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

Информационная безопасность и работа с персональными данными

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Обработка данных, управление и исследование сложных систем

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
Л.А. Нежельская

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1 Способен решать актуальные задачи фундаментальной и прикладной математики.

ОПК-4 Способен комбинировать и адаптировать 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-1.1 Анализирует проблемы в области фундаментальной и прикладной математики.

ИОПК-1.2 Формулирует задачи исследования.

ИОПК-1.3 Решает актуальные задачи фундаментальной и прикладной математики.

ИОПК-4.2 Учитывает основные требования информационной безопасности.

2. Задачи освоения дисциплины

– Освоить понятийный аппарат информационной безопасности.

– Ознакомиться с методами и средствами криптографической защиты информации.

– Получить представление о стандартах и нормативных документах в области информационной безопасности.

– Получить представление о составе и содержании организационных и технических мер по обеспечению безопасности персональных данных

– Ознакомиться с основными механизмами защиты от несанкционированного доступа и базовыми средствами защиты компьютерных систем и сетей

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку «ФТД. Факультативные дисциплины».

Дисциплина относится к факультативной части образовательной программы.

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

Первый семестр, зачет с оценкой

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: информатика, дискретная математика, компьютерные сети.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:

-лекции: 16 ч.

-лабораторные: 16 ч.

в том числе практическая подготовка: 16 ч.

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Общие понятия информационной безопасности

Основные понятия информационной безопасности. Классификация уязвимостей и угроз. Международные базы данных и реестры уязвимостей. Банк данных угроз безопасности информации ФСТЭК России. Атаки на компьютерные системы и сети. Меры противодействия угрозам безопасности.

Тема 2. Криптографические методы защиты информации.

Основные задачи криптографии. Криптографические системы. Криптографические протоколы. Криптографические функции хеширования. Электронная цифровая подпись. Криптографические стандарты.

Тема 3. Основные механизмы защиты от несанкционированного доступа.

Контроль целостности. Идентификация. Протоколирование и аудит. Управление доступом. Защита от вредоносных программ. Защита межсетевого взаимодействия. Защита информации при передаче по каналу связи. Предотвращение утечек информации.

Тема 4. Средства обеспечения информационной безопасности.

Межсетевые экраны. Виртуальные частные сети. Системы анализа защищенности. Системы обнаружения атак. Штатные средства защиты информации операционных систем. Аудит информационной безопасности. Защита вычислительной среды компании.

Тема 5. Стандарты и нормативные документы информационной безопасности

Стандарты в области информационной безопасности. Нормативные документы в области информационной безопасности. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, опроса по лекционному материалу, проверки лабораторных работ, и фиксируется в форме контрольной точки не менее одного раза в семестр. Практическая подготовка оценивается по результатам выполненных лабораторных работ.

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 с оценкой в первом семестре проставляется на основе выполнения студентами лабораторных работ и/или по результатам собеседования с использованием перечня контрольных вопросов по курсу. Схема контрольных вопросов соответствует компетентностной структуре дисциплины. При оценивании студенту необходимо продемонстрировать достижение всех запланированных индикаторов.

Критерии оценивания промежуточной аттестации.

Зачет с оценкой “отлично” по дисциплине проставляется, когда студент в совершенстве овладел материалом по всем разделам лекционного курса, а также показал требуемые умения и навыки при выполнении *всех* лабораторных работ.

Зачет с оценкой “хорошо” по дисциплине проставляется, когда студент овладел обязательным материалом по большинству разделов лекционного курса, возможно с некоторыми недостатками, а также показал требуемые умения и навыки при выполнении *большинства* лабораторных работ.

Зачет с оценкой “удовлетворительно” по дисциплине проставляется, когда студент овладел обязательным материалом по некоторым разделам лекционного курса, возможно с

некоторыми недостатками, а также показал требуемые умения и навыки при выполнении *части* лабораторных работ.

Зачет с оценкой “неудовлетворительно” по дисциплине проставляется, когда студент имеет существенные пробелы по теоретическим разделам дисциплины и не показал требуемые умения и навыки при выполнении части лабораторных работ.

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://moodle.tsu.ru/course/view.php?id=5226

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

в) Семинарских / практических занятий по дисциплине нет.

г) Методические указания по проведению лабораторных работ.

В задании к лабораторной работе формулируются цели лабораторной работы, а также способы их достижения. При подготовке к лабораторной работе студент обязан самостоятельно изучить методические рекомендации по проведению лабораторной работы, а также ответить на контрольные вопросы по лабораторной работе. Перед выполнением лабораторной работы преподавателем проводится инструктаж по достижению целей и решению задач лабораторной работы. По выполнению лабораторной работы студент готовит отчет, в котором указываются результаты выполнения лабораторной работы и делаются выводы. По теме лабораторной работы формулируются контрольные вопросы, позволяющие оценить уровень знаний студентов по ней.

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.

– Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка) (утв. ФСТЭК РФ 15.02.2008)

б) дополнительная литература:

– Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: учебное пособие. – М.: РИОР, 2021.

– Проскурин В. Г. Защита в операционных системах: учебное пособие. – М. : Горячая линия – Телеком, 2016.

– Малюк А.А. Защита информации в информационном обществе. Учебное пособие для вузов / А.А. Малюк. - Москва : Горячая Линия–Телеком, 2015. - 230 с.

– Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.. Защита информации в информационном обществе: учебное пособие. – М. : Горячая Линия – Телеком, 2015.

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:
– СКЗИ GnuPG для ОС Windows - https://www.gpg4win.org/
– ОС Windows 10
– 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
– ЭБС Лань – http://e.lanbook.com/
– ЭБС Консультант студента – http://www.studentlibrary.ru/
– Образовательная платформа Юрайт – https://urait.ru/
– ЭБС ZNANIUM.com – https://znanium.com/
– ЭБС IPRbooks – http://www.iprbookshop.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения лабораторных занятий, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации. Аудитории должны быть оснащены оборудованием (проектор, экран, монитор, системный блок) с доступом в Интернет.

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

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности НИ ТГУ.