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_» ___июня___ 20_23_ г.

Рабочая программа дисциплины

Введение в компьютерную безопасность

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.В.ДВ.03.02.01

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-2 – способность совершенствовать и реализовывать новые математические методы решения прикладных задач способность;

– ПК-1 – способность разрабатывать и применять математические методы, алгоритмы, программное обеспечение для решения задач научно-исследовательской и проектной деятельности;

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

ИПК-1.2 Применяет существующие математические методы, алгоритмы и программное обеспечение для решения задач в области профессиональной деятельности.

ИОПК-4.2 Учитывает основные требования информационной безопасности.

2. Задачи освоения дисциплины

– Ознакомить студентов с основами информационной безопасности компьютерных систем, атаками на сетевые протоколы и мерами по их предотвращению, криптографическими методами защиты информации, такими как шифрование информации, её хеширование и цифровая подпись, а также базовыми понятиями о системах контроля доступа и механизмах авторизации пользователей.

3. Место дисциплины в структуре образовательной программы

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

Второй семестр, зачет

5. Входные требования для освоения дисциплины

Для освоения дисциплины необходимо знать основы дискретной математики, общей алгебры, компьютерных сетей и операционных систем. Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: «Информационная безопасность и работа с персональными данными», «Математические методы и модели для компьютерных наук», «Введение в программную инженерию».

6. Язык реализации

Русский

7. Объем дисциплины

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

Основные понятия компьютерной безопасности
Виды атак на компьютерные системы
Правовое обеспечение компьютерной безопасности

Раздел 2. Основы сетевой безопасности
Атаки на телекоммуникационные протоколы
Межсетевые экраны
Изучение учебного материала

Раздел 3. Криптографическая защита информации
Введение в криптографию
Симметричные и ассиметричные криптосистемы
Hash-функции и цифровая подпись
Шифрование интернет-трафика на примере Transport Layer Security

Раздел 4. Управление доступом
Контроль доступа в компьютерных системах
Основные модели и механизмы контроля доступа в компьютерных системах

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем прохождение тестов в системе Moodle, а также выполнение учебного проекта.

Проектное задание:

Проект предназначен для группы от одного до трёх человек и заключается в реализации сервиса по хранению ключей пользователей и подписыванию ими электронной документации.

Сервис должен быть реализован как клиент-серверное приложение и поддерживать следующие функции.

a) Система аутентификации и авторизации пользователей.
b) Генерация, приём от клиента и хранение пары из открытого (public) и закрытого (private) ключей.
c) Генерация цифровой подписи, при помощи хранимого сервером закрытого ключа, для загружаемого пользователем документа.

Для реализации цифровой подписи могут быть использованы криптосистемы RSA, DSA, ECDSA, и др. Для генерации хеш-значения рекомендуются алгоритмы семейства SHA.

Результатом выполнения проекта является письменный отчёт.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Промежуточная аттестация осуществляется на основе собеседования при условии успешного выполнения проекта.

Список билетов к зачёту:

Билет 1

1. Информационная безопасность. Свойства безопасности информации.

2. AES (Advanced Encryption Standard). Режимы шифрования.

Билет 2

1. Уязвимость, угроза, атака. Классификация атак/угроз
2. MAC (message authentication code).

Билет 3

1. Межсетевые экраны (шлюзы сетевого и прикладного уровней).
2. Передача сеансового ключа (RSA и алгоритм Диффи-Хелмана). Perfect forward secrecy.

Билет 4

1. Канальный уровень. MAC flooding и spoofing.
2. Криптографическая система. Шифрование и расшифрование.

Билет 5

1. Межсетевые экраны (пакетные фильтры).
2. Симметричные и асимметричные шифры. Принципы криптографической защиты Кергкхоффса

Билет 6

1. DDoS атаки (DNS, HTTP, TCP, MAC-flooding).
2. Data Encryption Standard (DES)

Билет 7

1. Протокол DNS и атаки на него.
2. Шифры подстановки и перестановки.

Билет 8

1. Отличия TLS 1.3 и 1.2
2. Поточные и блочные шифры. RC4 и Salsa20

Билет 9

1. Дискреционная и мандатная политики контроля доступа (основные признаки и отличия)
2. Цифровая подпись

Билет 10

1. Терминология в области управления доступом
2. TLS Handshake 1.2

Билет 11

1. Методы реализации политик контроля доступа (IBAC, LBAC, RBAC, ABAC)
2. TLS Records, Alerts, История TLS

Дополнительные вопросы к зачёту:

1. Конфиденциальность, целостность и доступность информации.
2. Уязвимость, угроза, атака.
3. Активная атака (пример)
4. Пассивная атака (пример)
5. Пакетные фильтры
6. Шлюзы сетевого уровня
7. Канальный уровень

8. Коммутатор и маршрутизатор. Отличия.
9. Сетевой уровень TCP/IP
10. Транспортный уровень TCP/IP
11. Прикладной уровень TCP/IP
12. Стек TCP/IP инкапсуляция и декапсуляция данных
13. MAC-spoofing
14. IP-spoofing
15. DDoS-атака
16. Zero window stress
17. SYN-атака
18. HTTP Slow GET/POST
19. Шлюзы прикладного уровня
20. Отравление кэша DNS
21. DNS Amplification
22. Криптографическая система
23. Может ли сумма по модулю 2 (XOR) ключа с открытым тестом быть стойким шифром
24. Шифры подстановки
25. Шифры перестановки
26. Симметричный шифр
27. Ассиметричный шифр
28. Потоковый шифр
29. Блочный шифр
30. Раундовая функция в DES
31. Сеть Фейстеля
32. Triple DES
33. State в AES
34. Основные преобразования в AES
35. MAC (message authentication code)
36. RSA
37. Perfect forward secrecy
38. Протокол Диффи-Хеллмана
39. Цифровая подпись
40. Сертификаты
41. Типы записей в TLS
42. Client/Server Hello в TLS
43. TLS Records
44. Отличия TLS 1.2 и 1.3 (не менее двух)
45. Политика, механизм и модель контроля доступа
46. Граф доступов
47. Информационный поток
48. Дискреционная политика
49. Мандатная политика
50. Списки доступа
51. Ролевая модель
52. Атрибутная модель

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, 2019.

– П.Б. Хорев. Программно-аппаратная защита информации: учебное пособие. – ИНФРА-М, 2020.

– А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Основы криптографии: учебное пособие для вузов. – М.: Гелиос АРВ, 2005.

– В. Г. Жуков. Безопасность вычислительных сетей. Ч. I. Базовые протоколы стека TCP/IP – Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012.

– П. Н. Девянин. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебно-методическое пособие. – Горячая линия-Телеком, 2012.

– Н.А. Гайдамакин. Теоретические основы компьютерной безопасности. Учебное пособие. – Екатеринбург: изд-во Урал. Ун-та, 2008.

б) дополнительная литература:

– В. Ф. Шаньгин. Комплексная защита информации в корпоративных системах: учебное пособие. – ИНФРА-М, 2015.

– А.В. Бабаш. Криптографические методы защиты информации. Учебно-методическое пособие. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014.

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

в) ресурсы сети Интернет:

– 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:

– Microsoft PowerPoint или ПО для презентации файла в формате pdf (напр. Adobe Acrobat Reader).

б) информационные справочные системы:

– 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).

14. Материально-техническое обеспечение

Аудитория для проведения лекционных занятий должна быть оснащена мультимедийным оборудованием с доступом в интернет (проектор, экран, монитор, системный блок).

15. Информация о разработчиках

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