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 » _____ 2022 г.

Рабочая программа дисциплины

Криптографические протоколы

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.06.05

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 ознакомить с различными видами современных криптографических протоколов, стандартами в области криптографических протоколов, дать представление об основных атаках на криптографические протоколы.

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

Девятый семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Языки программирования, Компьютерные сети, Теория вероятностей и математическая статистика, Дискретная математика, Теория графов, Математическая логика и теория алгоритмов, Теория чисел, Общая алгебра, Профессиональный перевод специальной литературы, Методы и средства криптографической защиты информации, Основы построения защищённых компьютерных сетей.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 4 з.е., 144 часов, из которых:
-лекции: 32 ч.
-лабораторные: 32 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Введение в криптографические протоколы
Основные понятия. Классификация криптографических протоколов.
Атаки на криптографические протоколы.
Свойства, характеризующие безопасность протоколов.

Тема 2. Протоколы аутентификации сообщений
Схема имитозащиты. Оптимальные коды аутентификации.
Атаки на протоколы аутентификации сообщений.

Тема 3. Протоколы идентификации
Парольные схемы идентификации.
Протоколы идентификации на основе техники “запрос-ответ”.
Протоколы идентификации на основе техники доказательства знания.
Протоколы с нулевым разглашением.
Схема Лэмпорта (S/KEY). Протокол CHAP/MS-CHAP
Атаки на протоколы идентификации.

Тема 4. Протоколы распределения ключей
Протоколы передачи ключей
Протоколы открытого распределения ключей
Протоколы предварительного распределения ключей
Атаки на протоколы распределения ключей.

Тема 5. Групповые криптографические протоколы.

Схемы разделение секрета. Схемы цифровой подписи.
Атаки на групповые криптографические протоколы.

Тема 6. Прикладные криптографические протоколы.
Семейство протоколов IPsec. Протокол SSL/TLS. VPN-протоколы.
Атаки на прикладные криптографические протоколы

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.

Пример типового варианта задания для лабораторной работы:

- Требуется программно реализовать схему одноразовых паролей Лэмпорта (S/KEY). Описание криптографического протокола можно найти в слайдах лекций и rfc-документах: S/KEY (RFC 1760), https://datatracker.ietf.org/doc/html/rfc1760, A One-Time Password System (RFC 2289), https://datatracker.ietf.org/doc/html/rfc2289. При этом нужно найти партнера по заданию: один пишет клиента, другой - сервер, либо использовать технику парного программирования. В отчете по заданию требуется описать спецификацию реализованного протокола, важные детали и особенности реализации, формат сообщений протокола и пр. Лабораторная работа "сдается" преподавателю обоими исполнителями на базе подготовленного стенда и типовых сценариев работы, в которых демонстрируется штатный/нештатный режимы протокола.

Возможные варианты лабораторных заданий:

1. Реализовать протокол MS-CHAP.
2. Реализовать протокол Диффи - Хеллмана.
3. Реализовать протокол Нидхема-Шредера.
4. Реализовать протокол Ву-Лама.
5. Реализовать протокол Фиата-Шамира.
6. Реализовать цифровую подпись со скрытым каналом.
7. Реализовать неоспоримую цифровую подпись.
8. Реализовать цифровую подпись с назначенным проверяющим.
9. Реализовать отметку о времени создания документа.
10. Реализовать протокол электронного голосования.
11. Реализовать безопасное совместное вычисление.
12. Реализовать вычисление с шифрованными данными.
13. Реализовать депонирование ключей.
14. Реализовать раскрытие секретов по принципу «все или ничего».
15. Реализовать протокол сертифицированной электронной почты.
16. Реализовать протокол электронного аукциона.

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 девятом семестре проводится в устной/письменной форме с использованием перечня контрольных вопросов 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 вопросов к экзамену:

1. Действия противника при атаке на криптографические протоколы.
2. Свойства, характеризующих безопасность криптографических протоколов.
3. Общие предположения криптоанализа протоколов.
4. Классификация криптографических протоколов.
5. Протоколы аутентификации сообщений (ПАС), когда стороны доверяют друг другу.
6. ПАС, когда стороны не доверяют друг другу.
7. Атаки на ПАС и защита от них.
8. Виды протоколов идентификации на основе паролей
9. Схема Лэмпорта (протокол S/KEY).
10. Протокол CHAP/MS-CHAP
11. Протоколы идентификации (ПИ) на основе техники “запрос-ответ” с использованием симметричного шифрования
12. ПИ на основе техники “запрос-ответ” с использованием асимметричного шифрования
13. ПИ на основе техники “запрос-ответ” с использованием цифровой подписи
14. Протокол идентификации ISO и атака на него.
15. Протокол идентификации Нидхема-Шредера (NSPK) и атака на него.
16. Протокол идентификации Фиата-Шамира (свойства).
17. Протокол идентификации GQ (свойства).
18. Протокол идентификации Шнора (свойства).
19. Доказательство с нулевым разглашением гамильтонова цикла в графе.
20. Протокол привязки к биту (общая схема). Свойства связывания и сокрытия.
21. Протокол передачи ключей на основе техники “запрос-ответ”
22. “Бесключевой” протокол А.Шамира и атака на него.
23. Протокол широкоротой лягушки и атака на него
24. Протокол Нидхема-Шредера (NS) и атака на него
25. Протокол Kerberos.

26. Протокол передачи ключей Нидхема-Шредера (NSPK).
27. Протокол Oakley
28. Протокол Ву-Лама и атака на него.
29. Протоколы передачи ключей с использованием ЦП.
30. Протокол EKE (Encrypted Key Exchange) и атака на него.
31. Инфраструктура сертификатов открытых ключей.
32. Протокол DH (Диффи-Хеллмана) и атака “человек посередине”.
33. Протокол STS (station-to-station) и атака на него
34. Протокол MTI (Мацумото-Такашима-Имаи) и атака на него
35. Формальная схема $S(n)$ ПРК для сети с n абонентами.
36. Неравенство Блома.
37. Схема Блома.
38. KDP(n,q) - схема.
39. Пороговая схема А.Шамира.
40. Протокол DH с тремя участниками.
41. Протоколы AH и ESP. Туннельный и транспортный режимы IPSec.
42. Понятие защищенной ассоциации (SA). Организация работы IPsec.
43. Протокол SKEME.
44. Протокол ISAKMP (особенности, назначение, принципы работы).
45. Протокол IKE (особенности, назначение, принципы работы).
46. Протокол SSL/TLS (фаза рукопожатия - аутентификация и распределение ключа).
47. Жизненный цикл ключей (от регистрации пользователя до аннулирования ключа).

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 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 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 занятиях.

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

г) Методические указания по проведению лабораторных работ.

Для выполнения лабораторной работы студенту необходимо:

1. Изучить методические указания по выполнению лабораторной работы.
2. Реализовать требуемый криптографический протокол.
3. Прокомментировать преподавателю процесс вычислений протокола.

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.: Издательство Юрайт, 2016, 308 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. В 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата. - М.: Издательство Юрайт, 2017. - 209 с.

– Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата. - М.: Издательство Юрайт, 2017. - 245 с.

б) дополнительная литература:

– Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин. М.: Академия, 2009, 271 с.

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

– Мао Венбо. Современная криптография: теория и практика / Венбо Мао. М.: Издательский дом "Вильямс", 2005, 768 с.

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

– Введение в криптографию / Под общ. ред. В.В. Ященко. – 4-е изд., доп. М.: МЦНМО, 2012, 348 с.

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

в) ресурсы сети Интернет:

– Агибалов Г. П. Избранные теоремы начального курса криптографии : учебно-методический комплекс / Агибалов Г. П. - Томск : ИДО ТГУ, 2007. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000243893

– Управление ключами шифрования и безопасность сети [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/553/409/info

– Николенко С. Курс Криптографические протоколы [Электронный ресурс] // Лекториум - академический образовательный проект . URL: https://www.lektorium.tv/course/26036

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.).
– средства анализа криптографических протоколов AVISPA-SPAN, Scyther

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 лабораторных занятий и занятий лекционного типа, а также для проведения 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