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
« 19 » мая 20 22 г.

Рабочая программа дисциплины

Методы и средства криптографической защиты информации

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки / специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2022

Код дисциплины в учебном плане: Б1.О.06.04

СОГЛАСОВАНО:
Руководитель ОП
_____В.Н. Тренькаев

Председатель УМК
_____С.П. Сущенко

Томск – 2022

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-2 – Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности

– ОПК-10 – Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

– ОПК-13 – Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.

– ПК-2 – Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

– ПК-3 – Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-2.2 Определяет порядок настройки и эксплуатации программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности.

ИОПК-2.3 Формулирует предложения по применению программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности.

ИОПК-10.1 Осуществляет анализ тенденций развития методов и средств криптографической защиты информации.

ИОПК-10.2 Применяет средства криптографической защиты информации при решении задач профессиональной деятельности.

ИОПК-13.1 Предпринимает необходимые действия по сбору и анализу исходных данных для проектирования компонент программных и программно-аппаратных средств защиты информации в компьютерных системах.

ИОПК-13.2 Определяет параметры функционирования, архитектуру и интерфейсы компонент программных и программно-аппаратных средств защиты информации в компьютерных системах.

ИОПК-13.3 Проводит анализ компонент программных и программно-аппаратных средств защиты информации в компьютерных системах с целью определения уровня обеспечиваемой ими защищенности и доверия.

ИПК-2.1 Определяет угрозы безопасности и их возможные источники, каналы утечки информации.

ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации.

ИПК-2.3 Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации.

ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием.

2. Задачи освоения дисциплины

– Сформировать у студентов способность анализировать тенденции развития методов и средств криптографической защиты информации, в частности дать представление о базовых понятиях и задачах криптографии, методах криптографического анализа, ознакомить с современными стандартами в области криптографии.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль "Специализация".

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

Седьмой семестр, экзамен
Восьмой семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Языки программирования, Информатика, Введение в математику, Дискретная математика, Теория вероятностей и математическая статистика, Математическая логика и теория алгоритмов, Дискретная математика, Теория автоматов, Теория информации, Теория чисел, Общая алгебра, Теория вычислительной сложности, Профессиональный перевод специальной литературы.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 9 з.е., 324 часов, из которых:
-лекции: 64 ч.
-лабораторные: 16 ч.
-практические занятия: 48 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Введение в криптографию
Основные понятия и задачи криптографии.
Криптографический анализ. История криптографии.

Тема 2. Шифры замены и перестановки
Шифры замены. Криптоанализ шифров замены.
Шифры перестановки. Криптоанализ шифров перестановки.
Шифры замены и перестановки. Роторные шифры.

Тема 3. Абсолютно стойкие шифры
Вероятностная модель шифра по К.Шеннону.
Необходимые и достаточные условия абсолютной стойкости шифра.
Атака на основе шифртекста.

Тема 4. Блочные шифры
Принципы построения. Базовые операции. Сеть Фейстеля. SP-сеть.
Шифр DES. Шифр ГОСТ 28147-89 («Магма»). Шифр AES.
Упрощенные шифры DES и AES. Шифр «Кузнечик».

Тема 5. Поточные шифры
Схема поточного шифра. Генераторы псевдослучайных чисел.
Комбинирующий и фильтрующий генераторы. Шифр A5. Шифр RC4.

Тема 6. Ассиметричные шифры
Односторонняя функция с лазейкой. Шифр RSA.
Шифр Эль-Гамаля. Свойства шифра Эль-Гамаля.
Шифр Шамира. Атаки на RSA.

Тема 7. Цифровая подпись
Цифровая подпись RSA, Эль-Гамаля, DSS.
Атаки на цифровые подписи.
Инфраструктура открытых ключей.

Тема 8. Криптографические функции хеширования.
Имитовставка. Бесключевые и ключевые хэш-функции.
Конструкция Меркла-Дамгарда. Конструкция Губка. Стрибог.
SHA. MD4. HMAC. Атаки на хэш-функции.

Тема 9. Теория секретных систем Шеннона.
Алгебра секретных систем. Виды секретных систем.
Примеры секретных систем. Свойства секретных систем.

Тема 10. Методы криптоанализа.
Обзор методов криптоанализа. Линейный криптоанализ.
Дифференциальный криптоанализ. Слайдовая атака.
Корреляционная атака. Алгебраическая атака.
Атаки по побочным каналам.

Тема 11. Автоматная криптография.
Автоматы как компоненты криптосистем. Автоматные шифрсистемы.
Конечно-автоматная криптосистема с открытым ключом (FAPKC).
Поточные и автоматные шифрсистемы.

Тема 12. Средства криптографической защиты информации.
Обзор средств криптографической защиты информации.
Криптоконтейнеры. Криптопровайдеры. VPN-шлюзы.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, выполнения лабораторных работ/контрольных заданий и фиксируется в форме контрольной точки не менее одного раза в семестр.

Примеры типовых вариантов контрольных заданий:

- Зашифровать свою фамилию аффинным шифром, шифром Виженера, шифром Хилла, показывая корректность выбранных ключей.
- Используя CrypTool-Online (https://www.cryptool.org) подсчитать частные характеристики произвольного большого открытого текста, зашифровать любой текст с помощью сдвигового шифра и подсчитать частные характеристики зашифрованного текста. Далее сравнить с таковыми, полученными для произвольного отрытого текста, выдвинуть гипотезу о таблице замены, проверить гипотезу, сравнив с истинной таблицей замены.

- Построить таблицу шифрования произвольного шифра, когда множество открытых (шифрованных) текстов X=Y={0,1,2}, множество ключей K={0,1,2}. Реализовать атаку на основе шифртекста, при условии, что все ключи равновероятны, но среди открытых текстов есть сильно вероятный текст. Определить при перехвате какого шифротекста получается наилучший вариант восстановления открытого текста.
- Сгенерировать произвольный открытый текст (8 бит) и ключ (10 бит). Вычислить шифрованный текст (8 бит), который получается после первого раунда упрощенного варианта DES (Simplified DES). При этом представить все промежуточные результаты вычислений как при генерации раундовых ключей, так и при вычислении значений раундовой функции, т.е. после каждого P-блока, S-блока, XOR.
- Сгенерировать произвольный открытый текст (16 бит) и раундовый ключ (16 бит). Вычислить шифрованный текст (16 бит), который получается после первого раунда упрощенного варианта шифра AES (Simplified AES). При этом представить все промежуточные результаты вычислений, т.е. после каждого преобразования SubNibbles, ShiftRows, MixColumns, AddRoundKey.
- Построить псевдослучайную последовательность небольшой длины, выбрав малые произвольные параметры генератора (модуль, начальные значение и т.п.) и используя алгоритм середины квадрата, линейный конгруэнтный генератор, аддитивный генератор Фибоначчи, инверсный конгруэнтный генератор, регистр сдвига с линейной обратной связью, генератор с квадратичным остатком.
- Вычислить несколько элементов псевдослучайной последовательности при произвольно выбранном ключе, когда в качестве генератора используется упрощенный вариант RC4 (4 ячейки вместо 256). В решении представить все промежуточные результаты вычислений.
- Реализовать атаку на подпись RSA по выбранному шифротексту, когда при подписывании и шифровании используется одинаковый ключ, перехвачен шифротекст и известен открытый ключ отправителя сообщения, а требуется найти исходный открытый текст без знания закрытого ключа: выбрать параметры шифра, вычислить открытую и закрытую экспоненты, зашифровать произвольный открытый текст, провести необходимые вычисления со стороны атакующего, подписать замаскированное сообщение атакующего, провести финальные вычисления со стороны атакующего и восстановить открытый текст.
- Реализовать атаку на шифр Эль-Гамаля на основе шифртекста, когда при шифровании различных сообщений используется одно и тоже значение случайной величины: определить, что надо знать атакующему, выбрать параметры шифра, вычислить открытый и закрытый ключи, зашифровать необходимое количество произвольных открытых текстов, провести вычисления со стороны атакующего, убедится в правильности результатов атаки.

Пример типового варианта лабораторной работы:

- Выполнить линейный криптоанализ учебного блочного шифра. Учебный шифр и методика выполнения лабораторной работы представлены в книге Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их

анализа. – М: Гелиос АРВ, 2006. – 376с. Глава 9. Лабораторно-практические работы (стр.206-280).

- Выполнить дифференциальный анализ учебного блочного шифра. Учебный шифр и методика выполнения работы представлены в книге Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М: Гелиос АРВ, 2006. – 376с. Глава 9. Лабораторно-практические работы (стр.206-280)

Выполнение лабораторной работы/контрольного задания оценивается в 100 баллов:

0-20 Студент не разбирается в задаче, не знает методов решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

21-40 Студент слабо разбирается в задаче, плохо знает методы решения, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя.

41-60 Студент в целом удовлетворительно разбирается в задаче, использует методы решения при подсказке преподавателя, отвечает на вопросы неуверенно, но с негрубыми ошибками. Представляет работу на защите удовлетворительно.

61-80 Студент в целом уверенно разбирается в задаче, знает и использует методы решения практически самостоятельно, отвечает на вопросы с замечаниями. Представляет работу на защите в целом хорошо, с замечаниями.

81-100 Студент отлично разбирается в задаче, знает и использует методы решения самостоятельно, отвечает на вопросы уверенно. Представляет работу на защите отлично, уверенно.

Допуском до экзамена является выполнение 80% лабораторных работ/контрольных заданий, с оценкой за каждую не менее 50 баллов.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Экзамен в седьмом/восьмом семестре проводится в устной/письменной форме с использованием перечня контрольных вопросов/билетов по курсу. Схема вопросов экзамена должна соответствовать компетентностной структуре дисциплины. При оценивании необходимо продемонстрировать достижение всех запланированных индикаторов – результатов обучения. Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Примерный перечень билетов к экзамену (7 семестр):

Билет 1.

1. Криптоанализ. Основные криптоаналитические атаки.
2. Шифр DES: общая схема, функция шифрования, генерация раундовых ключей.

Билет 2.

1. Криптоанализ. Практическая и теоретическая стойкости.
2. Шифр ГОСТ 28147-89 (Магма): общая схема, функция шифрования, генерация раундовых ключей.

Билет 3.

1. Организация секретной связи с использованием симметричного, асимметричного, гибридного (комбинированного) шифрования.

2. Шифр AES: общая схема, базовые операции (Sub Bytes, Shift Rows, Mix Columns, Add Round Key).

Билет 4.

1. Аутентификация сообщений на базе имитовставки/цифровой подписи.
2. Режимы использования блочных шифров (сцепление, блочная гамма, имитовставка).

Билет 5.

1. Шифры простой замены. Шифр Цезаря. Сдвиговый шифр.
2. Сравнение блочных шифров ГОСТ 28147-89 и DES.

Билет 6.

1. Частотный криптоанализ шифров простой замены.
2. Вероятностная модель шифра по К.Шеннону. Атака на основе шифртекста.

Билет 7.

1. Шифры многоалфавитной замены. Шифр Виженера.
2. Абсолютно стойкие шифры. Теорема Шеннона.

Билет 8.

1. Криптоанализ шифров многоалфавитной замены. Метод Касиски.
2. Абсолютно стойкие шифры. Латинский квадрат.

Билет 9.

1. Шифры многозначной замены. Шифр пропорциональной замены.
2. Принципы построения блочных шифров. Сеть Фейстеля. SP-сеть.

Билет 10.

1. Полиграммные шифры. Шифр Хилла.
2. Маршрутные перестановки. Шифр вертикальной перестановки.

Билет 11.

1. Криптоанализ шифров вертикальной перестановки на основе запретных биграмм.
2. Поточные шифры. Комбинирующий и фильтрующий генераторы.

Билет 12.

1. Шифры гаммирования. Шифр Вернама. Одноразовый блокнот.
2. Поточные шифры на базе регистров сдвига с линейной обратной связью.

Билет 13.

1. Криптоанализ шифра гаммирования при перекрытиях.

2. Требования, предъявляемые к криптографическим генераторам псевдослучайных чисел.

Билет 14.

1. Синхронный и самосинхронизирующийся поточный шифры.
2. Шифр Эль-Гамаля.

Билет 15.

1. Поточные шифры. Генератор Геффе.
2. Шифр RSA. Корректность RSA.

Билет 16.

1. Поточные шифры. RC4.
2. Свойства шифра Эль-Гамаля.

Билет 17.

1. Поточные шифры. A5.
2. Шифр RSA. Атаки на RSA.

Билет 18.

1. Односторонняя функция. Три кандидата на одностороннюю функцию.
2. Цифровая подпись. Отказ от авторства. Приписывание авторства.

Билет 19

1. Асимметричный шифр. Атака подмены открытого ключа.
2. Цифровая подпись RSA.

Билет 20.

1. Атаки на цифровую подпись.
2. Функции хеширования. Конструкция Меркла-Дамгарда.

Билет 21

1. Цифровая подпись Эль-Гамаля.
2. Функции хеширования. Конструкция Губка.

Билет 22.

1. Требования к криптографическим хэш-функциям.
2. Асимметричный шифр. Шифр Шамира.

Билет 23.

1. Атака на основе «парадокса дней рождений»
2. Инфраструктура открытых ключей.

Билет 24.

1. Регистровое представление функции сжатия MD4 (5) и SHA-1(2)
2. Сравнение цифровой подписи с рукописной подписью.

Билет 25.

1. Линейный конгруэнтный генератор, аддитивный генератор. Свойства генераторов.
2. Хеш-функция Стрибог: общая схема, функция сжатия.

Билет 26.

1. Поточные шифры. Генератор с квадратичным остатком.
2. Ключевые хэш-функции на основе бесключевых. HMAC.

Примерный перечень вопросов к экзамену (8 семестр):

1. Схема секретной системы. Примеры секретных систем.
2. Параметры секретных систем: количество секретности, объем ключа и др.
3. Алгебра секретных систем.
4. Эндоморфная секретная система.
5. Идемпотентная секретная система.
6. Чистые и смешанные секретные системы.
7. Свойства чистых секретных систем.
8. Подобные секретные системы.
9. Ненадежность (условная энтропия) как теоретическая мера секретности.
10. Идеальная секретная система.
11. Автоматы как компоненты криптосистем: генераторы ключевого потока.
12. Автоматы как компоненты криптосистем: комбайнеры.
13. Автоматы как компоненты криптосистем: клеточные автоматы.
14. Автоматы как компоненты криптосистем: пурпурная машина.
15. Шифр Закревского.
16. Равносильность поточных и автоматных шифрсистем.
17. Конечно-автоматная криптосистема с открытым ключом (FAPKC).
18. Криптоанализ. Метод «встреча посередине».
19. Криптоанализ. Дифференциальный метод.
20. Криптоанализ. Линейный метод.
21. Криптоанализ. Корреляционный метод.
22. Криптоанализ. Алгебраический метод.
23. Атаки по побочным каналам.
24. Средства криптографической защиты информации. Криптоконтейнеры.
25. Средства криптографической защиты информации. Криптопровайдеры.
26. Средства криптографической защиты информации. VPN-шлюзы.

Критерии выставления оценок:

Отлично - студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении заданий на лабораторных/практических занятиях.

Хорошо - студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении заданий на лабораторных/практических занятиях.

Удовлетворительно - студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении заданий на лабораторных/практических занятиях.

Неудовлетворительно - студент имеет существенные пробелы по отдельным теоретическим разделам специальной дисциплины или не показал требуемые умения и навыки при выполнении заданий на лабораторных/практических занятиях.

11. Учебно-методическое обеспечение

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

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

в) План практических занятий по дисциплине.

1. Разбор примеров и решение задач по теме шифры замены
2. Разбор примеров и решение задач по теме шифры перестановки.
3. Разбор примеров и решение задач по теме абсолютно стойкие шифры.
4. Разбор примеров и решение задач по теме блочные шифры.
5. Разбор примеров и решение задач по теме поточные шифры.
6. Разбор примеров и решение задач по теме ассиметричные шифры.
7. Разбор примеров и решение задач по теме цифровая подпись.
8. Разбор примеров и решение задач по теме криптографические функции хеширования.

г) Методические указания по проведению лабораторных работ.

Для выполнения лабораторной работы студенту необходимо:

1. Изучить методические указания по выполнению лабораторной работы.
2. Реализовать требуемый метод криптоанализа.
3. Прокомментировать преподавателю процесс вычислений.

г) 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 контрольных заданий; подготовка к лабораторным занятиям; подготовка к рубежному контролю по теме/разделу (аттестации). Работу со слайдами (конспектом) лекции целесообразно проводить непосредственно после ее прослушивания. Необходимым 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. Контрольные задания и лабораторные работы, приведенные в планах занятий, выполняются студентами в обязательном порядке. Методические указания обучающимся по освоению дисциплины: целенаправленно, систематически и планомерно работать со слайдами лекций; изучать рекомендуемую литературу, добывая новые/обобщая полученные знания; тратить не менее часа в день на самостоятельную работу; консультироваться с преподавателем при возникновении вопросов; активно использовать учебно-методический комплекс на базе Moodle ТГУ; работать с тематическими форумами в сети Интернет.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Запечников С.В., Казарин О.В., Тарасов А.А. Криптографические методы защиты информации - М.: Юрайт, 2016, 308 с.

– Лось А.Б. Криптографические методы защиты информации - М.: Юрайт,2018, 473 с.

– Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации - М.: Горячая Линия – Телеком, 2014, 229 с.

– Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации -М.: Юрайт , 2017, 209 с.

– Бабаш А.В. Криптографические методы защиты информации-М.: РИОР,2019, 413 с.

б) дополнительная литература:

– Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. - М.: Гелиос АРВ, 2002, 480 с.

– Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа -М.: Гелиос АРВ, 2006, 376 с.

– Агибалов Г.П. Конечные автоматы в криптографии // Прикладная дискретная математика, 2009, Приложение № 2, С. 43–73

– Агибалов Г.П. Избранные теоремы начального курса криптографии - Томск: НТЛ, 2005, 116 с.

– Венбо Мао Современная криптография: теория и практика - М.: Вильямс, 2005, 768 с.

– Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си - М.: Триумф, 2002, 816 с.

– Кузьминов Т.В. Криптографические методы защиты информации - Новосибирск: Наука, 1998, 194 с.

в) ресурсы сети Интернет:

– Курс "Основы криптографии" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/691/547/info

– Курс "Математика криптографии и теория шифрования» [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/552/408/info

– Курс "Криптографические основы безопасности" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/28/28/info

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– ОС Windows/Linux, браузер Firefox/Яндекс

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

– бесплатная интегрированная среда разработки для Python/C++

– криптопровайдер КриптоПро CSP

– USB-токен JaCarta

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 практических и лабораторных занятий, а также занятий лекционного 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.

15. Информация о разработчиках

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