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

Введение в компьютерную безопасность

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-2 Способен совершенствовать и реализовывать новые математические методы решения прикладных задач.

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

ПК-2 Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-2.1 Использует результаты прикладной математики для освоения, адаптации новых методов решения задач в области своих профессиональных интересов.

ИОПК-4.2 Учитывает основные требования информационной безопасности.

ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.

2. Задачи освоения дисциплины

– Освоить понятийный аппарат компьютерной безопасности.

– Получить представление о нормативных документах в области компьютерной безопасности, о методах и средствах защиты компьютерных систем и сетей.

– Получить представление о практиках, методах и технологиях, позволяющих защитить компьютерные системы и сети от компьютерных атак.

– Ознакомить с различными видами современных криптографических протоколов.

3. Место дисциплины в структуре образовательной программы

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

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль «Введение в специализацию».

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

Второй 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: Информационная безопасность и работа с персональными данными.

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. Основы компьютерных систем и сетей.

- Принципы организации компьютерных сетей.
- Принципы построения современных операционных систем.

Тема 2. Понятия и задачи компьютерной безопасности.

- Основные понятия компьютерной безопасности.
- Атаки на компьютерные системы и сети.

Тема 3. Стандарты и нормативные документы компьютерной безопасности.

- Нормативные документы в области информационной безопасности.
- Стандарты в области информационной безопасности.

Тема 4. Механизмы и средства защиты компьютерных систем и сетей.

- Механизмы защиты компьютерных систем и сетей.
- Средства защиты компьютерных систем и сетей.

Тема 5. Криптографические протоколы

- Классификация криптографических протоколов.
- Атаки на криптографические протоколы.
- Протоколы идентификации.
- VPN-протоколы: IPSec, SSL/TLS.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем прохождения тестов в LMS IDO, 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 проставляется на основании выполнения практического контрольного задания, которое выполняется заочно (удаленно), а отчет о выполненном задании выкладывается в систему управления обучением ТГУ (LMS IDO) и оценивается преподавателем. При необходимости студент объясняет ход выполнения задачи при очной встрече.

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

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в LMS IDO
- https://lms.tsu.ru/course/view.php?id=5580

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

в) Семинарских / практических занятий по дисциплине нет.

г) Лабораторных работ по дисциплине нет.

д) Методические указания по организации самостоятельной работы студентов.

Самостоятельная работа организуется в следующих формах: работа со слайдами лекции; изучение вопросов, выносимых за рамки лекционных занятий; выполнение домашних заданий; подготовка к рубежному контролю по теме/разделу. Работу со слайдами (конспектом) лекции целесообразно проводить непосредственно после ее прослушивания. Необходимым элементом обучения является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологии. Изучение вопросов, выносимых за рамки лекционных занятий, предполагает самостоятельное изучение студентами дополнительной литературы.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. - Москва : Форум, 2021. – 416 с.

– Хорев, П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. – 3-е изд., испр. и доп. – Москва : ИНФРА-М, 2021. – 327 с.

– Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. – Санкт-Петербург: Лань, 2021. – 324 с.

– Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. – Москва: Издательство Юрайт, 2024. – 309 с.

б) дополнительная литература:

– Галатенко В.А. Основы информационной безопасности / В.А. Галатенко. – Москва: Национальный Открытый Университет ИНТУИТ, 2024. – 266 с.

– Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: учебное пособие. – М: ИНФРА-М, 2019, 202 с.

– Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009, 271 с.

в) ресурсы сети Интернет:

– Федеральная служба по техническому и экспортному контролю России - https://fstec.ru/

– Банк данных угроз безопасности информации ФСТЭК России- https://bdu.fstec.ru/

– National Vulnerability Database (NVD) - https://nvd.nist.gov/

– Основы информационной безопасности [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/10/10/info

– Антивирусная защита компьютерных систем [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/2259/155/info

– Безопасность сетей [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/102/102/info

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– эмуляторы компьютерной сети PNETLab, EVE-NG, GNS3

– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index–

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.

Аудитории для проведения занятий лекционного и семинарского типа индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации в смешенном формате («Актру»).

15. Информация о разработчиках

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, кафедра компьютерной безопасности, доцент.