

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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Проректор по ОД



Е.В. Луков

20 25 г.

Рабочая программа дисциплины

Криптографические протоколы

по направлению подготовки

10.03.01 Информационная безопасность

Направленность (профиль) подготовки:

Безопасность компьютерных систем

Форма обучения

Очная

Квалификация

Бакалавр

Год приема

2026

СОГЛАСОВАНО:

Руководитель ОП

В.Н. Треньяев

Председатель УМК

С.П. Сущенко

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-9.1. Обладает знанием и демонстрирует навыки применения методов и средств криптографической защиты информации.

ИОПК-9.2. Обладает знанием и демонстрирует навыки применения методов и средств защиты информации от утечки по техническим каналам.

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 Блоку 1 «Дисциплины (модули)».

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль Модуль «Специализация».

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

Седьмой семестр, экзамен

5. Входные требования для освоения дисциплины

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

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:

– лекции: 32 ч.

– лабораторные: 32 ч.

в том числе практическая подготовка: 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 SHAP/MS-SHAP. 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.

Практическая подготовка оценивается по результатам выполненных лабораторных работ.

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.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - <https://www.tsu.ru/sveden/education/eduor/>.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Экзамен в седьмом семестре проводится в устной/письменной форме с использованием перечня контрольных вопросов по курсу. Продолжительность экзамена 1,5 часа.

Схема вопросов экзамена соответствует компетентностной структуре дисциплины. Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

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 всех лабораторных работ.

Хорошо - студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал требуемые умения и навыки при выполнении большинства лабораторных работ.

Удовлетворительно - студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, а также показал требуемые умения и навыки при выполнении части лабораторных работ.

Неудовлетворительно - студент имеет существенные пробелы по отдельным теоретическим разделам специальной дисциплины и не показал требуемые умения и навыки при выполнении части лабораторных работ.

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» - <https://www.tsu.ru/sveden/education/eduor/>.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в LMS IDO

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

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.

д) 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 LMS IDO 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.
- Агibalов 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. Яценко. – 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:

- Агibalов Г. П. Избранные теоремы начального курса криптографии : учебно-методический комплекс / Агibalов 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.

Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта с перечнем основного оборудования	Адрес (местоположение) учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта (с указанием площади и номера помещения в соответствии с документами бюро технической инвентаризации)
Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Аудитория № 118 Учебная мебель, оборудование, программное обеспечение: 45 столов по 2 места; 90 стульев; 1 интерактивная доска; Microsoft Windows 10, Microsoft Office 2010. (Лицензия №47729022 от 26.11.2010).	634050, Томская область, г. Томск, пр-т Ленина, 36, стр.7 (78 по паспорту БТИ) Площадь 61,1 м².
Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Аудитория № 103 Учебная мебель, оборудование, программное обеспечение: 13 столов по 1 месту; 13 стульев; 1 меловая доска; 1 интерактивная доска; 1 проектор; 13 системных блоков (Intel Core i7-8700, AsusTek TUF B360-plus gaming, 16Гб DDR3); 13 мониторов; Microsoft Windows 10 Professional x64, Microsoft Office 2010 Standart, Microsoft Office 2003 Professional (only for MS Access), Microsoft Visual Studio 2022 Community, Visual Studio Code, Dr.Web Desktop Security Suite, 1С:Предприятие учебная версия, 7-Zip, Adobe Reader, Android Studio, Far Manager, FreeCommander, Google Chrome, Яндекс Браузер, GPL Ghostscript, Gsview, IntelliJ IDEA Community Edition, Java SDK, Lazarus, Mathsoft Mathcad 13, 15, Mathsoft Prime 3.1, StatSoft Statistica 13, FreeMat, Scilab, NetBeans IDE 22, Eclipse IDE 2024, PyCharm Community 2024, R Project, RapidMiner Studio,	634050, Томская область, г. Томск, пр-т Ленина, 36, стр.7 (7 по паспорту БТИ) Площадь 42,3 м².

Rstudio, Anaconda, JASP (Лицензия №47729022 от 26.11.2010, договор №7193 от 14.10.2015, договор № 2016 от 16.04.2018) нелинейный локатор «ЦИКЛОН - М1А», локатор-рефлектометр двухпроводных линий «БОР-1», сканирующий приемник AR 8200, оборудование радиодоступа WOP-2ac, Simple Promela Interpreter, ОС Astra Linux Special Edition, Secret Net Studio, ViPNet CSP, JaCarta SecurLogon, IDS/IPS Suricata, Infection Monkey, Wireshark, PfSense, Ntopng, Grype, Metasploit framework, Cisco Packet Tracer, GNS-3, EVE-NG, KatharaFramework, InfoWatch Traffic Monitor.	
Учебная аудитория для самостоятельной работы Аудитория № 103А Учебная мебель, оборудование, программное обеспечение: 13 столов по 1 месту; 13 стульев; 1 меловая доска; 1 интерактивная доска; 1 проектор; 13 системных блоков (Intel Core i7-4790/Ga H97 HD 3/2x 8Gb DDR 3); 13 мониторов; Microsoft Windows 10 Professional x64, Microsoft Office 2010 Standart, Microsoft Office 2003 Professional (only for MS Access), Microsoft Visual Studio 2022 Community, Visual Studio Code, Dr.Web Desktop Security Suite, 1С:Предприятие учебная версия, 7-Zip, Adobe Reader, Android Studio, Far Manager, FreeCommander, Google Chrome, Яндекс Браузер, GPL Ghostscript, Gsview, IntelliJ IDEA Community Edition, Java SDK, Lazarus, Mathsoft Mathcad 13, 15, Mathsoft Prime 3.1, StatSoft Statistica 13, FreeMat, Scilab, NetBeans IDE 22, Eclipse IDE 2024, PyCharm Community 2024, R Project, RapidMiner Studio, Rstudio, Anaconda, JASP (Лицензия №47729022 от 26.11.2010, договор №7193 от 14.10.2015, договор № 2016 от 16.04.2018).	634050,Томская область, г. Томск, пр-т Ленина, 36, стр.7 (72 по паспорту БТИ) Площадь 43 м².

15. Информация о разработчиках

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