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

Рабочая программа дисциплины

Социальная инженерия

по направлению подготовки

02.04.02 Фундаментальная информатика и информационные технологии

Направленность (профиль) подготовки:
Математика беспроводных сетей связи и интернета вещей
Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
С.П. Моисеева

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-2 Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение (в том числе отечественного производства) для решения задач профессиональной деятельности.

ОПК-4 Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-2.1 Обладает необходимыми знаниями основных концепций современных вычислительных систем и программного обеспечения (в том числе отечественного производства)

ИОПК-4.2 Учитывать основные требования информационной безопасности

2. Задачи освоения дисциплины

– Формирование способности понимать социальную значимость своей профессии, высокую мотивацию к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства.

– Формирование знаний, необходимых для осуществления комплексного инженерного подхода к организации информационной безопасности предприятия с учётом социальной реальности.

– Научиться выявлять источники, риски и угрозы информационной безопасности, разрабатывать политику компании в соответствии со стандартами безопасности, использовать математические модели, алгоритмы для моделирования опасных ситуаций и анализа рисков.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплины (модули)».

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, предлагается обучающимся на выбор. Дисциплина входит в модуль Введение в информационную безопасность.

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Первый семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются компетенции, сформированные в ходе освоения образовательных программ предшествующего уровня образования.

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: «Основы информационной безопасности»,

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:
-лекции: 32 ч.

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Введение. Социальная инженерия (СИ) как наука.
Тема 2. Основные концептуальные положения СИ.
Тема 3. История развития социальной инженерии.
Тема 4. Информация как предмет защиты.
Тема 5. Принципы и техники социальной инженерии.
Тема 6. Основная модель социальной инженерии.
Тема 7. Методы социальной инженерии.
Тема 8. Основные направления социальной инженерной деятельности.
Тема 9. Технологии социальной инженерии.
Тема 10. Социальная инженерия и социальное программирование.
Тема 11. Утечка корпоративной информации. Инсайдинг.
Тема 12. Пределы последствий при социоинженерных атаках.
Тема 13. Сопровождение социальных процессов в обществе.
Тема 14. Технологии защиты от социальных «хакеров».
Тема 15. Комплексный подход к разработке политик информационной безопасности предприятия.
Тема 16. Принципы оценки эффективности средств защиты.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения тестов по лекционному материалу, по темам, выполнения домашних заданий и фиксируется в форме контрольной точки не менее одного раза в семестр.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

10. Порядок проведения и критерии оценивания промежуточной аттестации

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

Примерный перечень теоретических вопросов:

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.

Примерный список тем рефератов:

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

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «LMS IDO».

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.

в) Методические указания по подготовке доклада и написанию реферата.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Аполлонский А. В., Домбровская Л. А., Примакин А. И., Смирнова О. Г., Основы информационной безопасности в ОВД: Учебник для вузов. – СПб.: Университет МВД РФ, 2010.

– Кевин Митник, Уильям Саймон — Призрак в Сети. Мемуары величайшего хакера. – М.: Издательство: «Эксмо», 2012. – 416 с..

б) дополнительная литература:

– Кузнецов М.В., Симдянов И.В. Социальная инженерия и социальные хакеры.-СПб: БХВ-Петербург, 2007. – 368 с.

– Вильям Л. Саймон, К. Митник. Искусство обмана. -М: Компания АйТи, 2004. – 123 с.

в) ресурсы сети Интернет:
– открытые онлайн-курсы
– https://vk.com/wall-98006063_7475
– https://habr.com/en/articles/83415/
– https://safe-surf.ru/users-of/article/642870/
– https:// https://www.cbr.ru/faq/information_security/
– Общероссийская Сеть КонсультантПлюс Справочная правовая система – https://www.consultant.ru/

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:
– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);
– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

б) информационные справочные системы:
– Электронный каталог Научной библиотеки ТГУ – https://koha.lib.tsu.ru/
– Электронная библиотека (репозиторий) ТГУ – https://vital.lib.tsu.ru/vital/access/manager/Index
– ЭБС Лань – https://e.lanbook.com/
– ЭБС Консультант студента – https://www.studentlibrary.ru/
– Образовательная платформа Юрайт – https://urait.ru/
– ЭБС ZNANIUM.com – https://znanium.com/
– ЭБС IPRbooks – https://www.iprbookshop.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.
Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.
Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

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