Приложение к рабочей программе дисциплины

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Наименование дисциплины	Защита в операционных системах
Специальность	10.05.01 Компьютерная безопасность
Специализация	Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
Форма обучения	очная
Разработчик(и)	Оленников Е.А., доцент кафедры информационной безопасности

1.Темы дисциплины для самостоятельного освоения обучающимися

Формализованные требования к защите ОС.
Зарубежные стандарты в области ИБ.
Методы и инструменты для оценки уровня защищенности ОС.
Анализ на проникновение.
Специализированные дистрибутивы Linux для задач ИБ.
Специализированные ресурсы для получения информации об уязвимостях ОС.
Тактики и техники атак.

2. План самостоятельной работы

п/п	Учебные встречи	Виды самостоятельной работы	Форма отчетности/ контроля	Количество баллов	Рекомендуемый бюджет времени на выполнение (ак.ч.)*
Семестр 7					
1.	УВ № 1-36. Лекционные и лабораторные занятия.	Проработка лекций. Чтение обязательной и дополнительной литературы. Подготовка докладов	Реферат	10	80
	Всего (часов) за семестр 7				80
Семестр 8					
1.	УВ № 1-36. Лекционные и лабораторные занятия.	Проработка лекций. Чтение обязательной и дополнительной литературы. Подготовка докладов	Реферат	10	80
	Всего (часов) за семестр 8				80
	ИТОГО: часов самостоятельной работы				160

3. Требования и рекомендации по выполнению самостоятельных работ обучающихся, критерии оценивания

3.1. Оформление отчета

Отчет представляется в форме реферата по выбранной теме.
Реферат должен иметь следующую структуру.
Титульный лист.
Введение (2-3 с.).
Основная часть (до 20 с.) включает в себя главы (с параграфами) или разделы. В тексте реферата слово «основная часть» не пишется.
Заключение (до 2 с.).
Список использованных источников и литературы.
Приложения (если есть).

3.2. Сроки выполнения, требования к объему.

Задания для самостоятельной работы выполняются в течение семестра, в котором читается данная дисциплина.

3.3. Критерии оценивания

При проведении текущего контроля для оценки заданий применяется система оценивания:

- 10 баллов. Реферат полностью раскрывает рассматриваемую тему, оформлен корректно, использованы современные и актуальные литературные источники. Сценарий не содержит синтаксических или логических ошибок, корректно выполняется, решает поставленную задачу.
- 5 баллов. Реферат не полностью раскрывает рассматриваемую тему, оформлен корректно, использованы современные и актуальные литературные источники. Сценарий содержит незначительные синтаксические или логические ошибки, корректно выполняется, частично решает поставленную задачу.
- 0 баллов - Задание не выполнено или выполнено на низком уровне.

4. Рекомендации по самоподготовке к промежуточной аттестации по дисциплине

4.1. Вопросы к дифференцированному зачету / экзамену для самопроверки:

7 семестр

1. Определение понятий: информационная безопасность, защита информации, конфиденциальность, доступность, целостность.
2. Свойства информации: ценность, достоверность, своевременность.
3. Предмет защиты информации. Объект защиты информации. Информационная безопасность АСОИ. Политика информационной безопасности. Система защиты информации.
4. Основные положения безопасности информационных систем. Основные принципы обеспечения информационной безопасности в информационных системах.
5. Определение понятий: угроза, угроза информационной безопасности АС, атака, злоумышленник, источник угрозы, уязвимость, окно опасности,
6. Классификация возможных угроз ИБ АС по ряду базовых признаков.
7. Угроза доступности. Угроза нарушения целостности. Угроза нарушения конфиденциальности.
8. Уровни доступа к информации.
9. Классификация злоумышленников.
10. Основные направления реализации угроз информационной безопасности.
11. Программно-технические меры ИБ.
12. Основные и вспомогательные сервисы безопасности.
13. Идентификация и аутентификация.
14. Классификация требований к системам защиты.
15. Формализованные требования к защите компьютерной информации АС.
16. Механизмы защиты операционных систем. Типовые функциональные дефекты ОС, приводящие к созданию каналов утечки данных.
17. Контроль доступа к данным в ОС. Субъекты и объекты доступа. Полномочия. Логическое управление доступом.
18. Дискреционные модели доступа. Модели безопасности на основе мандатной политики.

19. Принципиальные недостатки защитных механизмов ОС семейства Windows, Unix.
20. Система безопасности операционной системы Windows. SAM.
21. Система безопасности операционной системы Windows. Идентификаторы защиты. Маркеры доступа. Дескрипторы защиты и управление доступом.
22. Управление пользователями в ОС Windows. Децентрализованная (Рабочие группы) и централизованная (домены) модель управления. Групповая политика безопасности.
23. Методы компрометации учетной записи пользователя в Windows и методы противодействия компрометации учетной записи.
24. Методы эскалации привилегий в ОС Windows, меры противодействия.
25. Файловая система NTFS: контроль доступа к объектам файловой системы, квотирование, шифрование (EFS).
26. Методы компрометации системы контроля доступа, меры противодействия.
27. Дополнительные механизмы защиты ОС Windows.
28. Методы инструментального контроля уровня защищенности ОС.
29. Общие рекомендации по защите ОС Windows.

Вопросы к экзамену.

8 семестр

1. Базовые сервисы безопасности в Unix-like системах.
2. Типовые уязвимости Unix-like систем.
3. Примеры уязвимостей сервисов безопасности в Unix-like системах и меты противодействия (на примере одного из сервисов).
4. Базовые методы управление пользователями в Unix-like системах.
5. Методы компрометации учетной записи пользователя в Unix-like системах и методы противодействия.
6. Методы ограничения пользователей в Unix-like системах.
7. Методы повышения привилегий. Выполнение команд от имени других пользователей. Утилиты su, sudo.
8. Базовые методы контроля доступа к объектам ФС в Unix-like системах.
9. Расширенные средства контроля доступа к объектам ФС в Unix-like системах: специальные флаги, ACL.
10. Методы компрометации системы контроля доступа, меры противодействия в Unix-like системах (примеры).
11. Шифрование объектов ФС в Unix-like системах.
12. Реализация контроля целостности объектов ФС в Unix-like системах.
13. Мандатная модель управления доступом в Unix-like системах.
14. Сетевая безопасность в Unix-like системах. Общие положения.
15. Межсетевые экраны в Unix-like системах. Принцип работы, пример конфигурирования.
16. Системы аудита и службы системной журнализации. Общие принципы работы и конфигурирования.
17. Организация защищенного удаленного доступа в Unix-like системах.
18. Аудит безопасности в Unix-like системах. Общие принципы использования, используемые средства.
19. Подключаемые модули аутентификации (PAM). Общее описание, пример использования.
20. Принудительный контроль доступа (MAC). Описание политик, пример настройки.

Общие подходы к защите современных ОС.

4.2. Система оценивания

В 7 семестре предусмотрен зачет. Оценка за зачет студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время лабораторных работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины. Для получения зачета необходимо набрать не менее 61 балла.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «зачет» студент должен сдать минимум 75% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты.

В 8 семестре предусмотрен экзамен. Экзаменационная оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время лабораторных работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должно быть сдано минимум 50% лабораторных работ и сделан ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен сдать минимум 75% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен сдать минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами.

Результаты выполнения самостоятельной работы загружаются в pdf формате в соответствующий раздел дисциплины на образовательной платформе LMS ТюмГУ.