

УТВЕРЖДАЮ

Начальник разработки ПО



  
Симонова А.К.  
«    »    20    г.

## АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «DEFENDER CODE»

### Пояснительная записка

ЛИСТ УТВЕРЖДЕНИЯ  
А.В.00001-01 81 01-ЛУ

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

Руководитель разработки

\_\_\_\_\_ Рижская Д.А.  
“    ”    20   

Ответственный исполнитель

\_\_\_\_\_ Мирошникова М.А.  
“    ”    20   

2020



**УТВЕРЖДЕНО**

**А.В.00001-01 81 01-ЛУ**

**АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ  
«DEFENDER CODE»**

**Пояснительная записка**

**А.В.00001-01 81 01**

**Листов 7**

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

## АННОТАЦИЯ

В данном программном документе приведена пояснительная записка к программному продукту «Defender Code», предназначенному предназначенной для сканирования файлов, папок или дисков на предмет наличия вирусов и угроз безопасности. В данном программном документе, в разделе «Введение» указано наименование программы и условное обозначение темы разработки.

В разделе «Назначение и область применения» указано назначение программы и краткая характеристика области применения программы.

В данном программном документе, в разделе «Технические характеристики» содержатся следующие подразделы:

- постановка задачи на разработку программы, с описанием применяемых математических методов и описанием допущений и ограничений, связанных с выбранным математическим материалом;
- описание алгоритма и функционирования программы с обоснованием выбора схемы алгоритма решения задачи и возможные взаимодействия программы с другими программами;
- описание и обоснование выбора метода организации входных и выходных данных; Но
- описание и обоснование выбора состава технических и программных средств на основании проведенных расчетов и анализов.

В данном программном документе, в разделе «Источники, использованные при разработке» указан перечень научно-технических публикаций, нормативно-технических документов и других научно-технических материалов, на которые есть ссылки в основном тексте.

Оформление программного документа «Руководство оператора» произведено по требованиям ЕСПД (ГОСТ 19.101-77 <sup>1)</sup>, ГОСТ 19.103-77 <sup>2)</sup>, ГОСТ 19.104-78\* <sup>3)</sup>, ГОСТ 19.105-78\* <sup>4)</sup>, ГОСТ 19.106-78\* <sup>5)</sup>, ГОСТ 19.404-79 <sup>6)</sup>, ГОСТ 19.604-78\* <sup>7)</sup>).

---

<sup>1)</sup> ГОСТ 19.101-77 ЕСПД. Виды программ и программных документов

<sup>2)</sup> ГОСТ 19.103-77 ЕСПД. Обозначение программ и программных документов

<sup>3)</sup> ГОСТ 19.104-78\* ЕСПД. Основные надписи

<sup>4)</sup> ГОСТ 19.105-78\* ЕСПД. Общие требования к программным документам

<sup>5)</sup> ГОСТ 19.106-78\* ЕСПД. Общие требования к программным документам, выполненным печатным способом

<sup>6)</sup> ГОСТ 19.404-79 ЕСПД. Пояснительная записка. Требования к содержанию и оформлению

<sup>7)</sup> ГОСТ 19.604-78\* ЕСПД. Правила внесения изменений в программные документы, выполненные печатным способом

## СОДЕРЖАНИЕ

<b>АННОТАЦИЯ .....</b>	<b>2</b>
<b>СОДЕРЖАНИЕ .....</b>	<b>3</b>
<b>1. ВВЕДЕНИЕ .....</b>	<b>4</b>
1.1. Наименование программы.....	4
1.2. Условное обозначение темы разработки.....	4
<b>2. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ .....</b>	<b>4</b>
2.1. Назначение программы .....	4
2.2. Область применения программы .....	4
<b>3. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ .....</b>	<b>4</b>
3.1. Постановка задачи на разработку программы.....	4
3.2. Описание алгоритма и функционирования программы.....	4
3.2.1. Описание алгоритма программы.....	4
3.2.2. Описание функционирования программы .....	5
3.2.3. Возможные взаимодействия программы с другими программами....	5
3.3. Описание и обоснование выбора метода организации входных и выходных данных. ....	5
3.4. Описание и обоснование выбора состава программных средств .....	5
<b>4. ОЖИДАЕМЫЕ ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ     .....</b>	<b>5</b>
<b>5. ИСТОЧНИКИ, ИСПОЛЬЗОВАННЫЕ ПРИ РАЗРАБОТКЕ .....</b>	<b>6</b>
<b>ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ .....</b>	<b>7</b>

## **1. ВВЕДЕНИЕ**

### **1.1. Наименование программы**

Программный продукт «Defender Code»

### **1.2. Условное обозначение темы разработки**

Создать антивирусное программное обеспечение.

## **2. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ**

### **2.1. Назначение программы**

Программное обеспечение «Defender Code» предназначено для сканирования файлов, папок или дисков на предмет наличия вирусов и угроз безопасности.

### **2.2. Область применения программы**

Программа «DefenderCode» предназначена для быстрой проверки любого вида файлов на наличие в них вредоносного кода. Вызов программы производится пользователем в произвольный момент времени, если ему необходимо что-то проверить.

## **3. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ**

### **3.1. Постановка задачи на разработку программы**

Разрабатываемая антивирусная программа должна решать такие задачи как:

1. Быстрая проверка любого вида файлов на наличие в них вредоносного кода
2. Наличие пользовательского интерфейса
3. Быстрый вывод результата
4. Простота использования

### **3.2. Описание алгоритма и функционирования программы**

#### **3.2.1. Описание алгоритма 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.

Браузер отображает титульную страницу, полученную с сервера. Пользователь может выбрать его или перетащить вручную на страницу, затем отправить на проверку, приложив по желанию адрес электронной почты. В зависимости от

состояния страницы - “файл не приложен”, “файл приложен или отправлен”, “файл обработан и чист” и “файл обработан, найдена угроза”, лист на странице принимает зелёный, жёлтый, зелёный и красный соответственно. Результат сканирования отображается в виде alert-полоски в верхней части экрана: зелёная - файл чист (“Everything is OK!”), красная - обнаружена угроза безопасности (“Danger found: <вид угрозы> <имя файла>”). Если указан е-мэйл, то на него отправляется сообщение с таким же текстом.

### 3.2.2. Описание функционирования программы

Программа DefenderCode в ходе своей работы запускает детектор сигнатур yara и использует средства mailutils для отправки сообщений на электронную почту. Для сборки и запуска самой программы DefenderCode необходима система сборки Haskell-stack.

### 3.2.3. Возможные взаимодействия программы с другими программами

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

### 3.3. Описание и обоснование выбора метода организации входных и выходных данных.

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.

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.

### 3.4. Описание и обоснование выбора состава программных средств

Программное обеспечение должно быть легко модифицируемым в случае изменения требований.

## 4. ОЖИДАЕМЫЕ ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ

Технико-экономические показатели программного обеспечения соответствуют ожидаемым и обеспечивают выполнение следующих требований:

1. Система имеет дружелюбный пользователю интерфейс;
2. Предоставляемая информация адекватна правам пользователя;
4. В системе предусмотрены различные виды ввода и получения информации;

5. Сбои в работе ПО, а также аппаратных средств не замедляют работу системы.

## **5. ИСТОЧНИКИ, ИСПОЛЬЗОВАННЫЕ ПРИ РАЗРАБОТКЕ**

Анализатор сигнатур - <https://yararules.com/>

[illegible]