МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА»

Кафедра «Государственного, муниципального и корпоративного управления»

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

«Информационная безопасность»

Направление подготовки
38.04.04 «Государственное и муниципальное управление»

Профиль – Информационные технологии в государственном и муниципальном управлении

ОПОП академической магистратуры
«Государственное и муниципальное управление»

Формы обучения – очно-заочная, заочная

Рязань

1. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ДИСКУССИИ

Дискуссия – один из наиболее эффективных способов для обсуждения острых, сложных и актуальных на текущий момент вопросов в любой профессиональной сфере, обмена опытом и творческих инициатив. Такая форма занятий позволяет лучше усвоить материал, найти необходимые решения в процессе эффективного диалога.

Правила ведения дискуссии

Дискуссия – это деловой обмен мнениями, в ходе которого каждый выступающий должен стараться рассуждать как можно объективнее. Каждое высказывание должно быть подкреплено фактами. В обсуждении следует предоставить каждому участнику возможность высказаться. Каждое высказывание, позиция должны быть внимательно рассмотрены всеми участниками дискуссии. Необходимо внимательно слушать выступления других, размышлять над ними и начинать говорить только тогда, когда появляется уверенность в том, что каждое ваше слово будет сказано по делу. В ходе обсуждения недопустимо «переходить на личности», «навешивать ярлыки», допускать уничижительные высказывания и т.д. Отстаивайте свои убеждения в энергичной и яркой форме, не унижая при этом достоинство лица, высказавшего противоположное мнение. При высказывании другими участниками дискуссии мнений, не совпадающих с вашим, сохраняйте спокойствие, исходя из того, что каждый человек имеет право на собственное мнение. Любое выступление должно иметь целью разъяснение разных точек зрения и примирение спорящих. Говорите только по заданной теме, избегая любых бесполезных уклонений в сторону. Сразу же следует начинать говорить по существу, лаконично придерживаясь четкой логики, воздерживаясь от пространных вступлений. Остроту дискуссии придают точные высказывания. Следует вести себя корректно. Не используйте отведенное для выступления время для высказывания недовольства тому или иному лицу, тем более отсутствующим.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПОДГОТОВКЕ ПУБЛИЧНОГО ДОКЛАДА С ПРЕЗЕНТАЦИЕЙ

Доклад – это краткое публичное устное изложение результатов индивидуальной учебно-исследовательской деятельности студента, представляет собой сообщение о сути вопроса или исследования применительно к заданной тематике. Доклады направлены на более глубокое самостоятельное изучение обучающимися лекционного материала или рассмотрения вопросов для дополнительного изучения. Данный метод обучения используется в учебном процессе при проведении практических занятий в форме семинаров. Его задачами являются:

- формирование умений самостоятельной работы обучающихся с источниками литературы, их систематизация;
- развитие навыков логического мышления;
- углубление теоретических знаний по проблеме исследования.
- развитие навыков изложения своих мыслей и идей перед аудиторией, умения уверенно пользоваться научной терминологией.

Доклад должен представлять аргументированное изложение определенной темы, быть структурирован (по главам, разделам, параграфам) и включать разделы: введение, основная часть, заключение. В ходе доклада должны быть сделаны ссылки на использованные источники. В зависимости от тематики доклада он может иметь мультимедийное сопровождение, в ходе доклада могут быть приведены иллюстрации, таблицы, схемы, макеты, документы и т. д. В ходе доклада может быть использована доска, флип-чарт для иллюстрации излагаемых тезисов.

3. ПЛАН ПРАКТИЧЕСКИХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ

Тема 1. Понятие информационной безопасности

Вопросы для обсуждения:

- Понятие информационной безопасности
- Защита информации: понятие и значение
- Понятие доступности, целостности и конфиденциальности информации
- Компьютерное преступление
- Жизненный цикл информационных систем

Тема 2. Объектно-ориентированный подход к рассмотрению защищаемых систем.

Вопросы для обсуждения:

- Информационные системы.
- Структурный и процессно-ориентированный подходы.
- Основные определения и критерии классификации угроз.
- Основные угрозы: доступности, целостности, конфиденциальности.

Тема 3. Законодательный уровень информационной безопасности. Административный уровень информационной безопасности

Вопросы для обсуждения:

- Российское законодательство в области информационной безопасности
- Зарубежное законодательство в области информационной безопасности.
- Стандарты и спецификации в области информационной безопасности.
- Основные понятия административного уровня, политика безопасности.
- Жизненный цикл информационной системы. Синхронизация программы безопасности с жизненным циклом систем.
- Управление рисками

Тема 4. Процедурный уровень информационной безопасности

Вопросы для обсуждения:

- Основные классы мер процедурного уровня.
- Физическая защита.
- Поддержание работоспособности.
- Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Тема 5. Основные характеристики программно-технических мер. Идентификация и аутентификация

Вопросы для обсуждения:

- Основные понятия программно-технического уровня.
- Архитектурная безопасность. Экранирование. Анализ защищённости. Отказоустойчивость. Безопасное восстановление.
- Парольная аутентификация. Одноразовые пароли.
- Идентификация/аутентификация с помощью биометрических данных.

Тема 6. Протоколирование и аудит, шифрование, контроль целостности

Вопросы для обсуждения:

- Основные понятия. Активный аудит. Шифрование.
- Симметричный метод шифрования. Асимметричный метод шифрования.
- Секретный и открытый ключ. Криптография. Контроль целостности.
- Цифровые сертификаты. Электронная цифровая подпись.

Тема 7. Экранирование, анализ защищенности

Вопросы для обсуждения:

- Основные понятия. Экранирование. Фильтрация.
- Межсетевые экраны. Классификация межсетевых экранов.
- Архитектурная безопасность.
- Транспортное экранирование. Анализ защищенности.
- База данных уязвимостей. Сетевой сканер. Антивирусная защита.

Тема 8. Обеспечение высокой доступности

Вопросы для обсуждения:

- Эффективность услуг. Время недоступности.
- Основы мер обеспечения высокой доступности.
- Отказоустойчивость и зона риска. Обеспечение отказоустойчивости.
- Обеспечение обслуживаемости. Туннелирование.

4. КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ДИСЦИПЛИНЕ

1. Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб.
2. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.
3. Сложные системы. Структурный подход.
4. Основные определения и критерии классификации угроз.
5. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник.
6. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
7. Российское законодательство в области информационной безопасности.
8. Зарубежное законодательство в области информационной безопасности.
9. Стандарты и спецификации в области информационной безопасности.
10. Основные понятия, политика безопасности.
11. Жизненный цикл информационной системы.
12. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками.
13. Основные классы мер процедурного уровня.
14. Управление персоналом. Физическая защита.
15. Поддержание работоспособности.
16. Реагирование на нарушения режима безопасности.
17. Планирование восстановительных работ.
18. Основные понятия программно-технического уровня. Архитектурная безопасность.
19. Экранирование. Анализ защищённости.
20. Отказоустойчивость. Безопасное восстановление.
21. Основные понятия криптографии.
22. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации Kerberos.
23. Идентификация/аутентификация с помощью биометрических данных.
24. Управление доступом. Ролевое управление доступом.
25. Активный аудит. Шифрование.
26. Симметричный метод шифрования.
27. Асимметричный метод шифрования.
28. Секретный и открытый ключ.
29. Криптография. Контроль целостности
30. Цифровые сертификаты.
31. Электронная цифровая подпись.
32. Экранирование. Фильтрация. Межсетевые экраны.

33. Классификация межсетевых экранов.
34. Архитектурная безопасность.
35. Транспортное экранирование. Анализ защищенности.
36. Сетевой сканер. Антивирусная защита.

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СОГЛАСОВАНО **ФГБОУ ВО "РГРТУ", РГРТУ,** Перфильев Сергей Валерьевич, Заведующий кафедрой ГМКУ Простая подпись