Руководство пользователя по установке и использованию программы «ClamTK» в ОС Arch Linux

1. ВВЕДЕНИЕ
   1. Область применения

ClamTK — это графический пользовательский интерфейс для антивируса ClamAV, работающий с библиотеками Perl и Gtk. Он был разработан для обеспечения поиска и обнаружения вирусов в ОС Linux.

* 1. Краткое описание возможностей

- Сканирование выбранных файлов, каталогов или всей системы на наличие угроз.

- Просмотр подробных отчетов о сканировании.

- Планирование регулярных сканирований файлов системы.

- Простой графический интерфейс (GUI) для ClamAV.

* 1. Уровень подготовки пользователя

Пользователь должен обладать правами администратора, а также базовыми навыками работы с терминалом и менеджером пакетов Pacman.

1. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ
   1. Виды деятельности, функции

ClamTK предназначен для автоматизации следующих задач:

- Обнаружение вредоносного ПО.

- Проверка файлов, загруженных из интернета или полученных извне.

- Регулярный мониторинг критически важных областей файловой системы.

* 1. Условия применения

Технические средства и конфигурация: компьютер, совместимый с ОС Arch Linux; не менее 200 МБ на дисковом пространстве.

Операционная среда: предустановленная ОС Arch Linux с графическим интерфейсом (например, Gnome).

1. ПОДГОТОВКА К РАБОТЕ
   1. Порядок загрузки программ и данных

- Установка необходимых пакетов через терминал

sudo pacman -Syu clamtk

- Обновление базы сигнатур через терминал

sudo freshclam

* 1. Порядок проверки работоспособности

1. Запустить ClamTK из меню приложений или через терминал с помощью команды clamtk.

2. Проверить версии ClamAV и ClamTK: в главном окне нажать кнопку «About».

3. Выполнить быстрое сканирование домашнего каталога: в главном окне нажать кнопку «Scan a directory» -> нажать кнопку «OK».

1. ОПИСАНИЕ ОПЕРАЦИЙ
   1. Описание операций
      1. Сканирование выбранного каталога

Наименование: запуск сканирования указанного каталога.

Условия: запущенный ClamTK, необходимые права на чтение файлов в сканируемом каталоге.

Подготовительные действия: запустить ClamTK из меню приложений или через терминал с помощью команды clamtk.

Основные действия: в главном окне нажать кнопку «Scan a directory» -> выбрать нужный каталог -> нажать кнопку «OK». После завершения сканирования просмотреть отчет.

Заключительные действия: принять решение по каждому обнаруженному подозрительному файлу в отчете -> закрыть окно отчета.

* + 1. Настройка запланированного сканирования

Наименование: создание расписания для сканирований.

Условия: запущенный ClamTK.

Подготовительные действия: запустить ClamTK из меню приложений или через терминал с помощью команды clamtk.

Основные действия: в главном окне нажать кнопку «Scheduler» -> в открывшемся окне выставить время ежедневного сканирования -> нажать кнопку «+» для сохранения расписания.

Заключительные действия: закрыть окно планировщика.

1. АВАРИЙНЫЕ СИТУАЦИИ
   1. Длительные отказы технических средств, несоблюдение условий

- Прерванное сканирование: закрыть ClamTK и перезапустить его. При необходимости перезагрузить систему.

- Отсутствие интернета: ClamTK будет использовать последние доступные локальные базы. Запланированные обновления пропустятся.