УТВЕРЖДАЮ
Начальник разработки ПО

Симонова А.К
« » 20 г.

АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «DEFENDER CODE»

Руководство программиста

Лист утверждения

Руководитель разработки

_____ **Рижская Д.А.**

“_____”_____20__

Ответственный исполнитель

_____ **Мирошникова М.А.**

“_____”_____20__

2020

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

УТВЕРЖДЕНО

АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «DEFENDER CODE»

Руководство программиста

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Листов 8

2020

АННОТАЦИЯ

В данном программном документе приведено описание применения антивирусной программы «DefenderCode», предназначенной для обнаружения вирусов и вредоносных программ, а также для предотвращения заражения файлов или операционной системы вредоносным кодом.

В данном программном документе, в разделе «Назначение и условия применения программы» указаны назначение и функции, выполняемые программой, условия, необходимые для выполнения программы (объем оперативной памяти, требования к составу и параметрам периферийных устройств, требования к программному обеспечению и т.п.).

В разделе «Характеристика программы» приведено описание основных характеристик и особенностей программы (режим работы, средства контроля правильности выполнения и самовосстанавливаемости программы и т.п.).

В разделе «Обращение к программе» должно быть приведено описание процедур вызова программы (способы передачи управления и параметров данных и др.).

В данном программном документе, в разделе «Входные и выходные данные» приведено описание организации используемой входной и выходной информации.

В разделе «Сообщения» указаны тексты сообщений, выдаваемых программисту или оператору в ходе выполнения программы, описание их содержания и действий, которые необходимо предпринять по этим сообщениям.

Оформление программного документа «Руководство программиста» произведено по требованиям ЕСПД (ГОСТ 19.101-77 [1)], ГОСТ 19.103-77 [2)], ГОСТ 19.104-78* [3)], ГОСТ 19.105-78* [4)], ГОСТ 19.106-78* [5)], ГОСТ 19.504-79* [6)], ГОСТ 19.604-78* [7)]).

[1)] ГОСТ 19.101-77 ЕСПД. Виды программ и программных документов

[2)]ГОСТ 19.103-77 ЕСПД. Обозначение программ и программных документов

[3)] ГОСТ 19.104-78* ЕСПД. Основные надписи

[4)] ГОСТ 19.105-78* ЕСПД. Общие требования к программным документам

[5)] ГОСТ 19.106-78* ЕСПД. Общие требования к программным документам, выполненным печатным способом

[6)] ГОСТ 19.504-79* ЕСПД. Руководство программиста. Требования к содержанию и оформлению

[7)] ГОСТ 19.604-78* ЕСПД. Правила внесения изменений в программные документы, выполненные печатным способом

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ ПРОГРАММЫ

1.1. Назначение программы

Программа предназначена для проверки различных файлов компьютерного устройства от троянов, вирусов, шпионов и других вредоносных угроз.

1.2. Функции, выполняемые программой

В программном изделии реализованы следующие функции безопасности:

1. управление параметрами САВЗ: возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ;
2. управление установкой обновлений (актуализации) БД ПКВ САВЗ: получение и установку обновлений БД ПКВ: в автоматизированном режиме с сетевого ресурса; без применения средств автоматизации;
3. выполнение проверок объектов воздействия:

а) выполнение проверок с целью обнаружения зараженных КВ объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации;

б) выполнение проверок с целью обнаружения зараженных КВ объектов в режиме реального времени в файлах, полученных по каналам передачи данных;

в) выполнение проверок с целью обнаружения зараженных КВ объектов по команде; в режиме динамического обнаружения в процессе выполнения операций доступа к объектам; путем запуска с необходимыми параметрами функционирования своего кода внешней программой;

г) выполнение проверок с целью обнаружения зараженных КВ объектов сигнатурными и эвристическими методами.

4. ограничение программной среды:

а) возможность контроля доступа к веб-ресурсам;

б) возможность контроля за запуском ПО на защищаемом сервере.

1.3. Условия, необходимые для выполнения программы

1. Климатические условия эксплуатации программы

Климатические условия эксплуатации, при которых должны обеспечиваться заданные характеристики, должны удовлетворять требованиям, предъявляемым к техническим средствам в части условий их эксплуатации.

2. Минимальный состав технических средств:

В состав технических средств должен входить персональный компьютер (ПЭВМ), включающий в себя следующие общие требования:

а) 2 ГБ свободного места на жестком диске;

б) подключение к интернету для использования программного изделия, обновления БД;

в) минимальная скорость Интернета;

3. Минимальный состав программных средств

Системные программные средства, используемые программой, должны быть представлены лицензионной локализованной версией операционной системы. Допускается использование пакета обновления такого-то.

1.3.1. Объем оперативной памяти

- для 32-разрядной операционной системы – 1 ГБ;
- для 64-разрядной операционной системы – 2 ГБ.

1.3.2. Требования к составу периферийных устройств

Особые требования к составу периферийных устройств не предъявляются.

1.3.3. Требования к параметрам периферийных устройств

Особые требования к параметрам периферийных устройств не предъявляются.

1.3.4. Требования к программному обеспечению

Программа должна обеспечивать возможность выполнения перечисленных ниже функций:

а) стабильность и надежность работы;

б) размеры вирусной базы программы (количество вирусов, которые правильно определяются программой);

в) скорость работы программы, наличие дополнительных возможностей;

г) многоплатформенность.

1.3.5. Требования к персоналу (программисту)

Минимальное количество персонала, требуемого для работы программы, должно составлять не менее 2 штатных единиц — системный администратор и конечный пользователь программы — оператор.

В перечень задач, выполняемых системным администратором, должны входить:

а) задача поддержания работоспособности технических средств;

б) задачи установки (инсталляции) и поддержания работоспособности программного средства;

в) задача установки (инсталляции) программы.

2. 2. ХАРАКТЕРИСТИКА ПРОГРАММЫ

2.1. Описание основных характеристик программы

Антивирусное программное обеспечение «Defender Code» состоит из одной запускаемой формы и не имеет других составных частей.

2.1.1. Режим работы программы

Работа антивирусного программного обеспечения «DefenderCode» может осуществляться в одном режиме:

Стандартный режим – оконный режим работы в операционной системе (ОС).

2.1.2. Средства контроля правильности выполнения программы

Контроль правильности выполнения антивирусного программного обеспечения «DefenderCode» осуществляется встроенными средствами самого программного обеспечения, реализованных в виде: протоколирования событий, осуществление диагностики работы какого-либо устройства.

2.2. Описание основных особенностей программы

Антивирусное программное обеспечение «Defender Code» использует следующие методы:

1. Реакция веб-сервера на HTTP-запросы:
   - GET - выдаёт титульную страницу,
   - POST - ищет в принимаемых данных файл(ы) для проверки и текст - адрес электронной почты
2. Библиотеки Happstack-lite.
3. Подгружены наборы стилей Bootstrap.
4. Сигнатурный анализатор - используется версия 4.0.2, собранная с модулями crypto и androguard
5. Vue.js, позволяющий прикрепить файлы методом drag-n-drop.
6. Для отправки сообщений взяты сервис smtp.gmail.com, как один из самых простых для настройки, и библиотека smtp-mail для Haskell

2.2.1. Самовосстанавливаемость программы

Самовосстанавливаемость антивирусного программного обеспечения «DefenderCode» обеспечивается стандартными средствами операционной системы.

3. ОБРАЩЕНИЕ К ПРОГРАММЕ

3.1. Загрузка и запуск программы

Загрузка и запуск программы осуществляется способами, детальные сведения о которых изложены в руководстве пользователя операционной системы.

В случае успешного запуска программы на рабочем столе будет отображено Главное окно программы.

3.2. Выполнение программы

Получив файл, сервер вызывает сигнатурный анализатор Yara, отправив ему набор правил и сам файл. Вердикт анализатора собирается в формат HTML и отправляется на сторону клиента, а если предоставлен адрес электронной почты, то ещё и на почту.

3.3. Завершение работы программы

Завершение работы программы обеспечиваются стандартными средствами операционной системы.

или

Выполнение указанной функции возможно любым из перечисленных ниже способов:

1. последовательным выбором пунктов меню Файл-Выход (см. рисунок);
2. нажатием кнопки  .

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1. Организация используемой входной информации

Серверная часть «DefenderCode» в ходе своей работы получает на вход файл, который необходимо проверить. Загрузить файл можно двумя способами: либо выбрать его в дополнительном окне, либо перетащить в окно загрузки. Выбор этих двух способов обусловлен простотой и удобством использования, как для использования ПК, так и на телефонном устройстве.

4.2. Организация используемой выходной информации

Клиентская часть «DefenderCode» в ходе своей работы выводит строку, содержащую вердикт проверки: «Everything is okey!», в случае успешной проверки, и «Danger found: ...», подсвечивая строку соответствующим цветом, для лучшего восприятия пользователем, либо отправляет отчет на почту, что тоже очень удобно.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
Изм	измененных	замененных	новых	анулированных					