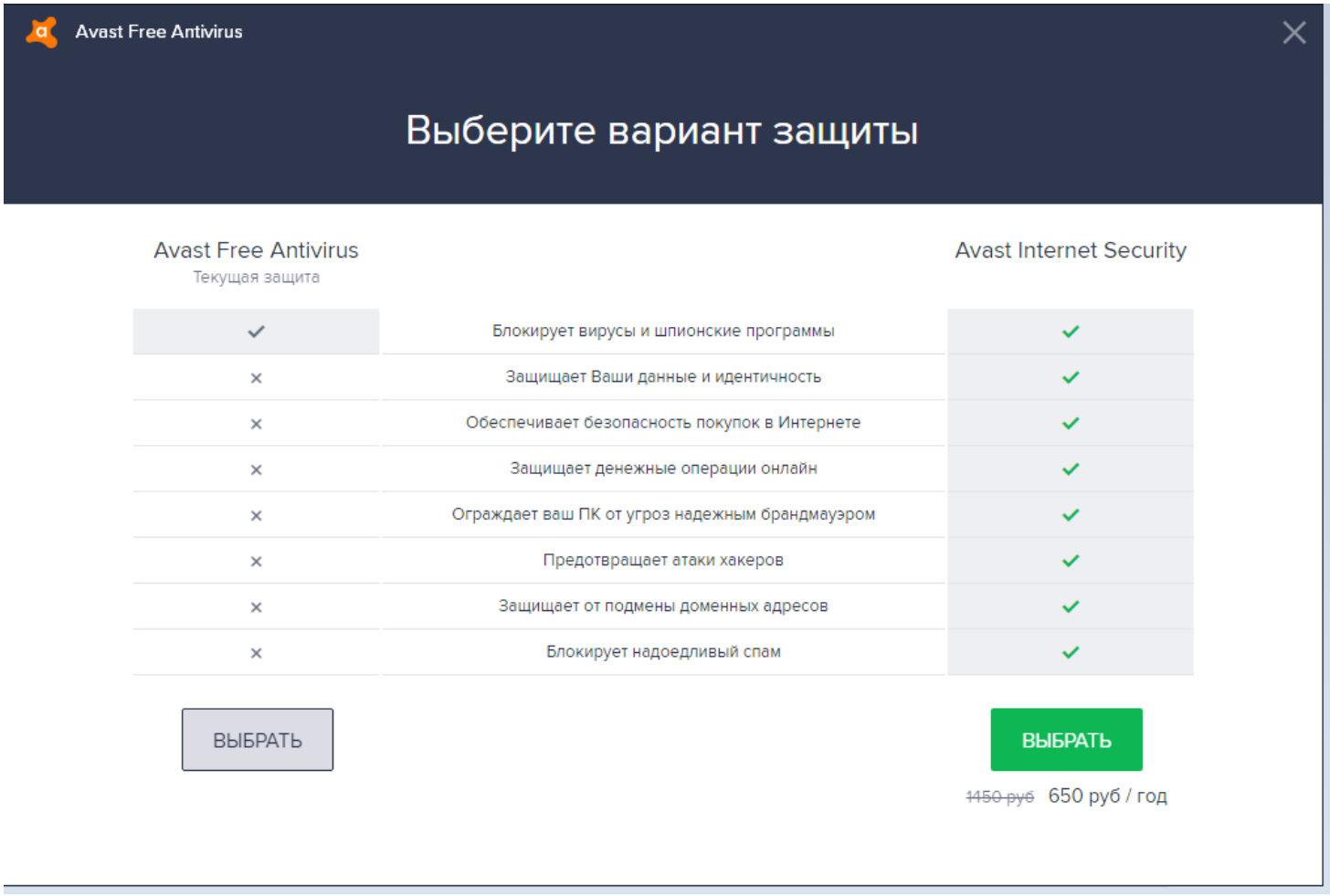
На рисунке 5. «Главное меню Avast» внизу рисунка есть кнопка активации программы. Avast в сравнении с Kaspersky Free лучше. Есть платная и бесплатная версия программы. Функции, которые в Касперском платны, то здесь они бесплатны.

Рисунок 5. «Главное меню Avast»



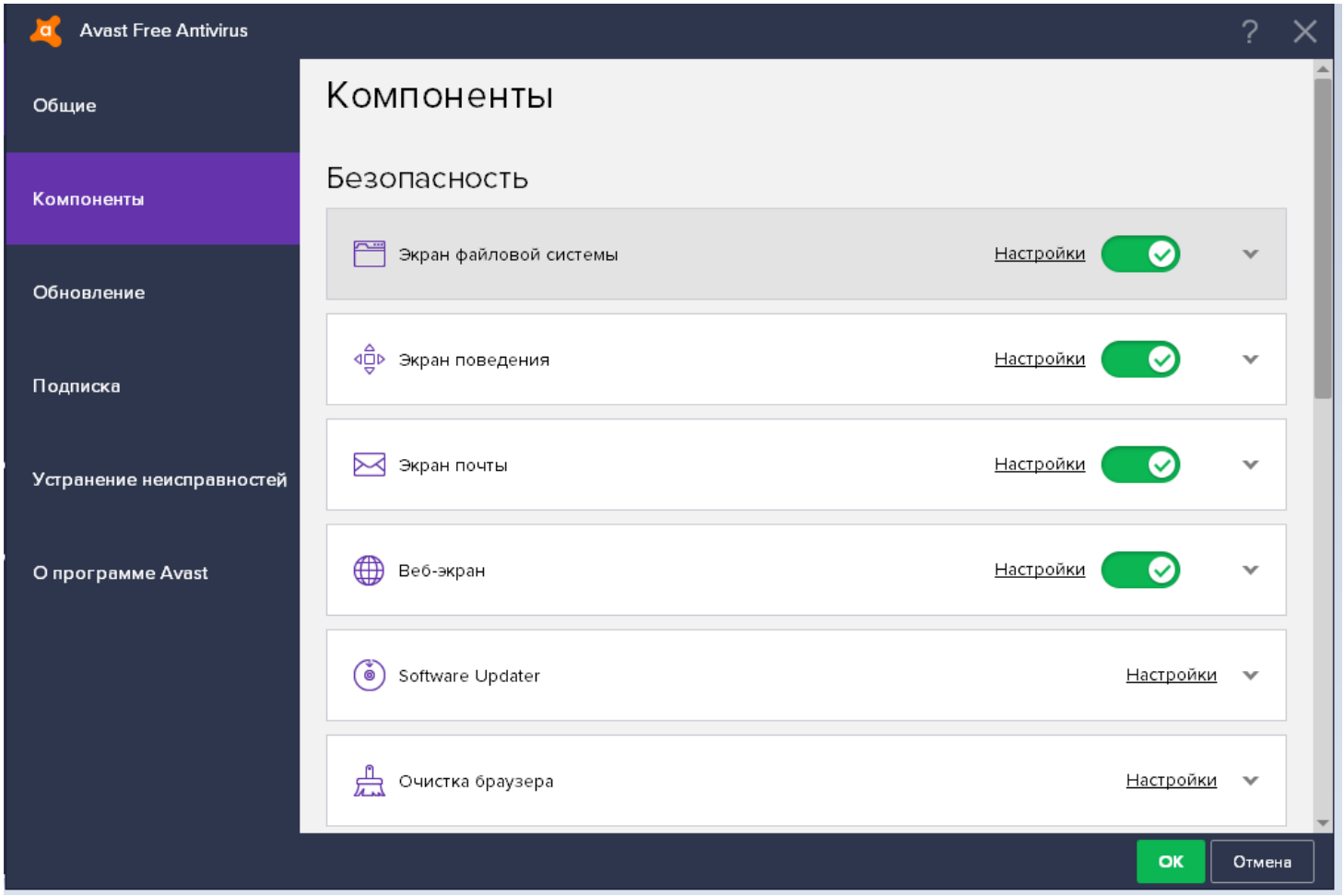

На рисунке 6. «Активация Avast» в бесплатной версии доступна функция блокировки вирусов и шпионских программ. А в платной версии дополнительно есть функции безопасных покупок в Интернете, защита денежных операций онлайн, предотвращение атак хакеров, блокирует надоедливый спам. Цена платной программы 650 рублей в год.

Рисунок 6. «Активация Avast»



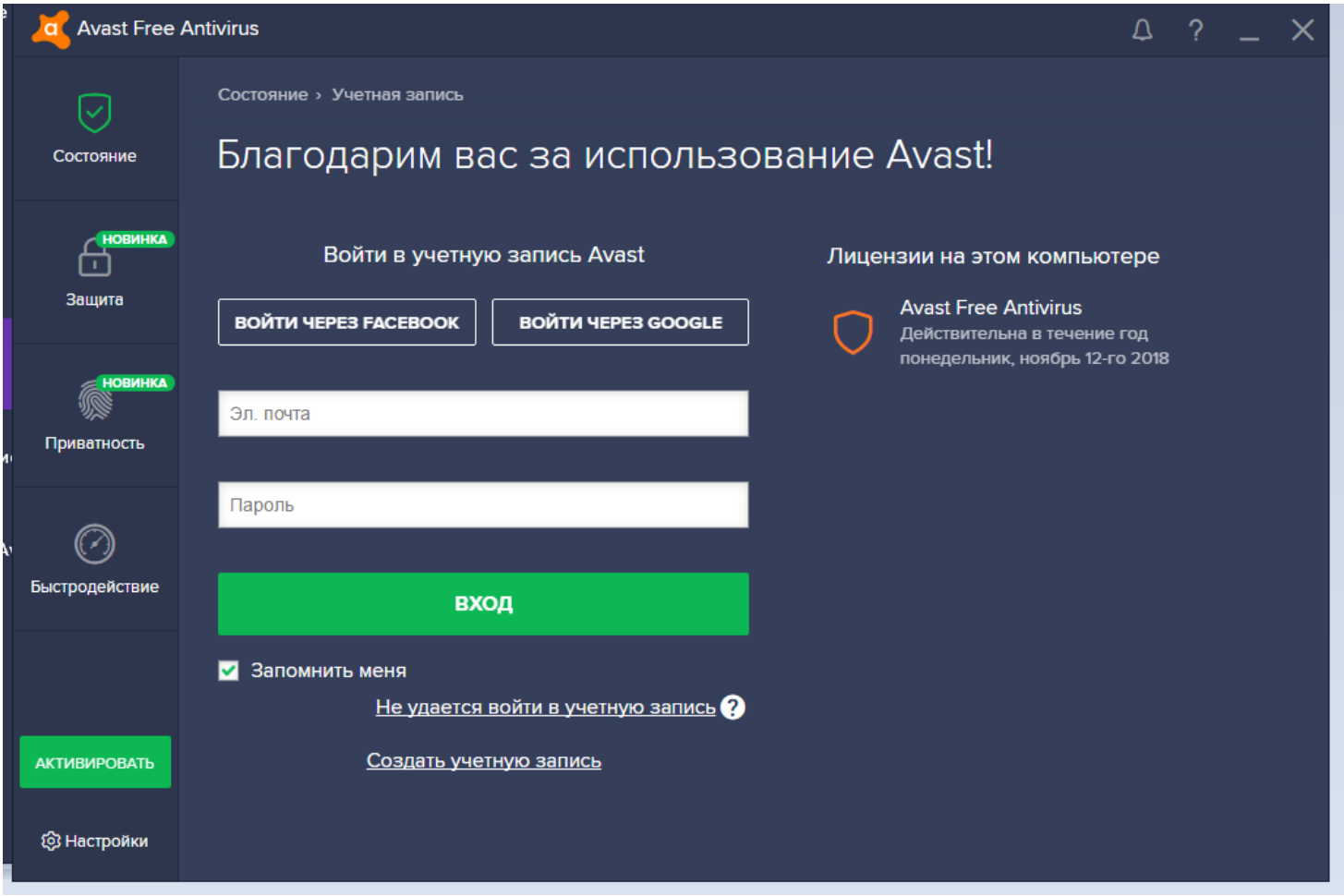

На рисунке 7. «Компоненты Avast» доступны следующие компоненты защиты: Экран файловой системы, Экран поведения, Экран почты, Веб-экран.

Рисунок 7. «Компоненты Avast»




На рисунке 8. «Учетная запись» Можно создать свою учетную запись. Также справа показывает действие лицензии, понедельник, 12 ноября 2018 года.

Рисунок 8. «Учетная запись»

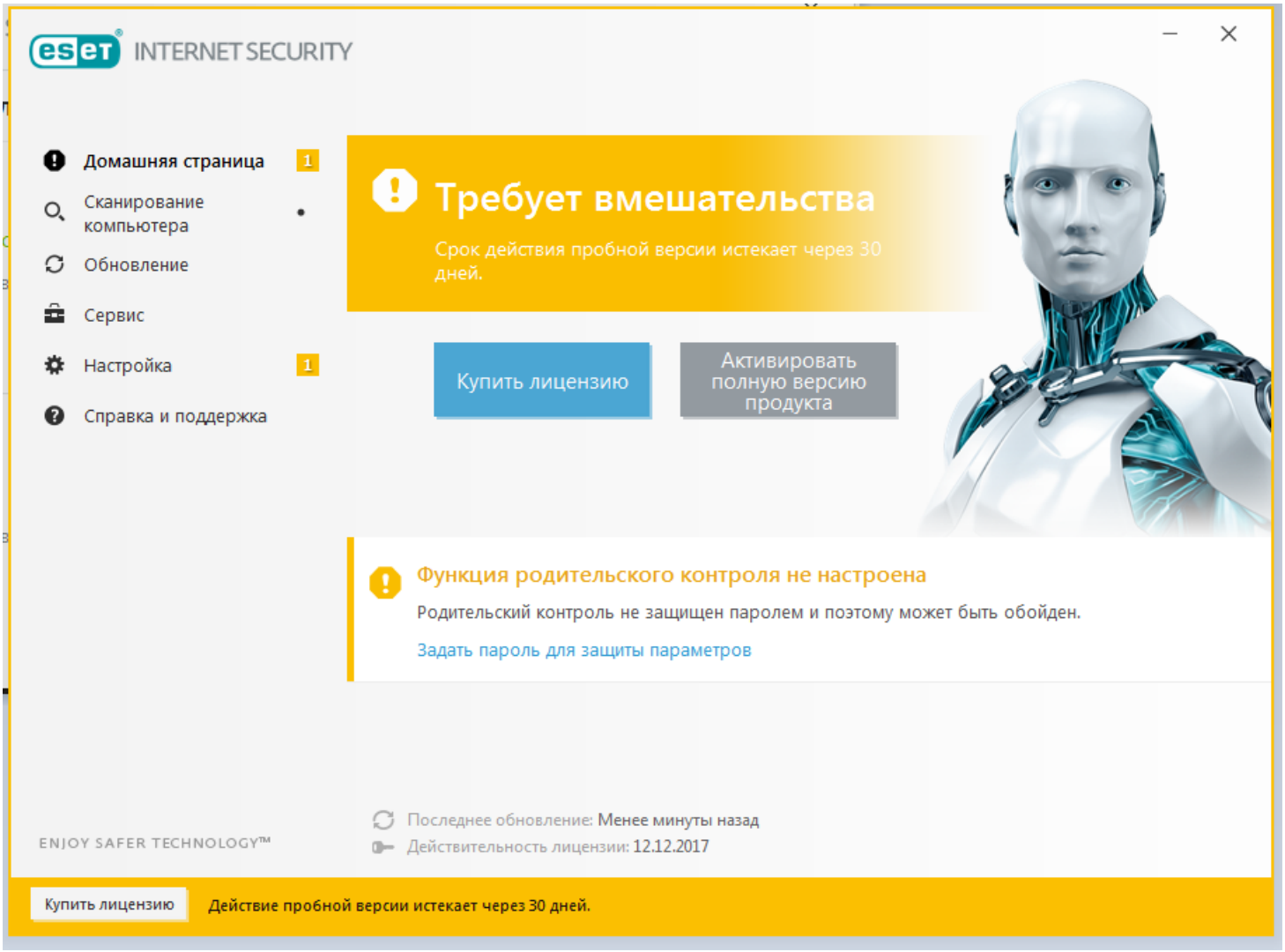



Вывод: Если вы обычный пользователь персонального компьютера для работы и дома достаточно будет данной программы. Простой интерфейс.

Eset Nod32 Smart Security Family

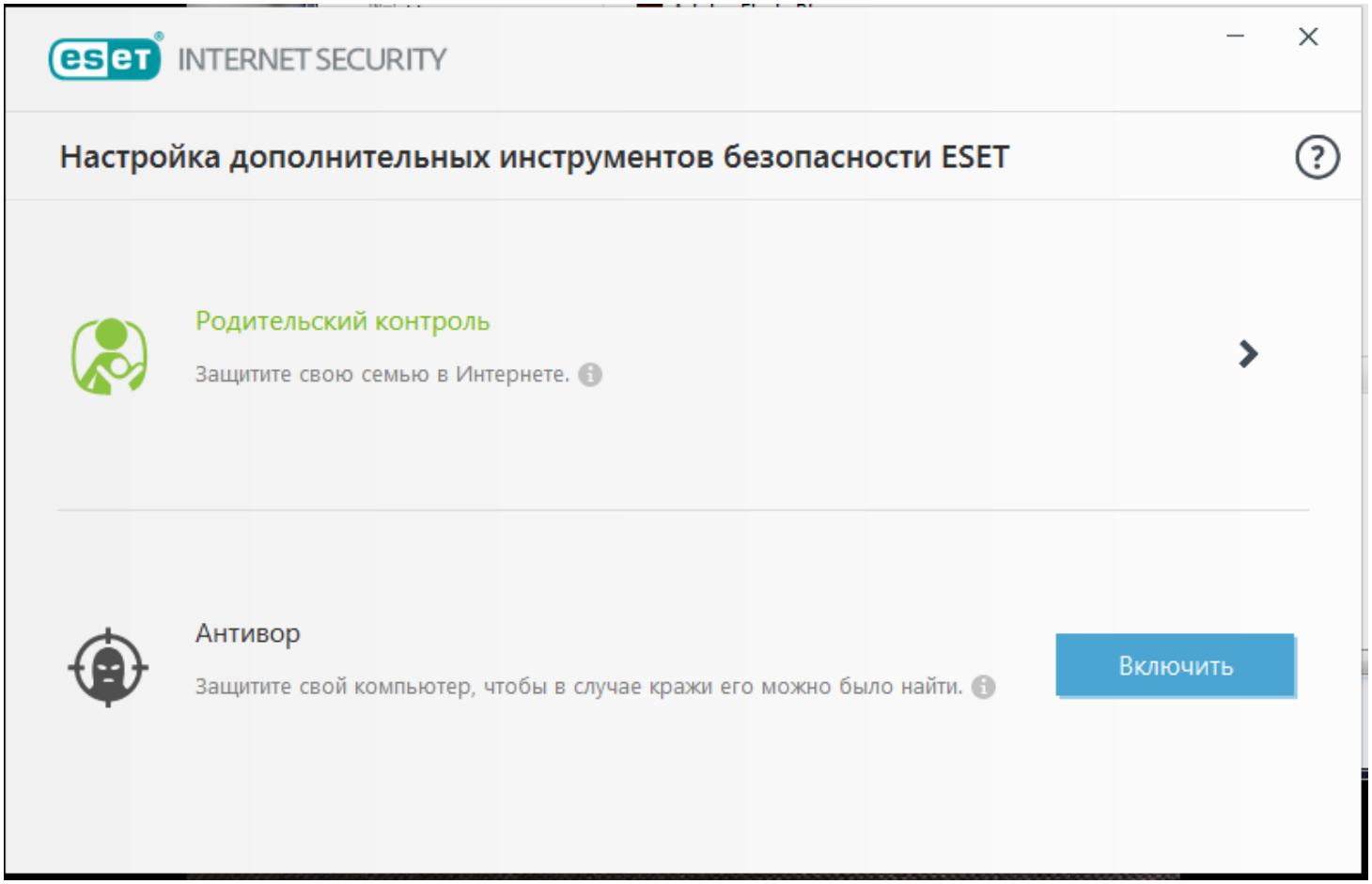
На рисунке 9. «Главное меню NOD32» Антивирус сообщает сразу о том, что это пробная версия и необходимо приобрести полную версию. Интерфейс сложнее чем в предыдущих программах. После установки данной программы сразу вышло много разных всплывающих окон. Автоматически началось сканирование компьютера, может быть это и хорошо, но большинство пользователей пугает такое количество ненужной ему информации.

Рисунок 9. «Главное меню NOD32»



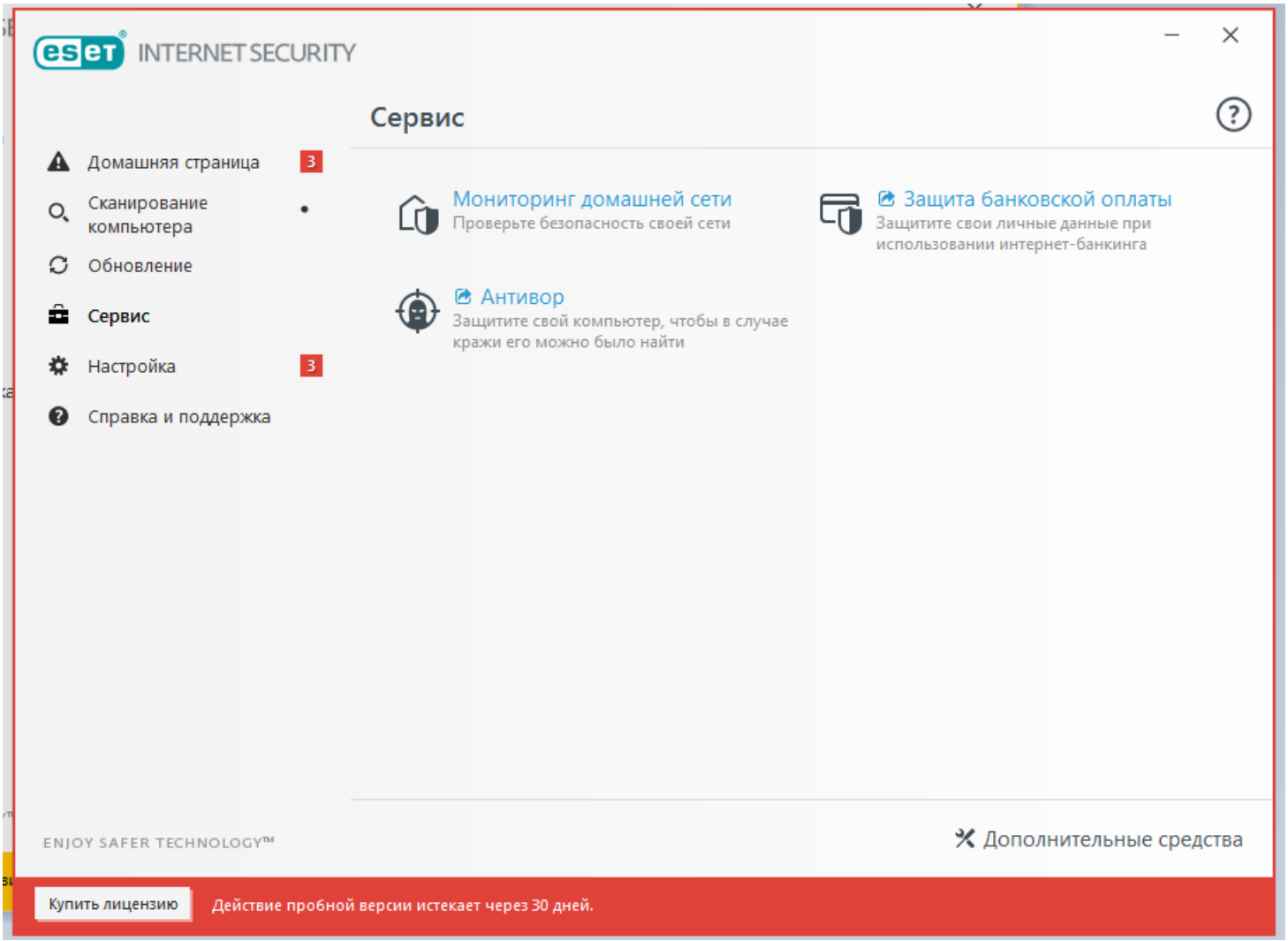

На рисунке 10 «Настройка» Есть родительский контроль и это замечательно. С помощью родительского контроля вы можете защитить своих детей от ненужной информации в интернете.

Рисунок 10. «Настройка»



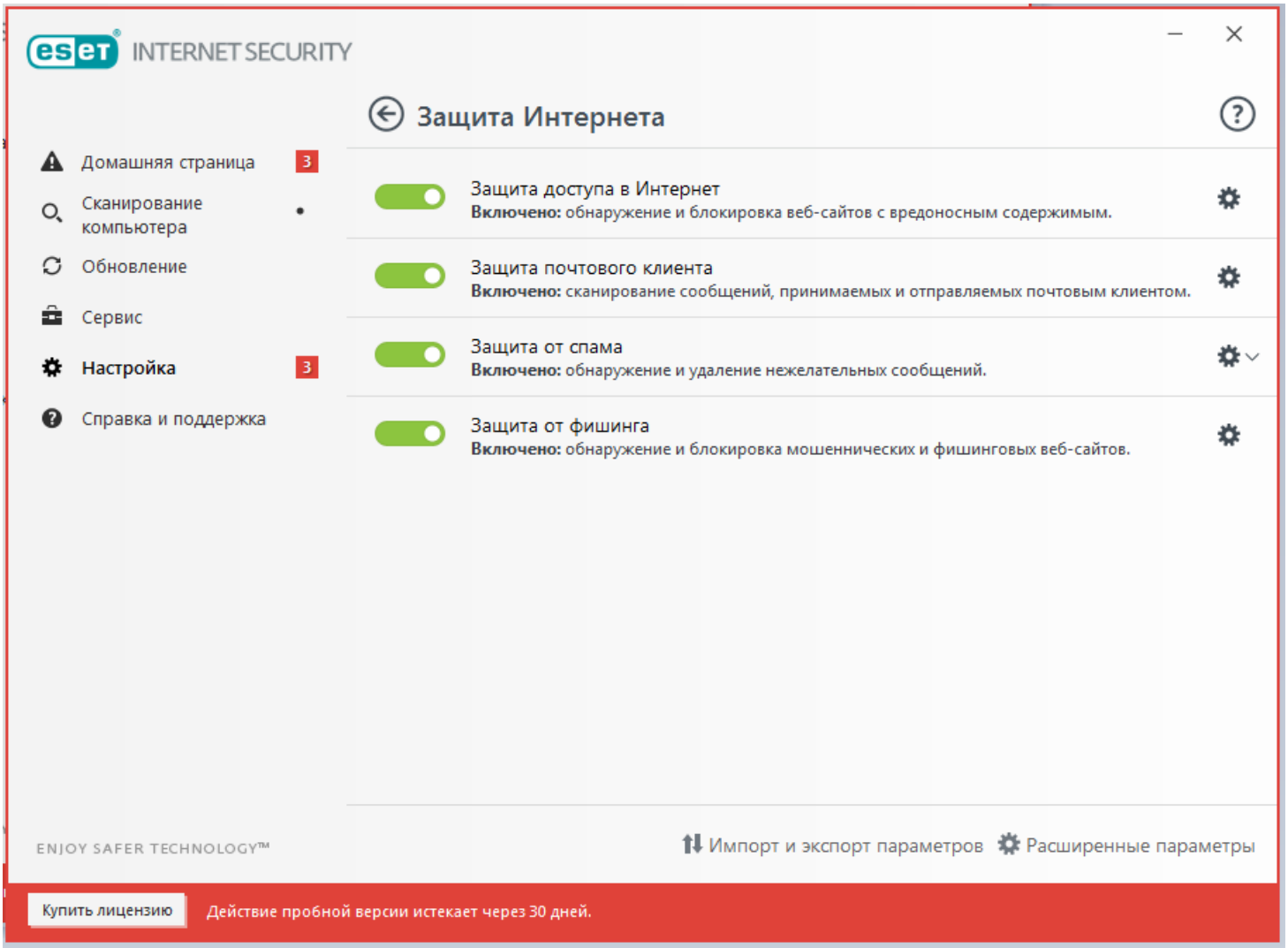

На рисунке 11 «Сервис» Во вкладке сервис есть следующие функции: Мониторинг домашней сети – проверяет безопасность вашей сети, Защита банковских оплат – это хорошо если вы пользуетесь интернет магазинами и совершаете покупки через интернет, Антивор – в случае кражи вашего компьютера.

Рисунок 11. «Сервис»



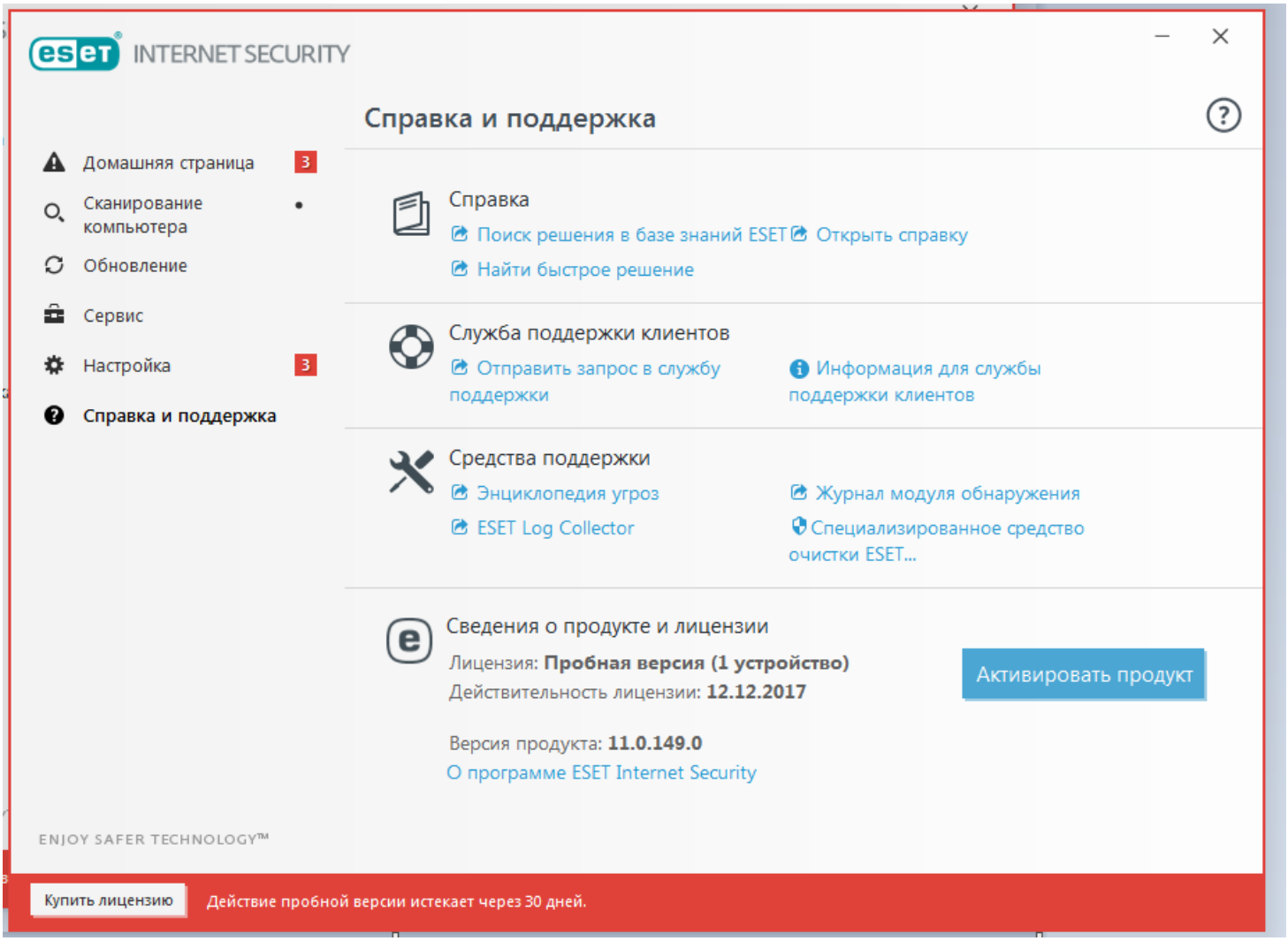

На рисунке. 12 «Защита Интернета» защита доступа в интернете – обнаружение и блокировка сайтов с вредоносным содержимым, защита от спама – обнаружение и удаление нежелательных сообщений, защита почтового клиента – сканирует сообщения которые отправляют и принимают. защита от фишинга – обнаружение и блокировка мошеннический веб-сайтов.

Рисунок 12. «Защита Интернета»




На рисунке 13. «Справка и поддержка» Также, как и в остальных антивирусных защитах, здесь есть справка и поддержка. Ниже на рисунке есть информация о программном продукте и лицензия. И если у вас есть ключ, то его можно ввести нажав на кнопку активировать продукт.

Рисунок 13. «Справка и поддержка»

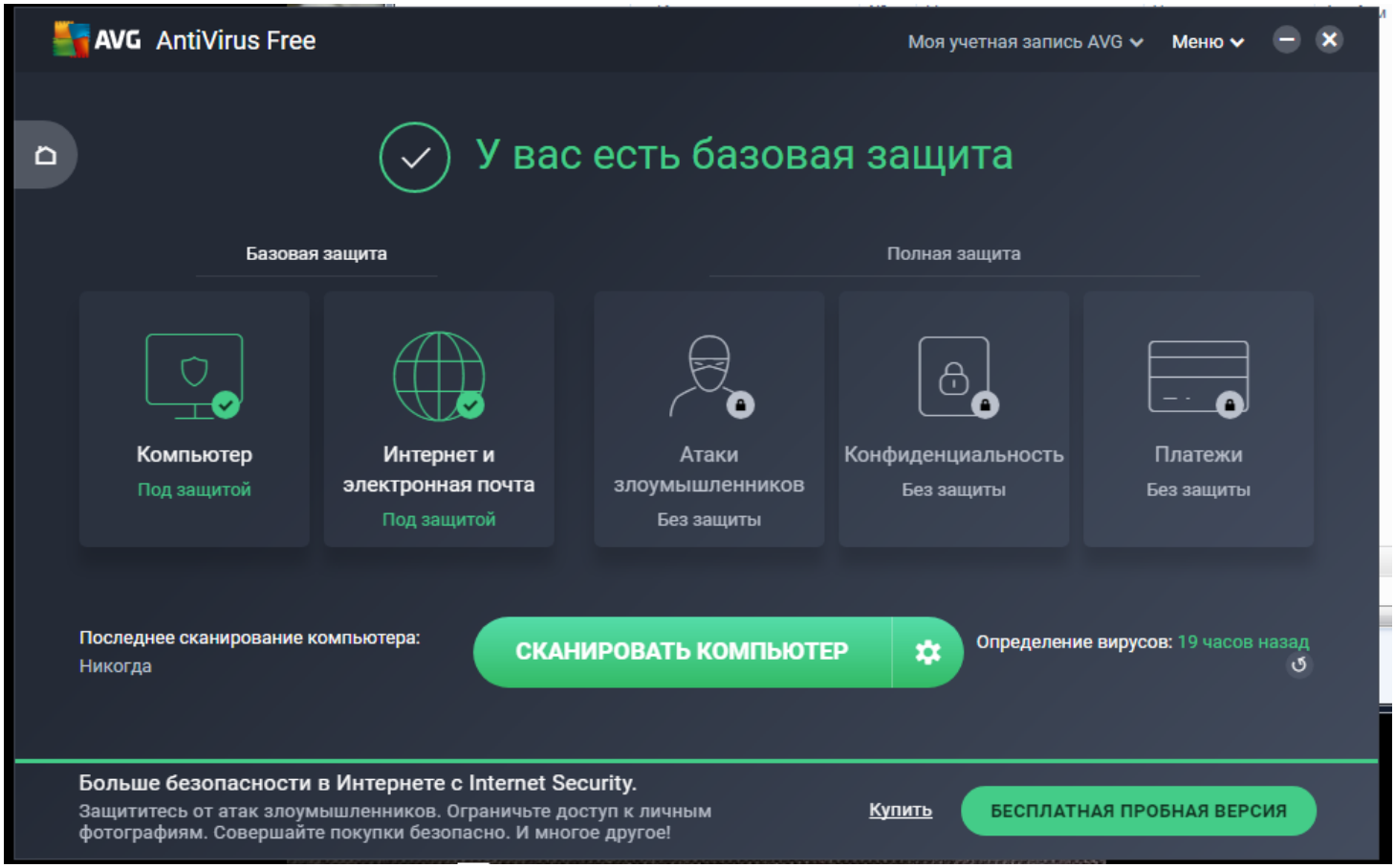



Вывод: Обычному пользователю будет сложно разобраться с данной программой. Такую антивирусную защиту можно ставить на рабочие компьютеры для большого количества пользователей, но только платную версию. На мой взгляд в данной антивирусной защите много всплывающих окон за время работы за компьютером.

AVG Free

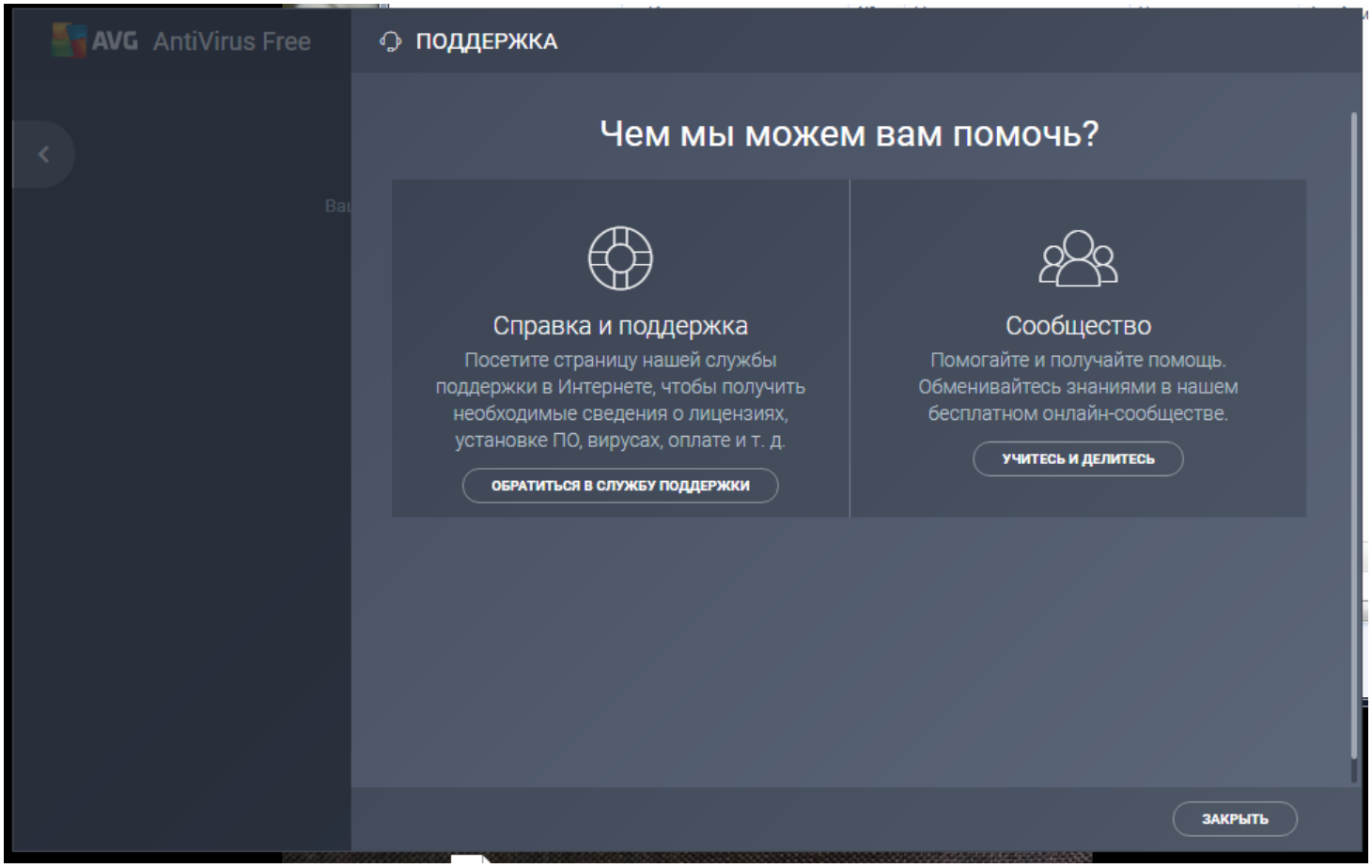
На рисунке 14. «Главное меню AntiVirus Free» сразу уведомляют о том, что выбрана базовая защита, но также есть полная защита. И различия между базовой и полной защитой. Можно попробовать пробную версию полной защиты.

Рисунок 14. «Главное меню AntiVirus Free»



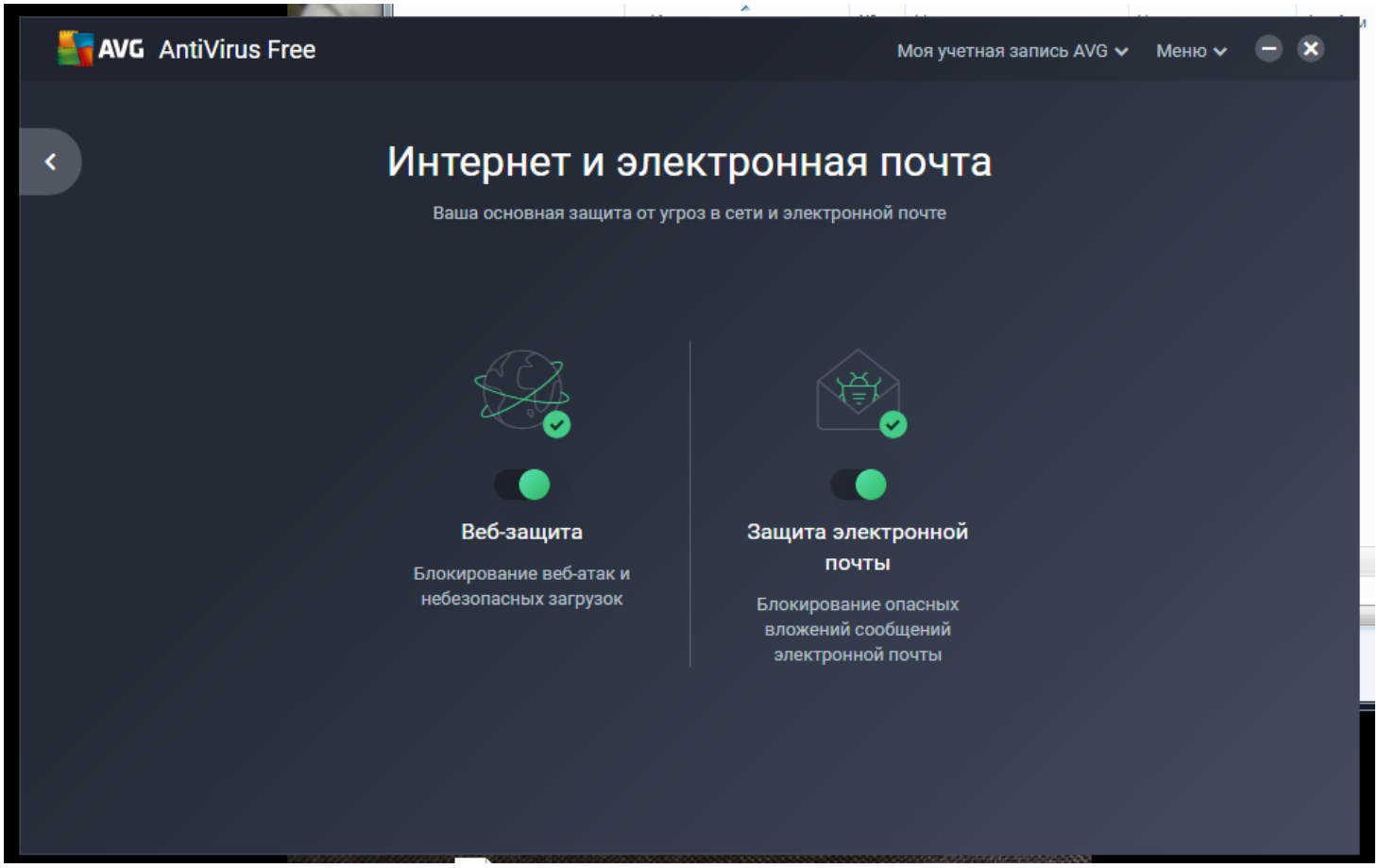

На рисунке 15. «Поддержка» Есть два варианта поддержки: Справка и поддержка – это посетить официальный сайт. Сообщество – это делится своими знаниям с другими пользователями и получать от них полезную информацию.

Рисунок 15. «Поддержка»




На рисунке 16. «Интернет и электронная почта» Есть функции защиты электронной почты и веб- защита, что является плюсом к данной программе.

Рисунок 16. «Интернет и электронная почта»




Вывод: Собрав все плюсы и минусы лучшие антивирусные программы это – Avast и NOD32. Но опираясь на личный жизненный опыт, я для себя выбираю Avast и Касперский.

## Заключение

Выбор способов защиты информации в информационной системе - сложная оптимизационная задача, при решении которой требуется учитывать вероятности различных угроз информации, стоимость реализации различных способов защиты и наличие различных заинтересованных сторон. [7]

Эффективность информационной безопасности означает, что затраты на ее осуществление не должны быть больше возможных потерь от реализации информационных угроз. Планирование безопасности информации осуществляется путем разработки каждой службой детальных планов защиты информации. [12]

Для того чтобы защитить информацию от вирусов, хакеров нужно выполнять рекомендации, указанные в главе 2, пункт 2.2 способы защиты информации. Но для

того чтобы выполнить данные рекомендации необходимо определится с выбором антивирусной защиты. На мой взгляд лучше всего выбрать антивирус Касперского лицензионную версию, купленную в магазине.

Если вы уверенный пользователь персонального компьютера, знаете, что можно скачивать с интернета, а что нет, то вам будет достаточно антивируса Kaspersky Free.

Есть ситуации, когда антивирусная защита не в силах спасти ваши данные. Как это и произошло на моем жизненном опыте.

Компьютер начал тормозить. Я хорошо знаю свой компьютер и догадывалась, что это скорее всего жесткий диск и необходимо покупать новый или копировать информацию. Информации было очень много за пять лет. Обучение, работа и личная жизнь абсолютно все хранилось на данном жестком диске. Используя свои знания я смогла сделать тест своего жесткого диска с помощью загрузочного диска live cd, программа Victoria. В результате теста было обнаружено огромное количество Bad-блоков. Что уже говорило о том, что необходимо срочно брать новый жесткий диск. Отсутствие финансов и моя халатность решили, что торопится особо не стоит. Итог лишилась всей информации за пять лет. Пробовала восстановить информацию с помощью различных программных продуктов, от самых простых, до самых сложных. Есть вероятность, что этими программными продуктами я просто его добила. Проблема на сегодняшний день осталась не решенной, надеюсь на аппаратное восстановление информации, но для этого нужно гораздо больше денег, чем на новый жесткий диск. Очень жалею, что не смогла сохранить свою информацию.
Задачи, сформулированные во введении, решены, цель работы достигнута.

## Список использованной литературы


1. Государство и право [Электронный ресурс] Виды и состав угроз информационной безопасности — Режим доступа: — www.allbest.ru Загл. с экрана. — Яз. рус. англ.
2. ВикипедиЯ [Электронный ресурс] информационная безопасность — Режим доступа: — ru.wikipedia.org Загл. с экрана. — Яз. рус. англ.
3. Безопасность [Электронный ресурс] информационная безопасность и виды возможных угроз— Режим доступа: — www.inf74.ru Загл. с экрана. — Яз. рус. англ.

4. ВикипедиЯ [Электронный ресурс] Вредоносная программа— Режим доступа: — ru.wikipedia.org Загл. с экрана. — Яз. рус. англ.
5. Экономическая информатика [Электронный ресурс] Введение в экономическую информатику — Режим доступа: — lessons-tva.info Загл. с экрана. — Яз. рус. англ.
6. СтудопедиЯ [Электронный ресурс] Виды и состав угроз информационной безопасности — Режим доступа: — studopedia.ru Загл. с экрана. — Яз. рус. англ.
7. ReferatBox [Электронный ресурс] Информационная безопасность — Режим доступа: — referatbox.com Загл. с экрана. — Яз. рус. англ.
8. Kaspersky [Электронный ресурс] Продукты — Режим доступа: — kaspersky.ru Загл. с экрана. — Яз. рус. англ.
9. Avast [Электронный ресурс] Главная— Режим доступа: — avast.ru Загл. с экрана. — Яз. рус. англ.
10. AVG [Электронный ресурс] Главная— Режим доступа: — avg.com Загл. с экрана. — Яз. рус. англ.
11. Eset [Электронный ресурс] Скачать— Режим доступа: — esetnod32.ru Загл. с экрана. — Яз. рус. англ.
12. Экономика [Электронный ресурс] основы экономики— Режим доступа: — finlit.online Загл. с экрана. — Яз. рус. англ.
13. Автор студенческих работ [Электронный ресурс] информационная безопасность — Режим доступа: — help-stud.ru Загл. с экрана. — Яз. рус. англ.