Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИСТЕТ»

В. В. Подтопельный

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности 10.05.03 " Информационная безопасность автоматизированных систем", специализация «Безопасность открытых информационных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

Рецензент

Доцент кафедры информационной безопасности института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» А. Г. Жестовский.

Подтопельный, В. В. Безопасность операционных систем: учебно-методическое пособие по изучению дисциплины для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем». – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 51 с.

Учебное пособие включает в себя рассмотрение теоретических вопросов в области защиты информации по дисциплине «Безопасность операционных сетей». В учебно-методическом пособии приведен тематический план изучения дисциплины. Представлены методические указания по изучению дисциплины. Даны рекомендации по подготовке к промежуточной аттестации в форме зачета и экзамена, и по выполнению самостоятельной работы. Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы дисциплины «Безопасность вычислительных сетей».

Пособие предназначено для студентов 2 – 3 курсов специальности 10.05.03 «Информационная безопасность автоматизированных систем» и смежных специальностей.

Табл. - 6, список лит. – 4 наименований

Пособие рассмотрено и одобрено в качестве электронного методического материала кафедрой информационной безопасности 19 мая 2022 г., протокол № 7

Учебно-методическое пособие по выполнению курсовых работ рекомендовано к использованию в учебном процессе в качестве локального электронного методического материала методической комиссией института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» 28 июня 2022 г., протокол № 4

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем», изучающих дисциплину «Безопасность операционных систем».

Цель освоения дисциплины:

В результате освоения дисциплины ожидается, что студенты получат знания о принципах построения операционных систем, защиты в операционных системах (ОС).

Для успешного освоения дисциплины, в соответствии с учебным планом, ей предшествуют «Основы информационной безопасности», «Пакеты прикладных программ», «Языки программирования», «Технологии и методы программирования».

Далее в пособии представлен тематический план, содержащий перечень изучаемых тем, обязательных лабораторных/практических работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины, возможно, вам потребует больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе Содержание дисциплины приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки, каждая тема имеет ссылки на литературу (или иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачету и/или экзамену.

В разделе «Балльно-рейтинговая система» приведен порядок применения балльно-рейтинговой системы контроля успеваемости.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделу ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу.

Программное обеспечение:

1.Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription (срок действия: три года);

2.Программное обеспечение распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU , по которой автор передаёт программное обеспечение в общественную собственность): операционная система Linux, ПО Virtual Box.

2. ТЕМАТИЧЕСКИЙ ПЛАН

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самост-ной работы, ч
Лекции (4-й семестр -17 ч ауд., 111,4 ч – сам. р.)				
1.1	Современные операционные системы	Тема 1.1 Введение. Основные понятия. Классификация операционных систем. Концептуальные основы операционных систем.	4	
1.2	Современные операционные системы	Тема 1.2 Архитектура операционной системы	4	20
1.3	Современные операционные системы	Тема 1.3 Управление процессами	4	20
1.4	Современные операционные системы	Тема 1.4 Управление памятью	4	20
1.5	Современные операционные системы	Тема 1.5 Прерывания	4	20
1.6	Современные операционные системы	Тема 1.6 Управление вводом-выводом	4	20
1.7	Современные операционные системы	Тема 1.7 Файловая система	4	11,4
Лекции (5-й семестр – 17 ч ауд., 75, 6 ч – сам. р.)				

2.1	Подсистемы защиты операционной системы	Тема 2.1 Основные функции подсистемы защиты операционной системы	8	10
2.2	Подсистемы защиты операционной системы	Тема 2.2 Управление доступом в операционных системах семейства UNIX	8	10
2.3	Подсистемы защиты операционной системы	Тема 2.3 Управление доступом в операционных системах семейства Windows	4	10
2.4	Подсистемы защиты операционной системы	Тема 2.4 Идентификация и аутентификация в ОС Linux	4	10
2.5	Подсистемы защиты операционной системы	Тема 2.5 Идентификация и аутентификация в ОС Windows	4	10
2.6	Подсистемы защиты операционной системы	Тема 2.6 Аудит ОС	4	25,6
			34	**187**

		Лабораторные занятия (4-й семестр)		
1.	Современные операционные системы	Лабораторная работа №1. Работа с файлами и дисками в ОС Windows	4	-
2.	Современные операционные системы	Лабораторная работа №2. Организация пакетных файлов и сценариев в ОС Windows	4	-
3.	Современные операционные системы	Лабораторная работа №3. Организация консоли администрирования в ОС Windows	4	-
4.	Современные операционные системы	Лабораторная работа №4. Мониторинг, оптимизация и аудит ОС Windows	4	-
5.	Современные операционные системы	Лабораторная работа №5. Работа с Реестром ОС Windows	4	-

6.	Современные операционные системы	Лабораторная работа №6. Работа с подсистемой безопасности в ОС Windows	4	-
7.	Современные операционные системы	Лабораторная работа №7. Модель безопасности ОС Windows	6	-
8.	Современные операционные системы	Лабораторная работа №8. Создание и управление доменной политикой	4	-
		Всего за семестр:	34	
		Лабораторные занятия (5-й семестр)		
1.	Подсистемы защиты операционной системы	Лабораторная работа №9. Конфигурирование доменной политики	4	-
2.	Подсистемы защиты операционной системы	Лабораторная работа №10. Конфигурирование и использование EFS. Восстановление данных	4	-
3.	Подсистемы защиты операционной системы	Лабораторная работа № 11. ОС семейства UNIX. Работа с файлами и каталогами. Управление пользователями. Защита файлов. Резервное копирование данных	8	-
4.	Подсистемы защиты операционной системы	Лабораторная работа № 12. Работа с процессами в операционной системе LINUX	8	-
5.	Подсистемы защиты операционной системы	Лабораторная работа №13. Особенности ОС Linux	8	-
6.	Подсистемы защиты операционной системы	Лабораторная работа №14. Механизмы безопасности в Linux	2	-
		Всего за семестр:	**34**	

		Курсовая работа (проект)		
2.1	Название первого раздела	Контрольная точка 1. Раздел 1	-	-

3.1	Название третьего раздела	Контрольная точка 2. Раздел 2	-	-
		Оформление проекта. Защита	33,75	-
			0	**0**

		Рубежный (текущий) и итоговый контроль		
2.1	Название второго раздела	Контроль 1 (не предусмотрен)	-	-
3.1	Название третьего раздела	Контроль 2 (не предусмотрен)	-	-
		Итоговый контроль (зачет)		
		Итоговый контроль (экзамен)		
			0	**0**

	Всего	**40**	**32**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

3.1. Раздел 1. Методы защиты ПО

3.1.1. Тема 1.1 Введение. Основные понятия. Классификация операционных систем. Концептуальные основы операционных систем

Перечень изучаемых вопросов:

1. Основные понятия;
2. Классификация операционных систем;
3. Концептуальные основы операционных систем: концепция процесса, концепция ресурса, концепция виртуальности, концепция прерывания.

Методические указания к изучению:

Предварительно требуется определить понятие системного программного обеспечения. Рассмотреть классификации ОС по областям, по типам, поддержки многозадачности, поддержки многонитевости, особенностям методов построения, режимам обработки данных.

Требуется рассмотреть особенности реализации концепции процесса (процесс задача, программа, задание). Перечень основных состояний процесса. Обратить внимание на классификации процессов.

Требуется рассмотреть концепцию ресурса. Рассмотреть классификацию ресурсов

Требуется рассмотреть концепцию виртуальности.

Требуется рассмотреть концепцию прерывания, действия ОС при выполнении прерывания, классы прерываний.

При работе над курсовым проектом обратите внимание на:

- описание уязвимостей, которые требуется приводить в первой (теоретической) главе.

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2008. - Т.2. Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007

Контрольные вопросы:

1. Приведите классификацию операционных систем.
2. Приведите классификации процессов.
3. Дайте определение процесса.
4. Охарактеризуйте классификацию ресурсов.
5. Приведите порядок действий ОС при выполнении прерывания.

3.1.2. Тема 1.2 АРХИТЕКТУРА ОПЕРАЦИОННОЙ СИСТЕМЫ

Перечень изучаемых вопросов:

1. Ядро и вспомогательные модули ОС.
2. Ядро в привилегированном режиме.
3. Многослойная структура ОС.
4. Аппаратная зависимость и переносимость ОС.
5. Микроядерная архитектура.
6. Совместимость и множественные прикладные среды.

Методические указания к изучению:

Предварительно требуется определить структурную организацию ОС на основе различных программных модулей. Рассмотреть типы ядер ОС.

Необходимо рассмотреть **два режима работы ядра ОС:**

− пользовательский режим (user mode),

− привилегированный режим, который также называют режимом ядра (kernel mode), или режимом супервизора (supervisor mode).

Требуется рассмотреть Многослойную структуру ОС (**средства аппаратной поддержки ОС, машинно-зависимые компоненты ОС, менеджеры ресурсов, интерфейс системных вызовов (API)**)

Следует рассмотреть аппаратную зависимость и переносимость ОС.

Требуется рассмотреть **микроядерную архитектуру**, набор функций микроядра

При работе над курсовым проектом обратите внимание на:

- описание уязвимостей ОС, которые требуется приводить в первой (теоретической) главе.

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2008. -Т.2. Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007.

Контрольные вопросы:

1. Приведите классификацию операционных систем.
2. Приведите классификации процессов.
3. Дайте определение процесса.
4. Охарактеризуйте классификацию ресурсов.
5. Приведите порядок действий ОС при выполнении прерывания.

3.1.3. Тема 1.3 УПРАВЛЕНИЕ ПРОЦЕССАМИ.

Перечень изучаемых вопросов:

1. Понятие процесса и потока.
2. Управление процессами и потоками.
3. Алгоритмы планирования.
4. Синхронизация процессов и потоков.

Методические указания к изучению:

Требуется обратить внимание на:

1. Способы управления процессам им и потоками:
- Планирование,
- Диспетчеризации,
- Состояния потока.
2. Алгоритмы планирования:
- Вытесняющие и невытесняющие алгоритмы планирования.
- Концепция квантования.
- Приоритетные алгоритмы планирования.
- Смешанные алгоритмы планирования.

3. Синхронизация процессов и потоков.
- Критическая секция.
- Блокирующие переменные.
- Семафоры.

При работе над курсовым проектом обратите внимание на:

- описание процессов ОС, которые требуется приводить в первой (теоретической) главе.

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2008. -Т.2. Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007.

Контрольные вопросы:

1. Приведите классификацию процессов.
2. Приведите классификации алгоритмов планирования.
3. Дайте определение синхронизации.
4. Охарактеризуйте классификацию управления потоками и процессами.

3.1.4 Тема 1.4 УПРАВЛЕНИЕ ПАМЯТЬЮ

Перечень изучаемых вопросов:

1. Иерархия памяти.
2. Управление памятью.
3. Типы адресации.
4. Виртуальная память и свопинг.
5. Алгоритмы управления памятью.

Методические указания к изучению:

Требуется обратить внимание на: функции ОС по управлению памятью в мультипрограммной системе, типы адресации, способы структуризации виртуального адресного пространства, виртуальную память и свопинг, алгоритмы управления памятью, алгоритмы управления памятью. Необходимо разобрать:

А. Алгоритмы управления памятью без использования механизма виртуальной памяти:

1 Распределение памяти фиксированными разделами.

2 Распределение памяти динамическими разделами.

3 Перемещаемые разделы.

Б. Алгоритмы управления памятью с использованием виртуальной памяти:

1 Страничное распределение.

2 Сегментное распределение.

3 Сегментно-страничное распределение.

При работе над курсовым проектом обратите внимание на:

- описание памяти ОС, которые требуется приводить в первой (теоретической) главе.

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2008. -Т.2. Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007э

Контрольные вопросы:

1. Приведите классификацию распределения памяти.
2. Приведите классификации алгоритмов управления памятью без использования механизма виртуальной памяти.
3. Дайте определение синхронизации.
4. Приведите классификацию алгоритмов управления памятью с использованием виртуальной памятью

3.1.5 Тема 1.5 ПРЕРЫВАНИЯ

Перечень изучаемых вопросов:

1 Понятие прерывания
2 Механизм прерываний
3 Функции централизованного диспетчера прерываний
4 Процедуры обработки прерываний, вызванные из текущего процесса
5 Системные вызовы

Методические указания к изучению:

Требуется обратить внимание на: три больших класса прерываний, (Программные прерывания, Внешние прерывания, Внутренние прерывания), два основных способа выполнения прерывания (Опрашиваемый (polled), Векторный (vectored)), приоритезацию и маскирование прерываний, двухуровневый механизм планирования работ при управлении прерываниями, системные вызовы в синхронном или асинхронном режимах.

При работе над курсовым проектом обратите внимание на:

- описание прерываний ОС, которые требуется приводить в первой (теоретической) главе.

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2008. -Т.2. Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007.

Контрольные вопросы:

1. Приведите классификацию прерываний.
2. Приведите два основных способа выполнения прерывания.
3. Дайте определение приоритизации и маскирования прерываний.
4. Приведите классификацию системных вызовов.

3.1.6 Тема 1.6 УПРАВЛЕНИЕ ВВОДОМ-ВЫВОДОМ

Перечень изучаемых вопросов:

1. Организация взаимодействия ос с устройствами ввода-вывода.
2. Многослойная модель подсистемы ввода-вывода.
3. Менеджеры ввода-вывода.
4. Драйверы устройств.

Методические указания к изучению.

Рассмотреть следующие аспекты темы:

1. Операция ввода-вывода может выполняться по отношению к программному модулю, запросившему операцию.
2. В самом общем виде программное обеспечение ввода-вывода можно разделить на четыре слоя.
3. Верхний слой менеджера. Нижний слой менеджера.
4. Порядок функционирования драйвера устройства.

При работе над курсовым проектом обратите внимание на:

- описание особенностей ввода-вывода ОС, которые требуется приводить в первой (теоретической) главе (в соответствии с темой курсовой работы).

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т: учебник для вузов / С. В. Запечников, Н. Г.Милославская. - Москва: Горячая линия-Телеком, 2008. -Т.2. Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007.

Контрольные вопросы:

1. Приведите особенности ввода-вывода по отношению к программному модулю, запросившему операцию.
2. Приведите особенности четырех слоев системы ввода-вывода
3. Приведите особенности верхнего слоя менеджера.
4. Приведите особенности нижнего слоя менеджера.

3.1.7 Тема 1.7 ФАЙЛОВАЯ СИСТЕМА

Перечень изучаемых вопросов:

1. Организация файловой системы (ФС), типы файлов.
2. Иерархическая структура файловой системы.
3. понятие о монтировании.
4. Физическая организация файловой системы.
5. Общая модель файловой системы.
6. Понятие о журналируемых файловых системах.
7. Физическая организация и адресация в файле.
8. Файловая система FAT.

Методические указания к изучению.

Рассмотреть следующие аспекты темы: основные цели использования файла, основные функции ФС, обычные файлы, специальные файлы, файлы-каталоги, параметры прав доступа, два основных подхода к определению прав доступа, понятие о монтировании, общая модель файловой системы (на логическом уровне, на физическом уровне), размещение файла в виде связанного списка кластеров дисковой памяти, непрерывное размещение файла, использование связанного списка индексов, перечисление номеров кластеров, занимаемых этим файлом, Таблица FAT (значения индексного указателя, размер таблицы FAT и разрядность используемых в ней индексных указателей определяется количеством кластеров в области данных, метод хранения адресной информации о файлах, ограничения FAT в Windows), Файловая система exFAT, Файловая система NTFS (основными отличительными свойствами NTFS, главная таблица файлов MFT (Master File Table), структура тома NTFS, записи о системных файлах NTFS в MFT, структура файлов NTFS), Файловая система Ext (логическая организация

файловой системы ext, структурная организация файловой системы ext, система адресации данных в файловой системе ext, три режима журналирования).

При работе над курсовым проектом обратите внимание на:

- описание особенностей ФС ОС, которые требуется приводить в первой (теоретической) главе (в соответствии с темой курсовой работы).

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.
2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.
3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2008. -Т.2. Средства защиты в сетях.
4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007.

Контрольные вопросы:

1. Приведите особенности ФС ОС.
2. Приведите особенности ФС FAT
3. Приведите особенности ФС NTFS.
4. Приведите особенности ФС ext.

3.2. Раздел 2. Подсистемы защиты операционной системы

3.2.1. Тема 2.1 ОСНОВНЫЕ ФУНКЦИИ ПОДСИСТЕМЫ ЗАЩИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ

3.2.2. Перечень изучаемых вопросов:

1. Политика изолированной программной среды.
2. Политика контроля информационных потоков.
3. Политика контроля прав доступа.

Методические указания к изучению:

Рассмотреть следующие аспекты темы:

С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами). В данном разделе речь пойдет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами.

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций и контролировать выполнение установленного порядка.

Отношение "субъекты-объекты" можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах - объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа.

Матрицу доступа, ввиду ее разреженности, неразумно хранить в виде двухмерного массива. Обычно ее хранят по столбцам, т. е. для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами.

Списки доступа - исключительно гибкое средство. С их помощью легко выполнить требование о гранулярности прав с точностью до пользователя. Посредством списков несложно добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством произвольного управления доступом.

Подавляющее большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Основное достоинство произвольного управления - гибкость.

Политика изолированной программной среды реализуется путем изоляции субъектов системы друг от друга и путем контроля порождения новых субъектов таким образом, чтобы в системы могли активизироваться субъекты только из определенного списка.

Политика контроля информационных потоков основана на разделении всех возможных информационных потоков между объектами системы на 2 непересекающихся множества: благоприятные и неблагоприятные информационные потоки. Цель данной политики – обеспечить невозможность возникновения в системе неблагоприятных информационных потоков.

При работе над курсовым проектом обратите внимание на:

- описание особенностей политики прав доступа в ОС, которые требуется приводить в первой (теоретической) главе (в соответствии с темой курсовой работы).

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т: учебник для вузов / С. В. Запечников, Н. Г.Милославская. - Москва: Горячая линия-Телеком, 2008. - Т.2 . Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007.

Контрольные вопросы:

1. Приведите особенности матриц доступа.
2. Приведите особенности контроля информационных потоков
3. Приведите особенности контроля прав доступа.
4. Приведите особенности моделей прав доступа.

3.2.2 Тема 2.2 УПРАВЛЕНИЕ ДОСТУПОМ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА UNIX

Перечень изучаемых вопросов:

Идентификатор пользователя, группы.

Модель полномочий Linux.

Дополнительные атрибуты безопасности.

Методические указания к изучению:

Рассмотреть следующие аспекты темы:

Администратор системы - пользователь root - имеет UID равный нулю (0). Кроме администратора, есть еще несколько идентификаторов пользователей, которые автоматически создаются системой при установке. EUID – это «эффективный» UID процесса. Управление правами доступа. **Sticky bit (он же бит закрепления в памяти), SUID (он же Set User ID), SGID (он же Set Group ID).** Дополнительные возможности по управлению правами доступа к файлам.

Построение файловой системы и разграничение доступа к файловым объектам имеет особенности, присущие данному семейству ОС. Рассмотрим кратко эти особенности. Все дисковые накопители (тома) объединяются в единую ***виртуальную файловую систему*** путем операции монтирования тома. При этом содержимое тома проецируется на выбранный каталог файловой системы. Элементами файловой системы являются также все устройства, подключаемые к защищаемому компьютеру (монтируемые к файловой системе). Поэтому разграничение доступа к ним осуществляется через файловою систему.

Каждый файловый объект имеет индексный дескриптор, в котором среди прочего хранится информация о разграничении доступа к данному файловому объекту. Права доступа делятся на три категории: доступ для владельца, доступ для группы и доступ для остальных пользователей. В

каждой категории определяются права на чтение, запись и исполнение (в случае каталога - просмотр).

Идентификатор пользователя называется UID - User Identifier, а идентификатор его группы - GID - Group Identifier. При каждом входе пользователя в систему, ядро Юникса регистрирует его UID и GID и выполняет все последующие процессы (программы) пользователя в соответствии с назначенными его UID и GID правами доступа.

Администратор системы - пользователь root - имеет UID равный нулю (0), и на него не распространяются никакие ограничения системы. То есть, он может читать любой файл в системе, добавлять-удалять устройства, администрировать аккаунты пользователей и делать все остальные присущие администрированию системы действия.

Кроме администратора, есть еще несколько идентификаторов пользователей, которые автоматически создаются системой при установке - такие как daemon (uid=1), bin (uid=2), sys (uid=3), adm (uid=4), lp, uucp, и nobody. Конкретные номера идентификаторов пользователей для этих имен, а также наличие приведенных здесь и других специальных системных аккаунтов **зависят от конкретного Unix.**

Эти системные аккаунты используются автоматически для разделения и безопасного выполнения системных задач (т.е. чтобы многие операции можно было запускать с полномочиями этих аккаунтов, а не суперпользовательскими).

EUID – это «эффективный» UID процесса. EUID используется для того, чтобы определить, к каким ресурсам и файлам у процесса есть право доступа. У большинства процессов UID и EUID будут одинаковыми. Исключение составляют программы, у которых установлен бит смены идентификатора пользователя.

Помимо этого в ОС данного класса используется эффективный идентификатор группы (EGID). GID – это идентификационный номер группы данного процесса. EGID связан с GID также, как EUID с UID.

Для каждого объекта файловой системы в модели полномочий Linux есть три типа полномочий: полномочия *чтения* (*r от read*), *записи* (*w от write*) и *выполнения* (*x от execution*). В полномочия записи входят также возможности удаления и изменения объекта. Право выполнения можно установить для любого файла. Потенциально, любой файл в системе можно запустить на выполнение, как программу в Windows. В Linux является ли файл исполняемым или нет, определяется не по его расширению, а по правам доступа. Кроме того, эти полномочия указываются отдельно для *владельца* файла, членов *группы* файла и для всех *остальных*.

Управление правами доступа происходит с помощью команды ***chmod***, управление владельцем файла происходит с помощью команды chown.

В Linux кроме прав чтения, выполнения и записи, есть еще 3 дополнительных атрибута:

1. Sticky bit (он же бит закрепления в памяти). Sticky bit появился в пятой редакции UNIX в 1974 году для использования в исполняемый файлах. Он применялся для уменьшения времени загрузки наиболее часто используемых программ. После закрытия программы код и данные оставались в памяти, а следующий запуск происходил быстрее. (отсюда и название - бит закрепления в памяти)

Сегодня sticky bit используется в основном для каталогов, чтобы защитить в них файлы. В такой каталог может писать ЛЮБОЙ пользователь. Из такой директории пользователь может удалить только те файлы, владельцем которых он является. Примером может служить директория /tmp, в которой запись открыта для всех пользователей, но нежелательно удаление чужих файлов.

2. SUID (он же Set User ID). Атрибут исполняемого файла, позволяющий запустить его с правами владельца. В Unix-подобных системах приложение запускается с правами пользователя, запустившего указанное приложение.

3. SGID (он же Set Group ID). Аналогичен SUID, но относиться к группе. При этом, если для каталога установлен бит SGID, то создаваемые в нем объекты будут получать группу владельца каталога, а не пользователя.

В Linux права доступа сохраняются в inode файла, и поскольку inode у каждого файла свой собственный, права доступа у каждого файла свои. Так же, права доступа пользователя и группы не суммируются. Если программа выполняется с правами пользователя и группы, которым принадлежит файл — работают только права хозяина файла.

При работе над курсовым проектом обратите внимание на:

- описание особенностей политики прав доступа в ОС, которые требуется приводить в первой (теоретической) главе (в соответствии с темой курсовой работы).

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т: учебник для вузов / С. В. Запечников, Н. Г.Милославская. - Москва: Горячая линия-Телеком, 2008. -Т. 2. Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007.

Контрольные вопросы:

1. Приведите особенности матриц доступа в ОС Linux.

2. Приведите особенности контроля информационных потоков в ОС Linux.
3. Приведите особенности контроля прав доступа в ОС Linux.
4. Приведите особенности моделей прав доступа в ОС Linux.

3.2.3 Тема 2.3 УПРАВЛЕНИЕ ДОСТУПОМ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА WINDOWS

Перечень изучаемых вопросов:

1. Объекты доступа.
2. Субъекты доступа
3. Методы доступа к объектам.
4. Права доступа к объектам.
5. Привилегии субъектов.
6. Маркер доступа пользователя.

Методические указания к изучению:

Рассмотреть следующие аспекты темы:

ОС Windows поддерживает 22 метода доступа субъектов к объектам. Шесть из них представляют собой стандартные методы доступа и поддерживаются для объектов всех типов.

Каждому методу доступа соответствует право на его осуществление. Эти права доступа называются специфичными, поскольку они специфичны для каждого типа объектов. Для каждого типа объектов может поддерживаться до 16 специфичных прав доступа.

В Windows каждый субъект доступа обладает некоторым набором привилегий. Привилегии представляют собой права на выполнение субъектом действий, касающихся системы в целом, а не отдельных ее объектов. В Windows каждый пользователь (в том числе и каждый псевдопользователь), работающий в системе, имеет свой маркер доступа (access token). Каждому процессу Windows назначается первичный маркер доступа (primary access token). Все пользователи и псевдопользователи ОС, включая администраторов и ОС, обладают ограниченными полномочиями.

Атрибуты защиты объекта Windows описываются специальной структурой данных, называемой дескриптором защиты (security descriptor).

В Windows NT все объекты ОС являются объектами доступа. Иерархия типов объектов имеет древовидную структуру. Операции, определенные над объектами некоторого типа, наследуются и объектами всех подтипов данного типа. Элементы списка избирательного контроля доступа н (access control entries, ACE).

Windows позволяет прикладным и сервисным процессам создавать объекты доступа нестандартных типов, перед созданием которых процесс должен зарегистрировать в системе данный тип объекта. Разграничение доступа субъектов к нестандартным объектам организуется так же, как и к стандартным.

Субъекты доступа. Субъекты доступа, которые поддерживает ОС Windows.

1. Пользователи - обычные пользователи и псевдопользователи. К псевдопользователям относятся следующие субъекты доступа:

• SYSTEM - ОС локального компьютера; этот псевдопользователь всегда входит в группу Administrators и имеет все привилегии;

• псевдопользователи с именами вида <имя_компьютера>$, где <имя_компьютера> - сетевое имя компьютера; эти псевдопользователи представляют ОС других компьютеров сети и используются при аутентификации рабочей станции на контроллере домена.

2. Группы пользователей. Группы пользователей могут пересекаться, т.е. каждый пользователь может входить в несколько групп. При этом для совместимости с программным интерфейсом POSIX, поддерживаемым среди групп, в которые входит пользователь, выделяется первичная группа, которая играет роль той единственной группы, в которую может входить пользователь в POSIX.

3. Специальные (временные) группы. В отличие от обычных групп членство пользователя в таких группах определяется ОС в зависимости от действий пользователя. Специальная группа не может быть объявлена первичной группой пользователя.

4. Относительные субъекты. Эти субъекты имеют смысл только в применении к объекту, для которого определяются права доступа. Существуют следующие относительные субъекты:

• CREATOR_OWNER - владелец объекта;

• CREATOR GROUP - первичная группа владельца объекта.

Относительные субъекты используются, если нужно описать права доступа пользователей к объектам по принципу «что кому принадлежит, то ему и доступно».

Также существует несколько предопределенных идентификаторов, которые используются ОС внутренне или зарезервированы для последующих версий.

Идентификаторы остальных субъектов доступа уникальны.

Члены предопределенной группы Administrators могут создавать, удалять и изменять свойства любых субъектов, а члены группы Account Operators - создавать, удалять и изменять свойства только непривилегированных субъектов (обычных пользователей). Если не ограничиваться использованием только стандартных средств администрирования, то для работы со списком субъектов достаточно иметь полный доступ к нескольким ключам реестра.

Станция в составе рабочей группы. Ресурсы каждой рабочей станции доступны другим рабочим станциям в составе группы. Информация безопасности, управляющая допуском пользователей к ресурсам рабочей станции, хранится на этой станции.

Член домена. В домене предусмотрено централизованное управление безопасностью через базу данных, хранящуюся на одном из серверов домена, который называется первичным контроллером домена (Primary Domain Con troller - P O C). Клиентская рабочая станция в составе гетерогенной вычислительной сети (например, IntranetWare и Windows NT). Удаленный доступ к ресурсам данной рабочей станции невозможен.

Изложенная выше структура носит название NT Directory Services (NTDS).

Профили пользователя представляют собой набор параметров, определяющих:

- настройки рабочего стола пользователя (положение значков, обои и т.д.);
- автоматические подключения сетевых дисков при входе в сеть;
- приложения, которые запускаются при старте операционной системы.

Различают следующие типы профилей пользователя:

- локальный профиль, хранящийся на рабочей станции;
- блуждающий, хранящийся на сервере - первичном контроллере домена - и
- изменяющийся пользователем;
- мандатный, хранящийся на сервере - первичном контроллере домена - и не
- изменяющийся пользователем.

Системная политика (System Policy) в Windows NT представляет собой некоторый набор значений, который присваивается соответствующим параметрам реестра в момент аутентификации пользователя в сеть. Системная политика определяется для пользователя, группы пользователей, и для компьютера. В случае, если какой-то параметр системной политики противоречит настройкам профиля пользователя, используется настройка системной политики.

Использование профилей и системных политик позволяет создать замкнутую рабочую среду, облегчающую выполнение пользователем производственных задач и затрудняющих выполнение не относящихся к основной производственной деятельности действий.

Помимо перечисленных выше групп определена группа Everyone. Эта группа включает по умолчанию в себя всех пользователей Windows NT. Список членов этой группы не может быть изменен. Стандартные группы не могут быть переименованы.

Методы доступа к объектам. ОС Windows поддерживает 22 метода доступа субъектов к объектам. Шесть из них представляют собой стандартные методы доступа и поддерживаются для объектов всех типов:

• удаление объекта;
• получение атрибутов защиты объекта;
• изменение атрибутов защиты объекта;

• изменение владельца объекта; при этом субъект может объявить новым владельцем объекта только себя;

• ACCESS_SYSTEM_SECURITY - получение и изменение параметров аудита в отношении объекта;

• SYNCHRONIZE - метод доступа, заключающийся в вызове системной функции WaitForSingleObject для данного объекта или функции WaitForMultipleObjects для списка объектов, включающего данный объект. Эти функции используются, когда поток должен ожидать какое-то изменение в состоянии объекта, не затрачивая на это процессорного времени. Обычно этот метод доступа применяется к объектам синхронизации, реже - к процессам и потокам.

Для каждого типа объекта поддерживается до шестнадцати специфичных методов доступа.

Права доступа к объектам. Каждому методу доступа соответствует право на его осуществление. Эти права доступа называются специфичными, поскольку они специфичны для каждого типа объектов. Для каждого типа объектов может поддерживаться до 16 специфичных прав доступа.

Каждому стандартному методу доступа, за исключением ACCESS_SYSTEM_SECURITY, также соответствует право доступа, дающее возможность реализации соответствующего метода доступа. Такие права доступа называются стандартными.

Windows NT поддерживает также общие (generic) или отображаемые (mapped) права доступа. Каждое из отображаемых прав доступа представляет собой некоторую комбинацию стандартных и специфичных прав доступа. Отображаемые права доступа могут быть предоставлены для доступа к объекту любого типа, однако конкретное содержание отображаемого права доступа зависит от типа объекта. Процесс преобразования отображаемого права доступа в набор прав на реализацию методов доступа к объекту называется отображением права доступа. Порядок отображения отображаемых методов доступа для объектов конкретного типа определяется при регистрации данного типа объектов.

Отображаемые права доступа введены в систему разграничения доступа по следующим двум причинам:

- отображаемые права доступа позволяют пользователю устанавливать права доступа к объекту, ничего не зная о специфике объектов данного типа;

- отображаемые права доступа необходимы для обеспечения совместимости с POSIX.

Последним классом прав доступа, поддерживаемых Windows, являются виртуальные права доступа, которые не могут быть предоставлены субъекту, но могут быть запрошены им.

Привилегии субъектов. В Windows каждый субъект доступа обладает некоторым набором привилегий. Привилегии представляют собой права на выполнение субъектом действий, касающихся системы в целом, а не отдельных ее объектов. Существуют следующие привилегии:

• завершать работу ОС и перезагружать компьютер;

• устанавливать системное время;

• анализировать производительность одного процесса тп.

Существует еще несколько привилегий, идентификаторы которых зарезервированы для использования в будущих версиях Windows.

При входе в систему пользователь получает привилегии, предоставленные ему индивидуально, а также привилегии, предоставленные группам, в которые он входит. Назначать привилегии субъектам доступа может только администратор. Обычно все привилегии пользователя, кроме привилегии получать оповещения от файловых систем, выключены. Для того, чтобы пользователь смог воспользоваться своей привилегией, он должен вначале ее включить с помощью системного вызова AdjustTokenPrivileges. После использования привилегию рекомендуется снова выключить.

Некоторые из перечисленных привилегий позволяют субъектам, обладающим ими, преодолевать те или иные элементы защиты ОС.

Маркер доступа пользователя. В Windows каждый пользователь (в том числе и каждый псевдопользователь), работающий в системе, имеет свой маркер доступа.

Маркер доступа (access token) - это объект специального вида, содержащий следующую информацию:

• идентификатор пользователя;

• идентификаторы групп и специальных групп, в которые входит пользователь;

• привилегии пользователя;

• идентификатор сеанса работы пользователя, к которому относится маркер доступа;

• атрибуты защиты, которые назначаются по умолчанию новым объектам, созданным пользователем в текущем сеансе работы;

• имя и идентификатор подсистемы, выдавшей маркер доступа (Advapi, если пользователь вошел в систему локально, NtLogon, если пользователь вошел в систему по сети через SMB-сервер, и т.д.);

• некоторую служебную информацию.

Маркер доступа содержит всю информацию о пользователе, необходимую системе разграничения доступа для принятия решений о предоставлении пользователю доступа к тем или иным объектам.

Каждому процессу Windows NT назначается первичный маркер доступа (primary access token) - маркер доступа пользователя, запустившего данный процесс. Субъект, обладающий соответствующей привилегией, может назначить процессу другой первичный маркер доступа. Отдельным потокам процесса могут назначаться свои маркеры доступа - маркеры олицетворения (impersonation access tokens).

Дескриптор защиты. Атрибуты защиты объекта Windows описываются специальной структурой данных, называемой дескриптором защиты (security descriptor), который содержит следующую информацию:

• идентификатор владельца объекта;

• идентификатор первичной группы владельца объекта;

• список избирательного контроля доступа (discretionary access control list, DACL) - список, полностью описывающий права различных субъектов на объект;

• системный список контроля доступа (system access control list, SACL) - используется при генерации сообщений аудита.

Если объект не имеет дескриптора защиты, при обращениях субъектов к нему права доступа не проверяются. В этом случае любой субъект имеет абсолютные права на данный объект.

Дескриптор защиты хранится вместе с объектом, при этом формат хранения объекта должен предоставлять такую возможность.

Элементы списка избирательного контроля доступа называются элементами контроля доступа (access control entries, ACE). Каждый элемент контроля доступа разрешает или запрещает некоторому субъекту определенные права доступа к объекту. Если список избирательного контроля доступа отсутствует в дескрипторе защиты, всем субъектам предоставляются все права доступа к объекту.

Владелец имеет право изменять дескриптор защиты объекта, даже если это явно запрещено ему списком избирательного контроля доступа. Пользователь, обладающий привилегией объявлять себя владельцем объекта (привилегия администратора), может объявлять себя владельцем тех объектов, для которых это явно запрещено ему списком избирательного контроля доступа. В остальном список избирательного контроля доступа полностью описывает права различных субъектов на доступ к данному объекту.

Каждая запись управления доступом (ACE) состоит из идентификатора пользователя или группы пользователей и совокупности разрешенных методов доступа.

Стандартные средства работы с файлами не поддерживают механизм разграничения доступа в полном объеме. Для того чтобы список избирательного контроля доступа файла можно было просматривать и редактировать, информация, содержащаяся в этом списке, должна удовлетворять следующим требованиям:

- все элементы списка, запрещающие доступ субъектов к объекту, должны находиться в начале списка;

- все элементы списка, запрещающие доступ субъектов к объекту, должны запрещать им все права доступа к объекту.

В отличие от UNIX в Windows отсутствует суперпользователь. Все пользователи и псевдопользователи ОС, включая администраторов и ОС, обладают ограниченными полномочиями. Однако субъект, обладающий привилегией администратора, может получить доступ к любому объекту ОС по любому методу доступа за исключением метода ACCESS_SYSTEM_SECURITY, для которого требуется привилегия аудитора. Для этого субъект должен вы полнить следующие действия:

- используя привилегию администратора, объявить себя владельцем объекта;

- используя полномочия владельца, предоставить себе необходимые права доступа к объекту;

- обратиться к объекту, используя полученные права.

При работе над курсовым проектом обратите внимание на:

- описание особенностей политики прав доступа в ОС, которые требуется приводить в первой (теоретической) главе (в соответствии с темой курсовой работы).

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т.: учебник для вузов / С. В. Запечников, Н. Г.Милославская. - Москва: Горячая линия-Телеком, 2008. -Т. 2. Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007.

Контрольные вопросы:

1. Приведите особенности матриц доступа в ОС Windows.
2. Приведите особенности контроля информационных потоков в ОС Windows.
3. Приведите особенности контроля прав доступа в ОС Windows.
4. Приведите особенности моделей прав доступа в ОС Windows.

3.2.4 Тема 2.4 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ В ОС LINUX

Перечень изучаемых вопросов:

1. Стандартная процедура идентификации и аутентификации.
2. Основные механизмы защиты паролей.
3. Шифрование паролей.

Методические указания к изучению:

Рассмотреть следующие аспекты темы:

Linux обеспечивает защиту паролей с помощью трех основных механизмов:

- шифрование паролей.

- механизм «теневых паролей».

- механизм подключаемых модулей аутентификации PAM (Pluggable Authentication Modules).

Механизм «теневых паролей». Механизм PAM представляет собой набор открытых библиотек подключаемых модулей аутентификации (PAM), предназначенных для выполнения ввода пароля и проверки его подлинности.

В Linux для шифрования паролей используется алгоритм DES. Зашифрованный пароль обычно помещается в файл /etc/passwd.

Стандартная процедура идентификации и аутентификации пользователя в ОС UNIX заключается в том, что система ищет имя пользователя в файле /etc/passwd, и если пользователь идентифицирован, то аутентификация заключается в сравнении введенного пароля с паролем, который хранится в зашифрованном виде. Следует отметить, что в настоящее время почти во всех версиях UNIX зашифрованный пароль не хранится в файле /etc/passwd, поскольку этот файл открыт для чтения всем пользователям, а хранится в закрытом файле /etc/shadow.

В безопасной системе стандартная процедура идентификации и аутентификации расширена. В ней предусмотрено больше правил, касающихся типов используемых паролей. Введены процедуры генерации и смены паролей. Изменены местоположение и механизм защиты некоторых частей базы данных паролей. Администратору аутентификации предоставлены дополнительные возможности для контроля действий пользователей.

Для реализации правил использования безопасных паролей в UNIX существуют средства. Задание администратором следующих требований к паролям:

- ограничение минимальной длины пароля;

- наличие в пароле обязательного минимального количества букв нижнего и верхнего регистров, цифр и специальных символов;

- запрещение пользователю введения собственных паролей; разрешение вводить только пароли, сгенерированные системой.

Задание администратором временных ограничений по частоте сменяемости и времени жизни паролей:

- автоматическое блокирование входа пользователя в систему при истекшем сроке действия пароля и при определенном числе неуспешных попыток входа;

- задание каждому пользователю количества и номеров терминалов для входа в систему;

- проверка системой паролей пользователей при их вводе на стойкость (вхождение идентификатора, имя пользователя, повторяемость символов и т. д.);

- хранение зашифрованных паролей в закрытом от доступа отдельном файле /etc/shadow.

Помимо этого, существует возможность блокирования по числу неуспешных попыток входа не только пользователя, но и терминала; при этом можно задать интервал времени между попытками регистрации. Также предусмотрено ведение записей об успешных и неуспешных попытках входа в систему.

Больше ограничить действия пользователя можно с помощью введения в его стартовый командный файл profile определенной команды, которая будет вызываться через команду exec. При этом если в стартовый командный файл добавить команды trap и exit, то пользователь сможет работать только с заданной ему командой.

Linux обеспечивает защиту паролей с помощью трех основных механизмов:

- шифрование паролей.
- механизм «теневых паролей».
- механизм подключаемых модулей аутентификации PAM (Pluggable Authentication Modules).

Шифрование паролей. В Linux для шифрования паролей используется алгоритм DES. Зашифрованный пароль обычно помещается в файл /etc/passwd. При попытке пользователя зарегистрироваться в системе введенный им пароль шифруется и затем сравнивается с записью в парольном файле. Для Linux были разработаны дополнительно к шифрованию еще два механизма защиты.

Механизм «теневых паролей». Суть этого механизма заключается в том, что зашифрованный парольный файл помещается в файл /etc/shadow, права на чтение которого принадлежат только суперпользователям. Для реализации подобной схемы защиты в Linux используется набор программных средств Shadow Suite. В большинстве дистрибутивов Linux механизм «теневых паролей» по умолчанию не задействован (кроме RedHat).

Механизм PAM представляет собой набор открытых библиотек подключаемых модулей аутентификации (PAM), предназначенных для выполнения ввода пароля и проверки его подлинности. Технология PAM позволяет реализовать новые возможности при создании системы защиты: в модулях безопасности применяются нестандартные процедуры шифрования (MD5 и им подобные); установка ограничений на использование пользователями системных ресурсов; установка разрешения отдельным пользователям регистрации только в фиксированные промежутки времени и только с определенных терминалов или узлов.

При работе над курсовым проектом обратите внимание на:

- описание особенностей механизма аутентификации в ОС, которые требуется приводить в первой (теоретической) главе (в соответствии с темой курсовой работы).

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2008. -Т. 2. Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007.

Контрольные вопросы:

1. Приведите особенности аутентификации в ОС Linux.
2. Приведите особенности использования паролей в ОС Linux.
3. Приведите особенности механизмы контроля паролей в ОС Linux.
4. Приведите особенности моделей прав доступа в ОС Linux.

3.2.5 Тема 2.5 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ В ОС Windows

Перечень изучаемых вопросов:

1. Стандартная процедура идентификации и аутентификации.
2. Основные механизмы защиты паролей.
3. Шифрование паролей.

Методические указания к изучению:

Рассмотреть следующие аспекты темы:

Верхний уровень подсистемы аутентификации Windows включает в себя процесс аутентификации WinLogon.exe и так называемые библиотеки-провайдеры или просто провайдеры - заменяемые библиотеки, реализующие большую часть высокоуровневых функций процесса аутентификации.

При выполнении второго этапа данной процедуры WinLogon использует привилегии псевдопользователя SYSTEM создавать маркеры доступа и выступать от имени ОС, а при выполнении третьего этапа - привилегию назначать процессам маркеры доступа.

Нижний уровень подсистемы аутентификации отвечает за хранение учетной информации о пользователях, в том числе и эталонных образов паролей. При аутентификации нижний уровень передает среднему уровню эталонный образ пароля пользователя, а при авторизации - список групп и привилегий пользователя.

Для генерации образа пароля стандартный пакет аутентификации MSV 1.0 применяет хэш-функцию MD4. Для совместимости с более ранними версиями Windows MSV 1.0 поддерживает другой формат образа пароля.

Администратор определяет, могут ли пользователи самостоятельно менять пароль в случае истечения максимального срока его действия или они должны уведомлять его об этом.

Механизм автоматической блокировки (lock out) при превышении максимально допустимого количества неудачных попыток входа в систему не распространяется на пользователя Administrator.

Подсистема аутентификации Windows состоит из нескольких программных модулей, связанных между собой, и разделена на три уровня. Средний уровень подсистемы аутентификации пользуется услугами нижнего уровня и предоставляет услуги верхнему.

Верхний уровень подсистемы аутентификации Windows включает в себя процесс аутентификации WinLogon.exe и так называемые библиотеки-провайдеры или просто провайдеры - заменяемые библиотеки, реализующие большую часть высокоуровневых функций процесса аутентификации.

WinLogon представляет собой обычный процесс Win32 API, выполняющийся от имени псевдопользователя SYSTEM. WinLogon автоматически запускается при старте ОС и остается активным до выключения питания или перезагрузки.

При входе пользователя в систему с локальной консоли в качестве провайдера по умолчанию выступает библиотека msgina.dll, которая осуществляет все взаимодействия между локальным пользователем и процессом аутентификации.

Вход пользователя в ОС производится следующим образом.

1. Провайдер получает от пользователя идентифицирующую и аутентифицирующую информацию.

2. Провайдер осуществляет аутентификацию, передавая имя и пароль на средний уровень подсистемы аутентификации с помощью системного вызова LogonUser. При этом, если аутентификация прошла успешно, создается маркер доступа пользователя.

3. Если маркер доступа пользователя создан успешно, провайдер осуществляет авторизацию пользователя, запуская процесс Userlnit.exe от имени аутентифицированного пользователя.

4. Процесс Userlnit загружает индивидуальные настройки пользователя из его профиля (profile), монтирует ключ реестра, соответствующий данному пользователю, и загружает программную среду пользователя. После этого Userlnit завершает работу.

При выполнении второго этапа данной процедуры WinLogon использует привилегии псевдопользователя SYSTEM создавать маркеры доступа и выступать от имени ОС, а при выполнении третьего этапа - привилегию назначать процессам маркеры доступа. Таким образом, если эти привилегии не будут предоставлены псевдопользователю SYSTEM, вход пользователей в систему станет невозможен.

В средний уровень подсистемы аутентификации входят локальный распорядитель безопасности (local security authority, LSA) и пакеты

аутентификации - заменяемые библиотеки, реализующие большую часть низкоуровневых функций аутентификации.

Так же, как и WinLogon, LSA представляет собой обычный процесс (по имени lsass.exe), выполняющийся от имени псевдопользователя SYSTEM. Аварийное завершение LSA приводит к аварийному завершению работы всей ОС. Как и WinLogon, LSA передоверяет большинство своих функций заменяемым библиотекам. Стандартная схема аутентификации реализуется пакетом MSV 1.0 (msv1_0.dll), могут быть установлены и другие пакеты аутентификации.

Пакет аутентификации осуществляет аутентификацию пользователя в процессе обработки системного вызова LogonUser. Аутентификация производится следующим образом.

1. Пакет аутентификации получает от верхнего уровня имя и пароль пользователя и генерирует образ пароля.

2. Используя услуги нижнего уровня, пакет аутентификации получает эталонный образ пароля и сравнивает его с образом пароля из п. 1.

3. При совпадении образов паролей LSA получает от нижнего уровня информацию о том, может ли данный пользователь начинать в данный момент работу с данной рабочей станцией.

4. При положительном результате проверки LSA формирует маркер доступа пользователя, получая необходимую информацию от нижнего уровня подсистемы аутентификации.

5. LSA передает сформированный маркер доступа верхнему уровню подсистемы аутентификации.

Нижний уровень подсистемы аутентификации отвечает за хранение учетной информации о пользователях, в том числе и эталонных образов паролей. При аутентификации нижний уровень передает среднему уровню эталонный образ пароля пользователя, а при авторизации - список групп и привилегий пользователя.

При стандартной конфигурации ОС нижний уровень подсистемы аутентификации включает в себя систему управления списком пользователей (Security Account Manager, SAM) и сервис NetLogon. SAM используется для извлечения информации из реестра локального компьютера, а NetLogon - информации из реестра контроллера домена. Администраторы системы могут устанавливать и другие сервисы аналогичного назначения.

Механизм автоматической блокировки (lock out) при превышении максимально допустимого количества неудачных попыток входа в систему не распространяется на пользователя Administrator.

Для пользователей могут быть установлены следующие флаги:

- пользователь обязан сменить пароль при ближайшем входе в систему (для вновь зарегистрированных пользователей);

- пользователь не может менять свой пароль (применяется для «групповых» пользователей (Guest, Anonymous и т. д.));

- на пользователя не распространяется ограничение максимального срока действия пароля (применяется в совокупности с предыдущим требованием);

- пользователь не может работать в системе (применяется для временного блокирования учетной записи пользователя).

Кроме того, могут быть введены следующие требования к процедуре авторизации пользователя. Может быть явно указан путь к профилю (profile) пользователя. В этом случае индивидуальные настройки пользователя будут загружаться не из системной директории локального компьютера, а из той директории того компьютера, которая указана в пути к профилю. В результате индивидуальные настройки пользователя могут быть сделаны одинаковыми для нескольких компьютеров. Пользователю может быть назначен скрипт (программа или командный файл), который будет автоматически выполняться при каждом входе пользователя в систему, локальном или удаленном. Пользователю может быть назначена домашняя директория, которая становится текущей по умолчанию для всех его программ.

Для пользователей домена Windows могут быть введены следующие дополнительные требования к процедурам идентификации, аутентификации и авторизации:

- время работы пользователя с ОС может быть ограничено;
- количество компьютеров, с которых пользователь может входить в домен, может быть ограничено (до восьми компьютеров);
- может быть установлена автоматическая блокировка учетной записи пользователя по истечении определенного времени;
- пользователю может быть запрещен интерактивный вход на любой компьютер домена; в этом случае пользователь может работать с доменом только извне.

Помимо вышеперечисленных требований и ограничений при идентификации и аутентификации пользователя также осуществляется проверка одной из следующих «привилегий»:

- входить в систему интерактивно;
- входить в систему через SMB-сервер;
- запускать сервис от своего имени;
- запускать от своего имени пакетное задание.

Альтернативные схемы идентификации и аутентификации. Поскольку и провайдеры, и пакеты аутентификации являются заменяемыми компонентами подсистемы аутентификации, администратор ОС может, установив нестандартный провайдер и/или пакет аутентификации, реализовать в Windows NT любую другую схему аутентификации. Для этого необходимо разместить в системной директории Windows NT необходимые библиотеки и внести изменения в соответствующие ключи реестра.

При этом в качестве аутентифицирующей информации может использоваться произвольная строка Unicode длиной до 128 символов.

При работе над курсовым проектом обратите внимание на:

- описание особенностей механизма аутентификации в ОС, которые требуется приводить в первой (теоретической) главе (в соответствии с темой курсовой работы).

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2008. -Т.2 . Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007.

Контрольные вопросы:

1. Приведите особенности аутентификации в ОС Windows.
2. Приведите особенности использования паролей в ОС Windows.
3. Приведите особенности механизмы контроля паролей в ОС Windows.
4. Приведите особенности моделей прав доступа в ОС Windows.

3.2.5 Тема 2.6 АУДИТ ОС

Перечень изучаемых вопросов:

1. Процедура аудита применительно к ОС.
2. Требования к аудиту операционной системы.
3. Политика аудита.
4. Реализация аудита в UNIX.
5. Реализация аудита в Windows.

Методические указания к изучению:

Рассмотреть следующие аспекты темы:

Политика аудита представляет собой совокупность правил, определяющих то, какие события должны регистрироваться в журнале аудита. Для обеспечения надежной защиты ОС в журнале аудита должны обязательно регистрироваться следующие события:

- попытки входа / выхода пользователей из системы;
- попытки изменения списка пользователей;

- попытки изменения политики безопасности, в том числе и политики аудита.

Система контроля регистрирует события в ОС, связанные с защитой информации, записывая их в контрольный журнал, в котором возможна фиксация проникновения в систему и неправильного использования ресурсов.

Политика аудита. Множество событий, информация о которых записывается в журнал аудита, определяется политикой аудита, которую назначают пользователи-аудиторы. Windows позволяет регистрировать в журнале аудита события следующих категорий:

• вход / выход пользователя из системы;
• доступ субъектов к объектам;
• использование субъектами доступа опасных привилегий;
• изменения в списке пользователей;
• изменения в политике безопасности;
• системные события;
• запуск и завершение процессов.

Считаются опасными следующие привилегии субъектов:

• получать оповещения от файловой системы;
• добавлять записи в журнал аудита;
• создавать маркеры доступа;
• назначать маркеры доступа процессам;
• создавать резервные копии информации;
• восстанавливать информацию на дисках с резервных копий;
• отлаживать программы.

Одним из наиболее сложных вопросов является вопрос о том, какой должна быть политика аудита. Политика аудита настолько сильно связана с особенностями эксплуатации конкретного экземпляра ОС, что сформулировать эталонную политику просто невозможно. Даже для конкретного экземпляра ОС нельзя сформулировать адекватную политику аудита «на все времена». Политика аудита должна постоянно меняться, реагируя на изменения в конфигурации ОС и на зарегистрированные опасные события.

При определении политики аудита следует иметь в виду, что адекватность политики заключается в том, что регистрируется ровно столько событий, сколько необходимо. Если подсистема аудита регистрирует слишком много событий, то, с одной стороны, журнал аудита переполняется слишком быстро, а с другой - аудитору трудно выделить в огромном объеме информации важные события.

Аудит в UNIX. Считается, что действие контролируется, если можно определить реального пользователя, который его осуществил. Концептуально при построении ОС UNIX некоторые действия нельзя контролировать на уровне действий реального пользователя. Например, пользовательские бюджеты, такие как lp, cron или uucp, используются анонимно, и их действия можно обнаружить только по изменениям в системной информации.

Система контроля регистрирует события в ОС, связанные с защитой информации, записывая их в контрольный журнал, в котором возможна фиксация проникновения в систему и неправильного использования ресурсов. Поскольку события, связанные с защитой информации, контролируются и учитываются вплоть до выявления конкретного пользователя, система контроля служит сдерживающим средством для злоумышленников.

В соответствии с требованиями безопасности ОС должна создавать, поддерживать и защищать журнал регистрации. Должна быть обеспечена возможность регистрации событий.

Для событий идентификации и аутентификации регистрируется также идентификатор устройства. Для действий с объектами регистрируются имена объектов.

Система контроля использует системные вызовы и утилиты для классификации действий пользователей, подразделяя их на события различного типа.

Существенно повышает эффективность контроля наличие регистрационного идентификатора пользователя (LUID). После прохождения пользователем процедур идентификации и аутентификации каждому процессу, создаваемому пользователем, присваивается регистрационный идентификатор пользователя. Данный идентификатор сохраняется с помощью таких команд как su.

Данный механизм контроля работы в режиме ядра генерирует контрольные записи по результатам выполнения пользовательских процессов с помощью системных вызовов ядра. Каждый системный вызов ядра содержит строку в таблице, в которой указывается связь системного вызова с контролем защиты информации и тип события, которому он соответствует.

Кроме того, используется таблица кодов ошибок, позволяющая классифицировать системные вызовы как конкретные события, связанные с защитой информации. Некоторые системные вызовы не имеют отношения к защите информации. Например, системный вызов getpid получает идентификатор процесса и не определяет никакого события, связанного с защитой информации. Таким образом, данный системный вызов не подлежит контролю.

Механизм контроля ядра выдает внутренний вызов в драйвер устройства для занесения записи в контрольный журнал. Информацию контроля система записывает непосредственно на диск, не дожидаясь синхронизации суперблоков в оперативной памяти и на диске, чем достигается ее защита от разрушения.

Аудит в Windows. Журнал аудита представляет собой файл с именем SecEvent.evt, расположенный в поддиректории system32config системной директории. Формат этого файла не документирован. Информация хранится в журнале аудита в открытом виде, защита журнала аудита организуется средствами подсистемы разграничения доступа. Поэтому администраторы

обязательно должны убедиться, что никто, кроме аудиторов, не имеет доступа к файлу журнала аудита.

Для просмотра журнала аудита используется стандартная утилита Event Viewer, которую можно применять и для просмотра других системных журналов. Эта утилита разрешает читать журнал аудита только членам группы Administrators, а также пользователям, обладающим привилегией аудитора. Эти ограничения доступа действуют и в том случае, когда системный раздел жесткого диска отформатирован под FAT или HPFS. Все пользователи, которые могут читать журнал аудита, могут и очищать его. Факт очистки журнала регистрируется сразу после очистки.

Пользователи, не имеющие возможности читать журнал аудита с помощью утилиты Event Viewer, но обладающие правом чтения файла SecEvent.evt, могут читать этот файл с помощью других программных средств. Поэтому права доступа субъектов к этому файлу должны быть ограничены.

Размер журнала аудита по умолчанию ограничен. Администратор может также определить поведение ОС при переполнении журнала аудита. Реакции при переполнении журнала аудита:

- старые события стираются по мере необходимости (по умолчанию);
- если самое старое событие в журнале аудита зафиксировано более N дней назад (число N выбирает администратор), одно или несколько самых старых событий стирается, в противном случае новые события не регистрируются до тех пор, пока не пройдет N дней с момента регистрации самого старого события;
- новые события не регистрируются до тех пор, пока журнал не будет очищен.

Добавлять записи в журнал аудита может лишь субъект, обладающий соответствующей привилегией. По умолчанию эта привилегия предоставляется только псевдопользователю SYSTEM. Обычно новые записи в журнал аудита добавляют ядро, подсистема Win32 и подсистема аутентификации Windows.

При работе над курсовым проектом обратите внимание на:

- описание особенностей механизма аутентификации в ОС, которые требуется приводить в первой (теоретической) главе (в соответствии с темой курсовой работы).

Литература:

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В.Информационная безопасность открытых систем. В 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2008. -Т. 2. Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. Москва: КУДИЦ-ПРЕСС, 2007.

Контрольные вопросы:

1. Приведите особенности аудита в ОС Windows.
2. Приведите особенности аудита в ОС Linux.
3. Приведите особенности построения политики аудита в ОС.
4. Приведите особенности процедур аудита в ОС.

4. ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

4.1. Текущая аттестация

В ходе изучения дисциплины студентам предстоит пройти следующие этапы текущей аттестации:

Преподаватель вправе выбрать методику оценивания знаний студентов: традиционная зачетно-экзаменационная либо балльно-рейтинговая.

Выбрана традиционная зачетно-экзаменационная методика оценивания знаний

Предусматривается: зачет, экзамен, курсовой проект

4.2. Порядок применения рейтинговой системы (не предусматривается)

В рамках балльно-рейтинговой системы выставляется оценка за качество выполнения и защиту лабораторных и контрольных работ.

Таблица 1. Шкала оценок уровня усвоения материала обучающимся

Вид деятельности	Доля	Кол-во ед.	Макс. балл за ед.	Всего
Обязательные виды деятельности				
1-й семестр				
Посещаемость занятий	20 %	N1	=200/N1	200
Выполнение лаб. работ (защита)	40 %	2	200	400
Контрольная работа 1	40 %	1	400	400

Вид деятельности	Доля	Кол-во ед.	Макс. балл за ед.	Всего
Итого:	100 %			1000
2-й семестр				
Посещаемость занятий	20 %	N2	=200/N2	200
Выполнение лаб. работ (защита)	40 %	2	200	400
Контрольная работа 2	40 %	1	400	400
Итого:	100%			1000
Всего				2000
Дополнительные задания (по выбору студента в каждом семестре)				
Подготовка реферата (видео-доклада)	20 %		200	200
Решение дополнительных задач контрольной работы	10 %		100	100
Выполнение задания в рамках НИРС	50 %		500	500

4.3 Условия получения положительной оценки

Завершающим этапом изучения дисциплины является промежуточная аттестация, представляющая собой:

Фонд оценочных средств для проведения текущего контроля успеваемости включает в себя:

- материалы для проведения текущего контроля успеваемости – варианты заданий;
- перечень компетенций и их элементов, проверяемых на каждом мероприятии текущего контроля успеваемости;
- систему и критерии оценивания по каждому виду текущего контроля успеваемости;
- описание процедуры оценивания.

Текущий контроль в форме опроса.

Текущий контроль осуществляется путем опроса по материалу, пройденному на предшествующих лекциях.

Оценивается (Таблицы 2,3,4,5,6):

- полнота усвоения пройденного материала,
- качество изложения пройденного материала (устно и письменно).

Таблица 2. Шкала оценок уровня усвоения материала обучающимся

Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Не может ответить на вопросы по пройденному материалу или графически изобразить на доске	Отвечает сбивчиво, путается в определениях и обозначениях, нуждается в помощи других обучающихся	Допускает незначительные ошибки при изложении пройденного материала, не полностью представляет связи между разделами изучаемой дисциплины	Четко отвечает на вопросы, может точно изобразить графическую часть пройденного материала, увязывает последовательность изученных разделов дисциплины

Таблица 3. Шкала оценок уровня освоения дисциплины по зачету

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Правильные ответы даны менее чем на 50% включительно. Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Имеются заметные нарушения норм литературной речи	Правильные ответы даны на 51-64% вопросов. Допускаются нарушения в последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются	Правильные ответы даны на 65-94% вопросов. Ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется	Правильные ответы даны на 95-100% вопросов. Ответы на поставленные в билете вопросы излагаются логично, последовательно и не требуют дополнительн

	нарушения норм литературной речи	умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи	ых пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания предмета. Соблюдаются нормы литературной речи

Таблица 4. Шкала оценок уровня освоения дисциплины по экзамену.

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетвори-тельно)	«3» (удовлетвори-тельно)	«4» (хорошо)	«5» (отлично)
Не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические задания, задачи	Усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий	Твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми умениями и навыками при выполнении практических заданий	Глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его изложил, не затрудняется с ответом при видоизменении задания, свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые

			решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок

Таблица 5. Шкала оценок уровня освоения дисциплины по тесту

Оценка			
Неудовлетвори-тельный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетвори-тельно)	«3» (удовлетвори-тельно)	«4» (хорошо)	«5» (отлично)
Менее 50 % правильных ответов	50-70 % правильных ответов	71-90 % правильных ответов	91-100 % правильных ответов

Таблица 6. Шкала оценок курсового проекта

Оценка			
Неудовлетвори-тельный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетвори-тельно)	«3» (удовлетвори-тельно)	«4» (хорошо)	«5» (отлично)
Работа носит реферативный характер, студент допускает существенные ошибки при защите, с большими затруднениями отвечает на вопросы, оформление работы не соответствует правилам	Работа носит реферативный характер, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении при защите, оформление работы имеет незначительные отклонения от правил	В работе углублены теоретические и практические знания, материал излагается грамотно и по существу, не допускается существенных неточностей в ответе на вопрос, оформление работы соответствует правилам	В процессе выполнения работы приобретены навыки самостоятельного планирования и выполнения научно-исследователь-ской работы; получен опыт сбора и обработки исходного материала, анализа научно-технической литературы,

			материал излагается грамотно оформление работы соответствует правилам

Критерии оценивания для проведения итоговой аттестации

Итоговая аттестация обучающихся проводится **в форме зачета (4-й семестр) и экзамена (5-й семестр)**.

Допуск к итоговой аттестации возможен при:

- всех выполненных, сданных (проверенных, защищенных) лабораторных работах, наличии отчётов по ним;
- наличии показателей приемлемого уровня освоения материалов курса: более 50 % посещений от общего числа требуемых по учебному плану.

Критерии оценивания:

- уровень усвоения материала, предусмотренного программой,
- умение выполнять задания, предусмотренные программой,
- уровень знакомства с дополнительной литературой,
- уровень раскрытия причинно-следственных связей,
- уровень раскрытия междисциплинарных связей,
- стиль поведения (культура речи, манера общения, убежденность, готовность к дискуссии),
- качество ответа (полнота, правильность, аргументированность, его общая композиция, логичность).

4.4 Примерные вопросы к зачету/экзамену по дисциплине

4.4.1 Вопросы к зачету:

1. Пользовательский интерфейс ОС. Классификация программных средств.
2. Основные функции ОС. Классификация ОС.
3. Концепция процесса. Типология процессов.
4. Концепция ресурсов. Концепция виртуальности.
5. Концепция прерывания. Классы прерываний.
6. Классификация операционных систем. Состав ядра ОС.
7. Модули ядра. Перечислить вспомогательные модули ОС и режимы.
8. Многослойная структура ОС. Микроядерная архитектура.
9. Управление процессами ОС. Понятия задание, задача, поток, нить и процесс.
10. Контекст процесса. Особенности работы нити процесса.

11. Планирование процессов. Концепции планирования процессов. Понятие кванта.

12. Способы организации процесса. Особенности организации процесса. Проблемы выполнения процессов на процессоре.

13. Понятие прерывания. Типы прерывания. Последовательность при обработке прерываний. Способы выполнения прерываний.

14. Особенности управления памятью в ОС.

15. Особенности работы виртуальной памяти и swapping. Алгоритмы распределения памяти. Алгоритмы управления памятью.

16. Механизмы распределения адресов в ОС. Распределение при реальных и виртуальных адресациях.

17. Файловые системы. Общая организация ФС.

18. Особенности ФС FAT и exFAT.

19. Особенности ФС NTFS.

20. Особенности файловых систем ext.

21. Сравнительный анализ файловых систем.

4.4.2 Вопросы к экзамену:

1. Пользовательский интерфейс ОС. Классификация программных средств

2. Основные функции ОС. Классификация ОС.

3. Концепция процесса. Типология процессов.

4. Концепция ресурсов. Концепция виртуальности.

5. Концепция прерывания. Классы прерываний.

6. Классификация операционных систем. Состав ядра ОС.

7. Модули ядра. Перечислить вспомогательные модули ОС и режимы.

8. Многослойная структура ОС. Микроядерная архитектура.

9. Управление процессами ОС. Понятия задание, задача, поток, нить и процесс.

10. Контекст процесса. Особенности работы нити процесса.

11. Планирование процессов. Концепции планирования процессов. Понятие кванта.

12. Способы организации процесса. Особенности организации процесса. Проблемы выполнения процессов на процессоре.

13. Понятие прерывания. Типы прерывания. Последовательность при обработке прерываний. Способы выполнения прерываний.

14. Особенности управления памятью в ОС.

15. Особенности работы виртуальной памяти и swapping. Алгоритмы распределения памяти. Алгоритмы управления памятью.

16. Механизмы распределения адресов в ОС. Распределение при реальных и виртуальных адресациях.

17. Файловые системы. Общая организация ФС.

18. Особенности ФС FAT и exFAT.

19. Особенности ФС NTFS.
20. Особенности файловых систем ext.
21. Сравнительный анализ файловых систем.
22. Особенности реализации функции безопасности в ОС. Краткие различия организации безопасности Unix и Windows.
23. Организация безопасности в Unix-системах.
24. Аутентификация в Unix-системах.
25. Аспекты механизмов безопасности Windows (ACE, ACL,SACL, DACL).
26. Привилегии субъектов в Windows. Маркеры доступа. Дескриптор защиты.
27. Авторизация в ОС Windows.
28. Дополнительные модули безопасности ОС.
29. Аудит в ОС .
30. Способы создания и управления процессами в ОС Linux.
31. Основные команды MS-DOS, ОС Linux. Особенности создания Bat-файлов, shell-сценариев.

5. ЗАКЛЮЧЕНИЕ

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится мало результативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста):
- исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводиться с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники:
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы:
- решить предложенные задачи, кейсы, ситуации;
- выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам:
2. Выполнение письменных контрольных и курсовых работ;
3. Подготовка и сдача зачетов, курсовых работ, итоговых экзаменов:
4. Написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

- индивидуальное занятие (домашние занятия) - важный элемент в работе студента по расширению и закреплению знаний;
- конспектирование лекций;
- получение консультаций для разъяснений по вопросам изучаемой дисциплины;
- подготовка ответов на вопросы тестов;
- подготовка к экзамену;
- выполнение контрольных, курсовых проектов и дипломных работ;
- подготовка научных докладов, рефератов, эссе;
- анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с рабочей программой учебной дисциплины. Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента не регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

Для овладения знаниями:

- чтение текста (учебника, первоисточника, дополнительной литературы);
- составление плана текста;
- конспектирование текста;
- выписки из текста;
- работа со словарями и справочниками;
- исследовательская работа;
- использование аудио- и видеозаписи;
- работа с электронными информационными ресурсами и ресурсами Internet:

Для закрепления и систематизации знании:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио-видеозаписей):
- составление плана и тезисов ответа;
- выполнение тестовых заданий;
- ответы на контрольные вопросы;
- аннотирование, реферирование, рецензирование текста;
- подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов;
- работа с компьютерными программами;
- подготовка к сдаче экзамена;

Для формирования умений:

- решение задач и упражнений по образцу;
- решение вариативных задач и упражнений:
- выполнение расчетно-графических работ;
- решение ситуационных производственных (профессиональных) задач;
- участие в научных и практических конференциях;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности;
- создание проспектов, проектов, моделей;
- экспериментальная работа, участие в НИР;
- рефлексивный анализ профессиональных умений с использованием аудио- видеотехники и компьютерных расчетных программ и электронных практикумов;
- подготовка курсовых проектов и дипломных работ;

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

6. ЛИТЕРАТУРА

1. Гордеев, А. В. Операционные системы: учебник для вузов / А. В. Гордеев. - Санкт-Петербург: Питер, 2009.

2. Иртегов, Д. В. Введение в операционные системы / Д. В. Иртегов. - Санкт-Петербург: БХВ-Петербург, 2008.

3. Запечников, С. В. Информационная безопасность открытых систем. В 2 т: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2008. -Т. 2. Средства защиты в сетях.

4. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие / С. В. Назаров. - Москва: КУДИЦ-ПРЕСС, 2007.

Локальный электронный методический материал

Владислав Владимирович Подтопельный

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

Редактор Г. А. Смирнова

Уч.-изд. л. 3,6. Печ. л. 3,25

Издательство федерального государственного бюджетного образовательного учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1