МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы бакалавриата
по направлению подготовки
09.03.01 Информатика и вычислительная техника,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы информационной безопасности

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Вычислительные системы и сети

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Задача дисциплины «Основы информационной безопасности» — сформировать у обучающихся теоретические знания и практические навыки в области защиты информации, чтобы они могли применять их для обеспечения конфиденциальности, целостности и доступности данных в своей профессиональной деятельности.

В дисциплине предусмотрено изучение пяти учебных тем, объединенных единым замыслом. Излагаются взгляды на информацию, как объект защиты с выделением характерных свойств защищаемой информации. На основе единого подхода рассматриваются девять исторически сложившихся направлений информационной защиты. Излагаются разработанные или модифицированные автором качественные модели информационной защиты. Завершается изучение дисциплины двумя темами, посвященными двум наиболее существенным угрозам информационной безопасности – информационным преступлениям и информационным войнам. В рамках, указанных тем приводится классификация информационных и компьютерных преступлений, объясняются их причины, дается уголовно-правовая характеристика некоторых преступных деяний, рассматриваются основные стратегии информационных войн и виды информационного оружия.

Целью дисциплины «Основы информационной безопасности» является формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих (действующих) направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты. Приобретенные знания позволят студентам правильно ориентироваться в категориях защищаемых информационных ценностей и приобрести минимально необходимый кругозор в проблемах информационной безопасности. На основе данной дисциплины предполагается более подробно изучать различные направления защиты компьютерной безопасности.

Задачи дисциплины «Основы информационной безопасности» заключаются в формировании у студентов базовых теоретических знаний о свойствах информации, подлежащих защите: конфиденциальности, целостности и доступности информации, а также о информационных активах, угрозах информационной безопасности, и методах защиты данных, а также в выработке практических навыков обеспечения конфиденциальности информации с помощью базовых криптографических алгоритмов.

К основным задачам дисциплины «Основы информационной безопасности» относятся:

• Изучение теоретических основ: изучение принципов, понятий, источников угроз и видов атак на информационные системы.

• Анализ рисков и уязвимостей: общие принципы оценки текущего состояния защищенности информации, выявление каналов утечки данных и уязвимостей.

• Управление информационной безопасностью: Ознакомление с методами контроля доступа к информационной системе, в том числе матрицами доступа, ролевой и мандатной моделями.

• Криптография: Изучение базовых криптографических алгоритмов. Обучение работе с симметричными криптографическими алгоритмами.

• Правовое регулирование: Изучение нормативно-правовой базы в области защиты информации.

Изучение дисциплины позволяет сформировать понимание структуры защиты данных и развить навыки, необходимые для обеспечения безопасности информационных систем.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

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

Знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;

- место информационной безопасности в системе национальной безопасности страны;

- виды, источники и носители защищаемой информации;

- источники угроз безопасности информации и меры по их предотвращению;

- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;

- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;

- современные средства и способы обеспечения информационной безопасности;

- основные методики анализа угроз и рисков информационной безопасности.

Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;

- классифицировать основные угрозы безопасности информации.

Владеть:

- профессиональной терминологией;

- навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем и объектов информатизации;

- методами защиты информации.

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 №3
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

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 80 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	Введение в информационную безопасность Содержание учебного материала: - Понятие информации и информационной безопасности. - Информация, сообщения, информационные процессы как объекты информационной безопасности. - Обзор защищаемых объектов и систем.
2	Основные понятия теории информационной безопасности Содержание учебного материала: - История становления теории информационной безопасности. - Предметная область теории информационной безопасности. - Систематизация понятий в области защиты информации.
3	Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации» Содержание учебного материала: - Основные принципы построения систем защиты. - Концепция комплексной защиты информации. - Задачи защиты информации. - Средства реализации комплексной защиты информации.
4	Информация как объект защиты Содержание учебного материала: - Понятие об информации как объекте защиты. - Уровни представления информации. Основные свойства защищаемой информации. - Виды и формы представления информации.
5	Информационные ресурсы и их защита Содержание учебного материала: - Информационные ресурсы. - Структура и шкала ценности информации. - Классификация информационных ресурсов. - Правовой режим информационных ресурсов.
6	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности Содержание учебного материала: - Информационная безопасность и ее место в системе национальной безопасности Российской Федерации.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.
7	Угрозы информационной безопасности Содержание учебного материала: - Анализ уязвимостей системы. - Классификация угроз информационной безопасности. - Основные направления и методы реализации угроз. - Неформальная модель нарушителя. - Оценка уязвимости системы.
8	Построение систем защиты от угрозы нарушения конфиденциальности Содержание учебного материала: - Определение и основные способы несанкционированного доступа. - Методы защиты от НСД. - Организационные методы защиты от НСД. - Инженерно-технические методы защиты от НСД. - Построение систем защиты от угрозы утечки по техническим каналам.
9	Методы контроля доступа к информации Содержание учебного материала: - Идентификация и аутентификация. - Основные направления и цели использования криптографических методов. - Защита от угрозы нарушения конфиденциальности на уровне содержания информации.
10	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа Содержание учебного материала: - Защита целостности информации при хранении. - Защита целостности информации при обработке. Защита целостности информации при транспортировке. - Защита от угрозы нарушения целостности информации на уровне содержания. - Построение систем защиты от угрозы отказа доступа к информации. - Защита семантического анализа и актуальности информации.
11	Политика и модели безопасности Содержание учебного материала: - Политика безопасности. - Субъектно-объектные модели разграничения доступа. - Аксиомы политики безопасности. - Политика и модели дискреционного доступа. - Парольные системы разграничения доступа. - Политика и модели мандатного доступа. Т - еоретико-информационные модели. - Политика и модели тематического разграничения доступа. - Ролевая модель безопасности.
12	Обзор международных стандартов информационной безопасности Содержание учебного материала: - Роль стандартов информационной безопасности. - Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. - Европейские критерии безопасности информационных технологий (ITSEC). - Федеральные критерии безопасности информационных технологий США. - Единые критерии безопасности информационных технологий. - Группа международных стандартов 270000.

№ п/п	Тематика лекционных занятий / краткое содержание
13	Информационные войны и информационное противоборство Содержание учебного материала: - Определение и основные виды информационных войн. - Информационно-техническая война. - Информационно-психологическая война.
14	Нормативно правовое регулирование защиты информации Содержание учебного материала: - Организационная структура системы защиты информации. - Законодательные акты в области защиты информации. - Российские и международные стандарты, определяющие требования к защите информации. - Система сертификации РФ в области защиты информации. - Основные правила и документы системы сертификации РФ в области защиты информации.
15	Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации Содержание учебного материала: - Основные механизмы защиты информации. - Система защиты информации. - Меры защиты информации, реализуемые в автоматизированных (информационных) системах. - Программные и программно-аппаратные средства защиты информации. - Инженерная защита и техническая охрана объектов информатизации. - Организационно-распорядительная защита информации. - Работа с кадрами и внутри объектовый режим. - Принципы построения организационно-распорядительной системы.
16	Управление информационной безопасностью предприятия Содержание учебного материала: - Объекты защиты информации на предприятии. - Классификация видов, способов, методов и средств защиты информации на предприятии. - Назначение и структура систем защиты информации. - Комплексная система защиты информации на предприятии.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Определение объектов защиты на типовом объекте информатизации. Основные признаки присутствия на компьютере вредоносных программ В ходе выполнения лабораторной работы студент знакомится с видами информационных активов согласно ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 58545-2019 , и учится выбирать из предложенного набора активов информационные. Далее студент распределяет активы по классам в соответствии с ГОСТ. В результате выполнения лабораторной работы студент получит навыки классификации информационных активов по видам угроз и классам защищенности, а также навыки обнаружения вредоносного программного кода на персональном компьютере.
2	Обнаружение сетевой активности В ходе выполнения лабораторной работы студент научиться перехватывать, фильтровать и анализировать сетевые пакеты для обнаружения подозрительной активности или изучения работы протоколов.

№ п/п	Наименование лабораторных работ / краткое содержание
	В результате выполнения лабораторной работы студент получит навыки обнаружения сетевой активности в защищаемой системе.
3	Справочно-правовые системы В ходе выполнения лабораторной работы студент выполняет поиск по реквизитам (номер, дата, принявший орган), поиск по тематике; поиск по ключевым словам; выполняет изучение редакции документа, поиск комментариев, использование ссылок. В результате выполнения лабораторной работы студент получит навыки работы в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.
4	Защита информации для автоматизированных рабочих мест. Управление правами пользователей в Windows Студент знакомится с основными ролями в операционной системе: пользователя и администратора, изучает различия в их возможностях. Выполняет такие базовые операции, как создание учетных записей пользователей с разным уровнем прав; настройка локальной политики безопасности (сложность паролей, блокировка учетной записи); ограничение доступа к файлам и папкам (NTFS-права); настройка персонального брандмауэра. В результате выполнения лабораторной работы студент получает навыки базовой настройки компонентов АРМ для обеспечения ИБ.
5	Криптографический алгоритм «Одноалфавитная подстановка» В ходе выполнения лабораторной работы студент изучает криптографический алгоритм «Одноалфавитная подстановка», составляет таблицу соответствия символов открытого текста и зашифрованного текста. Затем он разрабатывает блок-схему алгоритма и создает код программы на языках высокого уровня (Python, C++ и т.д.) для реализации данного криптоалгоритма. Далее выполняется шифрование и расшифрование контрольного текста.
6	. Криптографический алгоритм «Многоалфавитная одноконтурная обыкновенная подстановка» В ходе выполнения лабораторной работы студент изучает криптографический алгоритм «Многоалфавитная одноконтурная обыкновенная подстановка», составляет таблицу шифрования, в которой каждому символу открытого текста соответствует несколько (не менее трех) символов зашифрованного текста. Затем он разрабатывает блок-схему алгоритма и создает код программы на языках высокого уровня (Python, C++ и т.д.) для реализации данного криптоалгоритма. Далее выполняется шифрование и расшифрование контрольного текста.
7	Криптографический алгоритм «Многоалфавитная одноконтурная монофоническая подстановка» В ходе выполнения лабораторной работы студент изучает криптографический алгоритм «Многоалфавитная одноконтурная монофоническая подстановка», имеющего повышенную защиту от дешифрования статистическими методами, составляет таблицу монофонической замены, в которой каждому символу открытого текста соответствует или несколько символов зашифрованного текста в зависимости от частоты употребления этого символа в естественном языке. Затем студент разрабатывает блок-схему алгоритма и создает код программы на языках высокого уровня (Python, C++ и т.д.) для реализации данного криптоалгоритма. Далее выполняется шифрование и расшифрование контрольного текста.
8	Криптографический алгоритм «Многоалфавитная многоконтурная подстановка» В ходе выполнения лабораторной работы студент изучает криптографический алгоритм «Многоалфавитная многоконтурная подстановка» и составляет несколько контуров - таблиц замены, которые должны меняться по определенному правилу. Затем студент разрабатывает блок-схему алгоритма и создает код программы на языках высокого уровня (Python, C++ и т.д.) для реализации данного криптоалгоритма. Далее выполняется шифрование и расшифрование контрольного текста.
9	Криптографический алгоритм «Простая перестановка»

№ п/п	Наименование лабораторных работ / краткое содержание
	В ходе выполнения лабораторной работы студент изучает криптографический алгоритм «Простая перестановка» и выбирает размеры блока перестановки. Затем студент разрабатывает блок-схему алгоритма, выполняющего перемешивание символов исходного текста для получения криптограммы и обратную перестановку для восстановления из криптограммы открытого текста. Затем студент создает код программы на языках высокого уровня (Python, C++ и т.д.) для реализации данного криптоалгоритма. Далее выполняется шифрование и расшифрование контрольного текста.
10	Криптографический алгоритм «Перестановка, усложненная по таблице» В ходе выполнения лабораторной работы студент изучает криптографический алгоритм «Перестановка, усложненная по таблице», выбирает размеры блока перестановки и расположение скрытых элементов – неиспользуемых ячеек таблицы перестановки. Затем студент разрабатывает блок-схему алгоритма, выполняющего, с учетом наличия неиспользуемых ячеек таблицы, перемешивание символов исходного текста для получения криптограммы и обратную перестановку для восстановления из криптограммы открытого текста. Затем студент создает код программы на языках высокого уровня (Python, C++ и т.д.) для реализации данного криптоалгоритма. Далее выполняется шифрование и расшифрование контрольного текста.
11	Криптографический алгоритм «Перестановка, усложненная по маршрутам» В ходе выполнения лабораторной работы студент изучает криптографический алгоритм «Перестановка, усложненная по маршрутам», выбирает размеры блока перестановки, а также строит маршруты перестановки на основе многомерных графов. Затем студент разрабатывает блок-схему алгоритма, выполняющего, с учетом ограничения маршрутов, перемешивание символов исходного текста для получения криптограммы и обратную перестановку для восстановления из криптограммы открытого текста. Затем студент создает код программы на языках высокого уровня (Python, C++ и т.д.) для реализации данного криптоалгоритма. Далее выполняется шифрование и расшифрование контрольного текста.
12	Криптографический алгоритм «Гаммирование» В ходе выполнения лабораторной работы студент изучает криптографический алгоритм «Гаммирование», выбирает методы формирования гаммы – псевдослучайной последовательности бит. Затем студент разрабатывает блок-схему алгоритма, выполняющего формирование гаммы и ее наложение на открытый текст для получения крипторамы, а также аналогичный процесс для получения из криптограммы открытого текста. Далее, студент создает код программы на языках высокого уровня (Python, C++ и т.д.) для реализации данного криптоалгоритма. Далее выполняется шифрование и расшифрование контрольного текста.
13	Криптографический алгоритм основанный на аналитических преобразованиях В ходе выполнения лабораторной работы студент изучает криптографический алгоритм, основанный на операциях с матрицами. Студент выбирает размер матрицы и определяет методы ее ввода в программу. Затем студент разрабатывает блок-схему алгоритма, создающего криптограмму умножением вектора открытого текста на матрицу, а также аналогичный процесс умножения вектора криптограммы на транспонированную матрицу для получения из криптограммы открытого текста. Далее, студент создает код программы на языках высокого уровня (Python, C++ и т.д.) для реализации данного криптоалгоритма. Далее выполняется шифрование и расшифрование контрольного текста.
14	Криптографический алгоритм символьного кодирования В ходе выполнения лабораторной работы студент изучает криптографический алгоритм, основанный на кодировании символов. Студент формирует матрицы таблицу кодировки, используя по выбору преподавателя равномерный код, или неравномерный код с соблюдением условия Фано. Затем студент разрабатывает блок-схему алгоритма, создающего криптограмму путем кодирования открытого текста по таблице кодировки, а также обратный процесс преобразования криптограммы в открытый текст. Далее, студент создает код программы на языках высокого уровня (Python, C++ и

№ п/п	Наименование лабораторных работ / краткое содержание
	т.д.) для реализации данного криптоалгоритма. Далее выполняется шифрование и расшифрование контрольного текста.
15	Комбинированный криптографический алгоритм «Подстановка + перестановка» В ходе выполнения лабораторной работы студент изучает комбинированный криптографический алгоритм, основанный на сочетании методов шифрования заменой и подстановкой. Студент составляет таблицу перестановки на несколько алфавитов, а также таблицу перестановки. Затем студент разрабатывает блок-схему алгоритма, создающего криптограмму путем замены открытого текста по таблице подстановки с последующим перемешиванием символов по таблице перестановки. Далее, студент создает код программы на языках высокого уровня (Python, C++ и т.д.) для реализации данного комбинированного криптоалгоритма. Затем выполняется шифрование и расшифрование контрольного текста.
16	Комбинированный криптографический алгоритм «Перестановка + гаммирование» В ходе выполнения лабораторной работы студент изучает еще один комбинированный криптографический алгоритм, основанный на популярном в настоящее время сочетании методов шифрования перестановкой и гаммированием, что применяется в криптоалгоритмах DES, ГОСТ 28147-89 и многих других. Студент составляет таблицу перестановки на несколько алфавитов, а также продумывает механизм формирования и использования гаммы – псевдослучайной последовательности бит. Затем студент разрабатывает блок-схему алгоритма, создающего криптограмму путем перемешиванием символов открытого текста по таблице перестановки с последующим наложением гаммы. Далее, студент создает код программы на языках высокого уровня (Python, C++ и т.д.) для реализации данного комбинированного криптоалгоритма. Затем выполняется шифрование и расшифрование контрольного текста.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к лабораторным работам
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1. Формы психологической защиты человека от информационной перегрузки.

2. Социально вредная информация в СМИ.

3. Вредная и опасная информация в Интернет

4. Формы обмана и мошенничества в Интернет.

5. Формы незаконного использования информации. Законодательные меры против незаконного использования информации.

6. Модель информационной защиты каналов связи.

7. Стратегия обмана и ее использование в сфере информационной защиты.

8. Вопросы информационной безопасности в политике и дипломатии.

9. Организационно-распорядительные меры информационной защиты.

10. Традиционные направления информационной защиты и пути их интеграции.

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

№ п/п	Библиографическое описание	Место доступа
1	Кодирование и защита информации в документообороте: метод. указ. к практ. и лаб. раб. для студ. спец. Прикладная информатика (в экономике) по дисц. Информационная безопасность / В.И. Морозова, К.Э. Врублевский; МИИТ. Каф. Экономическая информатика. - М.: МИИТ, 2010. - 56 с.	URL: 03_19830.pdf (miit.ru). (дата обращения 08.02.2026) Текст : непосредственный.004.056.57 М 80
2	Шифрование с открытым ключом: метод. указ. к лаб. раб. по дисц. Информационная безопасность и защита информации для студ. спец. Автоматизированные системы обработки информации и управления, Информационные системы и технологии / Э.И. Костюковская, А.М. Удалов; МИИТ. Каф. Автоматизированные системы управления. - М.: МИИТ, 2008. - 28 с.	URL: 04-46051.pdf (miit.ru). (дата обращения 08.02.2026) Текст : непосредственный.004 К 72
3	Криптографическая защита компьютерной информации: метод. указ. к лаб. раб. по дисц. Теоретические основы компьютерной безопасности для студ., обуч. по напр. Информационная безопасность / Я. М. Голдовский, Б. В. Желенков, И. Е. Сафонова; МИИТ. Каф. Вычислительные системы и сети. - М.: МГУПС(МИИТ), 2013. - 36 с.	URL: 03-42764.pdf (miit.ru). (дата обращения 08.02.2026) Текст : непосредственный.004 Г60

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

- База данных документов ФСТЭК: https://fstec.ru/dokumenty-filter
- База данных стандартов: https://www.gost.ru/portal/gost/home/standarts

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

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

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

Ддисциплине (модулю).

Учебная аудитория для проведения учебных занятий:

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

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Зачет в 3 семестре.

Курсовая работа в 3 семестре.

10. Оценочные материалы.

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

Авторы:

доцент, к.н. кафедры
«Вычислительные системы, сети и
информационная безопасность» Я.М. Голдовский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова