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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор

_____ А. В. Замятин

«15» января 2023 г.

Рабочая программа дисциплины

Информационная безопасность и работа с персональными данными

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки :
Интеллектуальный анализ больших данных

Форма обучения
Очная

Квалификация
Магистр

Год приема
2023

Код дисциплины в учебном плане: Б1.О.02.02

СОГЛАСОВАНО:
Руководитель ОП
_____А.В. Замятин

Председатель УМК
_____С.П. Сущенко

Томск – 2023

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-1 – способность решать актуальные задачи фундаментальной и прикладной математики;

– ОПК-4 – способность 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

– Изучить общие понятия информационной безопасности

– Получить представление о методах и средствах обеспечения информационной безопасности, стандартах и нормативных документах информационной безопасности.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль «Общепрофессиональные дисциплины».

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

Первый семестр, зачет с оценкой

5. Входные требования для освоения дисциплины

Для освоения дисциплины необходимо владеть основами дискретной математики и информатики, обладать базовыми знаниями в области компьютерных систем и сетей, владеть навыками установки и настройки прикладного программного обеспечения.

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: 0 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Раздел 1. Общие понятия информационной безопасности

1.1. Основные понятия информационной безопасности.

1.2. Атаки на компьютерные системы и сети.

Раздел 2. Методы обеспечения информационной безопасности

2.1. Административно-организационные методы защиты информации

2.2. Криптографические методы защиты информации

Раздел 3. Средства обеспечения информационной безопасности
3.1. Межсетевые экраны. Виртуальные частные сети
3.2. Системы анализа защищенности. Системы обнаружения атак.
Раздел 4. Стандарты и нормативные документы информационной безопасности

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем проведения опоросов и лабораторных работ.

Типовые варианты заданий для лабораторных работ.

Тема: Общие понятия информационной безопасности. Цель: научить студентов владению основными понятиями информационной безопасности. Студент должен самостоятельно выполнить задание, выложить отчет в систему Moodle, продемонстрировать преподавателю при устной защите владение основными понятиями информационной безопасности. Вариант задания: используя Банк данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), изучить угрозы безопасности информации (описание угрозы, источники угрозы, объект воздействия, последствия реализации угрозы), характерные для выбранного студентом IT-объекта (облачные сервис, грид-система, BIOS, виртуальная среда, беспроводная сеть, ОС, web-приложение, хранилище больших данных, прикладное ПО и пр.), а также известные устраненные уязвимости для выбранного типа ПО (СУБД, АСУ ТП и т.п.).

Тема: Методы обеспечения информационной безопасности. Цель: научить студентов владению основными методами обеспечения информационной безопасности. Студент должен самостоятельно выполнить задания, выложить отчет в систему Moodle, продемонстрировать преподавателю при устной защите владение основными методами обеспечения информационной безопасности. Вариант задания "Классические шифры замены и перестановки": зашифровать свое ФИО: 1) лозунговым шифром; 2) шифром Виженера; 3) шифром вертикальной перестановки; расшифровать произвольное слово из предложенного списка и зашифрованное шифром Виженера при известном ключе.
Задание "Современные симметричные шифры".

Тема: Средства обеспечения информационной безопасности. Цель: научить студентов владению основными средствами обеспечения информационной безопасности. Студент должен самостоятельно выполнить задания, выложить отчет в систему Moodle, продемонстрировать преподавателю при устной защите владение основными средствами обеспечения информационной безопасности. Вариант задания "Встроенные средства защиты ОС Windows": написать краткий обзор методов и средств обеспечения информационной безопасности ОС Windows 10 на основе различных источников информации: официальный сайт компании Microsoft, учебные интернет-курсы Национального Открытого Университета «ИНТУИТ» и пр, используя консоль управления mmc (Microsoft Management Console), выполнить различные задания преподавателя, связанные с управлением доступом к данным, аудитом системы, работой с диспетчером сертификатов, созданием шаблона безопасности.

Тема: Стандарты и нормативные документы информационной безопасности. Цель: научить студентов владению основными стандартами и нормативными документами информационной безопасности. Студент должен самостоятельно выполнить задание, выложить отчет в систему Moodle, продемонстрировать преподавателю при устной защите владение основными основными стандартами и нормативными документами информационной безопасности. Вариант задания "Руководящие документы

Гостехкомиссии России": на сайте ФСТЭК России (Федеральная служба по техническому и экспортному контролю) http://fstec.ru/ найти Государственный реестр сертифицированных средств защиты информации, в данном реестре выбрать средство защиты, которое имеет сертификат на соответствие одному или нескольким руководящим документам либо по уровню контроля отсутствия НДВ (недекларированных возможностей), либо по классу защищенности СВТ (средств вычислительной техники), либо по классу защищенности МЭ (межсетевых экранов), либо по классу защищенности АС (автоматизированных систем), изучить соответствующий(ие) руководящий(ие) документ(ы), описать требования, которые предъявляются к выбранному средству защиты с точки зрения соответствия заданному классу защищенности, и выложить в систему Moodle.

Примерный перечень вопросов текущего контроля:

1. Дать определение одного их следующих понятий: шифр, секретный ключ, шифрование данных, симметричный шифр, асимметричный шифр, открытый ключ, закрытый ключ, хэш-функция (ключевая и безключевая), электронная цифровая подпись, аутентификация, протоколирование, активный аудит, управление доступом, матрица доступа, межсетевое экранирование, туннелирование, компьютерный вирус, политики безопасности, VPN-шлюз (шлюз безопасности).
2. Перечислить известные криптографические алгоритмы, используемые на практике (симметричные шифры, асимметричные шифры, хэш-функции, цифровые подписи).
3. Изложить основные свойства электронной цифровой подписи (хэш-функции).
4. Поставить задачу активного аудита/управление доступом/межсетевого экранирования.
5. Изложить функции межсетевого экрана (фильтрация и посредничество) и представить межсетевой экран моделью последовательности фильтров.
6. Перечислить параметры, по которым можно производить анализ информационного потока, существующие методы построения VPN-шлюзов, типичные проблемы, решаемые при анализе защищенности.
7. Объяснить функции системы обнаружения атак (СОА), перечислить виды сенсоров (агентов) СОА, охарактеризовать методы анализа СОА
8. Привести примеры классов (показателей) защищенности в соответствии с Руководящими документами Гостехкомиссии России.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет с оценкой в первом семестре проводится в письменной форме по билетам.

Примерный перечень вопросов к зачету с оценкой:

1. Изложить основные понятия информационной безопасности (ИБ).
2. Классифицировать атаки на компьютерные сети.
3. Перечислить атаки на коммуникационные протоколы.
4. Описать законодательные методы обеспечения ИБ.
5. Описать административно-организационные методы обеспечения ИБ.
6. Сравнить симметричные и асимметричные шифры.
7. Предоставить схему гибридной (комбинированной) криптосистемы.
8. Предоставить схему электронной цифровой подписи.
9. Изложить метод обеспечения целостности сообщения.

10. Изложить основные свойства электронной цифровой подписи.
11. Охарактеризовать парольный метод аутентификации.
12. Охарактеризовать аппаратную аутентификацию.
13. Охарактеризовать биометрическую аутентификацию.
14. Охарактеризовать аутентификацию на основе цифровых сертификатов.
15. Охарактеризовать аутентификацию на базе протокола «запрос-ответ».
16. Перечислить цели и задачи протоколирования и аудита.
17. Охарактеризовать статистический метод обнаружения атак.
18. Охарактеризовать сигнатурный метод обнаружения атак.
19. Охарактеризовать дискреционное управление доступом.
20. Охарактеризовать мандатное управления доступом.
21. Охарактеризовать ролевое управление доступом.
22. Перечислить функции, которые может выполнять межсетевой экран.
23. Классифировать компьютерные вирусы и вредоносные программы.
24. Изложить способы распространения и обнаружения вредоносных программ.
25. Изложить типовое содержание политики безопасности предприятия.
26. Охарактеризовать технологию построения виртуальных частных сетей.
27. Охарактеризовать технологию анализа защищенности сети.
28. Охарактеризовать технологию обнаружение атак на компьютерные сети.
29. Классифицировать системы обнаружения атак.
30. Охарактеризовать стандартные средства системы безопасности операционных систем.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle»

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

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

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

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

б) дополнительная литература:

– В. Ф. Шаньгин. Комплексная защита информации в корпоративных системах. – ФОРУМ, 2020.

– А.А. Малюк. Защита информации в информационном обществе: учебное пособие . – Горячая Линия - Телеком, 2015.

– А.П. Зайцев, Р.В.Мещеряков, А.А. Шелупанов. Технические средства и методы защиты информации: учебник . – Горячая Линия - Телеком, 2016.

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– MS PowerPoint, OpenPGP, ОС Windows 7(10), Oracle VM VirtualBox, Firefox, Advanced IP Scanner, WireShark, MSAT.

б) информационные справочные системы:

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

– 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
– Информационная безопасность: учебно-методический комплекс [Электронный ресурс] // Томский государственный университет. 2016. URL:
– http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000534758
– Научная электронная библиотека eLIBRARY.RU [Электронный ресурс] // «Научная электронная библиотека». URL: https://www.elibrary.ru/defaultx.asp

14. Материально-техническое обеспечение

Для реализации дисциплины необходимы лекционная аудитория и аудитория для проведения лабораторных работ. Аудитории должны быть оснащены оборудованием (проектор, экран, монитор, системный блок) с доступом в Интернет. Вся основная и дополнительная литература, необходимая для самостоятельной работы и подготовки к зачету с оценкой, имеется в научной библиотеке ТГУ.

15. Информация о разработчиках

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