Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Социальная инженерия

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Интеллектуальный анализ больших данных

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
А.В. Замятин

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-6 Способен исследовать современные проблемы и методы прикладной информатики и развития информационного общества;.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-6.1 Знает методы анализа прикладной области, информационных потребностей, технологии сбора, накопления, обработки, передачи и распространения информации

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– реферат.

Примерный список тем рефератов (ИОПК-6.1):

1. Принципы и техники социальной инженерии
2. Способы защиты от атак социальной инженерии
3. Утечка корпоративной информации и социальная инженерия
4. Психотипы и социальная инженерия
5. Методы социальной инженерии
6. Утечка информации в сети Интернет
7. Социальная инженерия в конкурентной разведке
8. Атаки с помощью социальных сетей
9. Фишинговые атаки.
10. Комбинированные схемы социальной инженерии
11. Ложные антивирусы
12. Лотереи
13. Троянские программы
14. Использование брендов известных фирм в организации атак
15. Техника претекстинга в социальной инженерии
16. Обратная социальная инженерия
17. Атаки с помощью сервиса FindFace
18. Анонимная сеть TOR
19. Способы получения корпоративной информации
20. Техническая разведка и её роль в организации атак СИ
21. Вредоносные программы в СИ
22. Службы разведки и СИ

Критерии оценивания реферата

Написание реферата преследует цель самостоятельного знакомства студентов с теоретической базой фундаментальных знаний по отдельным разделам социальной инженерии (по предложенной теме). Это позволит им в дальнейшем участвовать в творческом решении проблем информационной безопасности и научных подходов к организации безопасного использования современных информационно-телекоммуникационных технологий, содействовать реализации концепции устойчивого развития общества.

В процессе написания реферата студент должен решить следующие задачи:

1) Изучить проблемы по теме реферата с подбором литературы (источников).
2) Составить план реферата.
3) Обобщить собранный материал.

4) Написать реферат в соответствии с планом. В конце реферата сформулировать выводы, характеризующие отношение **автора реферата** к рассматриваемой проблеме и пути ее решения. Отправить реферат в текстовом формате на проверку. Ссылки на используемые источники в тексте реферата обязательны!

5) Подготовить доклад по теме реферата в виде файла в формате *.ppt.

Обязательные требования к написанию реферата:

- титульный лист с названием темы
- аннотация
- оглавление (содержание)
- текст реферата с указанием ссылок на цитируемые источники
- выводы
- список литературы, включая ссылки на адреса веб-сайтов с цитируемыми материалами.

При выполнении всех требований реферат оценивается «**зачтено**». В случае плагиата (копировании чужой работы) – **незачет** и студент получает у преподавателя новую тему.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Изучение курса завершается сдачей зачёта. Зачёт ставится при положительных результатах текущего контроля, положительных ответах на вопросы билета и сдаче реферата и доклада по одной из предложенных преподавателем тем. Методические материалы и требования к реферату включают критерии оценивания теоретических вопросов; процедуру формирования итоговой оценки, учитывающую оценки за каждую компетенцию.

Процедура формирования итоговой оценки включает степень самостоятельности студента при знакомстве с теоретической базой фундаментальных знаний по отдельным разделам социальной инженерии (по предложенной теме), полноту раскрытия темы, уровень обобщения собранного материала и отношение автора реферата к рассматриваемой проблеме и путям её решения.

Зачет проводится в устной форме по билетам. Билет содержит два теоретических вопроса. Продолжительность зачета 1,5 часа.

Примерный перечень теоретических вопросов (ИОПК-6.1):

1. Основные проблемы инженерно-технической защиты информации.
2. Виды информации, подлежащие защите. Государственная тайна.
3. Принципы и техники социальной инженерии.
4. Способы защиты от атак социальной инженерии.
5. Утечка корпоративной информации и социальная инженерия.
6. Психические состояния и социальная инженерия.
7. Методы социальной инженерии.
8. Утечка информации через Интернет.
9. Социальная инженерия в конкурентной разведке.
10. Социальная инженерия. Техника претекстинг.
11. Социальная инженерия Использование брендов известных фирм.
12. Социальная инженерия. Лотереи.
13. Социальная инженерия. Ложные антивирусы.
14. Социальная инженерия. Психотипы.
15. Фишинговые атаки.
16. Комбинированные схемы социальной инженерии.

17. Телефонный фишинг (вишинг).
18. Троянская программа.
19. Методы обратной социальной инженерии.
20. «Социальная инженерия» как наука.
21. Социальная инженерия и социальные сети.

Зачёт ставится при положительных результатах текущего контроля, положительных ответов на вопросы билета, сдаче подготовленного реферата и доклада по одной из предложенных преподавателем тем. План реферата и тема согласовываются с преподавателем.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Теоретические вопросы (ИОПК-6):

1. Основные проблемы инженерно-технической защиты информации.
2. Виды информации, подлежащие защите. Государственная тайна.
3. Принципы и техники социальной инженерии.
4. Способы защиты от атак социальной инженерии.
5. Утечка корпоративной информации и социальная инженерия.
6. Психические состояния и социальная инженерия.
7. Методы социальной инженерии.
8. Утечка информации через Интернет.
9. Социальная инженерия в конкурентной разведке.
10. Социальная инженерия. Техника претекстинг.
11. Социальная инженерия Использование брендов известных фирм.
12. Социальная инженерия. Лотереи.
13. Социальная инженерия. Ложные антивирусы.

Информация о разработчиках

Беляев Виктор Афанасьевич, канд. техн. наук, доцент, кафедра компьютерной безопасности института прикладной математики и компьютерных наук НИ ТГУ, доцент