

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

« 27 » \_\_\_\_\_ 20 22 г.

Рабочая программа дисциплины

**Информационная безопасность и работа с персональными данными**

по направлению подготовки

**09.04.03 Прикладная информатика**

Направленность (профиль) подготовки :

**Цифровизация государственного и муниципального управления**

Форма обучения

**Очная**

Квалификация

**Магистр**


Год приема

**2022**

Код дисциплины в учебном плане: Б1.О.02.02

СОГЛАСОВАНО:

Руководитель ОП

 Н.Л.Еремина

Председатель УМК

 С.П. Сущенко

Томск – 2022

## **1. Цель и планируемые результаты освоения дисциплины**

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-3. Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.2 Умеет работать с различными видами информации с помощью различных средств информационных и коммуникационных технологий.

## **2. Задачи освоения дисциплины**

– научиться проводить анализ проблем в области фундаментальной и прикладной математики;

– научиться формулировать задачи исследования в области фундаментальной и прикладной математики;

– решать актуальные задачи фундаментальной и прикладной математики;

– учитывать основные требования информационной безопасности при решении задач в области профессиональной деятельности.

## **3. Место дисциплины в структуре образовательной программы**

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль «Общепрофессиональные дисциплины».

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

Первый семестр, зачет с оценкой

## **5. Входные требования для освоения дисциплины**

Для успешного освоения дисциплины требуются компетенции, сформированные в ходе освоения образовательных программ предшествующего уровня образования.

## **6. Язык реализации**

Русский

## **7. Объем дисциплины**

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

-лекции: 16 ч.

-лабораторные: 16 ч.

Объем самостоятельной работы студента определен учебным планом.

## **8. Содержание дисциплины, структурированное по темам**

### **Тема 1. Общие понятия информационной безопасности**

Основные понятия информационной безопасности. Атаки на компьютерные системы и сети. Банк данных угроз безопасности информации ФСТЭК России.

### **Тема 2. Методы обеспечения информационной безопасности**

Административно-организационные методы защиты информации. Криптографические методы защиты информации. Логическое управление доступом. OpenPGP.

### **Тема 3. Средства обеспечения информационной безопасности.**

Межсетевые экраны. Виртуальные частные сети. Системы анализа защищенности. Системы обнаружения атак. Штатные средства обеспечения информационной безопасности операционных систем. Аудит информационной безопасности. Защита вычислительной среды компании. Социальная инженерия.

#### **Тема 4. Стандарты и нормативные документы информационной безопасности**

Стандарты в области информационной безопасности. Руководящие документы Гостехкомиссии России. Стандарты в области информационной безопасности.

#### **9. Текущий контроль по дисциплине**

Текущий контроль по дисциплине проводится путем контроля посещаемости, опроса по лекционному материалу, проверки лабораторных работ, и фиксируется в форме контрольной точки не менее одного раза в семестр.

#### **10. Порядок проведения и критерии оценивания промежуточной аттестации**

Теоретические и практические результаты формируются компетенциями ИОПК-3.2 и результатами обучения:

<b>№</b>	<b>Этапы формирования компетенций (разделы дисциплины)</b>	<b>Код и наименование результатов обучения</b>	<b>Вид оценочного средства (тесты, задания, кейсы, вопросы и др.)</b>
1.	Общие понятия информационной безопасности	ОР-1. ОР-2. ОР-3	лабораторные работы, вопросы, зачет, конспект самоподготовки, собеседование, опрос на занятиях.
2.	Методы обеспечения информационной безопасности	ОР-1. ОР-2. ОР-3	лабораторные работы, вопросы, зачет, конспект самоподготовки, собеседование, опрос на занятиях.
3.	Средства обеспечения информационной безопасности	ОР-1. ОР-2. ОР-3	лабораторные работы, вопросы, зачет, конспект самоподготовки, собеседование, опрос на занятиях.
4.	Стандарты и нормативные документы информационной безопасности	ОР-1. ОР-2. ОР-3	лабораторные работы, вопросы, зачет, конспект самоподготовки, собеседование, опрос на занятиях.

Промежуточная аттестация осуществляется по результатам собеседования при условии успешного выполнения ранее лабораторных работ.

Выполнение лабораторной работы 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 зачета с оценкой является выполнение 80% лабораторных работ, с оценкой за каждую не менее 80 баллов.

Критерии выставления оценок (для зачета с оценкой):

Отлично - Магистр показал творческое отношение к обучению, 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 - Магистр 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 - Магистр имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Неудовлетворительно - Магистр 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.

## **12. Перечень учебной литературы и ресурсов сети Интернет**

а) основная литература:

– Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: учебное пособие. – М.: РИОР, 2021.

– Проскурин В. Г. Защита в операционных системах: учебное пособие. – М. : Горячая линия – Телеком, 2016.

б) дополнительная литература:

– Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М. : ФОРУМ, 2020.

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

– Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.. Защита информации в информационном обществе: учебное пособие. – М. : Горячая Линия – Телеком, 2015.

в) ресурсы сети Интернет:

– Безопасность сетей [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: <http://www.intuit.ru/studies/courses/102/102/info>

– 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>

– Информационная безопасность: учебно-методический комплекс [Электронный ресурс] // Томский государственный университет. 2016. URL:  
<http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000534758>

### **13. Перечень информационных технологий**

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office OneNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook).

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.

Аудитории для проведения лабораторных занятий, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации. Аудитории должны быть оснащены оборудованием (проектор, экран, монитор, системный блок) с доступом в Интернет.

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 НИ ТГУ.