

**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  
02.03.02 Фундаментальная информатика и  
информационные технологии,  
утвержденной первым проректором РУТ (МИИТ)  
Тимониным В.С.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Основы информационной безопасности**

Направление подготовки: 02.03.02 Фундаментальная информатика и  
информационные технологии

Направленность (профиль): Квантовые вычислительные системы и сети

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 РУТ (МИИТ)  
ID подписи: 4196  
Подписал: заведующий кафедрой Желенков Борис  
Владимирович  
Дата: 24.10.2024

## 1. Общие сведения о дисциплине (модуле).

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.

Задачами дисциплины (модуля) "Основы информационной безопасности" являются:

- Разработка методов и средств технической защиты информации;
- Разработка технологических решений для обеспечения информационной безопасности в различных сферах.
- Организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;
- Разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности;
- Организация работы малых групп и коллективов исполнителей, сформированных для решения конкретных профессиональных задач.
- Сбор и анализ исходных данных для проектирования систем обработки и анализа информации с учетом необходимости ее защиты в соответствии с требованиями безопасности информации;
- Участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации;
- Участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации.
- Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

- Администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных системю.

## 2. Планируемые результаты обучения по дисциплине (модулю).

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

**ОПК-5** - Способен устанавливать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности;

**ПК-10** - Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

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):	80	80
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	48	48

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 64 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	<b>Введение в информационную безопасность</b> Содержание учебного материала: - Понятие информации и информационной безопасности. - Информация, сообщения, информационные процессы как объекты информационной безопасности. - Обзор защищаемых объектов и систем.
2	<b>Основные понятия теории информационной безопасности</b> Содержание учебного материала: - История становления теории информационной безопасности. - Предметная область теории информационной безопасности. - Систематизация понятий в области защиты информации.
3	<b>Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации»</b> Содержание учебного материала: - Основные принципы построения систем защиты. - Концепция комплексной защиты информации. - Задачи защиты информации. - Средства реализации комплексной защиты информации.
4	<b>Информация как объект защиты</b> Содержание учебного материала: - Понятие об информации как объекте защиты. - Уровни представления информации. Основные свойства защищаемой информации. - Виды и формы представления информации.
5	<b>Информационные ресурсы и их защита</b> Содержание учебного материала: - Информационные ресурсы. - Структура и шкала ценности информации. - Классификация информационных ресурсов. - Правовой режим информационных ресурсов.
6	<b>Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности</b> Содержание учебного материала: - Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. - Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.
7	<b>Угрозы информационной безопасности</b> Содержание учебного материала: - Анализ уязвимостей системы. - Классификация угроз информационной безопасности. - Основные направления и методы реализации угроз. - Неформальная модель нарушителя. - Оценка уязвимости системы.
8	<b>Построение систем защиты от угрозы нарушения конфиденциальности</b> Содержание учебного материала: - Определение и основные способы несанкционированного доступа.

№ п/п	Тематика лекционных занятий / краткое содержание
	<ul style="list-style-type: none"> <li>- Методы защиты от НСД.</li> <li>- Организационные методы защиты от НСД.</li> <li>- Инженерно-технические методы защиты от НСД.</li> <li>- Построение систем защиты от угрозы утечки по техническим каналам.</li> </ul>
9	<b>Методы контроля доступа к информации</b> Содержание учебного материала: <ul style="list-style-type: none"> <li>- Идентификация и аутентификация.</li> <li>- Основные направления и цели использования криптографических методов.</li> <li>- Защита от угрозы нарушения конфиденциальности на уровне содержания информации.</li> </ul>
10	<b>Построение систем защиты от угрозы нарушения целостности информации и отказа доступа</b> Содержание учебного материала: <ul style="list-style-type: none"> <li>- Защита целостности информации при хранении.</li> <li>- Защита целостности информации при обработке. Защита целостности информации при транспортировке.</li> <li>- Защита от угрозы нарушения целостности информации на уровне содержания.</li> <li>- Построение систем защиты от угрозы отказа доступа к информации.</li> <li>- Защита семантического анализа и актуальности информации.</li> </ul>
11	<b>Политика и модели безопасности</b> Содержание учебного материала: <ul style="list-style-type: none"> <li>- Политика безопасности.</li> <li>- Субъектно-объектные модели разграничения доступа.</li> <li>- Аксиомы политики безопасности.</li> <li>- Политика и модели дискреционного доступа.</li> <li>- Парольные системы разграничения доступа.</li> <li>- Политика и модели мандатного доступа.</li> <li>- Теоретико-информационные модели.</li> <li>- Политика и модели тематического разграничения доступа.</li> <li>- Ролевая модель безопасности.</li> </ul>
12	<b>Обзор международных стандартов информационной безопасности</b> Содержание учебного материала: <ul style="list-style-type: none"> <li>- Роль стандартов информационной безопасности.</li> <li>- Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC.</li> <li>- Европейские критерии безопасности информационных технологий (ITSEC).</li> <li>- Федеральные критерии безопасности информационных технологий США.</li> <li>- Единые критерии безопасности информационных технологий.</li> <li>- Группа международных стандартов 270000.</li> </ul>
13	<b>Информационные войны и информационное противоборство</b> Содержание учебного материала: <ul style="list-style-type: none"> <li>- Определение и основные виды информационных войн.</li> <li>- Информационно-техническая война.</li> <li>- Информационно-психологическая война.</li> </ul>
14	<b>Нормативно правовое регулирование защиты информации</b> Содержание учебного материала: <ul style="list-style-type: none"> <li>- Организационная структура системы защиты информации.</li> <li>- Законодательные акты в области защиты информации.</li> <li>- Российские и международные стандарты, определяющие требования к защите информации.</li> <li>- Система сертификации РФ в области защиты информации.</li> <li>- Основные правила и документы системы сертификации РФ в области защиты информации.</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
15	<p>Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации</p> <p>Содержание учебного материала:</p> <ul style="list-style-type: none"> <li>- Основные механизмы защиты информации.</li> <li>- Система защиты информации.</li> <li>- Меры защиты информации, реализуемые в автоматизированных (информационных) системах.</li> <li>- Программные и программно-аппаратные средства защиты информации.</li> <li>- Инженерная защита и техническая охрана объектов информатизации.</li> <li>- Организационно-распорядительная защита информации.</li> <li>- Работа с кадрами и внутри объектовый режим.</li> <li>- Принципы построения организационно-распорядительной системы.</li> </ul>
16	<p>Управление информационной безопасностью предприятия</p> <p>Содержание учебного материала:</p> <ul style="list-style-type: none"> <li>- Объекты защиты информации на предприятии.</li> <li>- Классификация видов, способов, методов и средств защиты информации на предприятии.</li> <li>- Назначение и структура систем защиты информации.</li> <li>- Комплексная система защиты информации на предприятии.</li> </ul>

## 4.2. Занятия семинарского типа.

### Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	<p>Определение объектов защиты на типовом объекте информатизации. Основные признаки присутствия на компьютере вредоносных программ</p> <p>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.</p>
2	<p>Обнаружение сетевой активности</p> <p>В результате выполнения лабораторной работы студент получит навыки обнаружения сетевой активности в защищаемой системе.</p>
3	<p>Справочно-правовые системы</p> <p>В результате выполнения лабораторной работы студент получит навыки работы в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.</p>
4	<p>Защита информации для автоматизированных рабочих мест. Управление правами пользователей в Windows</p> <p>В результате выполнения лабораторной работы студент получает навыки базовой настройки компонентов АРМ для обеспечения ИБ.</p>
5	<p>Криптографический алгоритм «Одноалфавитная подстановка»</p> <p>Криптографический алгоритм «Одноалфавитная подстановка».</p>
6	<p>Криптографический алгоритм «Многоалфавитная одноконтурная обыкновенная подстановка»</p> <p>В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифрования методом «Многоалфавитная одноконтурная обыкновенная подстановка».</p>

№ п/п	Наименование лабораторных работ / краткое содержание
7	Криптографический алгоритм «Многоалфавитная одноконтурная монофоническая подстановка» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифрования методом «Многоалфавитная одноконтурная монофоническая обыкновенная подстановка»
8	Криптографический алгоритм «Многоалфавитная многоконтурная подстановка» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифрования методом «Многоалфавитная многоконтурная монофоническая обыкновенная подстановка».
9	Криптографический алгоритм «Простая перестановка» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифрования методом «Простая перестановка».
10	Криптографический алгоритм «Перестановка, усложненная по таблице» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифрования методом «Перестановка, усложненная по таблице».
11	Криптографический алгоритм «Перестановка, усложненная по маршрутам» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифрования методом «Перестановка, усложненная по маршрутам».
12	Криптографический алгоритм «Гаммирование» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифрования методом «Гаммирование».
13	Криптографический алгоритм основанный на аналитических преобразованиях В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифрования методом аналитических преобразований на основе обработки прямой и транспонированной матриц.
14	Криптографический алгоритм символьного кодирования В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифрования методом символьного кодирования по кодовому алфавиту.
15	Комбинированный криптографический алгоритм «Подстановка + перестановка» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифрования методом «Подстановка + перестановка».
16	Комбинированный криптографический алгоритм «Перестановка + гаммирование» В результате выполнения лабораторной работы студент получает навыки программной реализации шифрования и расшифрования методом «Перестановка + гаммирование».

#### 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.	<a href="https://library.miit.ru/bookscatalog/metod/03_19830.pdf">https://library.miit.ru/bookscatalog/metod/03_19830.pdf</a>
2	Шифрование с открытым ключом: метод. указ. к лаб. раб. по дисц. Информационная безопасность и защита информации для студ. спец. Автоматизированные системы	<a href="https://library.miit.ru/bookscatalog/metod/04-46051.pdf">https://library.miit.ru/bookscatalog/metod/04-46051.pdf</a>

	<p>обработки информации и управления, Информационные системы и технологии / Э.И. Костюковская, А.М. Удалов; МИИТ. Каф.</p> <p>Автоматизированные системы управления. - М.: МИИТ, 2008. - 28 с.</p>	
3	<p>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.</p>	<a href="https://library.miit.ru/bookscatalog/metod/03-42764.pdf">https://library.miit.ru/bookscatalog/metod/03-42764.pdf</a>
4	<p>Информационная безопасность персональных компьютеров: учеб. пособие для студ. спец. САПР и строительных спец. по курсу Методы и средства защиты компьютерной информации. Ч.2 / В.Ю. Смирнов, О.В. Смирнова; МИИТ. Каф. САПР транспортных конструкций и сооружений. М.: МИИТ, 2010. - 88 с.</p>	<a href="https://library.miit.ru/miitpublishing/10-2256.pdf">https://library.miit.ru/miitpublishing/10-2256.pdf</a>
5	<p>Разработка мер защиты информационных ресурсов в корпоративной сети с выходом в интернет: учебно-метод. пособие по курс. работе для специалистов напр. Компьютерная безопасность / В. М. Алексеев; МИИТ. Каф. Управление и защита информации. - М.: РУТ(МИИТ), 2017. - 9 с.</p>	<a href="https://library.miit.ru/bookscatalog/metod/DC-435.pdf">https://library.miit.ru/bookscatalog/metod/DC-435.pdf</a>

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

- Электронно-библиотечная система Научно-технической библиотеки 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).

Интернет-браузер (Yandex и др.)

Microsoft Windows

Microsoft Office

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

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, лабораторных работ, курсового проектирования (выполнения курсовых работ):

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

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Курсовая работа в 3 семестре.

Экзамен 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