ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО

Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ

Начальник 27 кафедры

полковник

С. Войцеховский

«___» _____ 2022 г.

Практическое занятие № 11
по учебной дисциплине
«Защита информации»
на тему:

«Система контроля целостности Aide операционной системы МС ВС 3.0»

Рассмотрено и одобрено
на заседании кафедры № 27
« ___ » _____ 202_ г. протокол № ___

Санкт-Петербург
2022

I. ТЕМА И ЦЕЛЬ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

Тема практического занятия: «Система контроля целостности Aide операционной системы МС ВС 3.0».

Цель работы:

1. Приобрести практические навыки в использовании средств управления компьютером.

2. Закрепить знания о свойствах операционной системы.

3. Выработать практические умения и приобрести навыки в решении задач по настройке и работе с системой контроля целостности ОС МСВС 3.0.

Время - 180 мин.

Место – аудитория (класс) по расписанию занятий.

Учебно-материальное и методическое обеспечение

1. Лабораторные установки – персональные ЭВМ с установленным на них программным обеспечением.
2. Электронный практикум по ЗИ.
3. Учебно-методические материалы.

II. УЧЕБНЫЕ ВОПРОСЫ И РАСЧЕТ ВРЕМЕНИ

№ п\п	Учебные вопросы	Время, мин.
1.	***Вступительная часть. Контрольный опрос.***	5
2.	***Учебные вопросы.*** ОСНОВНАЯ ЧАСТЬ: 1. Настройка и работа с системой контроля целостности Aide в ОС МС ВС 3.0. 2. Создание скрипта для автоматизации запуска процесса проверки.	 80 80
3.	Заключительная часть. Задание и методические указания курсантам на самостоятельную подготовку	5

4.Выполнение работы

1. Настройка и работа с системой контроля целостности Aide в ОС МС ВС 3.0.

1**.1.** Сначала необходимо посчитать контрольную сумму с той директории (или файла), которую мы будем проверять на контроль целостности. Основной конфигурационный файл программы **aide.conf** находиться в директории **/etc/aide/** В файле можно указать множество параметров, но для начала достаточно только тех, которые указывают какие файлы добавлять в базу и какие атрибуты сохранять при этом. Подсчёт контрольной суммы будет производится по определённому набору правил, которые можно взять по умолчанию заданные в файле **aide.conf,** а можно задать свои правила (закомментировать заданные по умолчанию). Например преподаватель дал проверить директорию **/etc/aide** и отдельный файл **/etc/aide/aide.db.** Определяем группы атрибутов. Для этого заходим в файл **aide.conf** при помощи клавиши **F4**.

Находим строку

#Rull definition после которой указываются правила, например, создадим свои правила:

Standart=p+i+n+u+g+s

Где Standart это имя создаваемого нами правила, а

p-права

i-номер inode

n-количество ссылок на файл

u-владелец

g-группа

s-размер

тоже самое и

Advanced=p+i+n+u+g+s+md5

Тут ещё добавляется алгоритм вычисления контрольной суммы файлов md5 (также существуют другие алгоритмы вычисления контрольной суммы файлов, такие как **sha1**, **rmd160**, **tiger**).

Далее у нас в файле aide.conf имеется набор строк с каталогами, перед которыми стоит символ #. Этот символ означает комментарий и то, что данную строку можно не выполнять. Его нужно убрать перед выбранной нами директорией для её проверки. Можно также задать свою директорию, или файл по указанному нами пути для проверки на целостность, после этого нужно написать правило, которое мы создали:

/etc/aide Standart

/etc/aide/aide.db Advanced

все файлы в /etc/aide/ с набором атрибутов Standart,

файл /etc/aide/aide.db с набором атрибутов Advanced

выходим из файла aide.conf нажатием F10 и сохраняем его, затем инициируем программу создать базу.

В командной строке пишем

aide -i -c aide.conf и нажимаем Enter

Если запуск программы aide не произошёл, то необходимо указать полный путь к программе **/usr/bin/aide –i –c /etc/aide/aide.conf**

Будет создан файл aide.db.new. Его необходимо скопировать с именем **aide.db**. Делаем это нажатием клавиши **F5**, указываем путь и название файла /etc/aide/aide.db или просто aide.db. Это и есть база. Если посмотреть ее содержимое, то обнаружим набор строк, каждая из которых есть имя файла и далее через пробел его атрибуты и сигнатуры.

4.1.2. Для того чтобы проверить изменилась ли контрольная сумма указанной преподавателем папки или файла необходимо записать команду

aide --check

которая вводится в командной строке, после чего производится проверка, отчет о проверке помещается в файл **aide.log**. По умолчанию он находится в директории **/var/log/**

Если мы хотим прописать файл **aide.log** в другую директорию, например в **/etc/aide**/, то необходимо прописать ссылку на файл **aide.log** в файле **aide.conf** для этого изменить следующую строку

@@defint REPORTLOG /etc/aide/aide.log

это файл-отчет обо всех изменениях произошедших в указанных нами каталогах путем сравнения с созданной нами базой. Далее анализируем этот файл и делаем отчёт о проделанной работе.

Пример файла aide.log:

AIDE обнаружил различия между базой и файловой системой
Время старта:2014-01-17 13:50:33
Резюме
Всего файлов=4, из них добавленных=4, удалённых=0, изменённых=1

Добавленные файлы
added:/etc/aide/aide.db.new
added:/etc/aide/aide.db
added:/etc/aide/123
added:/etc/aide/aide.log
Изменённые файлы:
changed added:/etc/aide/aide.conf
Детальная информация об изменениях

File: /etc/aide/aide.conf
Size: old = 3063 , new = 3069

Время завершения : 2014-01-1713:50:33

Далее анализируем этот файл и делаем отчёт о проделанной работе.

Каждый раз приходится набирать вышеуказанные команды, для удобства проверки в графическом режиме можно сделать кнопку, которая будет проверять систему на целостность и выводить файл-отчет.

1. Создание скрипта для автоматизации запуска контроля целостности

Прежде чем создавать кнопку необходимо написать набор команд которые войдут в скрипт (более подробно см. конспект лекций по ОС за 6 семестр), после чего можно приступить к созданию кнопки.

Для создания кнопки на рабочем столе необходимо:

Щелкнуть правой кнопкой мыши на рабочем столе, в контекстном меню выбрать пункт Новый, затем Приложение, в появившемся окне указать имя Вашей кнопки (например: контроль целостности.kdelnk). Нажмите OK и появится кнопка.

Теперь необходимо связать эту кнопку непосредственно с вашим скриптом. Для этого следует щелкнуть правой кнопкой мыши на значке вашей кнопки, в контекстном меню выбрать пункт **Свойства**, потом **Выполнить**, затем нажать на кнопку **Просмотреть** и выбрать ваш скрипт (тем самым будет указан путь по которому кнопка будет взаимодействовать со скриптом).

Для того чтобы скрипт запускался в консольном режиме нужно поставить галочку в окошке **Запускать в терминале**.

При необходимости можно изменить рисунок на кнопке. Для этого - нажать на кнопку с рисунком и выбрать понравившееся вам изобаржение.

OK.– кнопка готова!

Теперь можно проверить работоспособность скрипта, кнопки и связи между ними. Для этого нужно нажать нашу кнопку, после нажатия на которую должна производится проверка контроля целостности указанной преподавателем директории и выводиться на экран монитора файл-отчёт (он же файл aide.log), после чего который необходимо проанализировать.

Отчетность по работе

По выполнению работы каждый курсант должен представить отчет. Отчет должен содержать:

– название практического занятия;

– текст индивидуального задания;

– цель работы;

– результаты проделанной работы;

– Выводы.

В процессе выполнения индивидуального задания или после завершения его выполнения преподаватель проводит собеседование с каждым курсантом по теме выполненной работы, проверяя также практические навыки, приобретенные в ходе занятия. Отчетный материал предоставляется преподавателю, а результаты защищаются.

Заключительная часть

В заключительной части подводятся итоги проделанной работы, дается краткая оценка действиям участников, прослеживается связь с теоретическими положениями и перспективой на будущую деятельность.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПРЕПОДАВАТЕЛЮ ПРИ ПРОВЕДЕНИИ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

Во вступительной части преподавателю объявить тему занятия, его цели, учебные вопросы, порядок его проведения, отметить практическую значимость знания назначения, основных возможностей и порядка работы системы контроля целостности Aide ОС МСВС 3.0.

Проверку готовности слушателей к занятию осуществить проверкой наличия у них рабочих тетрадей, а также постановкой контрольных вопросов по знанию материала предыдущего группового занятия.

Отработку учебных вопросов осуществлять путем выполнения заданий, выдаваемых всей группе.

При отработке первого вопроса основное внимание обратить на приобретение курсантами практических навыков настройки и работы с системой контроля целостности Aide в ОС МС ВС 3.0.

При отработке второго вопроса привить практические навыки по созданию скриптов для автоматизации процессов.

В заключительной части занятия оценить работу учебной группы в целом, подвести итоги занятия, выставить оценки слушателям, ответить на возникшие вопросы. Сформулировать задание на самоподготовку и объявить тему следующего занятия.

УЧЕБНЫЕ МАТЕРИАЛЫ

Вступительная часть

Товарищи курсанты, целью сегодняшнего занятия является - выработка практических умений и приобретение навыков в решении задач по настройке и работе с системой контроля целостности ОС МСВС 3.0.

Итак, тема сегодняшнего практического занятия - " Система контроля целостности Aide операционной системы МС ВС 3.0".

Для достижения поставленных учебных целей вам требуется отработать два учебных вопроса занятия:

1. Настройка и работа с системой контроля целостности Aide в ОС МС ВС 3.0.

2. Создание скрипта для автоматизации запуска процесса проверки.

Порядок проведения занятия будет следующий - сначала вы ответите на ряд контрольных вопросов, что позволит оценить вашу теоретическую готовность к занятию, а затем в рамках рассматриваемых вопросов занятия вы будете исполнять задания с использованием ПЭВМ. Ваша работа будет оцениваться на местах.

Контрольные вопросы до начала занятия.

Вопрос № 1: Какие функции выполняет системой контроля целостности?

Вопрос № 2: Каков принцип работы средств обеспечения контроля целостности?

Вопрос № 3: Охарактеризуйте систему контроля целостности Aide?

Подготовка к работе

Подготовка к работе проводится в часы самоподготовки. В ходе её каждый курсант обязан:

2.1. Изучить настоящее задание.

2.2. Повторить материал занятий, на которых рассматривались назначение, классификация и основы построения ОС МСВС 3.0.

Методические указания

3.1. В классе ПЭВМ курсанты самостоятельно под руководством преподавателя выполняют п. 4 настоящего задания.

3.2. При выполнении задания работу следует спланировать таким образом, чтобы в первую очередь изучить назначение, основные возможности и порядок работы система контроля целостности Aide ОС МСВС 3.0, а затем приступить к ее использованию для диагностики и исследования состояния папок и файлов.

Задание и методические указания курсантам на самостоятельную подготовку:

1. Изучить по конспекту лекций вопросы архивации и восстановления в операционной системе МС ВС 3.0.
2. Быть готовыми к настройке и работе со средством управления резервным копированием КСЗИ СВАС в ОС МС ВС 3.0.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.

Доцент 27 кафедры
к.т.н.
подполковник

С. Краснов

«___»_____20__г.