Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

Клочков А.Е.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»

Для студентов специалитета по специальности 10.05.03 очной формы обучения

Ульяновск, 2019

Методические указания для самостоятельной работы студентов по дисциплине «Безопасность операционных систем» / составитель: А.Е. Клочков. - Ульяновск: УлГУ, 2019. Настоящие методические указания предназначены для студентов специалитета по специальности 10.05.03 очной формы обучения. В работе приведены литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля и тесты для самостоятельной работы. Студентам очной формы обучения они будут полезны при подготовке к лекциям, семинарам, лабораторным и курсовым работам и к экзамену по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 2/19 от 19.03.2019 г.).

Содержание

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Проскурин, В. Г. Защита в операционных системах: учебное пособие для вузов / Проскурин В. Г. - Москва : Горячая линия - Телеком, 2014. - 192 с. - ISBN 978-5-9912-0379-1. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL:https://www.studentlibrary.ru/book/ISBN9785991203791.html

2. Мартемьянов, Ю. Ф. Операционные системы. Концепции построения и обеспечения безопасности: учебное пособие для вузов / Мартемьянов Ю. Ф. , Яковлев Ал. В., Яковлев Ан. В. - Москва: Горячая линия - Телеком, 2010. - 332 с. - ISBN 978-5-9912-0128-5. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785991201285.html

3. Некоммерческая интернет-версия СПС "КонсультантПлюс":

3.1 Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

3.2 Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

3.3 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")

Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

4. Основы информационной безопасности. Курс лекций. Часть 1 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2020 – 63 с.

5. Малюк А.А., Введение в информационную безопасность [Электронный ресурс]: Учебное пособие для вузов / А.А. Малюк, В.С. Горбатов, В.И. Королев и др.. Под ред. В.С. Горбатова. - М.: Горячая линия - Телеком, 2011. - 288 с. - ISBN 978-5-9912-0160-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201605.html.

6. Новиков В.К., Информационное оружие - оружие современных и будущих войн [Электронный ресурс] / Новиков В.К. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2013. - 262 с. - ISBN 978-5-9912-0166-7 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201667.html

7. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск: УлГУ, 2016. URL: http://edu.ulsu.ru/cources/750/interface/.

8. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ - Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

9. Основы информационной безопасности. Курс лекций. Часть 2 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2020 – 103 с.

10. Руссинович М., Соломон Д. Внутреннее устройство Microsoft Windows. 6-е изд. — СПб.: Питер, 2013. — 800 с.: ил. — (Серия «Мастер-класс»).

11. Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации: Учебное пособие. Изд. 4-е, перераб. и доп. – М.: Ленанд, 2016. -416 с.

12. Операционные системы. Практикум: учебное пособие С.В. Назаров, Л.П. Гудыно, А.А. Кириченко. — М.: КНОРУС, 2012. — 376 с. — (Для бакалавров).

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ЗАЩИТА ИНФОРМАЦИИ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

ТЕМА 1. ОСНОВНЫЕ ПОНЯТИЯ И ПОЛОЖЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННО ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Основные вопросы:

1. Базовые понятия и определения информационной безопасности
2. Основные принципы организации защиты информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [4] на с. 6-11.

Для самостоятельного изучения вопроса 1 следует обратиться к [3.1-3.3].

Вопрос 2 изложен в учебном пособии [4] на с. 12-15.

Для самостоятельного изучения вопроса 2 следует обратиться к [6] на стр. 25-34.

Контрольные вопросы по теме 1:

1. Основные составляющие информационной безопасности (ИБ).
2. Перечень оснований для ограничения информационных прав.
3. Раскрыть понятие ИБ.
4. Перечень видов информации с ограниченным доступом.
5. Предметы рассмотрения дисциплины.
6. Основные базовые свойства защищаемой информации.
7. Основные цели защиты информации (ЗИ).
8. Основная терминология по ИБ и ЗИ.
9. Основные принципы организации ЗИ.

Тесты для самостоятельной работы:

1. Коммерческую тайну не могут составлять следующие виды информации:

а) Техническая
б) информация о спросе и предложении,
в) информация о состоянии окружающей среды
информация о конкурентах

2. К внешним субъектам, способствующим обеспечению информационной безопасности, относятся

а) конкуренты
б) функциональные и отраслевые министерства и ведомства
в) сотрудники специализированных организаций, оказывающих услуги по договору;
г) служба внутреннего аудита в целом и ее сотрудники и т.д.

2.2. РАЗДЕЛ 1. ЗАЩИТА ИНФОРМАЦИИ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

ТЕМА 2. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Основные вопросы:

1. Угрозы информационной безопасности и их проявления
2. Классификация источников угроз информационной безопасности
3. Модель действий нарушителя

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [4] на с. 21-23.

Вопрос 2 изложен в учебном пособии [4] на с. 22-26.

Вопрос 3 изложен в учебном пособии [5] на с. 26-29.

Для самостоятельного изучения вопроса 3 следует обратиться к [3.1-3.3].

Контрольные вопросы по теме 2:

1. Раскрыть понятия угрозы, уязвимости и последствий реализации угрозы.

2. Назвать 3 примера уязвимостей информационной системы.

3. Привести вариант классификации источников угроз информационной безопасности.

4. Назвать 3 примера техногенных источников угроз.

5. Привести 3 примера актуальных стихийных источников угроз.

6. Назвать 3 примера антропогенных источников угроз.

7. Пояснить необходимость разработки модели действий нарушителя.

8. Внутренние и внешние нарушители.

Тесты для самостоятельной работы:

1. Что, из нижеперечисленного, является угрозой целостности информации?

а) Незаконное уничтожение или модификация информации

б) Утрата контроля над системой защиты;

в) Каналы утечки информации

2. Основной непреднамеренной искусственной угрозой не является:

а) Неправомерное отключение оборудования или изменение режимов работы устройств и программ

б) Отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи)

в) Неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной

г) Неумышленная порча носителей информации

3. Что, из перечисленного, не относится к основным преднамеренные искусственным угрозам?
а) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи
б) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др.)
в) применение подслушивающих устройств, дистанционная фото и видеосъемка
г) внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность)

4. Источниками угроз информационной безопасности не являются:
а) социальные источники
б) антропогенные источники
в) техногенные источники
г) стихийные источники

5. Что, из нижеперечисленного, относится к объективным уязвимостям?
а) Аппаратные закладки
б) Ошибки при эксплуатации технических средств
в) Нарушение режима конфиденциальности
г) Сбои электроснабжения
д) Повреждения жизнеобеспечивающих коммуникаций

6. Что, из нижеперечисленного, относится к субъективным уязвимостям?
а) Сбои электроснабжения
б) Повреждения жизнеобеспечивающих коммуникаций
в) Ошибки при эксплуатации технических средств
г) Аппаратные закладки
д) Нарушение режима конфиденциальности

2.3. РАЗДЕЛ 1. ЗАЩИТА ИНФОРМАЦИИ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

ТЕМА 3. ПРОГРАММНО-ТЕХНИЧЕСКИЙ УРОВЕНЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕГО ОРГАНИЗАЦИЯ

Основные вопросы:

1. Политика информационной безопасности
2. План защиты
3. План обеспечения непрерывной работы и восстановления работоспособности

Рекомендации по изучению темы:

Вопрос 1 изложен в лекции и в учебном пособии [7] на с. 40-48.

Для самостоятельного изучения вопроса 1 следует обратиться к [8] на с. 5-6 и [2] на с. 233-238.

Вопрос 2 изложен в лекции.

Вопрос 3 изложен в лекции и в учебном пособии [7] на с. 54-63.

Для самостоятельного изучения вопроса 3 следует обратиться к [8] на с. 22-28.

Контрольные вопросы по теме 3:

1. Основные разделы политики информационной безопасности (ПИБ) предприятия
2. Привести примеры типовых целей ПИБ
3. Варианты стратегий ответных действий на нарушение безопасности
4. Уровни ответственности пользователей и администраторов
5. Дать характеристику плану защиты (ПЗ)
6. Основные разделы ПЗ
7. Предназначение Плана обеспечения непрерывной работы и восстановления работоспособности
8. Дать характеристику основных мер реагирования на нарушения безопасности
9. Перечислить основные восстановительные работы

Тесты для самостоятельной работы:

1. Политика информационной безопасности (ПИБ) - это:

а) Совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса

б) Совокупность документированных технических решений, направленных на обеспечение безопасности информационного ресурса

в) Совокупность документированных процедурных решений, направленных на обеспечение безопасности инф. ресурса

2. Какая стратегия ответных действий на нарушение безопасности наиболее характерна для правоохранительных органов?
а) «Выследить и осудить»
б) «Защититься и продолжить»
в) «Выследить и отпустить после проведения профилактической работы»

3. Какие частные политики являются обязательными в типовой организации? Выбрать 3 варианта
а) Организации режима секретности
б) Использования Интернета
в) Разработки и лицензирования ПО
г) Обращения с информацией ограниченного доступа
д) Транспортировки носителей информации
е) Резервировании информации
ж) Проведения внешних и внутренних аудитов ИБ

4. Какие наиболее характерные угрозы ИС предприятия учитываются при составлении плана защиты? Выбрать 3 варианта
а) Точки доступа
б) Нелицензированные программные средства
в) Неправильно сконфигурированные системы
г) Отсутствие достаточных средств на счетах предприятия
д) Внутренние враги

5. В каком документе, из перечисленных, описывается схема оповещения конкретных лиц об инцидентах ИБ?
а) Политика информационной безопасности
б) План обеспечения непрерывной работы и восстановления работоспособности
в) План защиты

2.4. РАЗДЕЛ 2. ПОДСИСТЕМА БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА WINDOWS

ТЕМА 4. АНАЛИЗ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА WINDOWS

Основные вопросы:

1. Модели безопасности основных операционных систем
2. Достоинства и недостатки основных систем защиты

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 239-254.
Вопрос 2 изложен в учебном пособии [1] на с. 255-293.

Контрольные вопросы по теме 4:

1. Основные модели ОС
2. Механизмы защиты основных ОС
3. Основные проблемы обеспечения защиты ОС
4. Средства мониторинга защиты ОС
5. Регистрационные журналы ОС
6. Модели доступа современных ОС
7. Требования к защите информации от НСД в ОС
8. Отличия в защите различных ОС

Тесты для самостоятельной работы:

1. Имеется ли возможность в ОС Unix гарантированно удалять остаточную информацию встроенными средствами?

а) Да, имеется
б) Нет, т.к. отсутствуют соответствующие механизмы

2. Какое из утверждений относится к мандатным моделям управления доступом?

а) Модель, в которой владелец ресурса сам задает права доступа к нему
б) Модель, копирующая иерархическую структуру организации и позволяющая упростить администрирование
в) Модель, в которой режим доступа субъектов к объектам определяется установленным режимом конфиденциальности
г) Модель являющаяся наиболее универсальной и позволяющая контролировать доступ с учетом произвольных параметров среды, субъектов и объектов доступа

2.5. РАЗДЕЛ 2. ПОДСИСТЕМА БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА WINDOWS

ТЕМА 5. ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ В ОС СЕМЕЙСТВА WINDOWS

Основные вопросы:

1. Понятие защищённой операционной системы
2. Идентификация, аутентификация и авторизация в ОС семейства Windows

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 4-14.

Вопрос 2 изложен в учебном пособии [1] на с. 72-106.

Для самостоятельного изучения вопроса 2 следует обратиться к [9] на с. 67-76.

Контрольные вопросы по теме 5:

1. Что такое идентификация, аутентификация и авторизация
2. Какие основные схемы аутентификация Вы знаете?
3. Как хранятся пароли в ОС семейства Windows?
4. Что такое хэширование паролей?
5. Зачем нужно ограничивать сроки действия паролей?
6. Пояснить сущность процедур идентификации и аутентификации.
7. Процесс идентификации и аутентификации.
8. Что такое авторизация и администрирование.
9. Категории процесса аутентификации в зависимости от предъявляемых субъектом сущностей.
10. Типы процессов аутентификации.
11. Основные характеристики протоколов аутентификации.
12. Классификация основных протоколов аутентификации.

Тесты для самостоятельной работы:

1. Что из перечисленного относится к администрированию?

а) Регистрация действий пользователя в сети, включая его попытки доступа к ресурсам

б) Процедура проверки подлинности заявленного пользователя, процесса или устройства

в) Процедура распознавания пользователя по его имени

2. Что, из перечисленного, обычно не используется в качестве биометрических признаков при аутентификации потенциального пользователя

а) Отпечатки пальцев

б) Форма и размеры лица

в) Отпечаток стопы

г) Особенности голоса

2.6. РАЗДЕЛ 2. ПОДСИСТЕМА БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА WINDOWS

ТЕМА 6. АУДИТ В ОС СЕМЕЙСТВА WINDOWS

Основные вопросы:

1. Аудит и обнаружение вторжений
2. Протоколирование и активный аудит

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 110-123.
Вопрос 2 изложен в учебном пособии [2] на с. 304-306.

Контрольные вопросы по теме 6:

1. Что такое аудит в ОС?
2. Что такое протоколирование в ОС?
3. Сигнатура атаки
4. Злоупотребление полномочиями
5. Что такое подозрительная активность?
6. Генерация регистрирующей информации
7. Архитектура менеджер-агент

Тесты для самостоятельной работы:

1. Аутентификация – это

а) процедура проверки подлинности
б) присвоение субъектам и объектам идентификатора или сравнение идентификатора с перечнем присвоенных идентификаторов.
предоставление определённому лицу или группе лиц прав на выполнение определённых действий

2. Разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности)

а) мандатное
б) дискреционное
в) ролевое

2.7. РАЗДЕЛ 2. ПОДСИСТЕМА БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА WINDOWS

ТЕМА 7. ВОЗМОЖНОСТИ ШИФРОВАНИЯ ФАЙЛОВ В ОС СЕМЕЙСТВА WINDOWS

Основные вопросы:

1. Шифрующая файловая система EFS
2. Система шифрования дисков BitLocker

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [12] на с. 198-201.
Вопрос 2 изложен в учебном пособии [10] на с. 649-652

Контрольные вопросы по теме 7:

1. Шифрующая файловая система EFS
2. Возможности шифрующей файловой системы EFS
3. Принципы работы EFS
4. Используемые в EFS алгоритмы шифрования
5. Случайный ключ для шифрования файла FEK
6. Шифрование ключа FEK
7. Команда cipher и ее параметры
8. Основные возможности BitLocker
9. Шифрование и дешифрование дисков при помощи BitLocker

Тесты для самостоятельной работы:

1. Симметричным методом аутентификации является:

а) протокол Диффи-Хеллмана,
б) протокол Шнорра,
в) схема Kerberos
г) протокол Фиата-Шамира.

2. Основными атаками на протоколы аутентификации являются:

а) отражение передачи
б) повторная передача
в) маскарад
г) все ответы верны

2.8. РАЗДЕЛ 2. ПОДСИСТЕМА БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА WINDOWS

ТЕМА 8. ПРОЧИЕ ВОЗМОЖНОСТИ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА WINDOWS

Основные вопросы:

1. Повышение привилегий
2. Управление поведением UAC

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [10] на с. 659-667.
Вопрос 2 изложен в учебном пособии [10] на с. 667-670.

Контрольные вопросы по теме 8:

1. Интерфейс CryptoAPI
2. Возможности CryptoAPI
3. Работа с поставщиками службы шифрования CSP
4. Типы CSP в ОС семейства Windows
5. Контроль учетных записей пользователей UAC
6. Предпосылки к появлению UAC
7. Принцип работы UAC
8. События, приводящие к срабатыванию UAC
9. Настройка UAC
10. Недостатки UAC
11. Шаблоны безопасности в ОС семейства Windows
12. Возможности шаблонов безопасности
13. Настройки шаблонов безопасности

Тесты для самостоятельной работы:

1. В иерархию ключей обычно входят:

а) 1 ключ
б) 2 ключа
в) 3 ключа
г) 4 ключа

2.Среди электронных ключей наиболее стойкими являются:

а) Ключи с памятью
б) Ключи с микропроцессором
в) Оба ответа не верны

2.9. РАЗДЕЛ 2. ПОДСИСТЕМА БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА WINDOWS

ТЕМА 9. УСИЛЕНИЕ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА WINDOWS

Основные вопросы:

1. Защита от вредоносных программ и вирусов
2. Защита конфиденциальной информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [12] на с. 298-306.
Вопрос 2 изложен в учебном пособии [12] на с. 307-319.

Контрольные вопросы по теме 9:

1. Использование систем криптографической защиты информации
2. Наиболее известные системы криптографической защиты информации и особенности их работы
3. Противодействие вирусным атакам в системе
4. Выбор антивируса
5. Организация антивирусной защиты

Тесты для самостоятельной работы:

1. Одним из способов создания ключей на жестких дисках является:

а) Логическое превышение объема дорожки.
б) Уменьшение межсекторных промежутков.
в) Привязка к архитектуре компьютера
г) Изменение контрольной суммы.

2. Какой способ встраивания защитных механизмов является основным для проектируемых и проверяемых СЗИ?

а) вставка фрагмента проверочного кода
б) вставкой проверочного механизма в исходный код на этапе разработки и отладки программного продукта
в) преобразованием исполняемого файла к неисполняемому виду (шифрование, архивация с неизвестным параметром и т.д.) и применением для загрузки некоторой программы, в теле которой и осуществляются необходимые проверки;
г) комбинированный

2.10. РАЗДЕЛ 3. ПОДСИСТЕМА БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА UNIX

ТЕМА 10. АНАЛИЗ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА UNIX

Основные вопросы:

1. Защита информации в ОС семейства UNIX
2. SELinux – система повышенной безопасности

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [11] на с. 173-179.
Вопрос 2 изложен в учебном пособии [11] на с. 180-185.

Контрольные вопросы по теме 10:

1. Основные механизмы защиты в ОС семейства UNIX
2. Особенности организации файловой системы в UNIX
3. Принципиальные недостатки защитных механизмов ОС семейства UNIX
4. Альтернативные системы безопасности

Тесты для самостоятельной работы:

1. Способ защиты от трассировки программ по заданному событию, представляющий собой замыкание цепочек обработки событий минуя программы трассировки.

а) Пассивная защита
б) Активная защита первого типа
в) Активная защита второго типа
г) Активная защита третьего типа

2. Использование аппаратных особенностей микропроцессора относится к следующему классу защиты ПО от исследования:

а) Влияние на работу отладочного средства через общие программные или аппаратные ресурсы
б) Влияние на работу отладочного средства путем использования особенностей его аппаратной или программной среды.
в) Влияние на работу отладчика через органы управления или/и устройства отображения информации.
г) Использование принципиальных особенностей работы управляемого человеком отладчика.

2.11. РАЗДЕЛ 3. ПОДСИСТЕМА БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА UNIX

ТЕМА 11. ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ В ОС СЕМЕЙСТВА UNIX

Основные вопросы:

1. Основные принципы аутентификации в ОС семейства Unix
2. Основные механизмы защиты данных ОС Unix

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 92-99.
Вопрос 2 изложен в учебном пособии [2] на с. 285-291.

Контрольные вопросы по теме 11:

1. Особенности подсистемы безопасности в ОС семейства UNIX
2. Единая модель безопасности для ОС семейства UNIX
3. Парольная аутентификация в UNIX
4. Учетный файл зарегистрированных пользователей /etc/passwd
5. Содержимое файла /etc/passwd
6. Подключаемые модули аутентификации PAM
7. Идентификаторы пользователей UID, RUID, EUID
8. Учетный файл зарегистрированных групп /etc/group
9. Авторизация в ОС семейства UNIX
10. Проверка прав доступа при обращении к файлам в ОС UNIX
11. Работа из-под root
12. Редактирование файла sudoers с помощью утилиты visudo

Тесты для самостоятельной работы:

1. Защита от чтения на уровне системы может осуществляться

а) Введением атрибута Read Only для файлов;
б) Введением атрибута Hidden для файлов;
в) Введением запрета на чтение папки, в котором находится файл
г) Ни один вариант ответа не верен

2.12. РАЗДЕЛ 3. ПОДСИСТЕМА БЕЗОПАСНОСТИ В ОС СЕМЕЙСТВА UNIX

ТЕМА 12. АУДИТ В ОС СЕМЕЙСТВА UNIX

Основные вопросы:

1. Аудит и обнаружение вторжений
2. Протоколирование и активный аудит

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 124-133.
Вопрос 2 изложен в учебном пособии [2] на с. 304-308.

Контрольные вопросы по теме 12:

1. Подсистема аудита в UNIX
2. Централизованная система регистрации системных сообщений Syslog
3. Возможности системы Syslog
4. Компоненты Syslog
5. Работа системы Syslog
6. Syslog. Файл конфигурации Syslog syslog.conf

Тесты для самостоятельной работы:

1.Файлы, созданные процессом:

а) Наследуют идентификатор процесса и могут быть запущены только данным процессом
б) Наследуют идентификатор пользователя, запустившего процесс
в) Могут быть использованы только администратором