Главное управление по образованию

Минского областного исполнительного комитета

Учреждение образования

«Новопольский государственный аграрно-экономический колледж»

Специальность 2-40 01 01 «Программное обеспечение информационных технологий»

Специальность 2-40 01 01 35 «Программное обеспечение обработки экономической и деловой информации»

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**К ДИПЛОМНОМУ ПРОЕКТУ НА ТЕМУ**

**Программное средство защиты от файловых вирусов**

Разработал \_\_\_\_\_\_\_\_\_\_\_ Н.И. Володько

Руководитель проекта \_\_\_\_\_\_\_\_\_\_\_ В.Л. Захарич

Председатель цикловой комиссии \_\_\_\_\_\_\_\_\_\_\_ Т.Ю. Платонова

Консультанты \_\_\_\_\_\_\_\_\_\_\_ Т.Е. Волотовская

\_\_\_\_\_\_\_\_\_\_\_ Т.Л. Лобзанюк

Нормоконтроль \_\_\_\_\_\_\_\_\_\_\_ И.В. Усенко

Дипломный проект защищен с отметкой \_\_\_\_\_\_\_\_\_\_\_

Председатель ГКК

Новое Поле, 2020

Главное управление по образованию

Минского областного исполнительного комитета

Учреждение образования

«Новопольский государственный аграрно-экономический колледж»

Специальность *2-40 01 01 «Программное обеспечение информационных технологий»*

группа *2218*

УТВЕРЖДАЮ

Заместитель директора

по учебной работе

Т.Н. Крумкач

*«21» декабря 2020 г.*

**ЗАДАНИЕ**

**на дипломный проект**

учащегося *Володько Никиты Ивановича*

(фамилия, имя, отчество)

1. Тема проекта *Программное средство защиты от файловых вирусов*

Закреплена приказом по учреждению образования *21.02.2020 №123*

2. Срок сдачи учащимся законченного проекта *27.02.2021*

3. Исходные данные по проекту информация о вирусах

4. СОСТАВ ПРОЕКТА

а) Пояснительная записка

Введение

Основная часть

1 Назначение и область применения

1.1 Характеристика предметной области

1.2 Назначение программного средства

1.3 Описание аналогов

2 Технические характеристики

2.1 Постановка задачи на разработку программного средства

2.2 Описание программного средства

2.2.1 Общие сведения

2.2.2 Функциональное назначение

2.2.3 Описание логической структуры

2.2.4 Используемые технические средства

2.2.5 Вызов и загрузка

2.2.6 Входные данные

2.2.7 Выходные данные

2.2.8 Рекомендации по использованию

3 Ожидаемые технико-экономические характеристики

3.1 Экономический раздел

3.2 Охрана труда

Заключение

Список используемых источников

б) Графическая часть проекта

Лист 1 Диаграмма последовательности действий

Лист 2 Диаграмма вариантов использования

Лист 3 Диаграмма деятельности

5. Консультанты (с указанием разделов, относящихся к ним)

|  |  |
| --- | --- |
| Раздел | Консультант |
| Теоретическая часть | Захарич В.Л. |
| Моделирование и программирование | Захарич В.Л. |
| Экономический раздел | Лобзанюк Т.Л. |
| Охрана труда | Волотовская Т.Е. |

6. Календарный график работы на весь период проектирования

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование этапов дипломного проекта | Срок выполнения этапов проекта | Примечание |
| 1 | Выбор среды программирования | 18-24.12.2020 |  |
| 2 | Постановка задачи | 18-21.12.2020 |  |
| 3 | Введение | 21-24.12.2020 |  |
| 4 | Проектирование | 04-12.01.2021 |  |
| 5 | Охрана труда | 04.01-06.02.2021 |  |
| 6 | Экономический раздел | 29.01-06.02.2021 |  |
| 7 | Разработка проекта | 04.01-10.02.2021 |  |
| 8 | Описание проекта | 08-15.02.2021 |  |
| 9 | Тестирование | 15-19.02.2021 |  |
| 10 | Заключение. Графическая часть | 18-22.02.2021 |  |
| 11 | Оформление пояснительной записки | 22-27.02.2021 |  |

7. Дата выдачи задания: 28 декабря 2020 г.

Руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.Л. Захарич

(подпись)

Консультанты: Т.Е. Волотовская

(подпись)

Т.Л. Лобзанюк

(подпись)

Задание принял к исполнению Н.И. Володько

(подпись)

Председатель цикловой комиссии Т.Ю. Платонова

(подпись)



**СОДЕРЖАНИЕ**

Изм.

Лист

№ докум.

Подпись

Дата

Лист

3

ДП2218.02.102.081ПЗ

Разраб.

Володько Н.

Провер.

Захарич В.

Реценз.

Н. Контр.

Усенко И.

Утверд.

Программное средство защиты от файловых вирусов

Лит.

Листов

50

НГАЭК, 2020

[ВВЕДЕНИЕ 7](#_Toc64596719)

[ОСНОВНАЯ ЧАСТЬ 9](#_Toc64596720)

[1. Назначение и область применения 9](#_Toc64596721)

[1.1 Описание предметной области 9](#_Toc64596722)

[1.2 Назначение программного средства 21](#_Toc64596723)

[1.3 Анализ существующих разработок 22](#_Toc64596724)

[2 Технические характеристики 25](#_Toc64596725)

[2.1 Постановка задачи на разработку 25](#_Toc64596726)

[2.2 Описание программного средства 26](#_Toc64596727)

[2.2.1 Общие сведения 26](#_Toc64596728)

[2.2.2 Функциональное назначение 27](#_Toc64596729)

[2.2.3 Описание логической структуры 28](#_Toc64596730)

[2.2.4 Используемые технические средства 42](#_Toc64596731)

[2.2.5 Вызов и загрузка 43](#_Toc64596732)

[2.2.6 Входные данные 44](#_Toc64596733)

[2.2.7 Выходные данные 48](#_Toc64596734)

[2.2.8 Рекомендации по использованию 49](#_Toc64596735)

[3 Экономический раздел 56](#_Toc64596736)

[4 Охрана труда 62](#_Toc64596737)

[4.1 Характеристика трудовой деятельности и факторов среды при работе оператора 62](#_Toc64596738)

[4.2 Организация общественного контроля условий и безопасности труда 63](#_Toc64596739)

[4.3 Общественный контроль за состоянием охраны труда на объекте при проектируемой деятельности 67](#_Toc64596740)

[4.4 Ответственность за необеспечение трудоохранных требований 71](#_Toc64596741)

[ЗАКЛЮЧЕНИЕ 77](#_Toc64596742)

[СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 78](#_Toc64596743)

ПРИЛОЖЕНИЯ



# **ВВЕДЕНИЕ**

Все возрастающие усилия по созданию технологий защиты данных их уязвимость в современных условиях не только не уменьшается, но и постоянно возрастает. Актуальность проблем, связанных с защитой информации все более усиливается. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Например, конфиденциальность данных, которая обеспечивается применением различных методов и средств. Интенсивное развитие современных информационных технологий, и в особенности сетевых технологий, создает для этого все предпосылки.

Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Все чаще в средствах массовой информации появляются сообщения о различного рода проделках компьютерных злоумышленников, о появлении все более совершенных, саморазмножающихся программ. Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет.

Объект исследования – программное средство.

Предмет исследования – программное средство защиты от файловых вирусов.

Цель дипломного проекта – разработать программное средство защиты операционной системы от файловых вирусов.

Задачи на дипломный проект:

* изучить методы защиты операционной системы от файловых вирусов;
* разработать структуру программного средства;
* разработать и протестировать программное средство;
* рассчитать себестоимость и отпускную цену программного средства;
* изучить тему по охране труда «Организация общественного контроля за состоянием охраны труда».

Пояснительная записка к дипломному проекту состоит из 22 таблиц, 35 рисунков, 4 диаграмм и 15 источников.

В введении указана актуальность, объект, предмет исследования, цель и задачи дипломного проекта.

В введении раскрыта актуальность темы, определен объект исследования, предмет исследования, цель и задачи дипломного проекта.

В разделе «Назначение и область применения» раскрыта актуальность темы дипломного проекта, описаны виды вирусов, методы и способы борьбы с ними, проведен анализ аналогов.

В разделе «Проектирование» описана структура программного средства, выбор аппаратных средств, основные алгоритмы, методы разработки программных модулей, реализация взаимосвязи компонентов программного средства, а также рекомендации по использованию и описание графического интерфейса.

В экономическом разделе произведен расчет экономических характеристик.

В разделе «Охрана труда» изучена тема «Организация общественного контроля за состоянием охраны труда», в которой раскрыты такие вопросы как организация общественного контроля условий безопасности труда и общественный контроль за состоянием охраны труда на объекте при проектируемой деятельности.

В заключении подведены итоги разработки дипломного проекта, выделены преимущества, указаны перспективы модернизации и сопровождения разработанного программного средства.

# **ОСНОВНАЯ ЧАСТЬ**

1. Назначение и область применения

1.1 Описание предметной области

15 февраля 1946 года, была представлена новейшая и прогрессивная ЭВМ Eniac. Спустя 5 лет после её представления, американец Джон фон Нейман, заложил основы теории самовоспроизводящихся механизмов, он предложил метод создания таких механизмов, эти основы были опубликованы. Спустя некоторое время, учёный Ф. Ж. Шталь, используя материалы статьи Джона фон Неймана, запрограммировал на машинном языке биокибернетическую модель, в которой существа двигались, питаясь ненулевыми словами. Так же, в 1961 году, в фирме Bell Labs изобрели игру, в которой несколько ассемблерных программ, называемых организмами, загружались в память компьютера. Организмы, созданные одним игроком (то есть принадлежащие к одному виду), должны были уничтожать представителей другого вида и захватывать жизненное пространство. Победителем считался тот игрок, чьи организмы захватывали всю память или набирали наибольшее количество очков.

В сентябре 1984 года, был предложен новый термин «вирус». А уже зимой того же года, были опубликованы первые антивирусные утилиты. Они позволяли проанализировать текст загрузочного модуля и выявлять все текстовые сообщения и «подозрительные» участки кода (команды прямой записи на диск и др.). Благодаря своей простоте (фактически использовался только контекстный поиск) и эффективности они получили значительную популярность. Так же эти утилиты перехватывали операции записи и форматирования, выполняемые через [BIOS](https://ru.wikipedia.org/wiki/BIOS). Спустя некоторое время, в начале 1985 года, был создан первый резидентный антивирус, перехватывающий попытки записи на [дискеты](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D0%BA%D0%B5%D1%82%D0%B0) и [винчестер](https://ru.wikipedia.org/wiki/%D0%96%D1%91%D1%81%D1%82%D0%BA%D0%B8%D0%B9_%D0%B4%D0%B8%D1%81%D0%BA), и осуществляющий блокировку всех операций (запись, [форматирование](https://ru.wikipedia.org/wiki/%D0%A4%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)), выполняемые через BIOS.

Очередным этапом развития вирусов считается [1987 год](https://ru.wikipedia.org/wiki/1987_%D0%B3%D0%BE%D0%B4). К этому моменту получили широкое распространение сравнительно дешёвые компьютеры IBM PC, что привело к резкому увеличению масштаба заражения компьютерными вирусами. Именно в 1987 вспыхнули сразу три крупные эпидемии компьютерных вирусов. Первая эпидемия была вызвана вирусом Brain. За один год, этот вирус смог поразить более 18 тысяч компьютеров по всему миру. Вирус перезагружал компьютеры, на которых использовалось не лицензионное программное обеспечение. Он так же являлся первым невидимым вирусом, при попытке чтения заражённого сектора, он подставлял его незаражённый оригинал.

Вторая вирусная эпидемия была связанна с развитием глобальной сети интернет. В 1988 году, Робертом Моррисом был создан первый сетевой червь. Занимал червь всего 60 килобайт. Проникая в компьютер жертвы, червь подключал компоненты, позволяющие раскрывать пароли, имеющиеся в системе, что в свою очередь, позволяло программе маскироваться под задачу легальных пользователей системы, на самом деле занимаясь размножением и рассылкой копий. Он поразил свыше 6200 компьютеров. В результате вирусной атаки большинство сетей вышло из строя на срок до пяти суток. Компьютеры, выполнявшие коммутационные функции, работавшие в качестве файл-серверов или выполнявшие другие функции обеспечения работы сети, также вышли из строя.

Третья вирусная эпидемия была наиболее крупная. Появился вирус Datacrime, спящий вирус. Вирус распространялся и никак не выдавал себя, но начиная с 12 октября производил разрушение файловой системы на заражённых компьютерах. Всего было заражено более 100 тысяч ПЭВМ.

Начиная с 2010 года, проблема вирусов начинает принимать глобальный масштаб. 17 июня 2010 года, был обнаружен ранее не известный вирус Stuxnet. Вся проблема заключалась в том, что он был обнаружен не только на персональных компьютерах пользователей, но и в промышленных системах, управляющих автоматизированными производственными процессами. Это первый в истории вирус, который перехватывал и модифицировал информационный поток между программируемыми логическими контроллерами и рабочими станциями. Уникальность заключалась в том, что вирус мог физически разрушать инфраструктуру. Поэтому он мог быть использован как средство несанкционированного сбора данных и диверсий. Размер его, составлял всего 500 КБ.

Существует огромное количество различных вирусов. В таблице 1.1.1 приведена общая классификация типов вирусов.

Таблица 1.1.1 ­­– Общая классификация типов вирусов

|  |  |
| --- | --- |
| Наименование | Описание |
| Анти-антивирусный вирус | Компьютерная вирусная программа, объектом нападения которой являются антивирусные программы |
| Вариант вируса, штамм, модификация | Модифицированный вариант одного и того же вируса |
| Вирусная программа-червь | Паразитическая программа, обладающая механизмом саморазмножения. Программа способна размножать свои копии, но не поражать другие компьютерные программы. Проникает на компьютер из сети и рассылает свои функциональные копии на другие компьютерные сети |

Продолжение таблицы 1.1.1

|  |  |
| --- | --- |
| Вирусный мистификатор | Не являющееся вирусом почтовое сообщение. На компьютер пользователя мистификация приходит в виде письма, написанного в подчеркнуто нейтральном тоне, в котором указывается на якобы распространяющийся новый вирус. Пользователю предлагается найти некий файл с помощью поискового средства Windows и удалить его с диска |
| Вирусы-спутники | Формально являются файловыми вирусами. Не внедряются в исполняемые программы. Такие вирусы используют особенность системы, позволяющую программному файлу с тем же названием, но другим расширением действовать с разными приоритетами. Такие вирусы могут быть резидентными и маскировать файлы-двойники |
| Дроппер | Файл-носитель, устанавливающий вирус в систему. Техника, иногда используемая вирусописателями для сокрытия вирусов от антивирусных программ |
| Зоологический вирус | Вирусы, которые существуют только в антивирусных лабораториях, в коллекциях исследователей вирусов |
| Полиморфные вирусы | Вирусы с самомодифицирующимися расшифровщиками, использующие помимо шифрования кода специальную процедуру расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у него байтовых сигнатур |
| MtE вирусы | Полиморфные вирусы, созданные с помощью генератора полиморфизма |

Продолжение таблицы 1.1.1

|  |  |
| --- | --- |
| Резидентный вирус | Постоянно присутствующий в памяти вирус, написанный, как правило на низкоуровневом языке. Такие вирусы обладают возможностью эффективно заражать программы и противодействовать антивирусным средствам. |
| Скрипт-вирус | Вирус, написанный на языках Visual Basic, Basic Script, Java Script. На компьютер пользователя чаще всего проникают в виде почтовых сообщений, содержащих во вложениях файлы-сценарии. Программы на языках Visual Basic и Java Script могут располагаться как в отдельных файлах, так и встраиваться с HTML документ и в таком случае интерпретироваться с браузером, причем не только с удаленного сервера, но и с локального диска |
| Стелс-вирус | Вирусные программы, предпринимающие специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в зараженных объектах. Делятся на 2 типа: руткит и буткит |
| Шифрованные вирусы | Вирусы, которые сами шифруют свой код для затруднения их дизассемблирования и обнаружения в файле, памяти или секторе. Каждый экземпляр такого вируса будет содержать только короткий общий фрагмент – процедуру расшифровки – который можно выбрать в качестве сигнатуры. В случае каждого инфицирования он автоматически зашифровывает себя, и каждый раз по-разному. Таким способом вирус пытается избежать обнаружения вирусными программами. |

В таблице 1.1.2 приведена классификация именований вирусов

Таблица 1.1.2 – Классификация наименований вирусов

|  |  |
| --- | --- |
| Наименование | Описание |
| High Level Language вирусы | В данную группу объединяют вирусы, написанные на языках программирования высокого уровня, таких как C#, Java, Pascal |
| Троянские программы | В данную группу объединяют вирусы, которые осуществляют несанкционированные пользователем действия на его компьютере. |
| Silly-вирусы | Вирусы, которые не обладают никакими особенными характеристиками, вследствие чего нет необходимости присвоить таким вирусам особенные названия |
| Макровирусы | В данную группу объединяют вирусы, использующие особенности файлов офисных программ, а так же встроенные макроязыки данных приложений. |
| Скрипт-вирусы | В данную группу объединяют вирусы, написанные на различных интерпретируемых языках. Разделяют на 9 классов: VBS, JS, Wscript, HTML, Perl, PHP, IRC, Java, Bat. |
| Узкоспециализированное ПО | В данную группу объединяют вирусы, разработанные для инфицирования файлов конкретных программ. Выделяют 3 класса: ACAD, AutoLisp, SWF |
| Суффиксы | В эту группу входит 4 класса: вирусный конструктор, инсталлятор вируса. |
| Для DoS-атак | В данную группу объединяют вредоносные программы, разработанные для осуществления DoS атак с целью довести вычислительную технику до отказа в обслуживании |

Продолжение таблицы 1.1.2

|  |  |
| --- | --- |
| Потенциально опасное ПО | В данную группу объединяют программы, неспособные к самовоспроизведению и представляющие потенциальную опасность. В группу входит 4 классов: программы-шутки, хакерские утилиты, рекламные вирусы, программы, которые могут быть использованы злоумышленниками |
| Вирусы для разных ОС | В данную группу объединяют вредоносные программы, разработанные для определения ОС. Выделяют 19 классов. |
| Опасное ПО | Программы данной группы характеризируют как опасные и разделяют на 3 класса: Backdoor, Trojan, Exploit |
| Инструменты создания вредоносного ПО | В данную группу объединяют программы, которые используются для генерации или создания вирусов (вирусные конструкторы). |

В таблице 1.1.3 приведена классификация вирусов по видам заражаемых объектов.

Таблица 1.1.3 – Классификация вирусов по видами заражаемых объектов.

|  |  |
| --- | --- |
| Наименование | Описание |
| Файловые вирусы | Вирусы, заражающие двоичные файлы (в основном исполняемые файлы и динамические библиотеки). Чаще всего, такие файлы имеют расширение EXE, COM, DLL, SYS. Так же могут инфицировать файлы с расширениями DRV, BIN, OVL, OVY. Такие вирусы внедряются в файлы операционной системы, активируются при запуске пораженной программы и затем распространяются |
| Загрузочные (бутовые) вирусы | Вирусы, которые заражают загрузочные записи дискет, разделов жестких дисков, а также MBR жестких дисков |

Продолжение таблицы 1.1.3

|  |  |
| --- | --- |
| Макрокомандные вирусы (макровирусы) | Вирусы, заражающие файлы документов, используемые приложениями Microsoft Office и другими программами, допускающие наличие макрокоманд. Благоприятным фактором распространения вируса служит то, что все основные компоненты Microsoft Office могут содержать встроенные программы на полнофункциональном языке программирования, а в Microsoft Word эти макросы автоматически запускаются при открытии любого документа, его закрытии, сохранении и т.д. Учитывая то, что копирование макросов из документа в документ (в частности в общий шаблон) выполняется всего одной командой |

В зависимости от среды обитания вирусы можно разделить на:

– сетевые;

– файловые;

– загрузочные;

– файлово-загрузочные.

Сетевые вирусы распространяются по различным компьютерным сетям.

Файловые вирусы внедряются главным образом в исполняемые модули, а именно в файлы, имеющие расширения com и exe. Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). Файлово-загрузочные вирусы заражают как файлы пользователя, так и загрузочные сектора подключенных жестких дисков.

По способу заражения вирусы делятся на:

– резидентные;

– нерезидентные.

Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

– неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;

– опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;

– очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

Заражению часто подлежат файлы программ из пакета Microsoft office. В эти файлы при заражении всегда вставляются макросы, которые создаются на языке Visual Basic, который поддерживается в подавляющем большинстве продуктов Microsoft office.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия. Простейшие вирусы – паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. Вирусы-невидимки, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Наиболее трудно обнаружить вирусы-мутанты (полиморфные вирусы), содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые квазивирусные или «троянские» программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, могут разрушить загрузочный сектор и файловую систему дисков.

Так же следует не забывать про атаки с использованием внешних аппаратных устройств. Примером такой атаки является атака BadUSB, основанная на уязвимости USB устройств. Она устроена следующим образом: для определённого контроллера съёмного накопителя создаётся специальная прошивка, которая содержит код вируса, и уязвимый контроллер (съёмный накопитель) прошивается этой прошивкой. Модифицированная прошивка может исполнять любые команды злоумышленника, при этом оставаясь незамеченным в системе, так как все действия идут от эмулированного устройства ввода-вывода, например, сетевой карты, клавиатуры, мыши, или к примеру загрузочным устройством. Атака действует на все устройства, в которых есть USB порт, вне зависимости от установленной операционной системы. Единственное условие – должен быть установлен драйвер поддержки USB устройств.

Вирусы способны заражать такие объекты, как:

– исполняемые файлы;

– загрузчик системы;

– файлы документов.

Вирусы, которые заражают файлы, называются файловыми. Вирус в зараженных исполняемых файлах начинает свою работу при запуске той программы, в которой он находится.

Вирусы, которые заражают загрузчик операционной системы и главную загрузочную запись, называются загрузочными. Обычно загрузочные вирусы разделены на 2 части: первая часть находится в главной загрузочной записи, вторая находится в другом участке диска, или в кластере в области данных диска. Разделение на 2 части обусловлено тем, что в главную загрузочную запись невозможно записать что-либо большое.

С ростом угрозы, появлялось всё больше программ, решений и методов, для борьбы с ними, самыми актуальными методами обнаружения угроз являются:

– сигнатурный анализ;

– эвристический анализ;

– метод эмуляции исполнения программного кода.

При проверке компьютера на предмет угроз, в первую очередь применяется сигнатурный анализ. Он выполняется путем проверки содержимого анализируемого объекта на предмет наличия в нем сигнатур уже известных вирусов. Сигнатурой называется непрерывная конечная последовательность байт, необходимая и достаточная для однозначной идентификации угрозы. При этом сравнение содержимого исследуемого объекта с сигнатурами производится не напрямую, а по их контрольным суммам, что позволяет значительно снизить размер записей в вирусных базах, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения угроз и лечения инфицированных объектов. Записи в вирусных базах составляются таким образом, что благодаря одной и той же записи можно обнаруживать целые классы или семейства угроз.

Работа эвристического анализатора основывается на наборе эвристик (предположений, статистическая значимость которых подтверждена опытным путем) о характерных признаках вредоносного и, наоборот, безопасного исполняемого кода. Каждый признак кода имеет определенный вес (т. е. число, показывающее важность и достоверность этого признака). Вес может быть как положительным, если признак указывает на наличие вредоносного поведения кода, так и отрицательным, если признак не свойственен компьютерным угрозам. На основании суммарного веса, характеризующего содержимое объекта, эвристический анализатор вычисляет вероятность содержания в нем неизвестного вредоносного объекта. Если эта вероятность превышает некоторое пороговое значение, то выдается заключение о том, что анализируемый объект является вредоносным.

Эвристический анализатор также использует технологию Fly-Code – универсальный алгоритм распаковки файлов. Этот механизм позволяет строить эвристические предположения о наличии вредоносных объектов в объектах, сжатых программами упаковки (упаковщиками), причем не только известными разработчикам продукта, но и новыми, ранее не исследованными программами. При проверке упакованных объектов также используется технология анализа их структурной энтропии, которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, упакованных одинаковым полиморфным упаковщиком.

Поскольку эвристический анализатор является системой проверки гипотез в условиях неопределенности, то он может допускать ошибки как первого (пропуск неизвестных угроз), так и второго рода (признание безопасной программы вредоносной). Поэтому объектам, отмеченным эвристическим анализатором как «вредоносные», присваивается статус «подозрительные».

Метод эмуляции исполнения программного кода используется для обнаружения полиморфных и шифрованных вирусов, когда использование поиска по контрольным суммам сигнатур неприменимо или значительно усложнено из-за невозможности построения надежных сигнатур. Метод состоит в имитации исполнения анализируемого кода при помощи эмулятора – программной модели процессора и среды исполнения программ. Эмулятор оперирует с защищенной областью памяти (буфером эмуляции). При этом инструкции не передаются на центральный процессор для реального исполнения. Если код, обрабатываемый эмулятором, инфицирован, то результатом его эмуляции станет восстановление исходного вредоносного кода, доступного для сигнатурного анализа.

Сканирование является наиболее традиционным методом поиска вирусов. Оно заключается в поиске уже ранее обнаруженных вирусов. Антивирусные программы-сканеры, способные удалить обнаруженные вирусы, обычно называют полифагами. Недостаток метода сканирования в том, что невозможно обнаружить полиморфные вирусы, полностью меняющие свой код. Для этого нужно использовать более сложные алгоритмы поиска, включающие эвристический анализ. Сканнеры не способны защитить компьютер от новых вирусов, поэтому они не эффективны.

Наиболее эффективным методом обнаружения вирусов является эвристический анализ. Эвристический анализ зачастую используется совместно с сигнатурным анализом для поиска шифрующихся и полиморфных вирусов. В большинстве случаев эвристический анализ позволяет также обнаруживать и ранее неизвестные вирусы. В этом случае, скорее всего их лечение будет невозможно.

Самым ресурсо-затратным методом, является метод обнаружения изменений файлов. Заражая компьютер, вирус делает изменения на жестком диске, на обнаружении таких изменений и основывается этот метод. В системе может существовать одновременно очень большое количество процессов, которые так или иначе вносят изменения в файловую систему компьютера. Антивирусной программе приходится проверять и фильтровать каждую такую операцию ввода-вывода.

По статистике компании Dr. Web только 30% обнаруженных угроз приходится на сигнатурный анализ, остальные 70% приходятся на метод эвристического анализа и эмуляции исполнения.

Так же, с развитием ЭВМ и появлением нового оборудования, появились аппаратные уязвимости, которые полностью можно было устранить, только заменой оборудования на более новое, зачастую более дорогостоящее.

Примером аппаратной уязвимости является уязвимость Meltdown, позволяющая любой вирусной программе, путём выполнения определённых инструкций извлечь любые данные из кэша процессора. Атака возможна благодаря манипуляции с внеочередным исполнением внутри процессора. Технология внеочередного исполнения команд процессором создана для того, чтобы определить наиболее приоритетные инструкции в конвейере обработки инструкций и выполнить их в первую очередь. Однако этим процессом можно манипулировать таким образом, что можно извлечь любую информацию, начиная с обычной строки, заканчивая ключами шифрования и пользовательскими данными. Уязвимости подвержены все процессоры, которые выпускаются с 1995 года.

Способы противодействия компьютерным вирусам можно разделить на несколько групп:

– профилактика заражения и уменьшение предполагаемого ущерба от такого заражения;

– методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса;

– способы обнаружения и удаления неизвестного вируса.

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программные средства. Однако не существует антивирусных средств, гарантирующих полную защиту от вирусов, и заявления о существовании таких систем можно расценить как-либо недобросовестную рекламу, либо непрофессионализм. Таких систем не существует, поскольку на любой алгоритм антивируса всегда можно предложить контр-алгоритм вируса, невидимого для этого антивируса.

Основными признаками заражения вирусом являются:

– замедление работы компьютера;

– невозможность загрузки операционной системы;

– частые зависания и сбои в работе компьютера;

– прекращение работы или неправильная работы ранее функционировавших программ;

– увеличение количества файлов на диске;

– изменение размера файлов;

– периодическое появление на экране монитора неуместных системных сообщений;

– уменьшение объема свободной оперативной памяти;

– заметное возрастание времени доступа к файлам на жестком диске;

– изменение даты и времени создания файлов;

– разрушение файловой структуры (исчезновение файлов, искажение каталогов и др.).

Следует также обратить внимание на несколько терминов, применяемых при обсуждении антивирусных программ:

– ложное срабатывание – детектирование вируса в незараженном объекте (файле, секторе или системной памяти);

– сканирование по запросу – поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания;

– сканирование на лету – постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание). В этом режиме антивирус постоянно активен, он присутствует в памяти «резидентно» и проверяет объекты без запроса пользователя.

Далее приведены основные понятия и ключевые слова, необходимые для понимания предметной области.

Компьютерный вирус – это вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи

**Антивирусная программа (антивирус)** – изначально компьютерная программа, которая предназначена для обезвреживания вирусов и различного рода вредоносного ПО, с целью сохранности данных и оптимальной работы вашего персонального компьютера.

Сигнатура – непрерывная конечная последовательность байт, необходимая и достаточная для однозначной идентификации угрозы.

Шины устройств – подсистемы передачи данных между функциональными блоками компьютера (например, шина USB, PCI).

Хеш-сумма – уникальный идентификатор файла, представляющий собой последовательность цифр и букв заданной длины. Используется для проверки целостности данных.

Эксплойт – программа, фрагмент кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на систему.

Ядро программного средства – совокупность компонентов и связей между ними.

IRP пакет – пакет запроса ввода-вывода.

SSDT – таблица системных вызовов.

GDT – глобальная дескрипторная таблица.

IDT – таблица векторов прерываний.

LDT – локальная дескрипторная таблица.

1.2 Назначение программного средства

Основное назначение антивирусных программных средств – обеспечение базовой защиты, предотвращение угроз, восстановление системы и данных, защита конфиденциальных данных.

В состав базовой защиты в первую очередь входят функции:

– защиты от вирусов, червей, эксплойтов, троянских, шпионских и рекламных программ;

– проверка файлов, почтовых сообщений, интернет в автоматическом режиме и по требованию;

– мониторинг активности (сбор данных о работе программ на компьютере);

– откат действий вредоносной программы;

– постоянная защита от фишинговых сайтов;

– постоянная проверка файлов в автономном режиме.

В состав функции предотвращения угроз входит:

– поиск уязвимостей в операционной системе и установленном ПО;

– блокирование ссылок на заражённые сайты;

– распознавание вирусов по способу их упаковки;

В состав функции восстановления системы и данных входит:

– возможность упаковки программы на заражённый компьютер;

– функция самозащиты программы от выключения или остановки;

– восстановление корректных настроек системы после удаления вредоносного ПО;

– наличие инструментов для создания диска аварийного восстановления.

В состав функции защиты конфиденциальных данных входит:

– блокирование ссылок на фишинговые сайты;

– защита от всех видов кейлоггеров и шпионских программ.

1.3 Анализ существующих разработок

Основными критериями оценки антивирусных программных средств являются:

– стабильность и надежность работы – самый определяющий параметр, даже самый лучший антивирус окажется совершенно бесполезным, если он не сможет нормально функционировать на вашем компьютере, если в результате какого-либо сбоя в работе программы процесс проверки компьютера не пройдёт до конца;

– размер вирусной базы программы, сюда же следует отнести и возможность программы определять разнообразные типы вирусов, и умение работать с файлами различных типов (архивы, документы);

– скорость работы алгоритмов программы, к этому пункту относятся такая характеристика как скорость сканирования или проверки файла;

– кроссплатформенность.

Существует довольно много существующих разработок. Они делятся на платные и бесплатные, но самыми популярными из них, по количеству установок являются: NOD32, Kaspersky, Norton, Doctor Web, McAfee, Avira.

Самыми популярными антивирусными средствами в русскоговорящем сегменте являются Dr Web (доктор веб) и Kaspersky (антивирус Касперского).

В таблице 1.3.1 приведено сравнение антивирусных продуктов.

Таблица 1.3.1 – Сравнение антивирусных продуктов по различным параметрам

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Название антивирусной программы | Kaspersky | NOD 32 | Symantec | Dr. Web | 360 Total security |
| Поддержка в системах семейства Windows | Имеется | Имеется | Имеется | Имеется | Имеется |
| Поддержка в системах семейства Linux | Имеется | Не имеется | Не имеется | Имеется | Не имеется |
| Время загрузки системы | До 4 минут | До 3 минут | До 3 минут | До 4 минут | До 2 минут |
| Время сканирования системных папок | Меньше 20 минут | Меньше 10 минут | Меньше 15 минут | Меньше 17 минут | Меньше 10 минут |
| Загрузка ЦП | 5.5 – 8 % | 8%–12% | 4% –10% | 3% – 8% | 2.5% – 5% |
| Использование ОЗУ в простое | 210 мб | 138 мб | 157 мб | 120 мб | 107 мб |
| Антивирусный сканер и монитор | Имеется | Имеется | Имеется | Имеется | Имеется |
| Защита персональных данных | Имеется | Имеется | Имеется  (в платной версии) | Имеется | Имеется |
| Фаервол | Имеется | Имеется | Имеется | Не имеется | Не имеется |
| Защита почтового ящика | Имеется | Имеется | Имеется | Имеется | Не имеется |
| Работа в облаке | Не имеется | Не имеется | Имеется | Не имеется | Имеется |
| Обнаружение вторжения | Имеется | Имеется | Имеется | Имеется | Не имеется |
| Система обновлений | Имеется | Имеется | Имеется | Имеется | Имеется |
| Веб-защита | Имеется | Имеется | Не имеется | Имеется | Имеется |
| Антиспам | Имеется | Имеется | Имеется | Имеется | Не имеется |
| Поддержка большинства языков | Имеется | Имеется | Имеется | Имеется | Имеется |

Интерфейсы всех антивирусных средств ориентированы на обычного пользователя, поэтому являются интуитивно понятными.

На рисунке 1.3.1 изображен интерфейс антивирусного программного средства Dr Web.

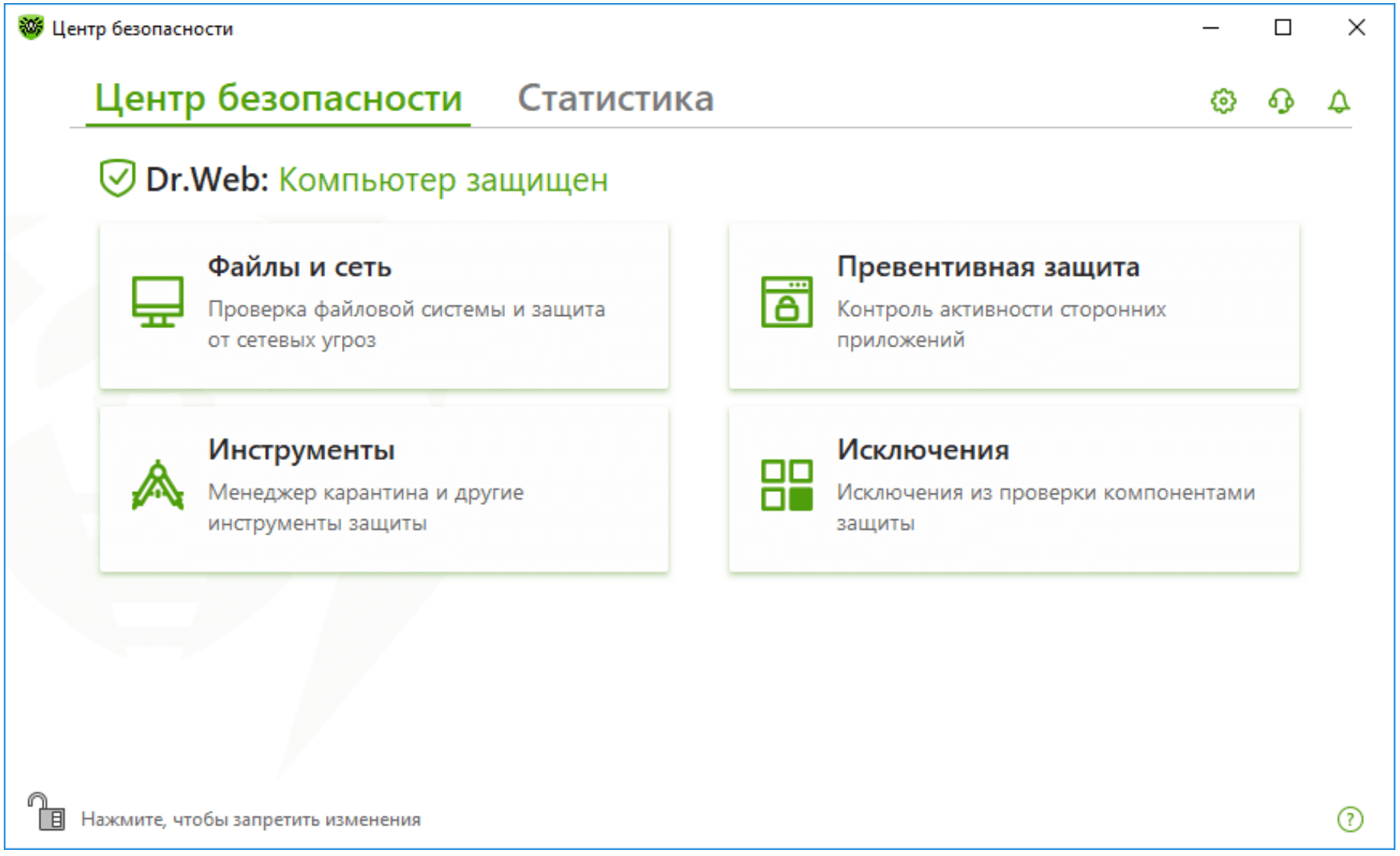


Рисунок 1.3.1 – Интерфейс программы Dr Web

На рисунке 1.3.2 изображен интерфейс антивирусного программного средства от лаборатории Касперского.

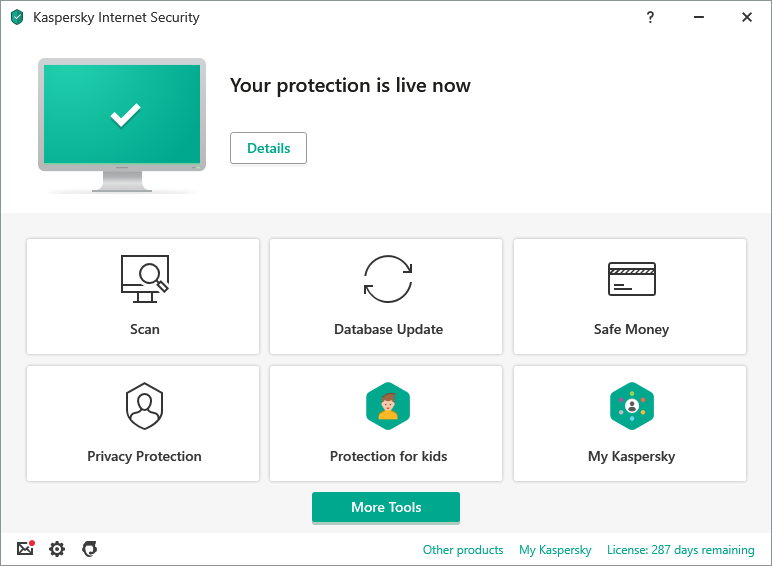


Рисунок 1.3.2 – Антивирус Касперского

У большинства антивирусных средств графический интерфейс очень простой по причине того, что вмешивание пользователя в работу практически не требуется, за исключением простой настройки, всё производится автоматически.

На основании проведенного сравнения, можно сделать вывод что одним из лучших антивирусных средств, является антивирус Касперского. Именно он обеспечивает наилучшую защиту от взломщиков, троянов и других видов вирусных программ.

2 Технические характеристики

2.1 Постановка задачи на разработку

Целью дипломного проекта является разработка программного средства, позволяющего защитить операционную систему от файловых вирусов.

Для достижения поставленной цели были сформулированы следующие задачи:

– разработать логическую структуру программного средства;

– разработать и протестировать библиотеки, модули и драйвер операционной системы.

Программное средство должно обеспечивать следующий функционал:

– защита операционной системы от файловых вирусов;

– хранение файловых вирусов в защищенном хранилище (карантин);

– ручное сканирование;

– настройка исключений;

– защита важных файлов с помощью криптографа;

– своевременное автоматическое обновление базы сигнатур;

– автоматическая проверку файлов в фоновом режиме.

2.2 Описание программного средства

2.2.1 Общие сведения

Программное средство защиты от вирусных файлов разработано на языке C# с использованием платформы .NET Framework.

.NET Framework – [программная платформа](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BB%D0%B0%D1%82%D1%84%D0%BE%D1%80%D0%BC%D0%B0#%D0%BA%D1%80%D0%BE%D1%81%D1%81%D0%BF%D0%BB%D0%B0%D1%82%D1%84%D0%BE%D1%80%D0%BC%D0%B5%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5), выпущенная компанией [Microsoft](https://ru.wikipedia.org/wiki/Microsoft) в [2002 году](https://ru.wikipedia.org/wiki/2002_%D0%B3%D0%BE%D0%B4). Основой платформы является общеязыковая среда исполнения [Common Language Runtime (CLR)](https://ru.wikipedia.org/wiki/Common_Language_Runtime), которая подходит для различных языков программирования. Функциональные возможности CLR доступны в любых языках программирования, использующих эту среду.

Плюсы использования платформы .NET:

– управление памятью, во многих языках разработчики должны предусматривать выделение и освобождение памяти, а также управлять временем жизни объектов, в приложениях .NET Framework эти функции выполняет среда CLR;

– общая система типов, в традиционных языках программирования базовые типы определяются компилятором, что осложняет взаимодействие между языками, в .NET Framework базовые типы определяются системой типов;

– обширная библиотека классов, разработчикам не требуется писать код для выполнения стандартных низкоуровневых операций программирования, так как они используют удобную библиотеку типов и членов, входящую в библиотеку классов .NET Framework;

– платформы и технологии разработки, платформа .NET Framework включает библиотеки для конкретных областей разработки приложений;

– взаимодействие языков, языковые компиляторы, ориентированные на .NET Framework, выдают промежуточный код, называемый языком CIL (Common Intermediate Language), который, в свою очередь, компилируется во время выполнения средой CLR;

– совместимость версий, приложения, разработанные на основе конкретной версии платформы .NET Framework, могут выполняться без доработок и на более поздних версиях платформы;

– параллельное выполнение, платформа .NET Framework помогает разрешать конфликты версий, поскольку на компьютере могут быть установлены несколько версий среды CLR.

Программное средство имеет модульную структуру. Все модули изолированы от ядра и не могут ему навредить каким-либо образом. Преимущества такого подхода в том, что для обновления программного средства не нужно его полностью выключать, что могло бы ослабить защиту во время обновления. Для обновления достаточно выключить нужный модуль и заменить его библиотеку на жестком диске.

2.2.2 Функциональное назначение

Программное средство позволяет защитить операционную систему от файловых вирусов, которые могут попасть на компьютер пользователя через различные источники, такие как съемные носители, дискеты, флеш-накопители, электронная почта, веб-страницы, интернет и локальные сети, а также через системы обмена мгновенными сообщениями.

Программное средство предоставляет пользователю следующий функционал:

– обнаружение и обезвреживание угроз в пассивном режиме;

– принудительное сканирование файлов и папок;

– хранение зараженных файлов в карантине;

– настройку исключений.

2.2.3 Описание логической структуры

На рисунке 2.2.3.1 изображена логическая структура программного средства.

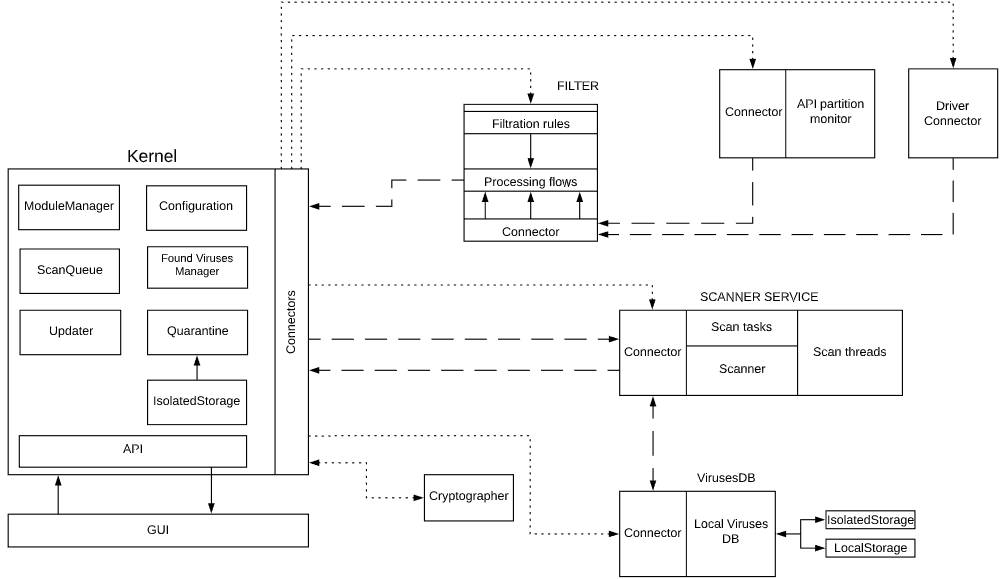


Рисунок 2.2.3.1 – Логическая структура программного средства

В таблице 2.2.3.1 приведено описание всех модулей программного средства.

Таблица 2.2.3.1 – описание компонентов и модулей программного средства

|  |  |
| --- | --- |
| Компонент | Описание |
| Kernel | Ядро программного средства, связывает воедино все модули, состоит из 8 компонентов |
| Filter | Модуль фильтрации, позволяет отфильтровать непригодные для сканирования файлы и пути, состоит из 3 компонентов |
| Api partition monitor | Модуль обнаружения создания или изменения файлов на жестком диске |
| Scanner service | Модуль сканирования файлов, состоит из 4 компонентов |
| Viruses DB | Модуль локальной базы сигнатур |
| Cryptographer | Модуль криптографа |
| GUI | Модуль графического интерфейса |

Окончание таблицы 2.2.3.1

|  |  |
| --- | --- |
| Driver connector | Модуль коннектора, позволяет соединить ядро программного средства с драйвером ядра операционной системы |

В таблице 2.2.3.2 приведено описание внутренних компонентов ядра программного средства

Таблица 2.2.3.2 – Компоненты ядра программного средства

|  |  |
| --- | --- |
| Компонент | Описание |
| ModuleManager | Менеджер модулей, предназначен для загрузки и управления работой сторонних DLL модулей |
| ScanQueue | Менеджер задач сканирования, хранит в себе активные задачи по сканированию файлов, компонент взаимодействует с сервисом сканирования |
| Updater | Модуль обновления, позволяет получать обновления через интернет |
| Configuration | Компонент конфигурации, содержит в себе настройки позволяющие задавать работу модулей и компонентов |
| Found Viruses Manager | Менеджер обнаруженных вирусов, хранит в себе полную информацию об обнаруженных вирусах |
| Quarantine | Компонент карантина, позволяет хранить обнаруженные вирусы в защищенном хранилище |
| Connectors | Компонент соединений, позволяет другим компонентам ядра взаимодействовать с DLL модулями |
| API | Компонент позволяющий связать ядро со сторонним пользовательским приложением |

Все DLL модули имеют одну схожую черту, все они имеют в своём составе один и тот же компонент, называемый коннектором. Коннектор позволяет связать модуль с другим модулем или приложением с помощью именованных каналов. Именованный канал представляет собой поток байтов, доступ к которому может иметь несколько приложений, данные в такой поток можно записывать и считывать.

При запуске ядра первоначально производится инициализация конфигурации, затем следует загрузка DLL модулей, инициализация входящих и исходящих подключений и только после этого производится инициализация внутренних компонентов ядра. Такой порядок обусловлен тем, что компоненты ядра работают с DLL модулями, чтобы удостоверится в работоспособности модулей, необходимо создать подключение к ним, если подключение успешно, то производится инициализация внутренних компонентов. Процесс полной инициализации изображен на блок-схеме 2.2.3.2.

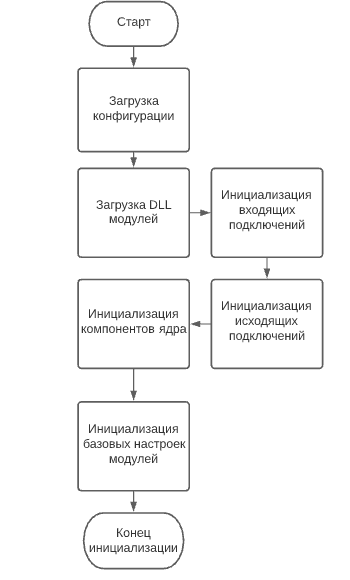


Рисунок 2.2.3.2 – Блок-схема процесса полной инициализации ядра

Менеджер модулей хранит описание и различные данные о DLL модуле. В таблице 2.2.3.3 описаны данные, которые хранит менеджер модулей о каждом модуле.

Таблица 2.2.3.3 – Описание хранимых данных о DLL модуле

|  |  |
| --- | --- |
| Наименование поля | Описание |
| ModuleName | Наименование модуля |
| ModuleAssembly | Ссылка на сборку модуля |
| IsRunning | Состояние модуля |

На рисунке 2.2.3.3 изображена блок-схема процесса загрузки DLL модуля.

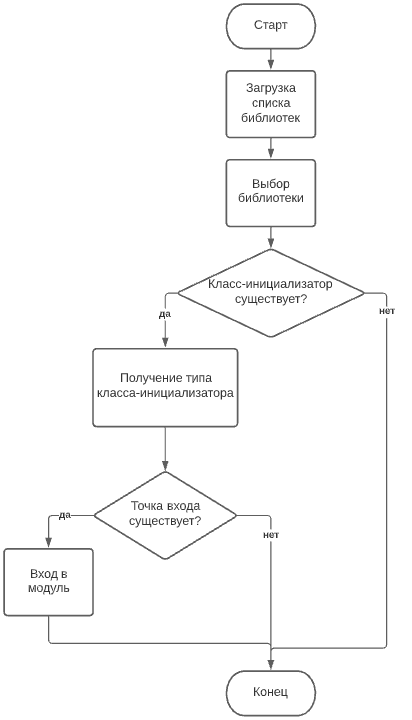


Рисунок 2.2.3.3 – Блок-схема процесса загрузки DLL модуля

Все DLL модули всегда инициализируют подключения к другим модулям. В таблице 2.2.3.4 описаны действия, выполняемые при инициализации каждого модуля.

Таблица 2.2.3.4 – Действия выполняемые при инициализации каждого модуля

|  |  |
| --- | --- |
| Наименование инициализируемого модуля | Описание действий |
| API Partition monitor | Запуск потока выполнения команд |

Окончание таблицы 2.2.3.4

|  |  |
| --- | --- |
| Filter | Загрузка стандартных правил фильтрации, запуск потоков-обработчиков |
| Scanner service | Запуск потоков-обработчиков |
| Viruses DB | Запуск потока обработки команд, загрузка файлов базы сигнатур в защищенное хранилище, загрузка сигнатур в ОЗУ из защищенного хранилища |

В таблице 2.2.3.5 описаны действия, выполняемые при инициализации каждого компонента ядра.

Таблица 2.2.3.5 – Действия выполняемые при инициализации каждого компонента ядра

|  |  |
| --- | --- |
| Наименование инициализируемого компонента | Описание действий |
| API | Установка событий, запуск потока-обработчика запросов |
| ScannerResponseHandler | Запуск потока-обработчика |
| ScanTasks | Запуск потока-обработчика, установка событий |
| FoundVirusesManager | Запуск потока-обработчика |
| Quarantine | Установка защищенного хранилища, проверка существования нужных директорий |

После полной инициализации производится базовая настройка подключенных модулей, а именно:

– установка проверяемых разделов в мониторе разделов;

– установка правил фильтрации;

– генерация или загрузка ключей шифрования;

– выгрузка всех сигнатур из модуля базы сигнатур в модуль сканнера.

Для мониторинга файловой системы в операционной системе используется класс FileSystemWatcher, который в свою очередь взаимодействует с Windows API (application programming interface). На рисунке 2.2.3.4 представлена блок-схема работы монитора изменений.

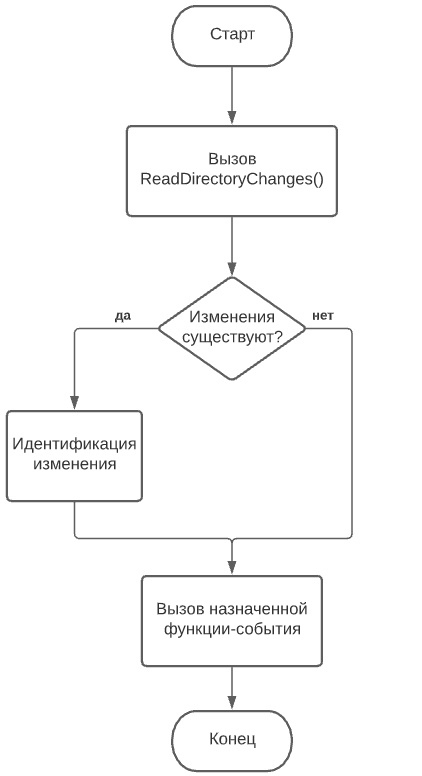


Рисунок 2.2.3.4 – Блок-схема алгоритма монитора изменений

При срабатывании события создания или редактирования файла, путь к файлу и идентификатор действия отправляются в сервис фильтрации.

Сервис фильтрации содержит в себе 3 компонента:

– правила фильтрации;

– коннектор;

– обработчики.

Компонент обработчика представляет собой 3 потока:

– поток обработки команд;

– поток обработки сообщений от модуля монитора разделов;

– поток обработки сообщений от модуля драйвер коннектора.

Существует 3 основных этапа фильтрации и 1 дополнительный. На первом этапе применяются фильтры расширения файлов, на втором фильтры путей, на третьем прочие правила фильтрации, на дополнительном этапе применяются не правила, а функции, в которые передается путь к файлу. Правило фильтрации представляет собой регулярное выражение. Поэтому в правила фильтрации можно добавить только правила, осуществляемые над строкой пути к файлу, а вот с помощью функции можно задать самые различные проверки (например проверка существования файла). На рисунке 2.2.3.5 изображена блок схема процесса фильтрации.

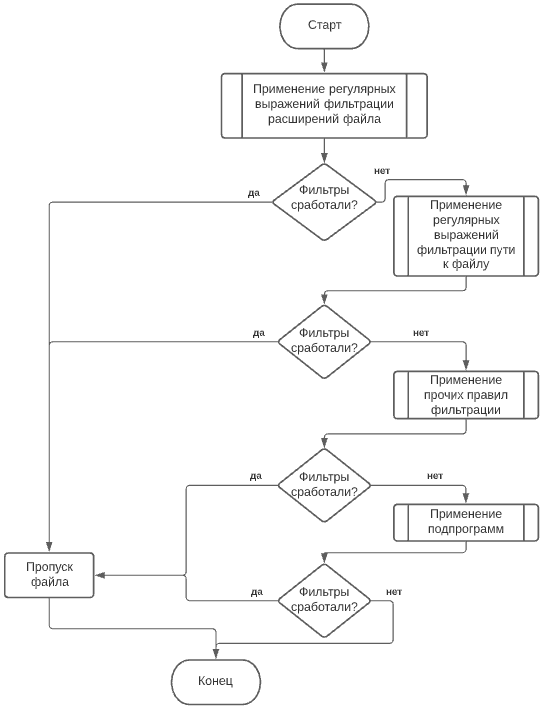


Рисунок 2.2.3.5 – Блок-схема процесса фильтрации

Если какой-либо из фильтров сработал, то файл просто пропускается, если же ни один из фильтров не сработал, то путь к файлу отправляется по именованному каналу дальше в ядро программного средства.

В ядре программного средства обработкой сообщений от модуля фильтра занимается компонент FileQueue, а который содержит в себе специально предназначенный для этого класс FilterHandler.

В таблице 2.2.3.6 приведено описание всех классов, которые содержит в себе компонент FileQueue.

Таблица 2.2.3.6 – Описание классов

|  |  |
| --- | --- |
| Класс | Описание |
| ScannerResponseHandler | Представляет собой обработчик результатов сканирования |
| FilterHandler | Представляет собой обработчик сообщений от фильтра |
| ScanTasks | Представляет собой менеджер активных задач сканирования |
| ScanTask | Представляет собой отдельную задачу сканирования |

При поступлении сообщения с путем к файлу производится проверка на наличие этого файла в листе вирусов, после этого создается задача сканирования. В таблице 2.2.3.7 приведено описание полей класса ScanTask, который представляет собой задачу сканирования.

Таблица 2.2.3.7 – Описание полей класса ScanTask

|  |  |
| --- | --- |
| Наименование поля | Описание поля |
| TaskId | Идентификатор задачи |
| File | Путь к файлу |
| ProbesCount | Количество попыток сканирования |

Все созданные задачи сканирования передаются через именованный канал прямо в модуль сканнера (ScannerService).

Сканнер при приёме задачи сканирования по именованному каналу добавляет её в свой локальный менеджер задач. Все задачи сканирования обрабатываются и выполняются потоками по мере возможности. Количество одновременно сканируемых файлов задается с помощью конфигурации. На рисунке 2.2.3.6 изображена блок-схема алгоритма поиска сигнатуры в файле.

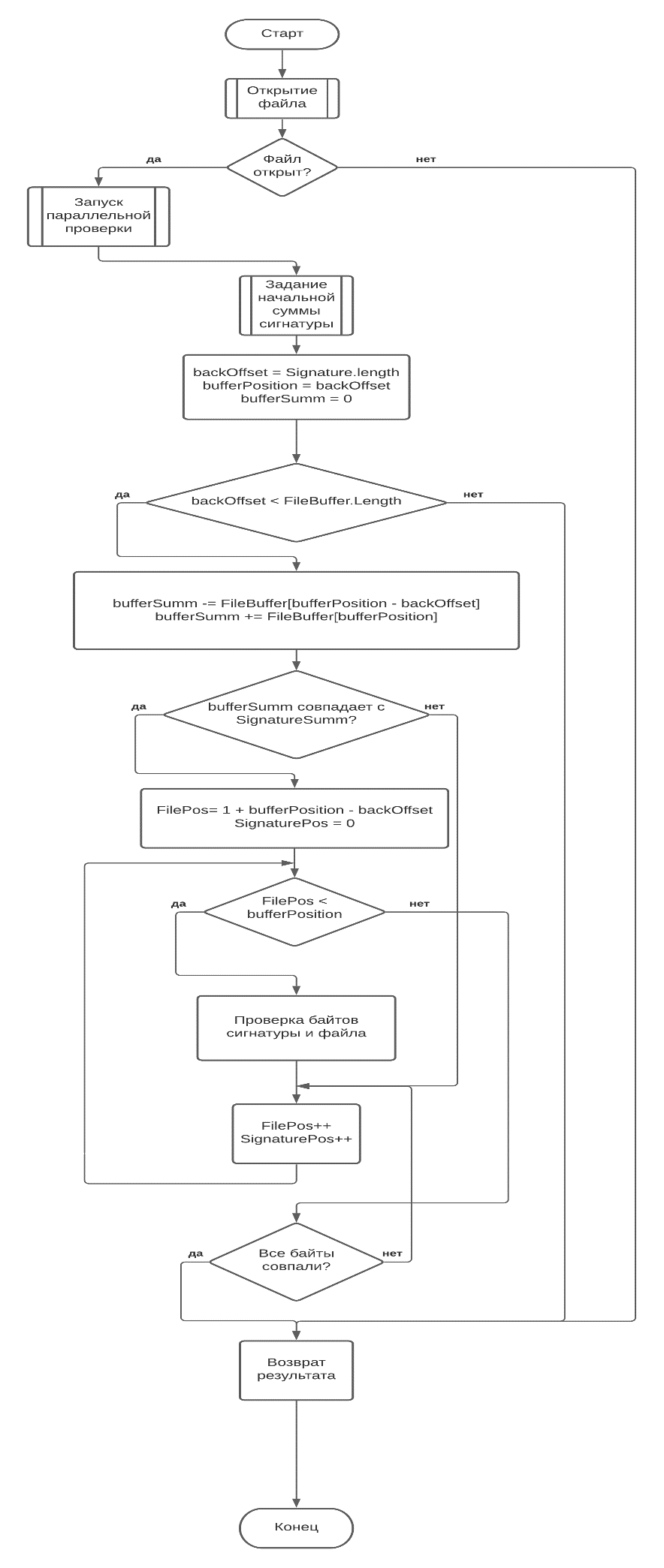


Рисунок 2.2.3.6 – Блок-схема алгоритма поиска сигнатуры

После того как задача сканирования была выполнена, результат сканирования возвращается в компонент FileQueue. Если задача была выполнена с ошибкой, то она повторяется ещё раз. Количество проб зависит от конфигурации компонента. Если задача была выполнена и в файле была обнаружена сигнатура вируса, то файл передается в компонент FoundVirusesManager. Если же в файле не была обнаружена вирусная сигнатура, то задача просто удаляется.

На рисунке 2.2.3.7 приведена блок схема алгоритма проверки файла начиная с создания задачи сканирования и заканчивая её удалением.

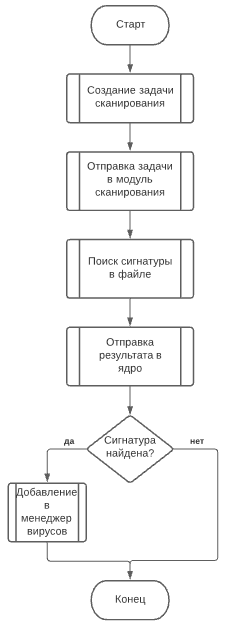


Рисунок 2.2.3.7 – Блок-схема алгоритма проверки файла

Компонент FoundVirusesManager содержит в себе полную информацию о файле и его принадлежности к вирусу. В таблице 2.2.3.8 приведено описание полей класса VirusInfo, который представляет собой информацию о вирусе.

Таблица 2.2.3.8 – Описание полей класса VirusInfo

|  |  |
| --- | --- |
| Наименование поля | Описание поля |
| id | Идентификатор вируса в таблице менеджера |
| inQuarantine | Находится ли вирус в карантине |
| fileInQuarantine | Путь к файлу в карантине |
| file | Путь к файлу на жестком диске |
| VirusId | Идентификатор вирусной сигнатуры |

Если в настройках программного средства включена опция авто перемещения вирусов в карантин, то вирус будет немедленно перемещен в карантин. За реализацию карантина отвечает компонент Quarantine.

Карантин представляет собой изолированное хранилище, доступ к которому может получить только та программа, которая создала это хранилище. В изолированном хранилище данные всегда изолированы по пользователю и по сборке. Учетные данные, такие как происхождение или строгое имя сборки, определяют идентичность сборки. Данные также могут быть изолированы по домену приложения с использованием аналогичных учетных данных. Для того, чтобы файл поместить в карантин, необходимо его сначала скопировать в защищенное хранилище, а затем удалить оригинал на жестком диске.

На рисунке 2.2.3.8 изображена блок-схема алгоритма перемещения файла в карантин.

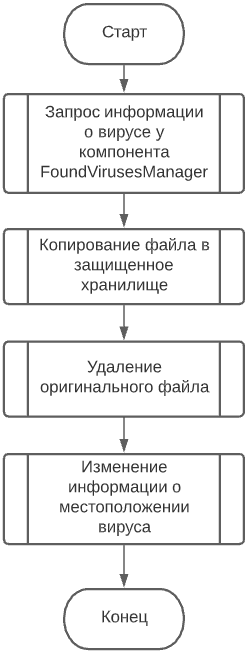


Рисунок 2.2.3.8 – Блок-схема алгоритма перемещения файла в карантин

Что бы другие программные средства могли взаимодействовать с ядром был реализован специальный API. Библиотека API связывается с ядром с помощью именованного канала. Ядро таким образом может принимать команды или уведомлять стороннее программное средство при возникновении различных событий (например событие обнаружение вируса). В приложении А изображена диаграмма последовательности действий работы ядра совместно с графическим интерфейсом пользователя.

Для осуществления действий над обнаруженными вирусами требуется вмешательство пользователя. На рисунке 2.2.3.9 изображена блок-схема взаимодействия ядра программного средства с пользователем при обнаружении вируса.



Рисунок 2.2.3.9 – Блок–схема взаимодействия

В таблице 2.2.3.9 приведено описание функционала библиотеки API.

Таблица 2.2.3.9 – Описание функций библиотеки API

|  |  |
| --- | --- |
| Функция | Назначение |
| ToQuarantine | Поместить вирус в карантин |
| RestoreFile | Восстановить файл из карантина |
| GetVirusInfo | Получить информацию о вирусе |
| ApplyingActions | Применить действия к вирусам |
| ClearScanQueue | Очистить очередь сканирования |
| AddToScan | Добавить файл для проверки в очередь сканирования |
| SetAutoScanRemovableDevices | Установить опцию авто сканирования съемных носителей |
| getAllViruses | Получить информацию о всех вирусах |
| DeleteFile | Удалить файл, где бы он не находился (в карантине или на жестком диске) |
| ClearConnectedDevices | Очистить таблицу подключенных устройств |

Окончание таблицы 2.2.3.9

|  |  |
| --- | --- |
| AddSimpleRule | Добавить простое правило фильтрации |
| RemoveSimpleRule | Удалить простое правило фильтрации |
| ClearSimpleRules | Удалить все простые правила фильтрации |

В таблице 2.2.3.10 приведено описание событий библиотеки API.

Таблица 2.2.3.10 – Описание событий библиотеки API

|  |  |
| --- | --- |
| Событие | Назначение |
| onScanCompleted | Срабатывает при выполнении сканирования |
| onScanFound | Срабатывает при обнаружении вируса |
| onVirusInfo | Срабатывает при получении информации о вирусе |

2.2.4 Используемые технические средства

В таблице 2.2.4.1 приведены минимальные аппаратно-программные характеристики компьютера пользователя.

Таблица 2.2.4.1 – Минимальные аппаратно-программные характеристики компьютера пользователя

|  |  |
| --- | --- |
| Компонент | Требование |
| Процессор | Любой x86 совместимый с тактовой частотой не менее 1GHz |
| Оперативная память | 1 GB RAM |
| Жесткий диск | 50MB HDD |
| Операционная система | Windows 8.1 |
| .NET Framework | V4.7.2 |

В таблица 2.2.4.2 приведено описание минимальных аппаратно-программных характеристик для .NET Framework.

Таблица 2.2.4.2 – Минимальные аппаратно-программные требования для .NET Framework

|  |  |
| --- | --- |
| Компонент | Требование |
| Оперативная память | 512MB |
| Свободное место на жестком диске | 4.5GB |
| Процессор | Любой x86 совместимый с тактовой частотой не менее 1GHz |
| Операционная система | Windows 7 SP1 |

В системах Windows 10 версии 1803 .NET Framework установлен по умолчанию.

2.2.5 Вызов и загрузка

Для обеспечения максимальной безопасности загрузка программного средства производится автоматически при загрузке операционной системы.

Текст будет добавлен после создания инсталлятора

2.2.6 Входные данные

Все входные данные в модули передаются с помощью именованных каналов. Именованные каналы представляют односторонние или дуплексные каналы для связи между сервером канала и одним или несколькими клиентами. Именованные каналы могут использоваться для межпроцессного взаимодействия локально или по сети. Любой процесс может действовать как сервер или клиент именованного канала.

Входящие именованные каналы модуля фильтра описаны в таблице 2.2.6.1.

Таблица 2.2.6.1 – Описание входных каналов модуля фильтра

|  |  |
| --- | --- |
| Именованный канал | Назначение |
| Filter.CommandPipe | Канал для команд |
| API\_MON\_FILTER | Канал для приёма сообщений от модуля мониторинга разделов жесткого диска и съемных носителей |
| DRIVER MON | Канал для приёма сообщений от драйвера мониторинга операций ввода-вывода |

Для выполнения команды в модуле фильтра, необходимо сначала отправить байт идентификатора команды, затем различные параметры, которые зависят от конкретной команды. Доступные команды модуля фильтра описаны в таблице 2.2.6.2.

Таблица 2.2.6.2 – Описание команд модуля фильтрации

|  |  |  |
| --- | --- | --- |
| Идентификатор команды | Передаваемые параметры | Назначение команды |
| 0 | Строка (регулярное выражение) | Добавить правило фильтрации расширения файла |
| 1 | Добавить правило фильтрации путей к файлам |
| 2 | Добавить прочее правило фильтрации |
| 3 | Строка | Добавить простое правило фильтрации |
| 4 | Удалить простое правило фильтрации |
| 5 | Ничего | Удалить все простые правила фильтрации |

Окончание таблицы 2.2.6.2

|  |  |  |
| --- | --- | --- |
| 6 | Ничего | Выключить модуль фильтрации |
| 7 | Очистить все правила |

Отличие обычного правила фильтрации от простого состоит в том, что обычное правило представляет собой регулярное выражение, простое правило это обычная строка. Путь считается отфильтрованным, если есть совпадение по регулярному выражению, или если строка простого правила была найдена в проверяемой строке. В таблице 2.2.6.3 приведены примеры правил фильтрации.

Таблица 2.2.6.3 – Правила фильтрации

|  |  |
| --- | --- |
| Правило | Назначение |
| ([^\s]+(?=\.(jpg|gif|png))\.\2) | Фильтрация пути к файлу с расширением jpg, png и gif |
| ^([a-zA-Z]:)?(\\[^<>:"/\\|?\*]+)+\\?$ | Фильтрация пути при присутствии в нём недопустимых символов |

В таблице 2.2.6.4 приведен пример простых правил фильтрации

Таблица 2.2.6.4 – Простые правила фильтрации

|  |  |
| --- | --- |
| Правило | Назначение |
| amdForever.dot | Фильтрация всех путей, ведущих к файлу amdForever.dot |
| C:\ | Фильтрация путей, ведущих к любой папке или файлу на разделе с буквой C |
| myName | Фильтрация папки или файла с именем myName |
| \myFolder\ | Фильтрация папки с именем myFolder |

Модули мониторинга разделов, криптографа, API и вирусной базы сигнатур в своём составе имеют только 1 именованный канал, предназначенный для приёма команд.

В таблице 2.2.6.5 приведено описание доступных команд модуля мониторинга разделов.

Таблица 2.2.6.5 – Описание команд модуля мониторинга разделов

|  |  |  |
| --- | --- | --- |
| Идентификатор команды | Передаваемые параметры | Назначение команды |
| 0 | Строка (путь к папке или накопителю) | Создать монитор изменений папки или раздела |
| 1 | Удалить монитор изменений папки или раздела |
| 2 | Ничего | Включить автопроверку съемных носителей |
| 3 | Выключить автопроверку съемных носителей |
| 4 | Очистить буфер информации о подключенных съемных носителях |
| 5 | Приостановить мониторинг разделов и съемных носителей |
| 6 | Активировать мониторинг разделов и съемных носителей |
| 7 | Выключить модуль |

В таблице 2.2.6.6 приведено описание доступных команд модуля локальной базы вирусных сигнатур. Модуль локальной базы сигнатур единственный из всех модулей, команды в который передаются в текстовом виде.

Таблица 2.2.6.6 – Описание команд локальной базы сигнатур

|  |  |
| --- | --- |
| Команда | Назначение команды |
| /reinit\_db | Перезагрузить всю информацию о вирусах |
| /upload\_to\_scanner | Выгрузить все сигнатуры в модуль сканнера |
| /shutdown | Выключить модуль |

В таблице 2.2.6.2 приведено описание входных именованных каналов модуля сканнера.

Таблица 2.2.6.2 – Описание входных именованных каналов сканнера

|  |  |
| --- | --- |
| Именованный канал | Назначение |
| Scanner.CommandPipe | Канал для команд |
| ScannerService.Input | Канал для приёма путей к сканируемым файлам |
| ScannerService.Signatures | Канал для приёма сигнатур вирусов от модуля базы сигнатур |

Для сканнера доступны только 2 команды, которые имеют идентификаторы 0 и 1. Первая команда позволяет очистить локальный буфер задач сканирования. Вторая команда позволяет отключить модуль.

2.2.7 Выходные данные

Выходные данные в модулях передаются так же, как и входные ­– с помощью именованных каналов

В таблице 2.2.7.1 приведено описание выходных именованных каналов.

Таблица 2.2.7.1 – Описание выходных именованных каналов

|  |  |  |
| --- | --- | --- |
| Наименование модуля | Наименование канала | Назначение |
| Filter | Filter.Output | Канал для передачи файлов для проверки |
| ScannerService | ScannerService.Output | Канал для передачи проверенных файлов |
| Cryptographer | Crypto.Data | Канал для передачи данных о процессе шифровки или расшифровки |
| API | API.User | Канал для передачи данных событий |
| API Monitor | API MON FILTER | Канал для отправки путей к файлам |
| VirusesDB | ScannerService.Signatures | Канал для передачи сигнатур в модуль сканнера |

В таблице 2.2.7.2 приведено описание данных, которые могут быть переданы по каналу API.User

Таблица 2.2.7.2 – Описание выходных данных

|  |  |  |
| --- | --- | --- |
| Идентификатор | Назначение | Выходные данные |
| 0 | Путь к просканированному файлу | Строка пути к файлу |
| 1 | Путь к найденному вирусу | Путь к файлу, системный идентификатор, идентификатор вируса |
| 2 | Полная информация о найденном вирусе | Системный идентификатор, путь к файлу, идентификатор вируса, флаг нахождения в карантине, путь к файлу в карантине |

2.2.8 Рекомендации по использованию

Программное средство запускается автоматически при загрузке системы. По умолчанию главная форма скрыта, чтобы её открыть необходимо сделать двойной щелчок по иконке в трее либо открыть контекстное меню и нажать на кнопку Открыть (рисунок 2.2.8.1)

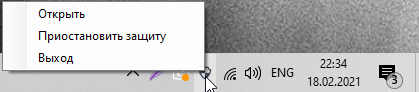


Рисунок 2.2.8.1 – Контекстное меню иконки

На рисунке 2.2.8.2 изображено главное окно программы

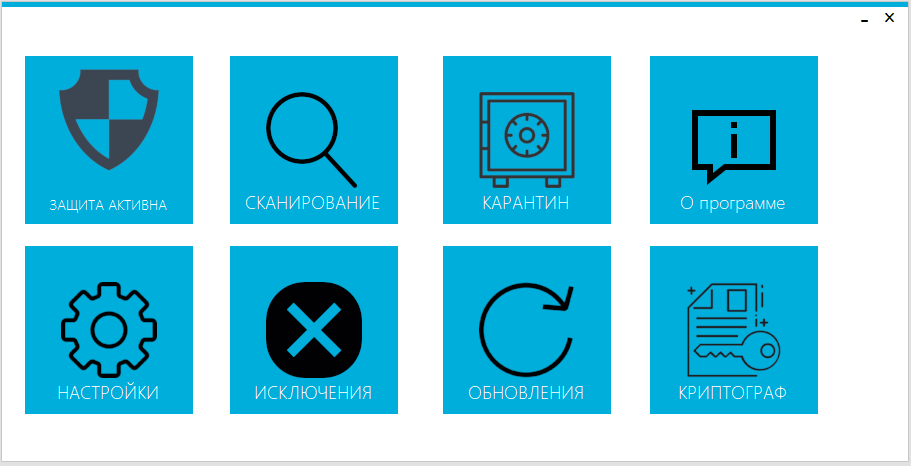


Рисунок 2.2.8.2 – Главное окно

При нажатии на кнопку «Сканирование» открывается окно настроек ручного сканирования.

При нажатии на кнопку «Настройки» открывается окно настроек программного средства.

При нажатии на кнопку «Карантин» открывается окно обозревателя карантина, в котором можно просмотреть файлы, находящиеся в карантине.

При нажатии на кнопку «Исключения» открывается окно настройки исключаемых из сканирования файлов и папок.

При нажатии на кнопку «Обновления» открывается окно, в котором можно просмотреть версию программного средства и вирусной базы сигнатур.

На рисунке 2.2.8.3 изображено окно настроек сканирования.

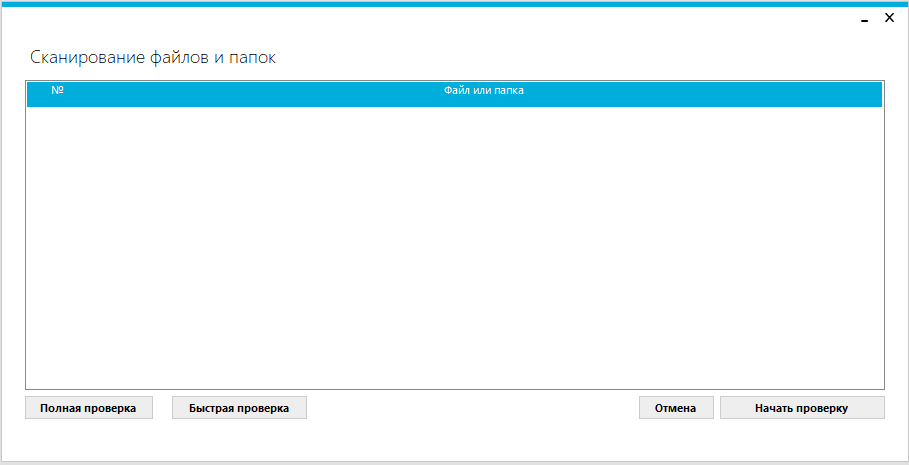


Рисунок 2.2.8.3 – Окно настроек сканирования

На форме расположены 4 кнопки:

* «Полная проверка», при нажатии на которую запускается процесс проверки всех файлов на всех разделах доступных жестких дисков;
* «Быстрая проверка», запускает проверку только исполняемых файлов на всех разделах доступных жестких дисков, за исключением системного раздела;
* «Отмена», возвращает на главную страницу;
* «Начать проверку», запускает проверку файлов.

Папки и файлы, которые необходимо проверить отображаются в списке. Проверяемые файлы и папки добавляются в список через контекстное меню (рисунок 2.2.8.4).

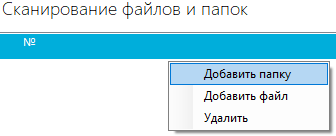


Рисунок 2.2.8.4 – Контекстное меню списка объектов сканирования

После старта сканирования открывается окно, на котором отображается ход сканирования (рисунок 2.2.8.5).

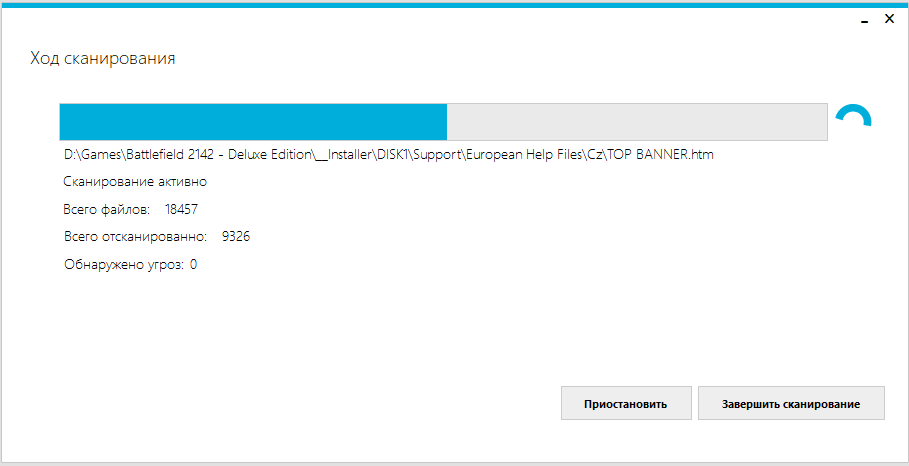


Рисунок 2.2.8.5 – Ход сканирования

На форме располагается 2 кнопки:

* «Приостановить», при нажатии на которую процесс сканирования будет приостановлен (но файлы, которые уже были поставлены в очередь на сканирование, будут просканированы вне зависимости от приостановки);
* «Завершить сканирование», при нажатии на которую сканирование будет завершено.

После того, как все файлы будут проверены, откроется окно с результатами сканирования (рисунок 2.2.8.6).

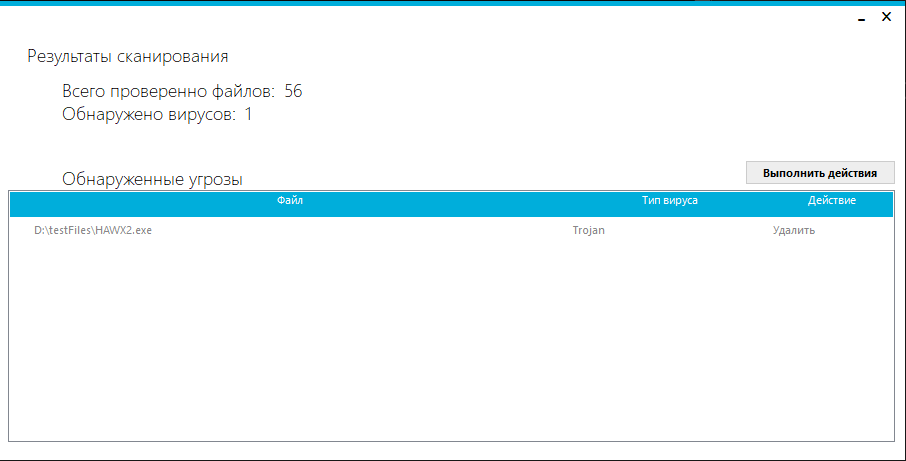


Рисунок 2.2.8.6 – Результат сканирования

В таблице расположена информация об обнаруженных вирусах (путь к файлу, тип вируса, осуществляемое действие). По умолчанию ко всем вирусам применяется удаление. Изменить действие можно через контекстное меню (рисунок 2.2.8.7).

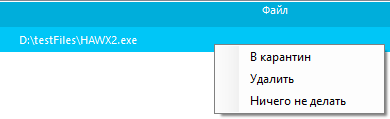


Рисунок 2.2.8.7 – Контекстное меню выбора действия

Все помещенные в карантин вирусы можно просмотреть в окне обозревателя карантина (рисунок 2.2.8.8).

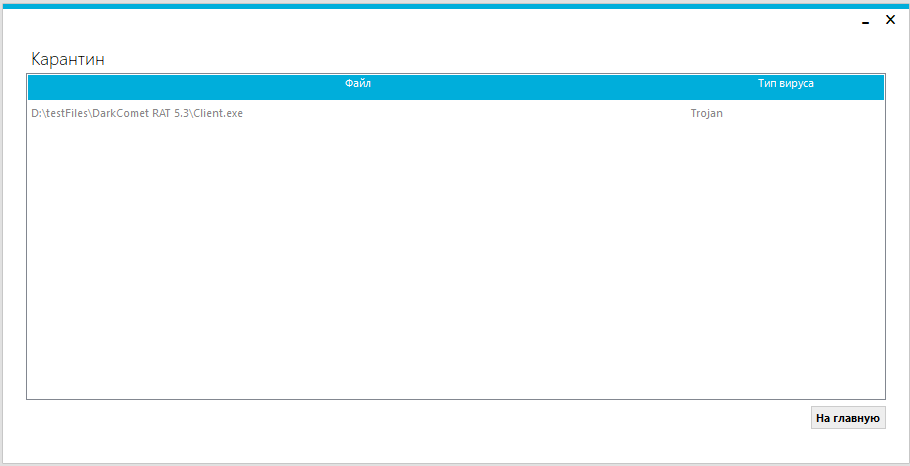


Рисунок 2.2.8.8 – Обозреватель карантина

Файлы, находящиеся в карантине, можно либо восстановить, либо удалить. Все действия осуществляются через контекстное меню (рисунок 2.2.8.9).

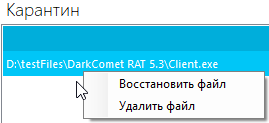


Рисунок 2.2.8.9 – Выбор действия над файлом в карантине

Находящийся в карантине файл можно либо восстановить, либо удалить.

На рисунке 2.2.8.10 изображена форма настроек. На форме настроек можно включить или выключить уведомления, автоматическую проверку съемных носителей (например флэш-накопителей) или установить действие, применяемое к обнаруженным вирусам по умолчанию.

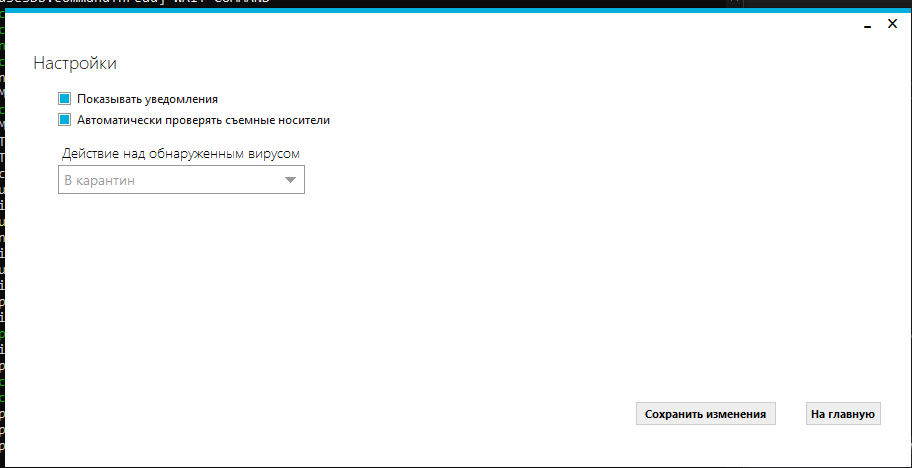


Рисунок 2.2.8.10 – Форма настроек

Для редактирования базы сигнатур существует утилита DBEditor. На рисунке 2.2.8.11 представлено главное окно редактора базы сигнатур.

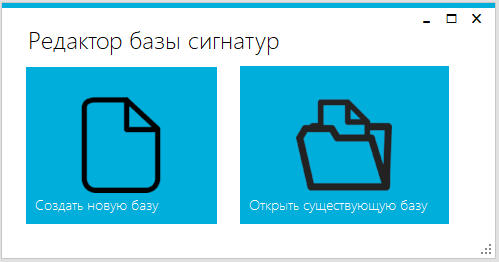


Рисунок 2.2.8.11 – Главное окно редактора сигнатур

После создания или открытия базы сигнатур появляется окно редактора. В таблице редактора отображается таблица, в которой есть 3 колонки, в которых отображается наименование вируса, его сигнатура и тип. На рисунке 2.2.8.12 изображено окно редактора.

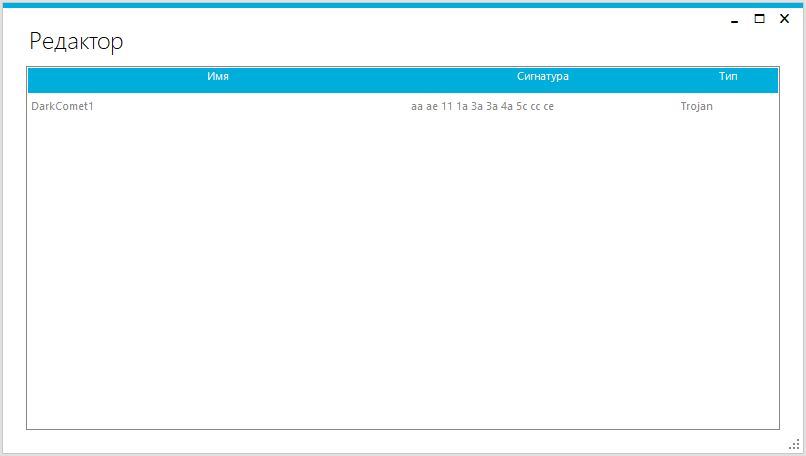


Рисунок 2.2.8.12 – Окно редактора

Добавление удаление и редактирование информации о вирусах в базе сигнатур производится через контекстное меню (рисунок 2.2.8.13).

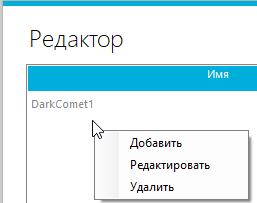


Рисунок 2.2.8.13 – Контекстное меню таблицы редактора

На рисунке 2.2.8.14 изображено окно добавления и редактирования информации о вирусе. Информацию о вирусе представляет собой:

* тип вируса;
* наименование вируса;
* сигнатура вируса, представляющая собой последовательность байт (на форме байты вводятся в виде шестнадцатеричной системы счисления).

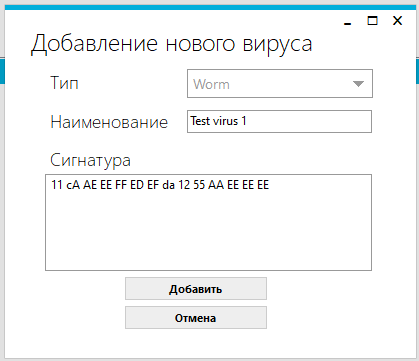


Рисунок 2.2.8.14 – Форма добавления и редактирования информации о вирусе

Шестнадцатеричная система включает в себя цифры от 0 до 10, а также буквы от A до F. Если не заполнить какое либо поле, либо ввести некорректную сигнатуру, то будет выдано соответствующее сообщение об ошибке (рисунок 2.2.8.15).

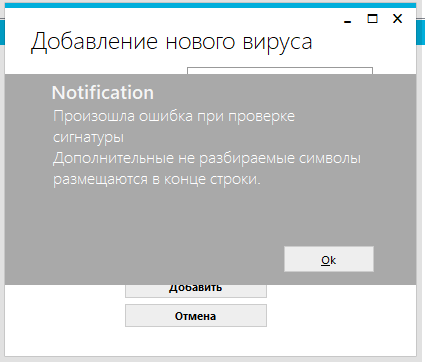


Рисунок 2.2.8.15 – Сообщение с ошибкой

Для сохранения всех изменений в базе, необходимо нажать на кнопку «Применить все изменения», которая появляется слева вверху.

3 Экономический раздел

<вступительный текст>

План разработки программного продукта представлен в таблице 3.1.1.

Таблица 3.1.1 – План разработки программного продукта

|  |  |
| --- | --- |
| Наименование этапов и видов работ | Трудоемкость, человеко-дни |
| Подготовительный этап – разработка и утверждение технического задания:  а) составление календарного графика работ | 2  1 |
| б) подбор и изучение литературы по теме | 1 |
| Изучение предметной области: | 3 |
| а) изучение аналогов | 1 |
| б) изучение основных понятий и объектов предметной области | 2 |
| Проектирование программного средства: | 3 |
| а) определение требований | 1 |
| б) определение логической структуры | 2 |
| Разработка программного средства | 7 |
| Тестирование и испытания | 1 |
| Внесение корректировок | 2 |
| Всего | 18 |

Месячная тарифная ставка каждого исполнителя определяется путем умножения действующей месячной тарифной ставки 1-го разряда на тарифный коэффициент, соответствующий установленному тарифному разряду (3.1.1).

МТСnр = МТС1р \* Кnр, (3.1.1)

где МТСnр – тарифная ставка за месяц n-го разряда, руб.;

МТС1р – тарифная ставка 1-го разряда за месяц, руб. (в 2021 г.);

Кnр – тарифный коэффициент n-го разряда.

МТС8р= 41 \* 2,17 = 88,97 руб.

Дневная тарифная ставка n-го разряда определяется делением месячной тарифной ставки n-го разряда на месячный норматив рабочего времени в часах и умножением на продолжительность рабочего дня в часах (3.1.2).

ДТСnр= \* 8, (3.1.2)

где МТСnр – тарифная ставка за месяц n-го разряда, руб.;

169.2 – месячный норматив рабочего времени, часы, (2021 г.).

ДТС8р= \* 8 = 4,20 руб.

Основная заработная плата исполнителей на конкретное ПС рассчитывается по формуле (3.1.3).

ЗПо = ДТСnр \* То \* Кпр, (3.1.3)

где ЗПо – основная заработная плата, руб.;

ДТСnр – тарифная ставка за день, руб.;

То – общая трудоемкость ПС, человеко-дней;

Кпр – коэффициент премирования (1,1 – 1,3).

ЗПо = 4,20 \* 18 \* 1,3 = 98,28 руб.

Дополнительная заработная плата на конкретное ПС включает выплаты, предусмотренные законодательством о труде (выплат, не связанных с основной деятельностью исполнителей), и определяется по нормативу в процентах к основной заработной плате (3.1.4).

Ндзп ≈ от 10 до 25%

ЗПд = , (3.1.4)

где ЗПд – дополнительная заработная плата на конкретное ПС, руб.;

Ндзп – норматив дополнительной заработной платы, %.

ЗПд = = 14,74 руб.

Отчисления в Фонд социальной защиты населения (ФСЗН) определяются в соответствии с действующими законодательными актами по нормативу в процентном отношении к фонду основной и дополнительной зарплаты исполнителей (3.1.5).

Офсзн = , (3.1.5)

где Офсзн – отчисления в Фонд социальной защиты населения, руб.;

Нфсзн – норматив отчислений в Фонд социальной защиты населения (34%).

Офсзн = = 38,42 руб.

Отчисления по обязательному страхованию от несчастных случаев на производстве и профессиональных заболеваний определяются в соответствии с действующими законодательными актами в зависимости от уровня риска отрасли, к которой относится организация-разработчик (3.1.1.6).

, (3.1.6)

где Обгс – отчисления по обязательному страхованию от несчастных случаев на производстве и профессиональных заболеваний, руб.;

Нбгс – норматив отчислений по обязательному страхованию от несчастных случаев на производстве и профессиональных заболеваний (0,6%).

Обгс = = 0,67 руб.

Расходы на материалы определяются с учетом действующих нормативов. По данной статье отражаются расходы на покупные полуфабрикаты и комплектующие изделия, необходимые для разработки ПС. Расчет целесообразно представить в табличной форме (таблица 3.1.2).

Таблица 3.1.2 – Расчет затрат на материалы, покупные полуфабрикаты и комплектующие изделия

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование материалов покупных полуфабрикатов и комплектующих изделий | Единица измерения | Количество | Цена приобретения, руб. | Сумма, руб. |
| Брошюрирование | шт. | 1 | 3,46 | 3,46 |
| Лист | блок | 0,5 | 8,00 | 4,00 |
| Диск | шт. | 1 | 2,75 | 2,75 |
| Конверт | шт. | 1 | 1,5 | 1,5 |
| Всего расходов | | | | 11,71 |

При создании ПП компьютер является неотъемлемым атрибутом. Такая техника имеет свои отличия в комплектации и мощности. От этих параметров и зависит общий расход электроэнергии. Как правило, чем мощнее ПК, тем больше киловатт он потребляет

В основном компьютер со средней мощностью потребляет от 250 до 350 ватт в час (0,25 – 0,35 кВт/ч). Более мощный процессор может потреблять до 450 ватт в час (0,45 кВт/ч). Расчет можно произвести по формуле 3.1.7

, (3.1.7)

где – установочная мощность i-го объекта основных производственных фондов, используемых для выполнения работ по данной теме, кВт;

– время фактического использования i-го объекта, ч;

– тариф за 1 кВт/ч энергии, руб., тариф уточняется в бухгалтерии предприятия (таблица 3.1.3).

руб.

Таблица 3.1.3 – Расчет затрат на топливно-энергетические ресурсы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование оборудования, используемого для научно-экспериментальных и технологических целей | Установочная мощность, кВт | Время использования, ч | Тариф за 1 кВт/ч | Сумма затрат, руб. |
| Персональный компьютер | 0,40 | 176 | 0,3777 | 26,59 |
| Всего затрат | | | | 26,59 |

Определяются прочие прямые расходы, связанные с амортизационными отчислениями на полное восстановление основных производственных фондов, арендная плата и лизинговые платежи, компенсация за износ (амортизацию) использованного в процессе создания научно-технической продукции оборудования по договоренности (4.8).

Рпр = ЗПо , (3.1.8)

где Нпр – норматив прямых расходов, Нпр ≈ от 10 до 20%.

Рпр = руб.

В процессе использования ОС изнашиваются и переносят свою стоимость по частям на изготавливаемую продукцию (3.1.9).

Ао = , (3.1.9)

где Ао – амортизационные отчисления, руб.;

– первоначальная стоимость объекта, руб.;

t – срок полезного использования.

Ао(год) = руб.

Ао(мес)  руб.

Данные затраты, связанные с необходимостью содержания аппарата управления, а также с расходами на общехозяйственные нужды, относятся на конкретное ПС по нормативу в процентном отношении к основной заработной плате исполнителей (3.1.10).

Рнр = , (3.1.10)

где Рнр – расчет накладных расходов, руб.;

Ннр – норматив накладных расходов по организации (≈ от 25 до 50%).

Рнр = руб.

Общая сумма расходов на ПС рассчитывается по формуле 3.1.11

Cп = ЗПо + ЗПд + Офсзн + Обгс + См + Рэл + Рпр + Ао + Рнр (3.1.11)

где Сп – сумма расходов на разработку программного средства, руб.;

ЗПо – основная заработная плата, руб.;

ЗПд – дополнительная заработная плата на программное средство, руб.;

Офсзн – отчисления в Фонд социальной защиты населения, руб.;

Обгс – отчисления по обязательному страхованию от несчастных случаев на производстве и профессиональных заболеваний, руб.;

См – сумма расходов на материалы, руб.;

Рэл – расчет стоимости топливно-энергетических ресурсов, руб.;

Рпр – расчет прочих прямых затрат, руб.;

Ао – амортизационные отчисления, руб.;

Рнр – расчет накладных расходов, руб.

Cп = 98,28 +14,74 +38,42 + 0,67 + 11,71+ 26,59 + 14,74 + 29,16 +24,57 = 258,88 руб.

По среднему уровню рентабельности в процентах от полной себестоимости определяется плановая прибыль ПС (3.1.12).

П = Сп, (3.1.12)

где Ур - средний уровень рентабельности, Ур от 10 до 30%.

П 77,66

Определяется приближенная (ориентировочная) отпускная цена ПС по формуле 3.1.13.1.

Цотп = Сп + П, (3.1.13)

Цотп = 258,88 + 77,66 = 336,54

По темам, выполняемым за счет внебюджетных средств (собственных средств, средств других предприятий и организаций, предпринимателей), определяется налог на добавленную стоимость по формуле 3.1.14.

НДС = Цотп , (3.1.14)

где Нндс – ставка налога (НДС), Нндс = 20%.

НДС 67,30

Отпускная цена определяется на основании цены разработчика, которая формируется на основе показателя рентабельности продукции. Рентабельность и прибыль по создаваемому ПС определяются исходя из результатов анализа рыночных условий, переговоров с заказчиком (потребителем) и согласования с ним отпускной цены, включающей налог на добавленную стоимость (3.1.15).

Цотп = Цотп + НДС, (3.1.15)

Цотп =336,54 + 67,30 = 403,84

Все приведенные выше расчеты представлены в сводной таблице 3.1.4.

Таблица 3.1.4 – Расчет ориентировочной цены ПС

|  |  |  |
| --- | --- | --- |
| Статьи затрат | Условные обозначения | Сумма, руб. |
| 1. Основная заработная плата | ЗПо | 98,28 |
| 2. Дополнительная заработная плата | ЗПд | 14,74 |
| 3. Отчисления в ФСЗН | Офсзн | 38,42 |
| 4.Отчисления по обязательному страхованию от несчастных случаев на производстве | Обгс | 0,67 |
| 5. Материалы, покупные полуфабрикаты и комплектующие изделия | См | 14,75 |
| 6. Топливно-энергетические ресурсы для научно-экспериментальных целей | Рэл | 26,59 |
| 7. Прочие прямые расходы | Рпр | 14,74 |
| 8. Амортизационные отчисления | Ао | 29,16 |
| 9. Накладные расходы | Рнр | 24,57 |
| 10. Полная себестоимость | Cп | 258,88 |
| 11. Плановые накопления (прибыль) | П | 77,66 |
| 12. Отпускная цена (без НДС) | Цотп | 336,54 |
| 13.1. Налог на добавленную стоимость | НДС | 67,30 |
| 14. Отпускная цена с НДС | Цотп | 403,84 |

Вывод: Отпускная стоимость ПС с НДС составила 408,60 руб.

**4** Охрана труда

4.1 Характеристика трудовой деятельности и факторов среды при работе оператора

В процессе работы на оператора могут воздействовать следующие опасные и вредные производственные факторы:

– движущиеся машины и механизмы;

– подвижные части производственного оборудования;

‒ повышенная запыленность воздуха рабочей зоны;

‒ повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека;

‒ повышенная или пониженная температура воздуха рабочей зоны;

‒ пониженная или повышенная влажность воздуха рабочей зоны;

‒ повышенный уровень шума на рабочем месте;

‒ повышенная или пониженная ионизация воздуха;

‒ повышенный уровень ионизирующих излучений;

‒ повышенный уровень статического электричества;

‒ повышенный уровень электромагнитного излучения;

‒ повышенная напряженность электромагнитного поля;

‒ повышенная напряженность электростатического поля;

‒ повышенная яркость света;

‒ прямая и отраженная блескость;

‒ статические перегрузки костно-мышечного аппарата и динамические локальные перегрузки мышц кистей рук;

‒ перенапряжение зрительного анализатора;

‒ умственное перенапряжение;

‒ монотонность труда;

‒ эмоциональные перегрузки.

Производственная (рабочая) среда включает в себя все, что окружает человека в процессе трудовой деятельности: техническое оснащение организации, особенности технологических процессов и производства, состояние зданий, строений, сооружений и инженерных коммуникаций, санитарно-гигиеническую и эстетическую обстановку, взаимоотношения в трудовом коллективе, уровень профессионального риска исходя из идентифицированных опасных и вредных производственных факторов и пр.

Производственные факторы делят на 2 типа: вредные и опасные. Вредный производственный фактор – это производственный фактор, воздействие которого на работника может привести его к заболеванию. Опасный производственный фактор – это производственный фактор, воздействие которого на работника может привести к его травме.

Оператор должен быть обеспечен средствами индивидуальной защиты в соответствии с типовыми отраслевыми нормами бесплатной выдачи средств индивидуальной защиты работникам связи, утвержденными постановлением Министерства труда и социальной защиты Республики Беларусь от 4 мая 2005 г. № 51 (Национальный реестр правовых актов Республики Беларусь, 2005 г., № 75, 8/12561).

4.2 Организация общественного контроля условий и безопасности труда

Целью общественного контроля условий и безопасности труда является усиление профилактической работы по предупреждению травматизма, нарушений правил, норм и инструкций по охране труда, соблюдение требований трудового законодательства и законных интересов работников, а также повышение персональной ответственности руководителей подразделений и непосредственных исполнителей за безопасное выполнение работ.

**Основными видами контроля за состоянием охраны труда в организациях являются:**

**– оперативный контроль руководителя работ и других должностных лиц;**

– административно–общественный контроль;

– контроль, осуществляемый службой охраны труда.

Трехступенчатый административно-общественный контроль является основной формой совместного контроля администрации образовательного учреждения и профсоюзной организации, комиссии по охране труда за состоянием условий и безопасности труда на рабочих местах в структурных подразделениях, а также за соблюдением всеми работниками требований трудового законодательства, стандартов безопасности труда, правил, норм, инструкций и других нормативно-технических документов по охране труда и пожарной безопасности.

Целью трехступенчатого контроля является усиление профилактической работы по предупреждению травматизма, нарушений правил, норм и инструкций по охране труда, соблюдение требований трудового законодательства и законных интересов работников, а также повышение персональной ответственности руководителей подразделений и непосредственных исполнителей за безопасное выполнение работ.

Руководство организацией трехступенчатого контроля осуществляет ректор и председатель первичной профсоюзной организации сотрудников образовательного учреждения.

Первая ступень контроля осуществляется руководителем структурного подразделения. На первой ступени контроля проверяется:

– выполнение мероприятий по устранению нарушений, выявленных предыдущей проверкой;

– состояние и правильность организации охраны труда и техники безопасности на рабочих местах;

– безопасность технологического оборудования, исправность ограждений, инструмента;

– эффективность работы вентиляции и температурный режим в помещениях и на рабочих местах;

– наличие и состояние спецодежды;

– наличие и исправность средств индивидуальной защиты;

– наличие и комплектность аптечек;

– наличие средств пожаротушения;

– санитарное и противопожарное состояние территории;

– наличие инструкций по охране труда на отдельные виды работ и по профессиям на рабочих местах;

– наличие в подразделении уголка по охране труда, наглядной агитации по охране труда и пожарной охране;

– своевременность и качество проведения обучения и инструктажа работников по охране труда;

– прохождение предварительных и периодических медицинских осмотров;

– соблюдение правил хранения материалов, оборудования, реактивов, пожаро и взрывоопасных веществ;

– соблюдение трудового законодательства (в частности, особенности регулирования труда несовершеннолетних, женщин и других категорий работников);

– состояние проходов, переходов, проездов и свободный доступ к средствам защиты;

– соблюдение правил при выполнении газоопасных и огневых работ, требований пожарной безопасности;

– соблюдение работающими правил электробезопасности при работе на электроустановках, с электроинструментом, на электрифицированном станочном оборудовании;

– соблюдение правил складирования материалов;

– исправность приточной и вытяжной вентиляции, местных отсосов, пыле– и газоулавливающих устройств;

– соблюдение правил безопасности при работе с вредными и пожароопасными веществами и материалами;

– наличие у работающих удостоверений, нарядов–допусков на выполнение работ с повышенной опасностью;

– чистота и порядок на рабочих местах;

– освещенность рабочих мест.

Устранение выявленных нарушений должно проводиться незамедлительно под непосредственным надзором руководителя структурного подразделения. Если недостатки, выявленные проверкой, не могут быть устранены силами работников подразделения, то руководитель структурного подразделения должен по окончании осмотра доложить об этом вышестоящему руководителю (директору, декану, проректору) для принятия соответствующих мер. В случае грубого нарушения правил, норм, инструкций по охране труда, которое может причинить ущерб здоровью работающих или привести к аварии, работа приостанавливается до устранения этого нарушения.

Результаты проверки записываются в журнале административно-общественного контроля, который хранится у руководителя структурного подразделения. По выявленным недостаткам и нарушениям, которые невозможно устранить незамедлительно, намечаются мероприятия по их устранению, определяются сроки и ответственные лица.

Руководитель структурного подразделения и уполномоченное лицо по охране труда информируют свои коллективы о нарушениях, выявленных в результате проверки на первой ступени контроля и о принятых мерах на собраниях коллектива.

Вторая ступень контроля проводится ежеквартально комиссией, возглавляемой деканом факультета, начальником управления и т.п. и уполномоченным по охране труда.

График проверки устанавливается руководителем структурного подразделения и вносится в план работы по охране труда.

На второй ступени контроля проверяются:

– организация и результаты работы первой ступени контроля;

– выполнение мероприятий, намеченных в результате проведения второй ступени контроля;

– выполнение приказов и распоряжений ректора, решений первичной профсоюзной организации, решений комиссий по охране труда, представлений уполномоченного лица по охране труда;

– выполнение мероприятий по материалам расследования несчастных случаев;

– выполнение мероприятий по предписаниям и указаниям органов надзора и контроля;

– размещение установок, стендов, оборудования в соответствии с правилами и нормами по охране труда и производственной санитарии;

– наличие и состояние защитных, сигнальных и противопожарных средств и устройств, контрольно-измерительных приборов;

– проведение в помещениях анализов воздушной среды на содержание токсичных газов, паров, пыли;

– проведение первичного инструктажа с каждым вновь поступающим на работу, а также в установленные сроки повторного инструктажа по охране труда с работниками;

– проверка знаний (выборочно) правил, инструкций по охране труда и пожарной безопасности работников;

– состояние уголков по охране труда, наличие и состояние плакатов по охране труда, сигнальных цветов и знаков безопасности;

– своевременность выдачи работникам и студентам соответствующей спецодежды, спецобуви и средств индивидуальной защиты;

– состояние санитарно-бытовых помещений и устройств;

– соблюдение установленного режима труда и отдыха, трудовой дисциплины.

Результаты проверки записываются в специальный журнал второй ступени контроля. При этом комиссия намечает мероприятия по устранению нарушений, назначает исполнителей и сроки исполнения. Если намеченные мероприятия, не могут быть устранены силами подразделения, то руководитель подразделения по окончании работы комиссии обязан доложить об этом вышестоящему руководителю (устно или служебной запиской) для принятия соответствующих мер. В случае грубого нарушения правил, норм, инструкций по охране труда, которое может причинить ущерб здоровью работающих или привести к аварии, работа приостанавливается до устранения этого нарушения. Контроль за выполнением этих мероприятий осуществляют уполномоченный по охране труда и инженер по охране труда и технике безопасности.

Руководитель подразделения обеспечивает выполнение мероприятий по устранению недостатков и нарушений по охране труда, выявленных комиссией второй ступени контроля.

Ежеквартально на собраниях подразделения руководитель и уполномоченный по охране труда информирует свой коллектив о состоянии охраны труда и техники безопасности, о ходе мероприятий, намеченных комиссией второй ступени контроля и мерах по устранению выявленных недостатков с принятием соответствующего решения в протоколе.

Третья ступень контроля проводится комиссией по охране труда, возглавляемой ректором (проректором по организационно–правовым вопросам) не реже 1 раза в год.

 В состав комиссии входят представители администрации, технических служб, работники служб охраны труда и пожарной безопасности, председатель первичной профсоюзной организации сотрудников, уполномоченные по охране труда.

На третьей ступени контроля рекомендуется проверять:

– организацию и результаты работы первой и второй ступени контроля;

– выполнение мероприятий, намеченных в результате проведения третьей ступени контроля;

– выполнение приказов и распоряжений вышестоящих органов контроля;

– выполнение мероприятий, предусмотренных коллективным договором, соглашениями по охране труда и другими документами;

– выполнение мероприятий по материалам расследования несчастных случаев и аварий;

– состояние и содержание зданий и сооружений, прилегающей территории в соответствии с нормативными требованиями по охране труда, состояние проезжей и пешеходной части дорог, переходов;

– соответствие технологического, грузоподъемного, транспортного и другого оборудования требованиям безопасности труда;

– исправность приточной и вытяжной вентиляции, пыле и газоулавливающих устройств;

– выполнение графиков планово–предупредительного ремонта оборудования;

– обеспечение работающих спецодеждой, спецобувью и другими средствами индивидуальной защиты, правильность их выдачи, учета, хранения;

– обеспеченность работников санитарно–бытовыми помещениями;

– своевременность и качество проведения обучения и инструктажей работников по безопасности труда;

– соблюдение установленного режима труда и отдыха, трудовой дисциплины;

– соблюдение правил внутреннего трудового распорядка работниками;

– наличие несчастных случаев на производстве (какая профилактическая работа проведена).

Результаты проверки записываются в журнал контроля, оформляются актом (копии или выписки из которого направляются в проверенное подразделение) и в недельный срок обсуждаются на совместном заседании ректората, президиума профкома или на заседании совместной комиссии по охране труда. На ректорате заслушиваются руководители тех подразделений, где выявлено неудовлетворительное состояние условий труда, допускаются нарушения правил, норм и инструкций по охране труда. Проведение заседаний оформляется протоколом с указанием мероприятий по устранению выявленных недостатков и нарушений, сроков исполнения и ответственных лиц. В необходимых случаях ректор издает приказ.

4.3 Общественный контроль за состоянием охраны труда на объекте при проектируемой деятельности

Согласно пункту 3 Указа Президента Республики Беларусь от 16 октября 2009 г. № 510 «О совершенствовании контрольной (надзорной) деятельности в Республике Беларусь» общественный контроль в форме проведения проверок вправе осуществлять только профсоюзы, их организационные структуры, объединения таких союзов и их организационные структуры в случаях и порядке, установленных законодательными актами.

Осуществление общественного контроля в форме проведения проверок другими организациями, а также физическими лицами не предусмотрено.

В развитие Указа № 510 принят Указ Президента Республики Беларусь от 6 мая 2010 г. № 240 «Об осуществлении общественного контроля профессиональными союзами» (далее – Указ № 240).

Виды общественного контроля, право на осуществление которого предоставлено профсоюзам, установлены Законом Республики Беларусь от 22 апреля 1992 года № 1605-ХП «О профессиональных союзах» (в редакции от 14 января 2000 года № 371-3), который в частности устанавливает, что профсоюзы вправе осуществлять общественный контроль за:

– соблюдением законодательства Республики Беларусь об охране труда в порядке, установленном законодательством;

– выполнением коллективного договора (соглашения);

– деятельностью организаций здравоохранения в области охраны здоровья;

– соблюдением нанимателем, собственником или уполномоченным им органом управления законодательства Республики Беларусь о труде;

– соблюдением нанимателем, собственником или уполномоченным им органом управления законодательства Республики Беларусь о профсоюзах.

Указом № 240 профсоюзам предоставлено право на осуществление и иных видов общественного контроля в форме мероприятий по наблюдению, анализу, оценке соблюдения требований законодательства по обеспечению трудовых и социально-экономических прав граждан (мониторинг), участия в работе коллегиальных органов, комиссий и иных предусмотренных законодательством, коллективными договорами (соглашениями) формах.

При этом все виды общественного контроля профсоюзами будут осуществляться не в форме проведения проверок.

Целью контроля за соблюдением законодательства об охране труда является создание здоровых и безопасных условий труда работников, предупреждение несчастных случаев на производстве и профессиональных заболеваний. Контроль осуществляться в форме проверок, обследований, характеризующих состояние условий и охраны труда, рассмотрения жалоб, заявлений и предусматривает выявление причин нарушений требований охраны труда и как следствие разработку мероприятий по их устранению и предупреждению.

Основными видами контроля являются:

– контроль за соблюдением законодательства об охране труда, осуществляемый руководителями и специалистами организации в соответствии с их должностными обязанностями;

– контроль по охране труда, осуществляемый службой охраны труда: производственный контроль за соблюдением требований промышленной безопасности на опасных производственных объектах, осуществляемый инспектирующих их организацией; периодический контроль за соблюдением законодательства об охране труда, осуществляемый руководителями структурных подразделений организаций с участием общественных инспекторов профсоюза по охране труда (уполномоченных лиц по охране труда работников); общественный контроль за соблюдением законодательства об охране труда, осуществляемый профсоюзом.

Па основе типовой инструкции в организациях с учетом характера их деятельности разрабатываются локальные нормативные правовые акты, регламентирующие проведение контроля за соблюдением законодательства об охране труда. Полномочия и ответственность руководителей и специалистов организации по осуществлению контроля за соблюдением законодательства об охране труда определяются их должностными инструкциями. Руководители и специалисты организаций осуществляют контроль за соблюдением актов законодательства о труде и охране труда, локальных нормативных правовых актов по охране труда: выполнением работниками функциональных обязанностей по охране труда: выполнением    постановлений, приказов, предписаний органов государственного надзора и контроля, вышестоящей организации, представлений технической инспекции труда профсоюза: мероприятий по улучшению условий и охраны труда, предусмотренных программами, планами, коллективными договорами, планами мероприятий по охране труда и т. д.

Периодический контроль за соблюдением законодательства об охране труда осуществляется руководителями структурных подразделений (производственных участков, цехов и т. д.) с участием общественных инспекторов профсоюза по охране труда. При отсутствии в организации профсоюза, с согласия руководителя организации для участия в проведении периодического контроля, могут привлекаться уполномоченные. Периодический контроль, осуществляемый руководителями структурных подразделений, проводится:

– ежедневно на участке в смене, лаборатории и иных аналогичных структурных подразделениях организации;

– ежемесячно в цехе, отделе, иных аналогичных структурных подразделениях организации: ежеквартально – в организации в целом (ежедневный контроль за состоянием охраны труда осуществляется руководителем структурного подразделения с участием общественного инспектора профсоюза по охране труда (уполномоченного лица но охране труда работников) в начале рабочего дня (смены).

Ежедневно проверяются:

– состояние территории, проходов, проездов;

– состояние и правильность организации рабочих мест;

– безопасность технологического оборудования, оснастки и инструмента, грузоподъемных и транспортных средств;

– наличие и правильное использование работающими средств индивидуальной защиты;

– соблюдение работниками требований безопасности при выполнении работ и т. д.

Результаты проверки с конкретными мероприятиями по устранению выявленных недостатков и нарушений записываются в журнал ежедневного контроля за состоянием охраны труда, установленной формы.

Ежемесячный контроль проводится начальником цеха с участием общественного инспектора профсоюза по охране груда (уполномоченного лица по охране труда работников), руководителей служб цеха и представителей службы охраны труда (инженера по охране труда).

Про­из­вод­ст­вен­ный кон­троль – кон­троль, обес­пе­чи­вае­мый производите­лем про­дук­ции (то­ва­ров), ра­бот и ус­луг, за со­блю­де­ни­ем требова­ний са­ни­тар­но-эпи­де­мио­ло­ги­че­ско­го за­ко­но­да­тель­ст­ва и выполнени­ем са­ни­тар­но-про­ти­во­эпи­де­ми­че­ских и про­фи­лак­ти­че­ских мероприятий, на­прав­лен­ный на со­хра­не­ние жиз­ни и здо­ро­вья лю­дей, сре­ды оби­та­ния при про­из­вод­ст­ве про­дук­ции (то­ва­ров), вы­пол­не­нии ра­бот и услуг.

Вход­ной кон­троль – кон­троль сы­рья и (или) про­дук­ции, по­сту­пив­ших к по­тре­би­те­лю или за­каз­чи­ку, пред­на­зна­чен­ных для даль­ней­ше­го использова­ния в про­из­вод­ст­ве.

Тех­но­ло­ги­че­ский кон­троль – кон­троль тех­но­ло­ги­че­ских па­ра­мет­ров про­из­вод­ст­ва про­дук­ции (то­ва­ров) в про­цес­се из­го­тов­ле­ния и ока­за­ния услуг.

Инспекционный контроль – контроль, осуществляемый уполномоченными органами с целью надзо­ра за со­блю­де­ни­ем тре­бо­ва­ний са­ни­тар­ных норм, пра­вил и ги­гие­ни­че­ских нор­ма­ти­вов.

Объ­ек­та­ми то­го или ино­го ви­да кон­тро­ля яв­ля­ют­ся производственные, об­ще­ст­вен­ные по­ме­ще­ния, зда­ния, со­ору­же­ния, санитар­но-за­щит­ные зо­ны, зо­ны са­ни­тар­ной ох­ра­ны, ат­мо­сфер­ный воз­дух, водо­снаб­же­ние, транс­порт, тех­но­ло­ги­че­ские про­цес­сы и обо­ру­до­ва­ние, сырье, про­из­во­ди­мая про­дук­ция (то­ва­ры), ус­ло­вия хра­не­ния, транспортиров­ки и реа­ли­за­ции, ра­бо­чие мес­та, вклю­чая ра­бо­таю­щих и оказы­вае­мые ус­лу­ги на­се­ле­нию.

Про­из­вод­ст­вен­ный кон­троль вклю­ча­ет:

– на­ли­чие офи­ци­аль­но из­дан­ных са­ни­тар­ных пра­вил и норм, аттестован­ных ме­то­дов и ме­то­дик кон­тро­ля сы­рья, про­дук­ции, про­из­вод­ст­ва, фак­то­ров сре­ды оби­та­ния в со­от­вет­ст­вии с осу­ще­ст­в­ляе­мой дея­тель­но­стью и дру­гой нор­ма­тив­ной до­ку­мен­та­ции;

– осу­ще­ст­в­ле­ние (ор­га­ни­за­цию) ла­бо­ра­тор­ных (тех­но­ло­ги­че­ских) иссле­до­ва­ний и ис­пы­та­ний на гра­ни­це са­ни­тар­но-за­щит­ной зо­ны и в зо­не влия­ния предприятия, на тер­ри­то­рии (про­из­вод­ст­вен­ной пло­щад­ке), на ра­бо­чих местах с целью оцен­ки влия­ния про­из­вод­ст­ва на сре­ду оби­та­ния че­ло­ве­ка и его здоровье а также сы­рья, по­лу­фаб­ри­ка­тов, го­то­вой про­дук­ции и тех­но­ло­гий их производ­ст­ва, хра­не­ния, транс­пор­ти­ров­ки, реа­ли­за­ции и ути­ли­за­ции;

– пе­ре­чень долж­но­стей ра­бот­ни­ков, под­ле­жа­щих ме­ди­цин­ским осмот­рам, про­фес­сио­наль­ной ги­гие­ни­че­ской под­го­тов­ке и ат­те­ста­ции;

– пе­ре­чень осу­ще­ст­в­ляе­мых юри­ди­че­ским ли­цом, ин­ди­ви­ду­аль­ным пред­при­ни­ма­те­лем ра­бот и ус­луг, вы­пус­кае­мой про­дук­ции (то­ва­ров);

– ме­ро­прия­тия, пре­ду­смат­ри­ваю­щие обос­но­ва­ние безо­пас­но­сти для здо­ро­вья и жиз­ни че­ло­ве­ка и сре­ды его оби­та­ния, вы­пус­кае­мой про­дук­ции и тех­но­ло­гии ее про­из­вод­ст­ва, кри­те­ри­ев безо­пас­но­сти и (или) без­вред­но­сти фак­то­ров про­из­вод­ст­ва, и раз­ра­бот­ку ме­то­дов кон­тро­ля, в том числе при поступлении сы­рья, хра­не­нии, транс­пор­ти­ров­ке, реа­ли­за­ции и ути­ли­за­ции про­дук­ции и от­хо­дов про­из­вод­ст­ва, а так­же про­цес­сов вы­пол­не­ния ра­бот, ока­за­ния ус­луг;

– пе­ре­чень форм уче­та и от­чет­но­сти, ус­та­нов­лен­ной дей­ст­вую­щим за­ко­но­да­тель­ст­вом по во­про­сам осу­ще­ст­в­ле­ния про­из­вод­ст­вен­но­го контроля;

– пе­ре­чень воз­мож­ных ава­рий­ных си­туа­ций, свя­зан­ных с ос­та­нов­кой про­из­вод­ст­ва, на­ру­ше­ния­ми тех­но­ло­ги­че­ских про­цес­сов, иных соз­даю­щих уг­ро­зу са­ни­тар­но-эпи­де­ми­че­ско­му бла­го­по­лу­чию на­се­ле­ния си­туа­ций, при воз­ник­но­ве­нии ко­то­рых осу­ще­ст­в­ля­ет­ся ин­фор­ми­ро­ва­ние ме­ст­ных исполни­тель­ных и рас­по­ря­ди­тель­ных ор­га­нов, ор­га­нов и уч­ре­ж­де­ний государ­ст­вен­но­го са­ни­тар­но­го над­зо­ра, на­се­ле­ния;

– дру­гие ме­ро­прия­тия, про­ве­де­ние ко­то­рых не­об­хо­ди­мо для осуществ­ле­ния эф­фек­тив­но­го кон­тро­ля за со­блю­де­ни­ем тре­бо­ва­ний санитар­ных норм, пра­вил и ги­гие­ни­че­ских нор­ма­ти­вов, вы­пол­не­ни­ем санитар­но-про­ти­во­эпи­де­ми­че­ских и про­фи­лак­ти­че­ских ме­ро­прия­тий.

4.4 Ответственность за необеспечение трудоохранных требований

За нарушения работниками законодательства о труде и правил охраны труда установлены следующие виды ответственности: дисциплинарная, материальная, административная и уголовная.

Дисциплинарная ответственность работников предусмотрена статьей 198 ТК. За совершение дисциплинарного проступка наниматель может применить к работнику следующие меры дисциплинарного взыскания: замечание, выговор, увольнение с работы.

За однократное грубое нарушение требований по охране труда, повлекшее увечье или смерть других работников, работник может быть уволен по инициативе нанимателя в соответствии с пунктом 9 статьи 42 ТК.

Работники отдельных отраслей экономической деятельности за нарушения требований охраны труда несут ответственность в соответствии с уставами (положениями) о дисциплине.

Полное или частичное лишение нарушителя премий, перенос отпуска на другое время и другие меры воздействия не являются мерами дисциплинарной ответственности (они не предусмотрены в статье 198 ТК) и могут применяться одновременно с привлечением его к той или иной ответственности.

Если же в нарушениях законодательства о труде и правил по охране труда имеются признаки состава преступления, виновный независимо от того, наложено ли на него дисциплинарное взыскание, может быть привлечен и к уголовной ответственности.

За причинение в результате нарушений требований по охране труда имущественного ущерба нанимателю работник независимо от привлечения его к дисциплинарной или уголовной ответственности может быть привлечен к материальной ответственности в соответствии со статьями 400-409 ТК.

Административная ответственность физических и юридических лиц установлена Кодексом Республики Беларусь об административных правонарушениях от 21 апреля 2003 года № 194-3, а порядок привлечения к административной ответственности – Процессуально-исполнительным кодексом Республики Беларусь об административных правонарушениях от 20 декабря 2006 года № 194-3.

В специальную главу КоАП (глава 18) выделены правонарушения против безопасности движения и эксплуатации транспорта.

В зависимости от характера правонарушений КоАП предусматриваются различные меры ответственности как для физических, так и для юридических лиц. При этом, в частности, установлено, что минимальный размер штрафа, налагаемого на физическое лицо, не может быть менее одной десятой базовой величины. Минимальный размер штрафа, налагаемого на индивидуального предпринимателя, не может быть менее двух базовых величин, а на юридическое лицо – менее десяти базовых величин.

Максимальный размер штрафа, налагаемого на физическое лицо, не может превышать пятидесяти базовых величин. Максимальный размер штрафа, налагаемого на индивидуального предпринимателя, не может превышать двухсот базовых величин, а на юридическое лицо – тысячи базовых величин при исчислении штрафа в базовых величинах.

Административные взыскания налагаются уполномоченными государственными органами и должностными лицами, которым предоставлено такое право. Основанием для наложения взысканий являются протоколы об административных правонарушениях, которые составляются уполномоченными должностными лицами, указанными в законодательных актах.

В ПИКоАП подробно регламентированы вопросы, связанные со всеми процессуальными действиями при привлечении к административной ответственности, а также установлен порядок исполнения и обжалования принятых решений.

Уголовная ответственность установлена, в частности, следующими статьями Уголовного кодекса Республики Беларусь от 9 июля 1999 года № 275-3:

– статья 199. Нарушение законодательства о труде;

– статья 233. Незаконная предпринимательская деятельность.

В результате расследования несчастных случаев на производстве может возникнуть вопрос об ответственности виновных лиц.

В соответствии с п.85 правил расследования и учета несчастных случаев на производстве и профессиональных заболеваний, утвержденных постановлением Совета Министров Республики Беларусь от 15.01.2004 № 30, наниматели, страхователи и должностные лица организаций, допустившие нарушение данных [правил](http://bii.by/tx.dll?d=67995&a=19#a19), привлекаются к ответственности в соответствии с законодательством.

За нарушение правил охраны труда, повлекшее несчастный случай на производстве, для нанимателя, страхователя, должностных лиц организаций могут наступать перечисленные ниже виды ответственности.

Уголовная ответственность за нарушение правил охраны труда возможна при возникновении профессионального заболевания, причинении телесного повреждения либо смерти человека. Уголовная ответственность установлена, в частности, следующими статьями:

– [часть первая](http://bii.by/tx.dll?d=33384&a=2849#a2849) ст.306 Уголовного кодекса Республики Беларусь. Нарушение правил техники безопасности, промышленной санитарии или иных правил охраны труда должностным лицом, ответственным за их соблюдение (нарушение правил охраны труда), повлекшее по неосторожности профессиональное заболевание либо причинение тяжкого или менее тяжкого телесного повреждения. Наказывается штрафом, или исправительными работами на срок до 2 лет, или ограничением свободы на срок до 3 лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения;

– [часть вторая](http://bii.by/tx.dll?d=33384&a=2850#a2850) ст.306 УК. Нарушение правил охраны труда, повлекшее по неосторожности смерть человека либо причинение тяжкого телесного повреждения двум или более лицам. Наказывается ограничением свободы на срок до 5 лет или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения;

– [часть третья](http://bii.by/tx.dll?d=33384&a=3891#a3891) ст.306 УК. Нарушение правил охраны труда, повлекшее по неосторожности смерть двух или более лиц. Наказывается лишением свободы на срок от 3 до 7 лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Кроме уголовной ответственности за нарушение правил охраны труда УК предусмотрена ответственность за иные преступления, связанные с обеспечением безопасности работников:

– нарушение правил производственно-технической дисциплины или правил безопасности на объектах использования атомной энергии ([ст.301](http://bii.by/tx.dll?d=33384&a=1024#a1024));

– нарушение правил производственно-технической дисциплины, правил безопасности на взрывоопасных предприятиях или во взрывоопасных цехах либо правил безопасности взрывоопасных работ ([ст.302](http://bii.by/tx.dll?d=33384&a=1025#a1025));

– нарушение правил безопасности горных или строительных работ ([ст.303](http://bii.by/tx.dll?d=33384&a=1026#a1026));

– нарушение правил пожарной безопасности ([ст.304](http://bii.by/tx.dll?d=33384&a=1027#a1027));

– нарушение проектов, обязательных для соблюдения требований технических нормативных правовых актов при производстве строительно-монтажных работ ([ст.305](http://bii.by/tx.dll?d=33384&a=1028#a1028));

– непринятие мер по спасению людей ([ст.307](http://bii.by/tx.dll?d=33384&a=1030#a1030));

– несообщение информации об опасности для жизни людей ([ст.308](http://bii.by/tx.dll?d=33384&a=1031#a1031));

– нарушение санитарных норм, правил и гигиенических нормативов ([ст.336](http://bii.by/tx.dll?d=33384&a=4333#a4333));

– служебную халатность ([ст.428](http://bii.by/tx.dll?d=33384&a=2704#a2704)).

Ответственность по [ст. 306](http://bii.by/tx.dll?d=33384&a=1029#a1029) УК несут только должностные лица, на которых в силу их служебных полномочий или по специальному распоряжению непосредственно возложена обязанность обеспечивать соблюдение правил охраны труда на определенном участке работы.

Руководители предприятий, учреждений и организаций, их заместители, главные инженеры, главные специалисты могут быть привлечены к ответственности по данной статье, если они не приняли мер к устранению заведомо известного нарушения правил охраны труда, либо дали указания, противоречащие этим правилам, или, взяв на себя непосредственное руководство отдельными видами работ, не обеспечили соблюдение тех же правил. В иных случаях должностные лица, виновные в ненадлежащем исполнении своих служебных обязанностей по обеспечению безопасных условий труда (например, в непринятии мер по разработке соответствующих инструкций, по созданию условий для выполнения правил охраны труда, в неосуществлении надлежащего контроля за их соблюдением), могут нести ответственность за преступления против интересов службы.

За нарушение правил охраны труда наступает при наличии факта нарушения норм соответствующих нормативных правовых актов, в том числе технических и локальных нормативных правовых актов. Административная ответственность установлена, в частности, следующими статьями:

– [часть 1](http://bii.by/tx.dll?d=61999&a=3959#a3959) ст.9.17 Кодекса Республики Беларусь об административных правонарушениях (далее - КоАП). Нарушение должностным или иным уполномоченным лицом работодателя или индивидуальным предпринимателем требований по охране труда, содержащихся в нормативных правовых актах, в том числе технических и локальных нормативных правовых актах. Штраф в размере от 5 до 40 базовых величин (далее - БВ);

– [часть 2](http://bii.by/tx.dll?d=61999&a=4070#a4070) ст.9.17 КоАП. То же деяние, совершенное повторно в течение 1 года после наложения административного взыскания за такое же нарушение. Штраф в размере от 15 до 50 БВ;

– [часть 4](http://bii.by/tx.dll?d=61999&a=2975#a2975) ст.9.19 КоАП. Иные нарушения законодательства о труде, кроме нарушений, предусмотренных ст.[9.16-9.18](http://bii.by/tx.dll?d=61999&a=105#a105) КоАП и частями [1](http://bii.by/tx.dll?d=61999&a=1333#a1333) и [3](http://bii.by/tx.dll?d=61999&a=1244#a1244) настоящей статьи, причинившие вред работнику. Штраф в размере от 2 до 20 БВ;

– [статья 9.20](http://bii.by/tx.dll?d=61999&a=109#a109) КоАП. Сокрытие страхователем наступления страхового случая при обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний. Штраф в размере от 2 до 10 БВ, на индивидуального предпринимателя - от 10 до 50 БВ, а на юридическое лицо - от 50 до 100 БВ.

С 31 января 2018 г. несообщение или несвоевременное сообщение страхователем о несчастном случае на производстве или профессиональном заболевании в случаях, предусмотренных законодательством, а равно нарушение установленного порядка расследования такого несчастного случая влекут наложение штрафа в размере от 10 до 50 БВ ([ст.9.20](http://bii.by/tx.dll?d=61999&a=4334#a4334) КоАП в редакции Закона Республики Беларусь от 08.01.2018 № 95-З).

Статьи [198-204](http://bii.by/tx.dll?d=33380&a=1748#a1748) Трудового кодекса Республики Беларусь. Противоправное, виновное неисполнение или ненадлежащее исполнение работником своих трудовых обязанностей (дисциплинарный проступок) может повлечь за собой:

– замечание;

– выговор;

– увольнение (пп.[4](http://bii.by/tx.dll?d=33380&a=151#a151), 5, [7-9](http://bii.by/tx.dll?d=33380&a=8500#a8500) ст.42, [п.1](http://bii.by/tx.dll?d=33380&a=2385#a2385) ст.47 ТК).

– лишение полностью или частично дополнительных выплат стимулирующего характера на срок до 12 месяцев ([подп.3.3](http://bii.by/tx.dll?d=292768&a=12#a12) п.3 Декрета Президента Республики Беларусь от 15.12.2014 № 5 «Об усилении требований к руководящим кадрам и работникам организаций», далее - Декрет № 5).

Дисциплинарная ответственность за нарушение правил охраны труда, в том числе повлекшее тяжелые последствия, предусматривается в коллективных договорах, правилах внутреннего трудового распорядка, иных локальных нормативных правовых актах, трудовых договорах (контрактах) работника.

Трудовой договор, заключенный на неопределенный срок, а также срочный трудовой договор до истечения срока его действия может быть расторгнут нанимателем в случае однократного грубого нарушения правил охраны труда, повлекшего увечье или смерть других работников ([п.9](http://bii.by/tx.dll?d=33380&a=8501#a8501) ст.42 ТК).

В целях укрепления общественной безопасности и дисциплины [подп.1.4](http://bii.by/tx.dll?d=69084&a=20#a20) п.1 Директивы Президента Республики Беларусь от 11.03.2004 № 1 «О мерах по укреплению общественной безопасности и дисциплины» требует от руководителей государственных органов, иных организаций независимо от форм собственности обеспечить безусловное привлечение работников организаций к дисциплинарной ответственности вплоть до увольнения за нарушение требований по охране труда, повлекшее увечье или смерть других работников.

Одним из основных критериев оценки выполнения [Директивы](http://bii.by/tx.dll?d=69084&a=15#a15) № 1 следует считать обеспечение здоровых и безопасных условий труда, промышленной, пожарной, ядерной и радиационной безопасности, безопасности движения и эксплуатации транспорта, формирование правопослушного поведения, здорового образа жизни, навыков по обеспечению личной и имущественной безопасности граждан, в том числе в подчиненных (расположенных на подведомственной территории) органах и организациях.

Если в результате несчастного случая на производстве застрахованному лицу был причинен материальный или моральный вред, то виновные в его причинении лица могут нести ответственность действующего законодательства.

Если в результате нарушения требований охраны труда, несчастного случая на производстве нанимателю, страхователю, организации был причинен материальный ущерб, то работник независимо от привлечения его к уголовной, административной или дисциплинарной ответственности может быть привлечен к материальной ответственности согласно ст.[400-409](http://bii.by/tx.dll?d=33380&a=3236#a3236) ТК.

[Декрет](http://bii.by/tx.dll?d=292768&a=8#a8) № 5 изменяет правила удержания из заработной платы, производимые по инициативе нанимателя ([ст.408](http://bii.by/tx.dll?d=33380&a=3555#a3555) ТК).

Так, руководители организаций вправе удерживать из заработной платы работника по распоряжению нанимателя ущерб, причиненный нанимателю по вине работника, в размере до трех его среднемесячных заработных плат. При этом при каждой выплате заработной платы размер такого удержания (при взыскании сумм, в том числе по исполнительным документам, общий размер всех удержаний) не может превышать 50 % заработной платы, причитающейся к выплате работнику, если возможность большего размера удержания (общего размера всех удержаний) не установлена законодательными актами ([подп.3.6](http://bii.by/tx.dll?d=292768&a=15#a15)п.3 Декрета № 5).

Подпункт 3.5 п.3 Декрета № 5 предоставляет право руководителям организаций расторгать трудовой договор (контракт) с работником, допустившим нарушение производственно-технологической, исполнительской или трудовой дисциплины, повлекшее причинение организации ущерба в размере, превышающем три начисленные среднемесячные заработные платы работников Республики Беларусь. При этом указанное действие (бездействие) работника признается грубым нарушением трудовых обязанностей, а увольнение по данному основанию производится с одновременным уведомлением (в день увольнения) соответствующего профсоюза.

# **ЗАКЛЮЧЕНИЕ**

Цель дипломного проекта достигнута – изучена предметная область и разработано программное средство защиты от файловых вирусов. Все задачи выполнены в полном объеме:

определен объект и предмет исследования, актуальность, цели и задачи дипломного проекта;

изучены основные понятия, определены этапы работы;

описаны аналоги;

определены задачи на разработку программного средства, описана полная структура, основные сведения, входные и выходные данные, разработан графический интерфейс, диаграммы «Диаграмма состояния», «Диаграмма вариантов использования» и «Диаграмма деятельности»;

в полном объеме описан каждый модуль;

произведен расчет себестоимости и цены программного средства; изучена тема по охране труда «Организация общественного контроля за состоянием охраны труда» с вопросами: характеристика трудовой деятельности и факторов среды при работе оператора, организация общественного контроля условий и безопасности труда, общественный контроль за состоянием охраны труда на объекте при проектируемой деятельности а так же ответственность за необеспечение трудоохранных требований.

Описаны все необходимые сведение по теме программных средств защиты от файловых вирусов. Программное средство разработано на языке C# с использованием языка C++ для разработки драйверов операционной системы. Тестирование программного средства показало работоспособность, целостность и структурированность. Программное средство имеет модульную структуру, что обеспечивает возможность быстрого освоения использования, сопровождения, а также доработку при необходимости.

# **СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ**

1 Харитонов, С.С. 1С Бухгалтерский и налоговый учет / С.С.  Харитонов.  – СПб.: Лидер, 2019. – 640 с.

2 Кэнту, В.М. TransactSQL: Для профессионалов / В.М. Кэнту. – СПб.: Питер, 2016. – 1101 с.

3 Гофман, В.Э. MySql. Быстрый старт / В.Э. Гофман – СПб.: Петербург, 2018. – 288 с.

4 Ушаков, Д.П. Справочник для мастеров / Д.П. Ушаков. – СПб: Питер, 2017. – 320 с.

5 Павловская, Т.А. Программирование на языке высокого уровня / Т.А.  Павловская. – СПб: Питер, 2018. – 393 с.

6 Мансуров, К.Т. Основы работы с регистрами сведений / К.Т.  Мансуров. – СПб: Питер, 2015. – 773 с.

7 Боров, С.А. 1C: Предприятие учебный курс / С.А. Боров – СПб.: Питер, 2019. – 228 с.

8 Рубанцев, В.С. Самоучитель 1C: Предприятие в примерах / В.С.  Рубанцев – СПб.: Питер, 2016. – 123 с.

9 Осипов, Д.Е. Профессиональное программирование / Д.Е. Осипов – СПб: Питер, 2017 – 322 c.

10 Культин, Н.Б. Основы запросов в 1С / Н.Б. Культин – СПб.: Питер, 2019 – 464 c.

11 Маркин, А.В. 1С для профессионалов / А.В. Маркин. – СПб.: Питер, 2019. – 144 c.

12 Окулов, С.М. Практическое пособие профессионального разработчика / С.М. Окулов – СПб.: Питер, 2018. – 120 c.

13 Бьянкуцци, Ф.А. Пионеры программирования. Диалоги с создателями наиболее популярных языков программирования / Ф.А. Бьянкуцци, Ш.  Уорден. – СПб.: Питер, 2018. – 608 c.

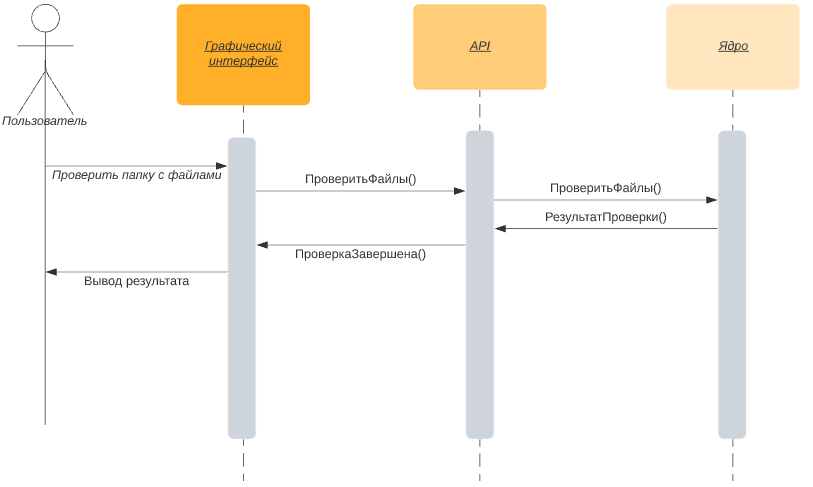
14 Керниган, Б.Д. Создание информационных баз для начинающих / Б.Д.  Керниган, Д.М. Ритчи. – СПб.: Питер, 2016. – 288 c.

15 Шохирев, М.В. Лучшие решения для бизнеса на 1С / М.В.  Шохирев.  –  СПб.: Питер, 2015. – 279 c.

**ПРИЛОЖЕНИЯ**

**ПРИЛОЖЕНИЕ А**

**ДИАГРАММА ПОСЛЕДОВАТЕЛЬНОСТИ ДЕЙСТВИЙ**



**ПРИЛОЖЕНИЕ Б**

**ДИАГРАММА ВАРИАНТОВ ИСПОЛЬЗОВАНИЯ**

**ПРИЛОЖЕНИЕ В**

**ДИАГРАММА ДЕЯТЕЛЬНОСТИ**

**ПРИЛОЖЕНИЕ Г**

**ЛИСТИНГ**