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

«__» _____ 20__ г.

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
2023

Код дисциплины в учебном плане: Б1.О.04.01

СОГЛАСОВАНО:
Руководитель ОП
_____А.Ю. Матросова

Председатель УМК
_____С.П. Сущенко

Томск – 2023

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:

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.

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.

Каждая из заявленных компетенций отражает несколько образовательных результатов:

ОР-2.1.1 Владеть: современными информационно-коммуникационными технологиями для решения задач в области прикладной математики с учетом требований информационной безопасности;

ОР-2.1.2 Уметь: использовать известные криптографические системы для обеспечения безопасности компьютерных систем;

ОР-2.1.3 Знать: виды политик контроля доступа и соответствующие модели безопасности для разработки и анализа механизмов контроля доступа компьютерных систем;

ОР-4.2.1 Знать: основные требования информационной безопасности к политикам контроля доступа и криптографическим протоколам защиты данных;

ОР-4.2.2 Знать: основные направления атак на распространённые телекоммуникационный протоколы для организации мер по противодействию таким атакам;

ОР-2.1.4 Владеть: навыками проведения контрольных проверок работоспособности и эффективности примитивов разработки систем контроля доступа и механизмов их реализации для разработки безопасных компьютерных систем;

ОР-2.1.5 Уметь: разрабатывать требования к безопасному функционированию телекоммуникационных систем и оценивать их работоспособность и эффективность;

ОР-2.1.6 Уметь: разрабатывать требования к программно-аппаратным реализациям криптографических алгоритмов и оценивать их работоспособность и эффективность в рамках поставленной задачи.

2. Задачи освоения дисциплины

- Научиться использовать современные информационно-коммуникационные технологии для решения задач в области прикладной математики с учетом требований информационной безопасности.
- Научиться использовать известные криптографические системы для обеспечения безопасности компьютерных систем.

- Научиться использовать основные виды политик контроля доступа и соответствующие модели безопасности для разработки и анализа механизмов контроля доступа компьютерных систем.
- Научиться анализировать основные требования информационной безопасности к политикам контроля доступа и криптографическим протоколам защиты данных.
- Научиться учитывать основные направления атак на распространённые телекоммуникационный протоколы для организации мер по противодействию таким атакам.
- Научиться применять существующие примитивы разработки систем контроля доступа и механизмы их реализации для разработки безопасных компьютерных систем.
- Научиться применять знания математических основ криптографических алгоритмов для их программной реализации и внедрения в компьютерные системы.
- Научиться обеспечивать безопасное функционирование телекоммуникационных протоколов.

3. Место дисциплины в структуре образовательной программы

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 освоения дисциплины необходимо знать основы дискретной математики, общей алгебры, компьютерных сетей и операционных систем.

Пререквизиты дисциплины: Введение в программную инженерию, 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. Общие понятия компьютерной безопасности

Основные понятия компьютерной безопасности. Конфиденциальность, целостность и доступность информации. Виды атак на компьютерные системы. Правовое обеспечение компьютерной безопасности.

Тема 2. Основы сетевой безопасности

Атаки на телекоммуникационные протоколы. Стек TCP/IP и атаки на него. DDoS атаки (DNS, HTTP, TCP, MAC-flooding). MAC flooding и spoofing. Межсетевые экраны. Шлюзы сетевого и прикладного уровней, пакетные фильтры.

Тема 3. Криптографическая защита информации

Введение в криптографию. Шифры подстановки и перестановки. Симметричные и ассиметричные криптосистемы. Поточные и блочные шифры. AES (Advanced Encryption Standard) и DES. Режимы шифрования. Hash-функции и цифровая подпись. Передача сеансового ключа (RSA и алгоритм Диффи-Хелмана). Perfect forward secrecy. Шифрование интернет-трафика на примере Transport Layer Security. Отличия TLS 1.3 и 1.2.

Тема 4. Управление доступом.

Контроль доступа в компьютерных системах. Дискреционная и мандатная политики контроля доступа. Основные модели и механизмы контроля доступа в компьютерных системах. Методы реализации политик контроля доступа (IBAC, LBAC, RBAC, ABAC).

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем прохождения тестов в системе moodle, выполнения и представления группового проекта и фиксируется в форме контрольной точки не менее одного раза в семестр.

Типовые задания и иные необходимые для текущего контроля материалы приведены в Приложении 1 к рабочей программе «Фонд оценочных средств».

10. Порядок проведения и критерии оценивания промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме устного зачёта по теоретическому материалу. Каждый билет для устного зачёта состоит из двух теоретических вопросов по различным темам дисциплины, а также сопровождается дополнительными вопросами по темам дисциплины.

Примеры вопросов к зачёту

1. Конфиденциальность, целостность и доступность информации.
2. Цифровая подпись
3. Дискреционная и мандатная политики контроля доступа
4. Передача сеансового ключа (RSA и алгоритм Диффи-Хелмана). Perfect forward secrecy.
5. Симметричные и асимметричные шифры.

Остальные вопросы и также критерии оценивания приведены в Приложении 1 к рабочей программе «Фонд оценочных средств»

Для допуска к устному экзамену необходимо прохождение текущей аттестации, которая включает следующие пункты.

1. Выполнение группового проекта

2. Прохождение тестов в системе moodle. Тест считается пройденным, если обучающийся верно ответил на 70% вопросов или более. В случае неудачи – предоставляется дополнительная попытка.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=5580

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).

в) Самостоятельная работа студентов при изучении дисциплины предусмотрена в следующих видах и формах:

1. изучение теоретического материала на основе курса лекций, предложенной литературы и учебно-методического обеспечения (перечень литературы проведён ниже);
2. прохождение теста в системе moodle;
3. выполнение группового проекта.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

- Башлы П.Н. Информационная безопасность и защита информации : учебное пособие / Башлы П.Н., Бабаш А.В., Баранова Е.К.. — Москва : Евразийский открытый институт, 2012. — 311 c.
- Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2021. — 327 с.
- Алферов А.П. Основы криптографии: учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 479 с.
- Жуков, В. Г. Безопасность вычислительных сетей. Ч. I. Базовые протоколы стека TCP/IP [Электронный ресурс] : учеб. пособие / В. Г. Жуков. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 124 с.
- Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебно-методическое пособие / П. Н. Девянин. — Москва : Горячая линия-Телеком, 2012. — 320 с.
- Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие. Екатеринбург: изд-во Урал. Ун-та, 2008. - 212 с.

б) дополнительная литература:

- Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 592 с.
- Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.
- Малюк, А. А. Защита информации в информационном обществе : учебное пособие для вузов. / А. А. Малюк - Москва : Горячая линия - Телеком, 2015. - 230 с.

в) ресурсы сети Интернет:

- Курс “Безопасность сетей” [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/102/102/info (дата обращения: 01.09.2021).
- Описание атак на криптографические протоколы [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc7457 (дата обращения: 01.09.2021).
- Спецификация протокола Transport Layer Security [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc8446 (дата обращения: 01.09.2021).

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

Программное обеспечение для показа презентаций с лекциями и представления отчётов по групповым проектам обучающихся (напр. Adobe Acrobat Reader или Microsoft PowerPoint или их аналоги). Проекты выполняются студентами с использованием свободно-распространяемого программного обеспечения.

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

Для реализации дисциплины необходимы лекционные аудитории и аудитории для проведения практических занятий. Проектор требуются для демонстрации материала в рамках изучаемых разделов и проведения защиты проектов в конце семестра.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

Для совместной работы над групповым проектом рекомендуется использовать соответствующие информационные технологии (например, discord, github и их аналоги).

15. Информация о разработчиках

Твардовский Александр Сергеевич, канд. физ.-мат. наук, старший преподаватель кафедры компьютерной безопасности.