

# Содержание

<b>Введение .....</b>	<b>3</b>
-----------------------	----------

## **ЛАБОРАТОРНАЯ РАБОТА № 1**

### **Изучение средства защиты в операционной системе**

<b>Microsoft Windows NT 4.0.....</b>	<b>5</b>
--------------------------------------	----------

## **Часть 1. КОНТРОЛЬ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ.....5**

1. Теоретическая часть.....	5
1.1. Основные понятия и определения .....	5
1.2. Выполнение основных операций .....	9
1.2.1. Вход в систему .....	9
1.2.2. Создание новой группы.....	10
1.2.3. Создание нового пользователя.....	11
1.2.4. Установка прав пользователей .....	13
1.2.5. Политика учетных записей .....	14
1.2.6. Ограничение доступа к ресурсу .....	14
1.2.7. Смена владельца каталога (папки) .....	16
1.2.8. Аудит .....	17
2. Практическая часть.....	19
2.1. Создание новых пользователей и групп.....	19
2.2. Задание прав доступа к файлу .....	19
2.3. Смена владельца файла.....	20
2.4. Установка режима аудита доступа к файлам и каталогам.....	20

## **Часть 2. СОЗДАНИЕ И ИСПОЛЬЗОВАНИЕ ПАРОЛЕЙ..... 21**

1. Теоретическая часть.....	21
2. Практическая часть.....	25
Контрольные вопросы .....	27

## **ЛАБОРАТОРНАЯ РАБОТА № 2**

### **Изучение системы защиты в операционной системе Windows XP .....**

1. Теоретическая часть.....	29
1.1. События .....	29
1.2. Управление доступом.....	33
1.3. Администрирование учетных записей в Windows XP .....	37

1.4. Внедрение программ через реестр.....	41
1.5. Закрытая (замкнутая) программная среда.....	46
1.6. Реализация закрытой программной среды через реестр Windows.....	50
2. Практическая часть.....	51
Контрольные вопросы .....	52

### **ЛАБОРАТОРНАЯ РАБОТА № 3**

#### **Изучение подсистемы защиты в операционной системе Windows 7..... 54**

1. Теоретическая часть.....	54
1.1. Управление учетными записями.....	54
1.1.1. Создание учетных записей пользователей .....	54
1.1.2. Контроль учетных записей (управление учетными записями).....	65
1.1.3. Политики учетных записей.....	72
1.2. Закрытая программная среда встроенными средствами ОС .....	76
1.2.1. Политика ограниченного использования программ (SRP — software restriction policy).....	76
1.2.2. AppLocker.....	84
1.3. Процессы-серверы в Windows.....	96
1.4. Аудит в Windows 7.....	99
1.4.1. Журнал аудита .....	99
1.4.2. Политика аудита .....	101
1.5. Службы в Windows 7 .....	104
1.5.1. Что такое службы .....	104
1.5.2. Как отключить службы.....	104
1.6. Запуск программ с помощью планировщика заданий.....	107
1.7. Шифрованная файловая система (EFS) ОС Windows 7.....	111
2. Практическая часть.....	111

### **ЛАБОРАТОРНАЯ РАБОТА № 4**

#### **Изучение средств защиты информации в ОС Linux ..... 114**

#### **Часть 1. ПРАВА ДОСТУПА В СИСТЕМЕ И ПОВЫШЕНИЕ ПРАВ**

#### **ПОЛЬЗОВАТЕЛЕЙ ..... 114**

1. Теоретическая часть.....	114
1.1. Права доступа в системе Linux.....	114
1.1.1. Пользователи и группы.....	114
1.1.2. Виды прав доступа.....	117
1.1.3. Права доступа и администрирование системы.....	119

1.1.4. Дополнительные биты доступа .....	121
1.2. Повышение полномочий пользователя .....	124
1.2.1. Что такое sudo и где она используется? .....	124
1.2.2. Запуск программ с правами администратора в терминале .....	125
1.2.3. Получение прав суперпользователя для выполнения нескольких команд .....	125
1.2.4. Получение прав суперпользователя для выполнения множества команд .....	126
1.2.5. Использование традиционного root-аккаунта и команды su .....	126
2. Практическая часть .....	126
2.1. Порядок выполнения работы .....	126
Контрольные вопросы .....	127
<b>Часть 2. АУДИТ В СИСТЕМЕ LINUX .....</b>	<b>127</b>
1. Теоретическая часть .....	127
1.1. Аудит системных событий в Linux .....	127
1.1.1. Подсистема аудита: архитектура и принцип работы .....	127
1.1.2. Установка подсистемы аудита .....	128
1.1.3. Конфигурирование .....	129
1.1.4. Создание правил .....	129
1.1.5. Файлы правил .....	130
1.1.6. Анализ журнальных файлов .....	131
1.1.7. Ausearch: поиск и анализ событий .....	134
1.1.8. Анализ процессов .....	135
2. Практическая часть .....	136
2.1. Порядок выполнения работы .....	136
Контрольные вопросы .....	136
<b>Часть 3. ВСТРОЕННЫЕ СРЕДСТВА ШИФРОВАНИЯ В СИСТЕМЕ LINUX .....</b>	<b>137</b>
1. Теоретическая часть .....	137
1.1. Консольные команды .....	137
1.1.1. PGP (команда GPG, от GnuPG) .....	137
1.1.2. TrueCrypt .....	138
1.1.3. LUKS .....	140
2. Практическая часть .....	141
2.1. Порядок выполнения работы .....	141
Контрольные вопросы .....	142

## **ЛАБОРАТОРНАЯ РАБОТА № 5**

### **Знакомство с системой защиты Windows server 2003 ..... 143**

Введение ..... 143

### **Часть 1. КОНТРОЛЬ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ..... 144**

Теоретическая часть ..... 144

Практическая часть..... 151

Контрольные вопросы ..... 168

### **Часть 2. ПАРОЛИ ..... 169**

Теоретическая часть ..... 169

Практическая часть..... 176

### **Список использованной литературы ..... 184**