МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Введение в специальность

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (в сфере связи, информационных и коммуникационных технологий)

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная ФГАОУ ВО РУТ (МИИТ)
ID подписи: 4196
Подписал: заведующий кафедрой Желенков Борис Владимирович
Дата: 01.09.2026

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Введение в специальность» являются формирование компетенций по основным разделам теоретических и практических основ безопасности компьютерных систем, терминологии, доктрины информационной безопасности, базовых принципов работы компьютерных систем.

Основными задачами дисциплины являются:

• Ознакомление с терминами и определениями информационной безопасности;

• Ознакомление с доктриной информационной безопасности;

• Изучение способов представления информации в компьютерных системах;

• Изучение принципов обработки данных;

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- виды угроз информационной безопасности в современном обществе;

- объективные информационные потребности личности, общества и государства;

- принципы работы информационно-коммуникационных технологий, программных средств системного и прикладного назначения

Уметь:

- использовать различные методы, в том числе математические, при обработке данных

- использовать информационные технологии с учетом угроз информационной безопасности для обеспечения объективных потребностей личности, общества и государства;

- применять современные ИТ в различных предметных областях и обеспечивать эффективную адаптацию и безопасность функционирования ИТ в конкретных условиях.

Владеть:

- использовать информационные технологии с учетом угроз информационной безопасности для обеспечения объективных потребностей личности, общества и государства;
- выбирать необходимые информационно-коммуникационные технологии для решения задач профессиональной деятельности

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №1
Контактная работа при проведении учебных занятий (всего):	32	32
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	16	16

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 112 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Основные термины и определения в информационной безопасности Рассматриваемые вопросы: - Рассматриваются основные термины и определения в соответствии с -ГОСТ 50922-2006.
2	Доктрина информационной безопасности Рассматриваемые вопросы: - Безопасность компьютерных систем.
3	Информация и ее кодирование в компьютерных системах Рассматриваемые вопросы: - Информация, данные – основные понятия. - Единицы измерения количества информации. Двоичная система счисления. - Представление символьной информации в виде двоичных кодов. - Расчет длины кода символа для кодирования заданного алфавита. - Перевод из десятичной системы в двоичную. - Перевод из двоичной системы в десятичную. - Шестнадцатеричная и восьмеричная системы счисления. - Перевод из двоичной системы в шестнадцатеричную, восьмеричную и обратно. - Перевод из десятичной системы счисления в произвольную. - Перевод из произвольной системы счисления в десятичную. - Представление дробных чисел.
4	Выполнение арифметических операций Рассматриваемые вопросы: - Представление числовой информации в вычислительной технике. - Двоичная арифметика. - Шестнадцатеричная арифметика. - Прямой код. - Обратный код. - Дополнительный код. - Сложение и вычитание чисел в различных кодах. - Признаки переполнения разрядной сетки. - Форматы данных. - Операции умножения и деления для чисел в двоичном коде.
5	Основы безопасной работы в сети INTERNET.Задачи информационной безопасности Рассматриваемые вопросы: - Социальные сети. - Угрозы и уязвимости. - Классификация угроз информационной безопасности. - Нежелательный контент. - Несанкционированный доступ. - Утечки информации. - Потеря данных. - Мошенничество. - Кибервойны. - Кибертерроризм.

№ п/п	Тематика лекционных занятий / краткое содержание
6	Анализ угроз ИБ предприятия Рассматриваемые вопросы: - Что такое угроза ИБ. - Источники угроз. - Анализ информационной безопасности организации - Оценка информационной безопасности - Моделирование информационных потоков. - Моделирование угроз. - Поиск уязвимых зон. - Матрица угроз. - Матрица активов. - Матрица контроля. - Обработка матриц. - Деревья атак или деревья ошибок. - Деревья атак как структурированный и иерархический способ сбора возможных угроз
7	Информационная безопасность организации Рассматриваемые вопросы: - Требования к системе защиты ИБ. - Модель системы безопасности. - Этапы создания и обеспечения системы защиты информации. разработка базовой модели системы, которая будет функционировать в компании. - Разработка системы защиты. - Поддержка работоспособности системы, регулярный контроль и управление рисками. - Виды конфиденциальных данных. - Личные конфиденциальные данные. - Служебные конфиденциальные данные. - Судебные конфиденциальные данные. - Коммерческие конфиденциальные данные. - Профессиональные конфиденциальные данные. - Угрозы конфиденциальности информационных ресурсов. - Рассматриваются внутренние и внешние угрозы. - Происхождение попыток НСД. - Через сотрудников, с помощью программного обеспечения злоумышленники осуществляют атаки, которые направлены, с помощью аппаратных компонентов. - Аппаратная и программная ИБ. - Уровень идентификации. - Уровень шифрования.
8	Правовая защита информации Рассматриваемые вопросы: - Неправомерный доступ к компьютерной информации. - Создание, использование и распространение вредоносных компьютерных программ. - Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. - Объекты защиты в концепциях ИБ. - Носители информации, права граждан, организаций и государства на доступ к информации, система создания, использования и распространения данных

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Термины и определения информационной безопасности В результате выполнения работы студент получит понимание о целях, задачах информационной безопасности, о нормативных документах.
2	Системы счисления В результате выполнения работы студент получит навыки представлению чисел в различных системах счисления, переводу из одной системы в другую.
3	Арифметические операции В результате практического занятия студент получит навыки выполнению операций сложения и вычитания над числами в различных системах счисления.
4	Представление дробных чисел В результате практического занятия студент получит навыки по представлению дробных чисел в различных системах счисления и правилам их перевода из одной системы счисления в другую.
5	Кодирование В результате практического занятия студент получит навыки по представлению чисел со знаком в прямом, обратном и дополнительном кодах; выполнению сложения и вычитания над числами со знаком; определению переполнения разрядной сетки.
6	Умножение и деление В результате практического занятия студент получит навыки по выполнению операций умножения и деления по различным машинным алгоритмам
7	Анализ угроз ИБ предприятия В результате выполнения работы студент получит понимание о источниках угроз информационной безопасности организации. Оценка информационной безопасности В результате выполнения работы студент получит понимание о моделировании информационных потоков, моделировании угроз, поиске уязвимых зон.
8	Виды конфиденциальных данных В результате выполнения работы студент получит понимание о личных конфиденциальных данных, служебных конфиденциальных данных, судебных конфиденциальных данных, коммерческих конфиденциальных данных, профессиональных конфиденциальных данных.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к практическим занятиям
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа

1	Введение в информационную безопасность и защиту информации : учебное пособие / В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. — Новосибирск : НГТУ, 2017. — 132 с. — ISBN 978-5-7782-3233-4. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/118219 (дата обращения: 30.04.2025)
2	Введение в информационную безопасность и защиту информации : учебное пособие / В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. — Новосибирск : НГТУ, 2017. — 132 с. — ISBN 978-5-7782-3233-4. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/118219 (дата обращения: 30.04.2025)
3	Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 324 с. — ISBN 978-5-507-49077-6. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/370967 (дата обращения: 30.04.2025)
4	Введение в информационную безопасность и защиту информации : учебное пособие / В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. — Новосибирск : НГТУ, 2017. — 132 с. — ISBN 978-5-7782-3233-4. — Текст : электронный // Лань : электронно-библиотечная система	https://e.lanbook.com/book/118219 (дата обращения: 11.03.2026)

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Научно-техническая библиотека РУТ(МИИТ) http://library.miit.ru/

Форум специалистов по информационным технологиям http://citforum.ru/

Интернет-университет информационных технологий http://www.intuit.ru/

Тематический форум по информационным технологиям http://habrahabr.ru/

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

- ОС Windows
- Microsoft Office
- Интернет-браузер (Yandex и др.)

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

-Учебная аудитория для проведения учебных занятий (занятий лекционного типа, практических занятий):

- компьютер преподавателя, рабочие станции студентов, мультимедийное оборудование, доска.

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Зачет в 1 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

заведующий кафедрой, доцент, к.н.
кафедры «Вычислительные системы
и квантовые коммуникации» Б.В. Желенков

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова