

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

Введение в специальность

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. Тренкаев

Председатель УМК
С.П. Сущенко

Томск – 2025

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:
ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности..

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-2.1. Понимает современные информационно-коммуникационные технологии, используемые для решения задач профессиональной деятельности.

ИОПК-2.2. Понимает базовые принципы функционирования программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности.

ИОПК-2.3. Определяет порядок настройки и эксплуатации программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности.

ИОПК-2.4. Формулирует предложения по применению современных информационно-коммуникационных технологий, используемых для решения задач профессиональной деятельности.

2. Задачи освоения дисциплины

– дать представление об области, объектах и видах профессиональной деятельности, в том числе ознакомить с трудовыми функциями специалиста по безопасности компьютерных систем и сетей.

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

Второй семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Информатика, Архитектура вычислительных систем, Дискретная математика.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 2 з.е., 72 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

Тема 1. Основы компьютерных систем и сетей.

- Принципы организации компьютерных сетей.
- Принципы построения современных операционных систем.

Тема 2. Понятия и задачи компьютерной безопасности.

- Основные понятия компьютерной безопасности.
- Атаки на компьютерные системы и сети.

Тема 3. Стандарты и нормативные документы компьютерной безопасности.

- Руководящие документы Гостехкомиссии России.
- Отраслевые стандарты в области информационной безопасности.

Тема 4. Механизмы и средства защиты компьютерных систем и сетей.

- Основные механизмы защиты компьютерных систем и сетей.
- Средства защиты информации компьютерных систем и сетей.

Тема 5. Защита информации в компьютерных системах и сетях.

- Обслуживание средств защиты информации в компьютерных системах и сетях
- Администрирование средств защиты информации в компьютерных системах и сетях
- Оценивание уровня безопасности компьютерных систем и сетей
- Разработка средств защиты информации компьютерных систем и сетей

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине фиксируется в форме контрольной точки не менее одного раза в семестр.

Проведение текущего контроля успеваемости по дисциплине осуществляется в рамках проектного обучения. Формируются команды по 3-5 студентов для совместной групповой работы, которая заключается в реализации проекта в области направления «Информационная безопасность». В ходе работы над проектом команде студентов требуется выполнить доклад с заявкой на проект, обзорный доклад по предметной области, выполнить промежуточные отчеты о проделанной работе, провести финальную защиту проекта. В зависимости от темы проекта ключевым действием может быть администрирование средств защиты информации, разработка средств защиты информации, анализ безопасности компьютерной системы или сети.

Текущий контроль успеваемости по дисциплине осуществляется на базе оценки докладов (заявка на проект, обзорный доклад предметной области, промежуточный отчет). Доклады оцениваются по бинарной системе (зачет/незачет): зачет – команда в целом удовлетворительно разбирается в выбранной теме проекта, знает материал, отвечает на вопросы с замечаниями или с негрубыми ошибками; незачет – команда слабо разбирается в выбранной теме проекта, плохо знает материал, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя. Оценка за проделанную работу выставляется всей команде, но не отдельным ее участникам.

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

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет во втором семестре проводится в рамках проектного обучения. Формируются команды по 3-5 студентов для совместной групповой работы, которая заключается в реализации проекта в области направления «Информационная безопасность».

В ходе работы над проектом команде студентов требуется выполнить следующие задачи:

- 1) выбрать тему проекта, сделать доклад с заявкой на проект, совместно с преподавателем определиться с формой проведения проекта, целью и задачами проекта;
- 2) изучить выбранный объект защиты, а также механизмы его защиты, сделать обзорный доклад по предметной области проекта;

3) выполнить промежуточные отчеты о проделанной работе, а также провести финальную защиту проекта. Промежуточная аттестация осуществляется на основе защиты проекта. Продолжительность зачета 1 час.

Критерии оценивания промежуточной аттестации:

Зачет по дисциплине – команда овладела материалом по выбранной теме проекта, возможно с некоторыми недостатками, а также на финальной защите проекта продемонстрировала приобретенные в ходе выполнения проекта высокие/хорошие знания/умения/навыки по теме проекта. Оценка за проделанную работу выставляется всей команде, но не отдельным ее участникам.

Незачет по дисциплине – команда не прошла текущий контроль успеваемости по дисциплине, а также на финальной защите проекта продемонстрировала низкий уровень знаний/умений/навыков по теме проекта. Оценка за проделанную работу выставляется всей команде, но не отдельным ее участникам.

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

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в LMS iDO.

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

в) Методические указания по организации самостоятельной работы студентов.

При разработке проекта следует использовать следующую типовую схему описания проекта: название; описание проблемы; цель проекта; задачи проекта; содержание деятельности; срок реализации проекта; ожидаемые результаты проекта; ресурсы проекта; возможные риски проекта. При разработке проекта нужно: соизмерять желания и возможности; подумать над тем, чего вы действительно хотите добиться; интересоваться мнениями участников проекта; честно планировать своё время и делать всё в свое время. Проект реализуется в несколько этапов, в целом аналогичных этапам подготовки научного исследования и квалификационной работы: выбор темы; разработка и организация плана проекта; осуществление запланированной проектной деятельности; презентация проекта; оценка и анализ результатов.

12. Перечень учебной литературы и ресурсов сети Интернет

а) Основная литература:

– Нестеров С.А. Основы информационной безопасности: учебное пособие. – М: Лань, 2019, 324 с.

– Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: учебное пособие. – М: ИНФРА-М, 2019, 202 с.

– Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. – М: ИНФРА-М, 2020, 327 с.

– Шаньгин В.Ф. В. Комплексная защита информации в корпоративных системах: учебное пособие. – М: ИНФРА-М, 2015, 590 с.

б) Дополнительная литература:

– Галатенко В.А. Основы информационной безопасности: учебное пособие. – М: Интернет-Университет Информационных Технологий, 2010, 205 с.

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

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

- в) Ресурсы сети Интернет:
- Банк данных угроз безопасности информации ФСТЭК России-
<https://bdu.fstec.ru/>
 - National Vulnerability Database (NVD) - <https://nvd.nist.gov/>
 - Основы информационной безопасности [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: <http://www.intuit.ru/studies/courses/10/10/info>
 - Антивирусная защита компьютерных систем [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: <http://www.intuit.ru/studies/courses/2259/155/info>
 - Безопасность сетей [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: <http://www.intuit.ru/studies/courses/102/102/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.).
- Системы управления проектом (Trello, YouGile и т.п.)

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 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.

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 № 104	634050, Томская область, г. Томск, пр-т Ленина, 36, стр.7 (12 по паспорту БТИ) Площадь 85,4 м ² .

Учебная мебель, оборудование, программное обеспечение: 50 столов; 100 стульев; 2 интерактивных доски, акустическая система; Microsoft Windows 10, Microsoft Office 2010. (Лицензия №47729022 от 26.11.2010)	
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 НИ ТГУ.