Министерство образования Калининградской области

государственное бюджетное учреждение Калининградской области

профессиональная образовательная организация

«Колледж информационных технологий и строительства»

(ГБУ КО ПОО «КИТиС»)

**Отчет по учебной практике**

УП.04 Сопровождение и обслуживание программного обеспечения компьютерных систем

по ПМ.04 Сопровождение и обслуживание программного обеспечения компьютерных систем

Специальность 09.02.07 «Информационные системы и программирование»

Сроки прохождения практики:

с «13» февраля 2023 г. по «6» марта 2023 г.

Место практики ГБУ КО ПОО «КИТиС»

|  |  |
| --- | --- |
| Выполнил: | студент 2 курса,  группы ИСп 21-2К  Карпов Ярослав Максимович  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) |
| Проверила: | Большакова-Стрекалова Анна Викторовна  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (оценка)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, дата) |

Калининград 2023

Содержание

1 Обеспечение внедрения и поддержки программного обеспечения

компьютерных систем

1.1 Инструктаж по технике безопасности

1.2 Описание выбранного аппаратного и программного обеспечения

1.3 Методы внедрения и анализа функционирования программного

обеспечения

1.4 Сценарий и техническое задание на внедрение ПО

1.5 Загрузка и установка программного обеспечения

2 Проблемы совместимости и методы их устранения

2.1 Тестирование на совместимость в безопасном режиме

2.3 Средства диагностики оборудования

2.4 Измерение и анализ эксплуатационных характеристик качества

программного обеспечения

2.5 Оптимизация и модификация ПО

2.6 Разработка руководства оператора

3 Этапы сопровождения и обслуживания ПО

3.1 Разработка технического задания на сопровождение

4 Методы и средства защиты компьютерных систем

4.2 Тестирование интерфейса

4.3 Тестирование контента

4.4 Анализ рисков. Выявление первичных и вторичных ошибок

4.5 Обнаружение вируса и устранение последствий его влияния

4.6 Тестирование защиты программного обеспечения

5. Индивидуальное задание [13]

5.1 Практические работы

5.2 Разработка технико-экономического обоснования. Формирование бизнес-цели проекта. Разработка устава проекта обеспечения

5.3 Виды вирусных программ и их структура

Заключение

Список использованных источников

Введение

Учебная практика по дисциплине ПМ 04

«Сопровождение и обслуживание программного обеспечения компьютерных систем»

Цель практики: Учебная практика по специальности направлена на формирование у обучающихся умений, приобретение практического опыта для последующего освоения ими общих и профессиональных компетенций по специальности.

Устанавливаемое программное обеспечение: Kaspersky

Антивирусное программное обеспечение нужно для защиты компьютера от кибер-угроз. Оно обеспечивает безопасность для компьютера.

Антиви́рус Каспе́рского — антивирусное программное обеспечение, разрабатываемое «Лабораторией Касперского». Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также от неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS (только для версий, именуемых «Kaspersky Internet Security 2009+, где '+' — порядковый номер предыдущего регистра, ежегодно увеличиваемый на единицу в соответствии с номером года, следующим за годом выпуска очередной версии антивируса»). Антивирус Касперского является самым продаваемым в России и имеет много достоинств, например он обеспечивает безопасность от многих вирусных программ, имеет расширение для браузеров, которое блокирует баннеры, спам, не дает переходить на опасные сайты, обеспечивает безопасное хранение данных. Однако у него есть еще недостатки. К ним относится сильная нагрузка на систему, может нормальные файлы воспринимать за вирус, есть навязчивые функции. Данный антивирус имеет бесплатную пробную версию с лицензией на 30 дней чтобы понять, устраивает он вас или нет.

1 Обеспечение внедрения и поддержки программного обеспечения компьютерных систем

1.1 Инструктаж по технике безопасности

Антивирус нужно загружать с официального сайта:

<https://www.kaspersky.ru/home-security>

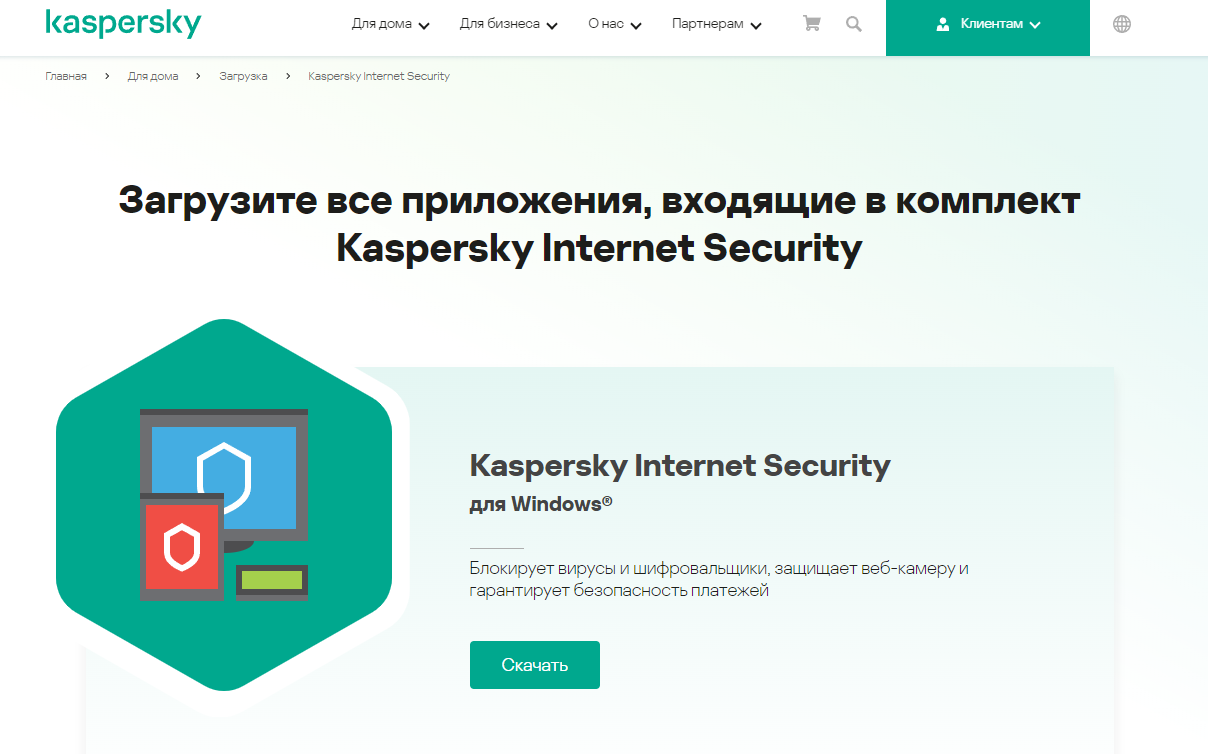


Рисунок 1 – официальный сайт

1. Не следует скачивать антивирус с посторонних сайтов, так как можно поймать вредоносное ПО, которое может нанести вред системе или устройству.
2. Если же на компьютере стоял антивирус, его нужно удалить, так как он может конфликтовать с другим антивирусом и вызывать ошибки.
3. Нужно обновлять антивирус, потому что разработчики в новых версиях исправляют ошибки, которые могут вызывать сбой.
4. Лучше ставить антивирус на чистую операционную систему, чтобы не было конфликтов и сбоев.
5. Не стоит ставить антивирус на слабый пк, так как он может замедлять его работу.

1.2 Описание выбранного программного обеспечения.

Антивирус Касперского – программное обеспечение, разработанное лабораторией Касперского для защиты компьютера от вредоносного ПО, которым являются вирусы, трояны, черви, программы-шпионы и т.д. Также он защищает данные, блокирует переходы на фишинговые ссылки. Как и любой антивирус имеет два вида проверки: быстрая проверка и полная проверка. Быстрая проверка проверяет установленные приложения и места, где обычно встречаются вирусы. Полная проверка проверяет все файлы, внешние и внутренние накопители. Этот антивирус имеет платную и бесплатную версию. Платная версия может защитить все ваши устройства, имеет более лучшую защиту. Бесплатная же версия защищает только одно устройство, имеет базовую защиту, которая уступает защите в платной версии. Kaspersky имеет много различных вариаций антивируса, такие как Kaspersky Security для бизнеса, Kaspersky internet security для дома и т.д.

Достоинства:

1. Защиты от всех видов интернет-угроз.
2. Полноценная защита от всех видов вирусов и атак, которая включает эвристический анализ, поведенческую блокировку, проверку по всем базам.
3. Проверка трафика, почтовых сообщений и скачиваемых файлов в режиме реального времени.
4. Защита от спама и фишинга.
5. Родительский контроль.
6. Защита от утечек всей конфиденциальной информации.
7. Автоматическое обновление баз.
8. Постоянный сетевой контроль.

Недостатки:

1. Необходимость регулярно платить за лицензионный ключ.
2. Большая нагрузка на систему, которая приводит к медленной работе маломощных компьютеров.
3. Занимает много места и оперативной памяти при работе.
4. При выполнении проверки требуется закрытие других программ, что иногда бывает просто невозможно.
5. Воспринимает некоторые нормальные файлы, как вредоносные.
6. Определенные функции программы могут быть слишком навязчивыми и надоедать пользователю.

Требования для установки:

ОС: Windows 7, windows 10, Mac OS

512 мб ОЗУ

Процессор 1ГГц и выше.

1500мб свободного места на диске.

1.3 Методы внедрения и анализа функционирования программного обеспечения

Для внедрения антивируса Касперского нужно:

1. Загрузить и установить антивирус
2. Зарегистрироваться в My Kaspersky чтобы получать новости о обновлениях, стабильных и новых версиях, новых функций и так далее.
3. Выбрать нужную версию.

Функциональность:

1. Функция отката, позволяющая устранить последствия деятельности вредоносных программ;
2. Средства от интернет-мошенничества (в частности, фишинга и кейлоггеров) для повышения степени защиты личных данных и другой ценной информации;
3. Защита данных при выполнении финансовых операций в интернете
4. Защита от сетевых хакерских атак;
5. Контроль изменений (сообщает о готовящихся изменениях параметров браузера, в том числе вызванных установкой рекламных программ, панелей инструментов);
6. Защита от сбора данных (запрещает сайтам отслеживать сценарии пользования интернетом и собирать личные данные);
7. Контроль интернет-трафика (помогает оптимизировать расходы при подключении к интернету через Wi-Fi, 3G и 4G);
8. Защита от программ-шифровальщиков;
9. Проверка безопасности публичных сетей Wi-Fi (помогает защитить от кражи данных через незащищенные сети);
10. Защита от несанкционированного подключения к веб-камере;
11. Поиск уязвимостей в программах;
12. режим Безопасных программ (разрешает запуск только доверенных приложений и ограничивает работу всех подозрительных программ);
13. Обеспечение актуальной информацией о репутации программ и веб-сайтов;
14. Блокирование нежелательного контента (в частности, рекламных баннеров и спам-рассылок);
15. Управление доступом детей к веб-сайтам и программам, а также контроль их общения в социальных сетях;

1.4 Сценарий и техническое задание и внедрение ПО

1) Антивирус нужно сначала скачать с официального сайта, а затем установить.

2) При возможности, ввести ключ активации для лицензии антивируса. Для этого в нижнем правом углу заходим в ‘Лицензирование’.

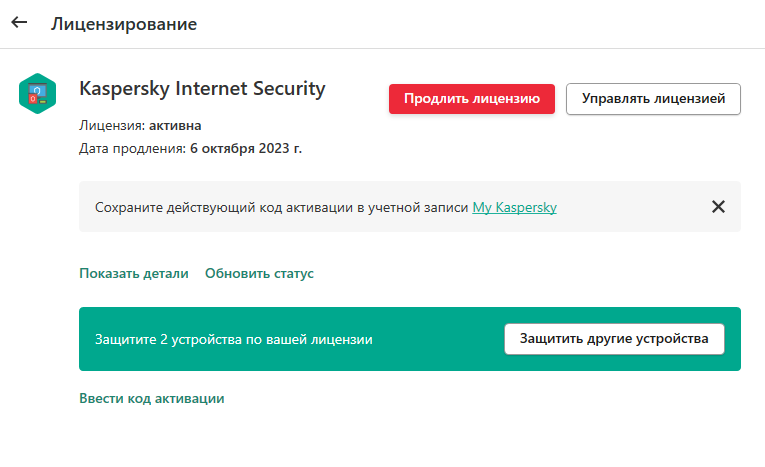


Рисунок 2 – параметры активации

Затем нажимаем на ссылку ‘Ввести код активации’ и активируем антивирус.

3) Его можно настроить, включить все нужные функции для защиты.

Для этого переходим во вкладку настройки **⚙.**

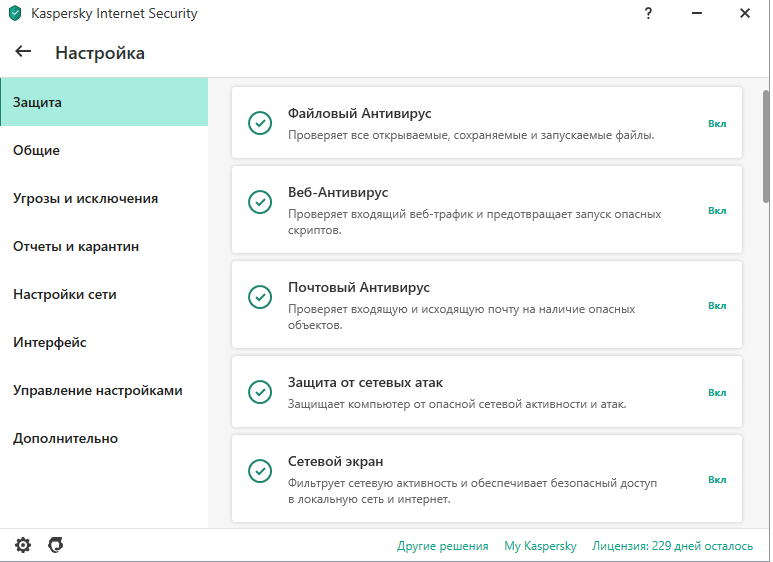


Рисунок 3 - настройки

Здесь можно включить нужные вам функции. Желательно включить все.

4) Можно включить расширение для браузера, который блокирует баннеры,

Для этого в настройка в разделе ’Контроль безопасности’ включить анти -баннер.

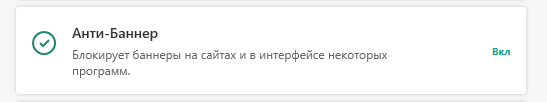


Рисунок 4 – расширение Анти-Баннер

Потом переходим в браузер, в моем случае Google Chrome и нажимаем на пункт расширения и включаем Kaspersky Protection

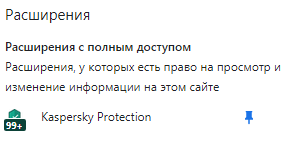


Рисунок 5 – окно с расширениями в Google Chrome

1.5 Загрузка и установка программного обеспечения

Антивирус скачиваем с официального сайта: <https://www.kaspersky.ru/home-security>

Заходим в проводник, во вкладке ‘Загрузки’ открываем установочный файл:

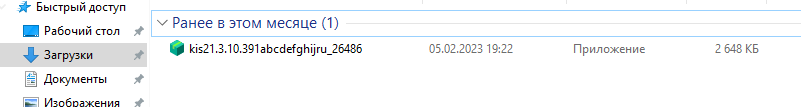


Рисунок 6 – установочный файл

Запускается мастер установки Kaspersky

Нас попросят принять лицензионное соглашение. Нажимаем ‘принять’ и начинается установка.

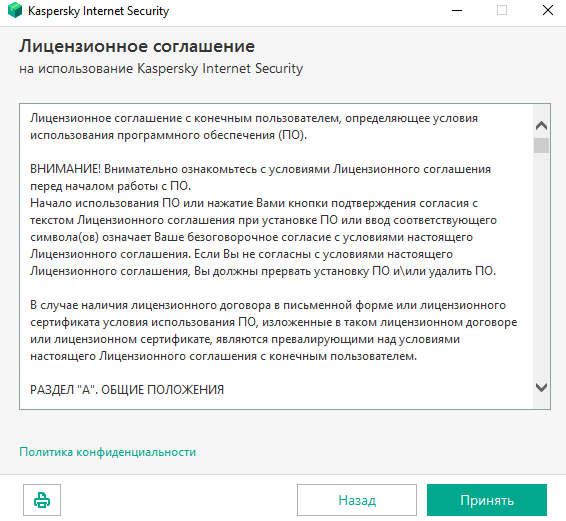


Рисунок 7 – лицензионное соглашение

После установки его можно настроить, как показано на рисунках 2-3.

2 Проблемы совместимости и методы их устранения

После установки антивируса может возникнуть проблема с его работой.

Антивирус начинает вызывать ошибки и сбои. Причиной этой проблемы может заключатся в наличии другого антивируса, который конфликтует с Касперским. Чтобы эту проблему решить, нужно удалить другой антивирус, который у вас до этого был установлен. Это можно сделать через параметры приложений или через панель управления.

Также Касперский может быть несовместим с конкретной операционной системой. Когда происходит попытка установки антивируса система может выдать ошибку о проблемах с совместимостью.

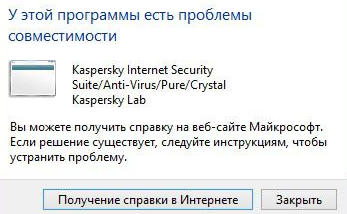
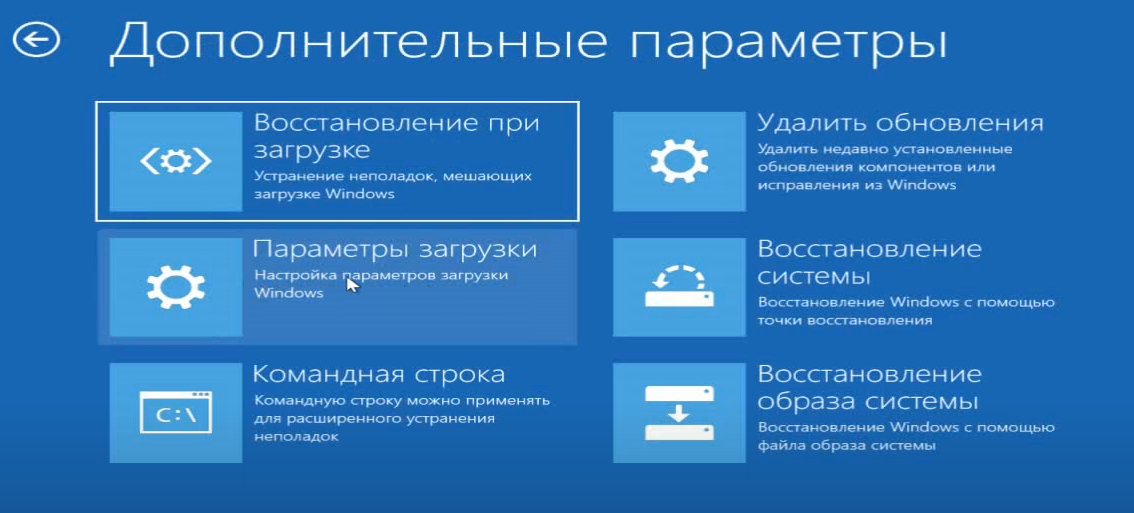


Рисунок 8 – проблем совместимости.

Решить ее можно переустановкой программы, или установкой другой версии. Также может помочь установка другой версии операционной системы.

2.1 Тестирование в безопасном режиме

Чтобы войти в безопасный режим, нужно открыть меню ‘Пуск’ и нажать кнопку ‘Перезагрузка’. Переходим в ‘Дополнительные параметры’, затем в параметры загрузки и перезагружаем компьютер. Выбираем ‘Безопасный Режим.

****

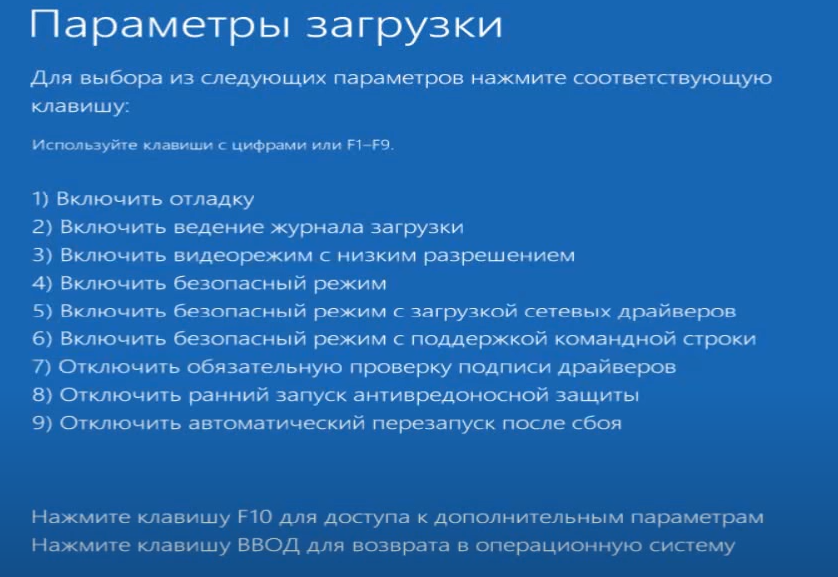


Рисунок 9 - 10 – параметры запуска

Далее запускаем антивирус и смотрим, корректно ли все работает.

Запускаем проверки, обновления, работают ли настройки, расширения.

Если все работает нормально, значит антивирус работает корректно.

2.3 Средства диагностики оборудования

Для диагностики компьютера можно использовать:

1. AIDA64
2. FurMark
3. Victoria HDD
4. Kaspersky

AIDA64 – утилита, которая представляет детальные данные о компьютере, позволяет тестировать аппаратное обеспечение для обнаружения ошибок. При помощи него можно, например нагрузить процессор и посмотреть, как он работает под нагрузкой.

FurMark - утилита, для проверки работы видеокарты под нагрузкой. Она нагружает видеокарту и показывает ее данные, такие как степень загрузки и температуры. Ее еще используют для проверки на появления артефактов.

Victoria HDD – утилита для проверки HDD дисков на наличие дефектов.

Kaspersky – антивирус для проверки системы на вирусы, вредоносное ПО и т.д.

2.4 Измерение и анализ эксплуатационных характеристик качества

программного обеспечения.

Антивирус Касперского относится к коммерческим антивирусам, то есть за его работу нужно будет купить лицензионный ключ для его активации.

Этот антивирус имеет хорошую надежность, так как он официальный, эффективность, потому что он не пропускает вирусы.

Он очень удобен в использовании, имеет приятный и удобный интерфейс.

2.5 Оптимизация и модификация ПО.

Антивирус может нагружать систему, из-за чего она может медленнее работать. В качестве оптимизации, чтобы уменьшить нагрузку, в настройках можно включить функцию ‘Откладывать выполнение задач проверки’ при высокой нагрузке на процессор и дисковые системы.

3.1 Техническое задание на сопровождение

Продление лицензии неисключительных прав на использование программного обеспечения на 57 рабочих мест на 1 год.

Программные средства антивирусной защиты устройств, рабочих и серверов должны обеспечивать реализацию следующих функциональных возможностей:

1. Антивирусная защита устройств, рабочих станций и серверов;
2. Обновления антивируса, в которых разработчики исправляют ошибки.
3. Централизованное управление, мониторинг и обновление программных средств;
4. Обновление базы данных сигнатур вредоносных программ и атак; Программные средства антивирусной защиты систем рабочих станций под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:

Microsoft Windows ХР Professional;

Microsoft Windows XP Professional x64 Edition;

Microsoft Windows 7 Professional/Enterprise/Ultimate;

Microsoft Windows 7 Professional/Enterprise/Ultimate x64. Программные средства антивирусной защиты систем серверов под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС: -Windows Server (х32&64) 2003/2008/2008R2/2012.

4.2 Тестирование интерфейса

Антивирус касперского имеет достаточно простой и удобный интерфейс для работы с антивирусом. Все вкладки имеют понятные значки и описания.

В главном окне каспеского вы можете просмотреть информацию о состоянии защиты компьютера, о работе Файлового Антивируса, Веб-Антивируса, о выполнении задач антивирусной проверки, а также рекомендации по улучшению защиты устройства.

Кроме того, в главном окне программы вы можете выполнить следующие действия:

1. открыть окно Проверка для управления задачами проверки;
2. открыть окно Обновление для управления задачами обновления;
3. открыть окно Лицензирование для управления ключами программы;
4. открыть Центр защиты;
5. перейти к просмотру новостей о Kaspersky Internet Security и о защите от компьютерных угроз в целом;
6. прочитать рекомендации по улучшению защиты вашего компьютера;
7. открыть окно Приватность, чтобы изменить настройки приватности;
8. открыть окно KasperskySafeKids;
9. войти в учетную запись My Kaspersky или выйти из нее.
10. Элементы управления главного окна программы
11. Главное окно программы включает в себя следующие элементы управления:
12. индикатор состояния защиты (в виде компьютера);
13. большие кнопки в нижней части окна;
14. маленькие кнопки по нижнему краю окна.
15. Индикатор состояния защиты информирует пользователя о текущем статусе защиты компьютера:
16. зеленый цвет означает, что ваш компьютер должным образом защищен;
17. желтый и красный цвет предупреждают о наличии различных проблем, связанных с параметрами и работой антивируса.
18. Помимо индикатора состояния защиты, в правой области главного окна программы приводится описание состояния защиты, перечислены последние проблемы и угрозы безопасности компьютера, зафиксированные в Центре защиты, а также новости и рекомендации "Лаборатории Касперского".

4.3 Тестирование контента

На главной странице имеются все необходимые функции для проверки компьютера на вредоносное ПО

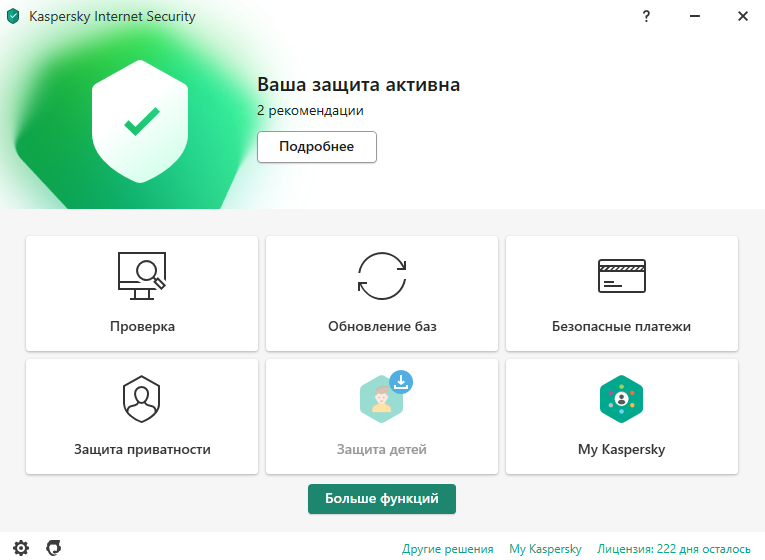


Рисунок 11 – главная страница антивируса

Вкладка ‘Проверка’ имеет несколько видов проверки, такие как:

1. Быстрая проверка
2. Полная проверка
3. Выборочная проверка

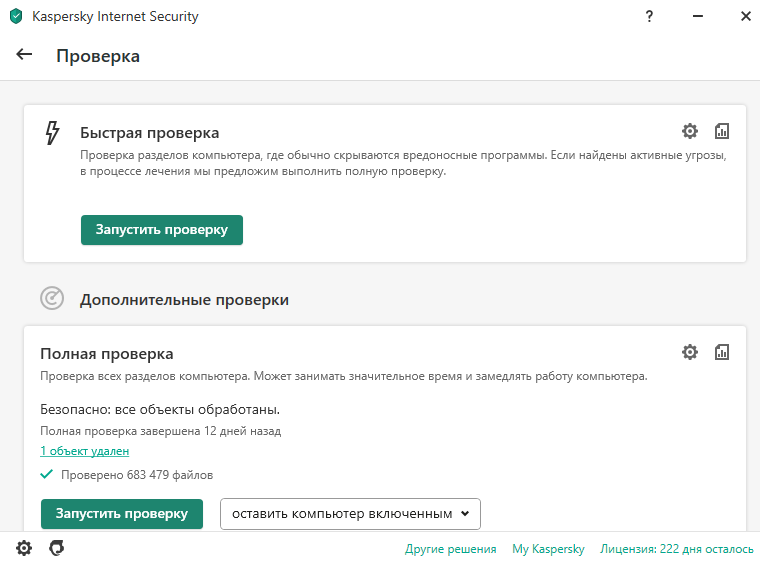


Рисунок 12 - проверки

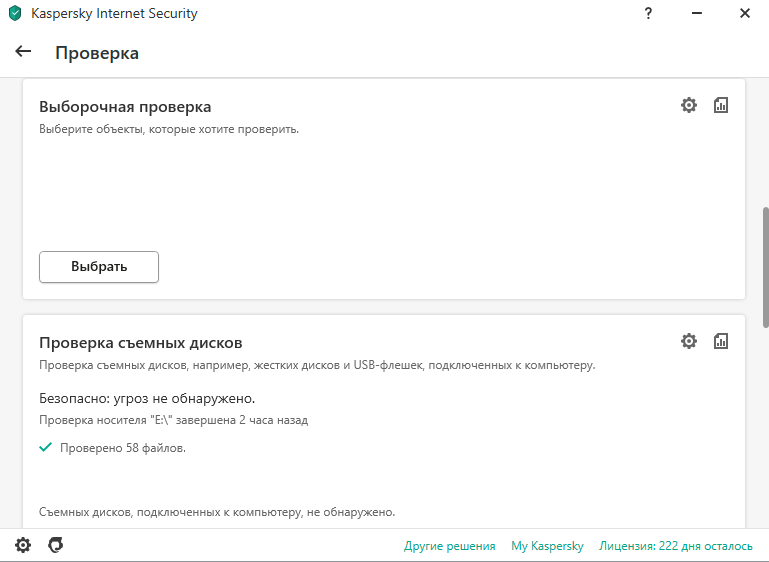


Рисунок 13 - проверки

Быстрая проверка представляет собой проверку тех областей, в которых обычно появляется вредоносное ПО.

Полная проверка представляет собой проверку всего компьютера. Она может занимать больше времени и замедлять работу компьютера.

Выборочная проверка проверяет те области, которые выбирает пользователь.

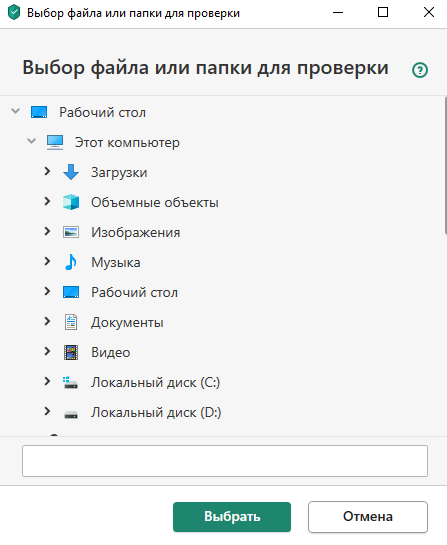
Нажав на кнопку ‘выбрать’, открывается список разделов компьютера. 

Рисунок 14 – окно, с выбором файла

Далее нужно выбрать то что нужно и нажать кнопку ‘выбрать’.

После чего начнется проверка, выбранного пользователем файла или раздела.

На главной странице (Рисунок 9) также имеется вкладка ‘Обновление баз’. По сути, это обновления антивируса. Если выполнить обновление баз, антивирус обновится до новой версии.

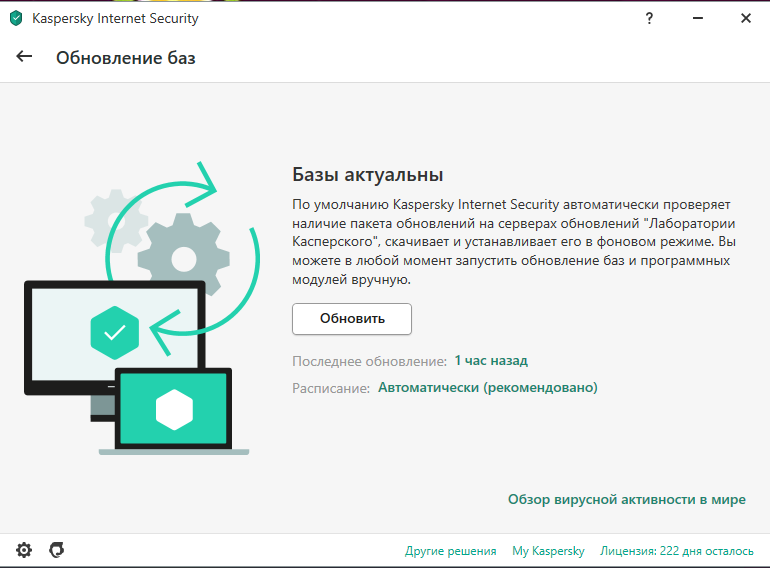


Рисунок 15 – окно с обновлениями

Их можно их можно обновлять вручную, либо сделать их обновления автоматическими, по умолчанию будет выбрано Автоматическое обновление. Если же нужно его поменять, нужно нажать на ссылку ‘Автоматически (Рекомендовано), то откроется страница настроек обновлений.

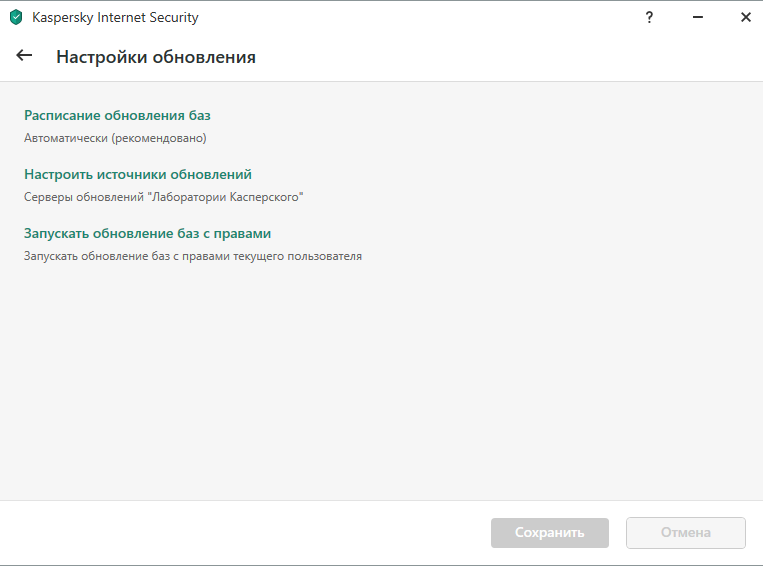


Рисунок 16 – настройки обновлений

Далее кликнуть по ссылке ‘Расписание обновления баз и выбрать тот вид обновления, который нужен.

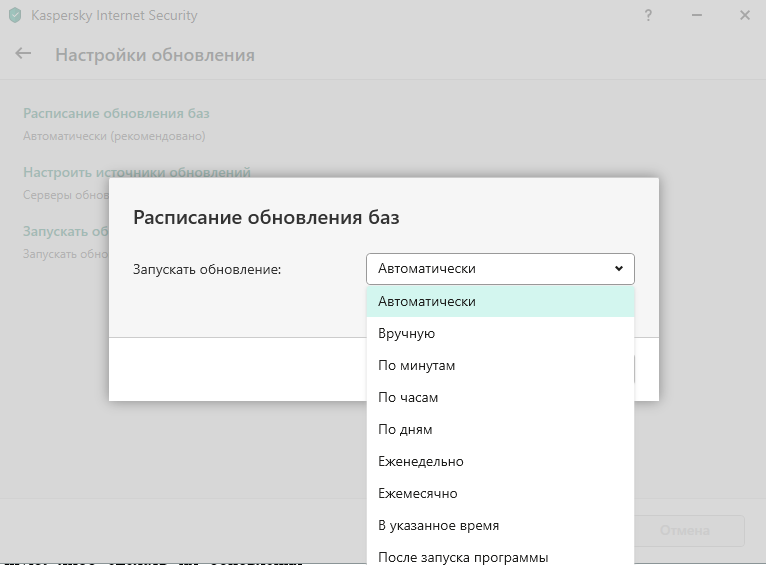


Рисунок 17 – расписание обновлений

Далее идет вкладка ‘Безопасные платежи’

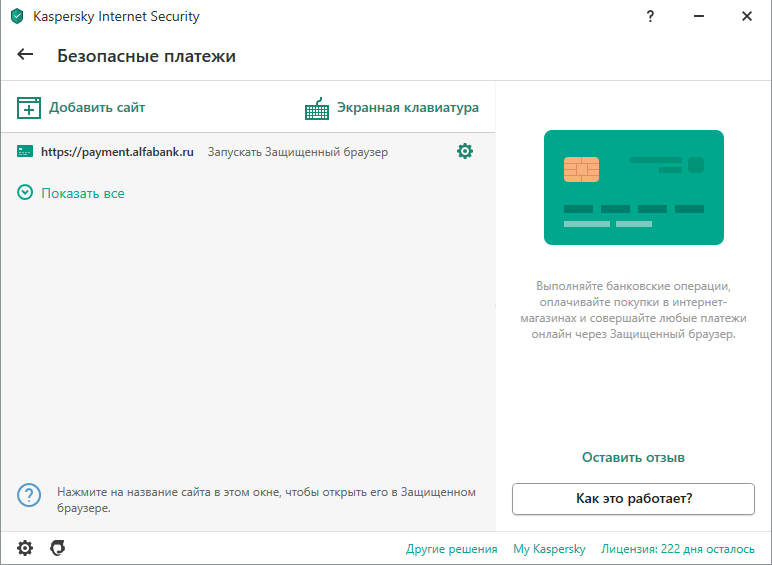


Рисунок 18 – безопасные платежи

Оплата через банковские карты будет происходить в так называемом ‘ Защищенном браузере’, его можно определить по зеленой рамке.

Здесь можно выбрать сайт, на котором происходит оплата, чтобы он переходил в защищенный браузер. Чтобы это сделать нужно, нажать на ссылку ‘Добавить сайт’ и в появившемся поле вставить ссылку сайта.

Во вкладке ‘Защита приватности’ В ней можно включить защиту веб-камеры и данных.

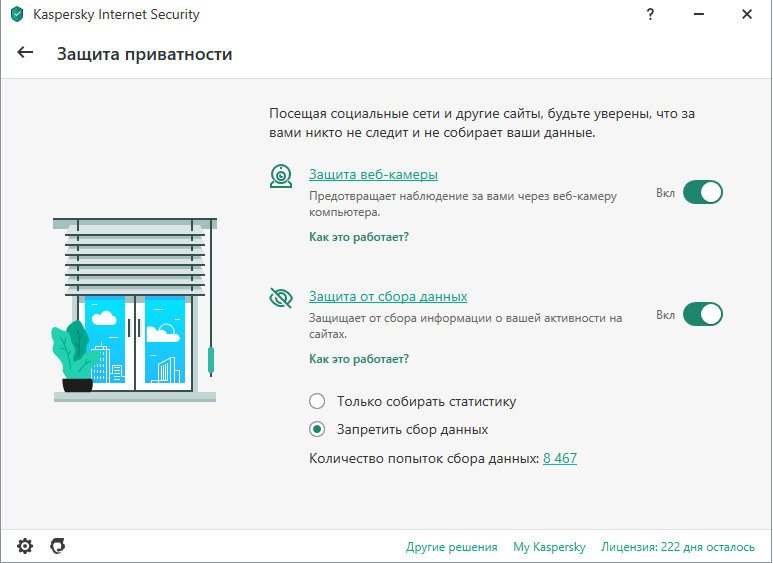


Рисунок 19 – приватность

Интерфейс можно редактировать. Для это переходим в настройки и кликаем на пункт ‘ Интерфейс ‘

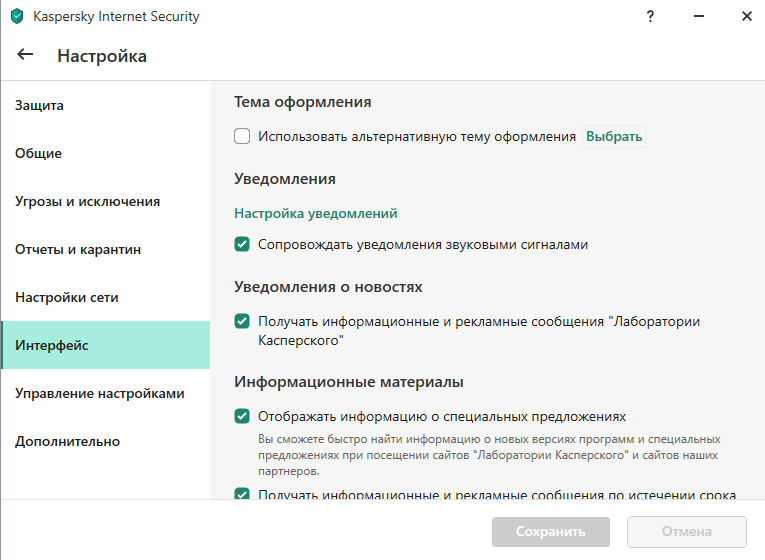


Рисунок 20 -настройки интерфейса

Здесь можно настроить оформление, уведомления и информационные материалы.

4.4 Анализ рисков. Выявление первичных и вторичных ошибок.

Во время тестирования и во время эксплуатации никаких ошибок не было выявлено

4.5 Обнаружение вируса и устранение последствий его влияния

Антивирус обычно сам сканирует на вредоносное ПО загруженные из интернета файлы и их удаляет. Но вирус можно обнаружить еще при сканировании системы. Для этого нужно запустить проверку в антивирусе и подождать пока она завершится. Если за всю проверку он найдет Вредоносное ПО, он его удалит.

5 Индивидуальное задание

5.1 Практические работы

Практическая работа 1 – Внедрение программного обеспечения.

Внедрение программного обеспечения — процесс настройки программного обеспечения под определенные условия использования, а также обучение работе с программным продуктом.

Внедрение программного продукта состоялось в том случае, если программное обеспечение работает корректно, а сотрудники компании научились работать с ним.

Результатом проекта внедрения должен быть прозрачный, четко регламентированный, документированный и автоматизированный процесс сопровождения.

Основные этапы внедрения программного продукта:

1. Техническое задание

2. Настройка

3. Тестирование

4. Эксплуатация

Эффекты от внедрения можно разделить на две большие категории: эффект, получаемый на стратегическом уровне, т.е. на уровне бизнеса, и тактический эффект, который получат все участники процесса.

1: Стратегический эффект

\* обеспечение прозрачности и измеряемости достижения стратегических целей;

\* снижение вероятности проявления рисков в сфере информационных технологий;

\* повышение рентабельности IT-услуг за счет снижения сроков проведения проекта, снижения издержек поддержки и т.д.;

\* повышение инвестиционной привлекательности IT-проектов;

\* повышение доверия бизнеса к IT за счет качественно обработанных запросов IT-отделами от бизнеса.

2: Тактический эффект

\* уменьшение сроков и снижение стоимости обработки новых запросов;

\* улучшение качества IT-услуг – это вовремя выполненные работы с заранее определенным качеством;

\* увеличение эффективности используемых ресурсов – хорошо организованный и формализованный процесс позволяет четко определить роли и ответственности каждого участника этого процесса;

\* более четкое и реалистичное планирование;

\* значительное уменьшение времени на принятие решения;

\* снижение влияния человеческого фактора.

Сопровожде́ние (поддержка) программного обеспечения — процесс обновления, улучшения и устранения ошибок программного обеспечения (ПО) после передачи на эксплуатацию.

Сопровождение ПО — это одна из фаз жизненного цикла программного обеспечения, следующая за фазой передачи ПО на эксплуатацию.

Определение процесса сопровождения:

•SWEBOK: Сопровождение ПО – вся совокупность деятельности, необходимой для обеспечения поддержки программных систем.

•IEEE 1219 (Standard for Software Maintenance): Сопровождение ПО – определяется стандартом IEEE Standard for Software Maintenance в качестве модификации программного продукта после передачи на эксплуатацию для устранения сбоев, улучшение показателей производительности и/или других характеристик (атрибутов) продукта, или адаптации продукта для использования в модифицированном окружении.

•ГОСТ Р ИСО/МЭК 12207: Сопровождение – модификация программного продукта в части его кода и документации для решения возникающих проблем при эксплуатации или реализации потребностей в улучшениях тех или иных характеристик продукта.

Сопровождение поддерживает функционирование программного продукта на протяжении всего операционного жизненного цикла, то есть периода его эксплуатации.

В процессе сопровождения фиксируются и отслеживаются запросы на модификацию (также называемые “запросами на изменения” – change requests, в частности, в контексте конфигурационного управления), оценивается влияние предлагаемых изменений, производится модификация кода и других активов (артефактов) продукта, проводится необходимое тестирование и, наконец, выпускается обновленная версия продукта. Кроме того, проводится обучение пользователей и обеспечивается их ежедневная поддержка при работе с текущей версией продукта.

Практическая работа №2 «Техническая поддержка ПО»

Образец договора технической поддержки программного обеспечения.

1.2. Техническая поддержка - оказываемые услуги по настройке,

обслуживанию, адаптации и модификации Продуктов или устранению

имеющихся в них ошибок, а также предоставлению обновлений и

дополнительных программных модулей, иные действия, предусмотренные в

разделе 2 настоящего Договора.

1.3. Ошибка – ошибка в коде продукта, в результате которого данный

Продукт не способен работать в соответствии функциональными

возможностями, указанными в предоставленной на него технической

документации, за исключением случаев:

(1) нарушения Заказчиком правил эксплуатации Продуктов в

соответствии с требованиями предоставленной на них технической

документации;

(2) использования Продуктов на оборудовании или совместно с

программным обеспечением, которые не были рекомендованы

Исполнителем.

2. Предмет договора техподдержки ПО

2.1. Исполнитель обязуется оказывать по заявкам Заказчика услуги по

Технической поддержке, а Заказчик принимать и оплачивать оказываемые

Исполнителем услуги.

2.2. Стороны согласовали возможность оказания услуг по

Технической поддержке в следующем объеме и составе:

\* установка Продуктов на оборудование Заказчика;

\* настройка Продуктов на оборудовании Заказчика, включая их

адаптацию;

\* модификация Продуктов по отдельному заказу;

\* предоставление выпускаемых обновлений Продуктов;

\* устранение ошибок в Продуктах;

\* консультирование по порядку использования Продуктов.

2.3. Услуги по Договору оказываются в соответствии с Соглашением

об уровне услуг (SLA), являющимся неотъемлемой частью настоящего

Договора.

Практическая работа №3 «Защита ПО»

Методы доказательства правильности программ могут быть

применены для анализа безопасности ПО при существенных ограничениях

на размеры и сложность создаваемых программ. Поэтому в частных случаях они могут оказаться более эффективными, чем другие известные методы анализа программ, которые исследуются в следующих разделах данной работы.

Методы, используемые для анализа и оценки безопасности ПО,

разделяют на две категории: контрольно-испытательные и логико-

аналитические. В основу данного разделения положены принципиальные различия в точке зрения на исследуемый объект (программу).

Контрольно-испытательные методы анализа рассматривают РПС

через призму фиксации факта нарушения безопасного состояния системы, а логико-аналитические - через призму доказательства наличия отношения эквивалентности между моделью исследуемой программы и моделью РПС.

Контрольно-испытательные делятся на те, в которых контролируется

процесс выполнения программы и те, в которых отслеживаются изменения в операционной среде, к которым приводит запуск программы.

При проведении анализа безопасности с помощью логико-

аналитических методов строится модель программы и формально

доказывается эквивалентность модели исследуемой программы и модели РПС. В простейшем случае в качестве модели

В целом полный процесс анализа ПО включает в себя три вида

анализа:

\* лексический верификационный анализ;

\* синтаксический верификационный анализ;

\* семантический анализ программ

Каждый из видов анализа представляет собой законченное

исследование программ согласно своей специализации.

Результаты исследования могут иметь как самостоятельное значение,

так и коррелироваться с результатами полного процесса анализа.

Лексический верификационный анализ предполагает поиск

распознавания и классификацию различных лексем объекта исследования

(программа), представленного в исполняемых кодах. При этом лексемами

являются сигнатуры. В данном случае осуществляется поиск сигнатур

следующих классов:

\* сигнатуры вирусов;

\* сигнатуры элементов РПС;

\* сигнатуры (лексемы) "подозрительных функций";

\* сигнатуры штатных процедур использования системных ресурсов и

внешних устройств.

Поиск лексем (сигнатур) реализуется с помощью специальных

программ-сканеров.

Синтаксический верификационный анализ предполагает поиск,

распознавание и классификацию синтаксических структур РПС, а также построение структурно-алгоритмической модели самой программы.

Решение задач поиска и распознавания синтаксических структур РПС

имеет самостоятельное значение для верификационного анализа программ, поскольку позволяет осуществлять поиск элементов РПС, не имеющих сигнатуры. Структурно-алгоритмическая модель программы необходима для реализации следующего вида анализа - семантического.

Семантический анализ предполагает исследование программы

изучения смысла составляющих ее функций (процедур) в аспекте

операционной среды компьютерной системы. В отличие от предыдущих

видов анализа, основанных на статическом исследовании, семантический

анализ нацелен на изучение динамики программы - ее взаимодействия с окружающей средой. Процесс исследования осуществляется в виртуальной

операционной среде с полным контролем действий программы и

отслеживанием алгоритма ее работы по структурно-алгоритмической

модели.

Семантический анализ является наиболее эффективным видом

анализа, но и самым трудоемким. По этой причине методика сочетает в себе

три перечисленных выше анализа. Выработанные критерии позволяют

разумно сочетать различные виды анализа, существенно сокращая время

исследования, не снижая его качества.

Практическая работа 4.

|  |  |
| --- | --- |
| Комплектующие | Модель |
| Процессор | Intel core I 5 12400F |
| Оперативная память | 32гб DDR4 |
| Видеокарта | Nvidia Geforce GTX 1660 SUPER |
| Материнская Плата | GIGABYTE B660M GAMING DDR4 |
| SSD | 250гб |
| HDD | 1тб |
| Блок питания | 600w |

5.2 Разработка технико-экономического обоснования. Формирование бизнес-цели проекта. Разработка устава проекта обеспечения

Общая структура бизнес-проекта: резюме, краткое содержание, описание бизнеса, анализ рынка, план маркетинга, план производства, организационный план, финансовый план, анализ и оценка рисков.

Бизнес-план начинается с краткого изложения сути проекта, то есть с резюме или выводов. Они обычно пишутся в самую последнюю очередь, но именно они являются первым пунктом бизнес-плана. Выводы рекомендуется делать краткими. Резюме — это самостоятельный рекламный документ, т.к. в нем содержатся основные положения всего бизнес-проекта.

Описание фирмы:

1. История фирмы:

1. дата и место создания фирмы, ее юридический статус к настоящему времени;
2. имена основателей фирмы, директоров,
3. основные изменения, произошедшие в структуре фирмы, ее руководстве, юридическом статусе с момента основания.
4. основные достижения фирмы в той области деятельности, которая подлежит анализу в бизнес-проекте.

2. Сведения о предприятии и предпринимателе;

Основные технико-экономические и финансовые показатели, характер производимой продукции, рынок сбыта, партнеры, клиенты, ближайшие цели и перспективы развития, наличие лицензий.

3. Социальная направленность и масштабность проекта:

1. указывается направленность на решение местных проблем;
2. возможные перспективы развития, выход на зарубежный рынок и т.п. Также в этом разделе проводится анализ сферы деятельности фирмы.

Цели и задач

План должен раскрывать заявленные цели и задачи предприятия.

1. Этот анализ также называют ситуационным анализом. Сильные и слабые стороны идеи — это те характеристики идеи, которые могут быть проконтролированы предпринимателем, на которые он может оказать воздействие. Они обычно относятся к настоящему времени.
2. Здесь рассматриваются следующие факторы:
3. **организационные** (организационно-правовая форма, наличие помещений собственных или арендованных):
4. **маркетинговые**(место расположения, маркетинговый комплекс, рынок, его сегмент; конкуренты; чем продукт (услуга) будет отличаться от конкурентной),
5. **технические** (производственные фонды: состояние и ресурсы),
6. **финансовые** (наличие собственных средств);
7. **кадровые**(навыки и профессиональные недостатки, насколько идея отвечает идеям, знаниям и умениям предпринимателя).

5.3 Практическая работа 13 ‘Виды вирусных программ и их структура’

Цель: рассмотреть виды вирусных программ и их структуру.

Виды вирусов

Существует довольно разных вирусных программ, вот их виды:

1. Черви — это программа с вредоносным кодом, которая атакует компьютеры в сети и распространяется через нее. Активный сетевой червь может снижать продуктивность устройства жертвы, удалять файлы или даже отключать определенные программы.



Рисунок 21- вирус червь.

1. Вирусы-маскировщики - утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.
2. Вирусы – шпионы - эти вирусы могут проникнуть в вашу операционную систему для отслеживания вводимой с клавиатуры информации, изменения настроек и снижения производительности вашего устройства, для сбора таких конфиденциальных данных, как данные для входа, электронная почта, история просмотров, а также данные кредитной карты.
3. Рекламные вирусы — это программы, которые предназначены для показа рекламы на вашем компьютере, перенаправления запросов поиска на рекламные веб-сайты и сбора маркетинговой информации о вас (например, какого рода сайты вы посещаете), чтобы реклама соответствовала вашим интересам.
4. Вирусы – блокировщики – вирус, который не дает войти в сеть, блокирует запуск компьютера, даже в безопасном режиме.
5. Троянские вирусы — это тип вредоносных программ, маскирующихся под легитимное ПО. Он часто используется киберпреступниками для кражи личных данных, слежения за пользователями и получения несанкционированного доступа к системам.



Рисунок 22 – троянский вирус

1. Майнер – это вирус, который нагружает железо и добывает из него криптовалюту.

Структура компьютерного вируса

Структурно компьютерный вирус можно представить состоящим из двух частей: головы и хвоста. Головой называется часть вируса, которая первой получает управление. Хвост вируса — это части вируса, расположенные отдельно от головы. В простейшем случае вирус может состоять из одной головы, и действительно файловые вирусы обычно так и устроены. Такие вирусы называются несегментированными. В отличие от них сегментированные вирусы имеют располагающийся отдельно хвост и в какой-то мере аналогичны оверлейным файлам.

Заключение

Сейчас антивирус является одним из самых важных ПО на компьютере или любом другом устройстве, так как в интернете очень много вирусов и вредоносных ПО, которые могут нанести вред устройству.

Антивирус касперского является довольно эффективным антивирусным ПО для защиты компьютера. Он не дает переходить по опасным ссылкам, загружать вредоносное ПО.

Одними из главных преимуществ касперского являются удобный интерфейс и хорошая защита.

Список использованных источников:

1. Поддержка <https://support.kaspersky.com/>
2. Официальный сайт <https://www.kaspersky.ru/>
3. Энциклопедия <https://ru.wikipedia.org/>
4. Форум <https://forum.kasperskyclub.ru/>
5. ВКонтакте <https://vk.com/kaspersky>
6. YouTube <https://www.youtube.com/channel/UCGhEv7BFBWdo0k4UXTm2eZg>
7. Отзывы <https://otzovik.com/reviews/antivirus_kaspersky/>
8. Оформления для антивируса <https://www.kaspersky.ru/blog/skin-customization/>
9. История <https://ru.wikipedia.org/wiki/%D0%9B%D0%B0%D0%B1%D0%BE%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B8%D1%8F_%D0%9A%D0%B0%D1%81%D0%BF%D0%B5%D1%80%D1%81%D0%BA%D0%BE%D0%B3%D0%BE>
10. Другие продукты <https://www.kaspersky.ru/home-security>