

**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)**

**Защита информации**

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): 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: 08.10.2024

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

Целью освоения учебной дисциплины «Защита информации» является формирование профессиональных компетенций по основным разделам дисциплины.

Основными задачами дисциплины являются:

- освоение студентами базовых методов и средств защиты информации (организационных, технических, программных);
- ознакомление с законодательством и стандартами в этой области;
- студенты должны изучить теоретические основы компьютерной безопасности и уметь применять теорию на практике.

## 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;

**ОПК-7** - Способен участвовать в настройке и наладке программно-аппаратных комплексов;

**ПК-5** - Способность администрировать процесс управления безопасностью сетевых устройств, программного обеспечения, средств обеспечения безопасности удаленного доступа.

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

### **Знать:**

- виды защиты информации, основные понятия и определения;
- стандарты и нормативные документы оценки информационной безопасности (ИБ) программного обеспечения и средств вычислительной техники;
- типы атак и методы противодействия атакам;
- службы и механизмы безопасности;
- методы шифрования;
- алгоритмы симметричных и асимметричных криптосистем;
- информационный процесс управления криптографическими ключами;
- виды и алгоритмы электронной подписи (ЭП);

- концепцию построения систем защиты информации;
- основы квантовой криптографии.

**Уметь:**

- применять на практике методы противодействия атакам, методы и средства защиты информации от несанкционированного доступа (НСД);
- определять технические каналы утечки информации и способы их закрытия;
- использовать стандарты и нормативные документы при анализе ИБ и/или при построении системы защиты;
- использовать на практике службы и механизмы безопасности;
- структурировать угрозы ИБ, определять модель угроз и модель нарушителя;
- администрировать процесс управления безопасностью;
- разрабатывать архитектуру и определять состав системы обеспечения информационной безопасности.

**Владеть:**

- навыками оценки вероятности возникновения угроз ИБ и проведения анализа рисков реализации угроз;
- навыками формирования политики безопасности;
- основами проектирования систем защиты информации;
- навыками применения инженерно-технических, программно-аппаратных и криптографических средств защиты информации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 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 №5
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	48	48
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 100 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>МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ</b> Рассматриваемые вопросы: - виды защиты информации; - методы защиты компьютерной информации; - законодательные меры защиты информации (нормативные правовые акты РФ в области защиты информации).
2	<b>СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ</b> Рассматриваемые вопросы: - средства защиты компьютерной информации; - криптографические средства защиты информации; - стандарты (оценочные стандарты и технические спецификации).
3	<b>УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ</b> Рассматриваемые вопросы: - классификация и характеристики угроз; - способы несанкционированного доступа; - основные способы и каналы утечки информации; - преодоление программных средств защиты.
4	<b>СЛУЖБЫ И МЕХАНИЗМЫ ИБ</b> Рассматриваемые вопросы: - виды служб и механизмов безопасности; - взаимосвязь между службами и реализующими их механизмами; - комплекс требований к системе компьютерной безопасности.
5	<b>МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ</b>

№ п/п	Тематика лекционных занятий / краткое содержание
	<p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- серия международных стандартов 27000;</li> <li>- рекомендации X.800;</li> <li>- общие критерии оценки безопасности информационных технологий, ISO/IEC 27000:2018 и другие.</li> </ul>
6	<p><b>НАЦИОНАЛЬНЫЕ СТАНДАРТЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- обзор стандартов;</li> <li>- TCSEC;</li> <li>- STCSPES;</li> <li>- ГОСТы;</li> <li>- ITSEC и другие.</li> </ul>
7	<p><b>ФЕДЕРАЛЬНЫЕ СТАНДАРТЫ ОЦЕНКИ БЕЗОПАСНОСТИ КС</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- критерии, ГОСТы, руководящие и нормативные документы;</li> <li>- защита автоматизированных систем и средств вычислительной техники: классификация, требования по защите информации от НСД, классы защищенности;</li> <li>- стандарты безопасности в сети Internet: МЭ, протоколы защищенной передачи информации.</li> </ul>
8	<p><b>АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- основные средства защиты компьютерной информации и их функции (Zecurion Zgate; Secret Disk; КриптоПро CSP; другие разработки);</li> <li>- криптопроцессоры;</li> <li>- защита от изменения потока сообщений и прерывания передачи, защита от навязывания ложных сообщений в каналы связи;</li> <li>- межсетевые экраны.</li> </ul>
9	<p><b>БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- формальные методы доказательства правильности программ и их спецификаций;</li> <li>- методы и средства анализа безопасности ПО;</li> <li>- контрольно-испытательные и логико-аналитические методы.</li> </ul>
10	<p><b>БЕЗОПАСНОСТЬ ТЕХНИЧЕСКИХ СРЕДСТВ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- требования к техническим средствам;</li> <li>- анализ безопасности технических средств;</li> <li>- подходы к оценке информационной безопасности.</li> </ul>
11	<p><b>СЕТЕВЫЕ КОНФИГУРАЦИИ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- требования к обеспечению конфиденциальности;</li> <li>- требования к обеспечению целостности информации в сетевых конфигурациях.</li> </ul>
12	<p><b>БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- подходы к оценке информационной безопасности в сетях;</li> <li>- типы сетевых атак;</li> <li>- методы противодействия атакам;</li> <li>- защита от несанкционированного доступа (основные принципы системы AAA, методы аутентификации);</li> <li>- управление доступом к ресурсам (задачи, требования и модели доступа).</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
13	<b>ПОРЯДОК ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КС</b> Рассматриваемые вопросы: - оценка актуальности угроз безопасности информации; - оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности; - оценка способов реализации (возникновения) угроз безопасности информации.
14	<b>ПОЛИТИКА БЕЗОПАСНОСТИ</b> Рассматриваемые вопросы: - политика безопасности; - аксиомы политики безопасности; - политика дискреционного доступа; - политика мандатного доступа; - политика тематического разграничения доступа.
15	<b>КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ</b> Рассматриваемые вопросы: - методы защиты виды, классификация; - шифрование, стенография, кодирование, сжатие и др.. - средства криптографической защиты информации (СКЗИ); - сертифицированные криптографические средства защиты информации в России.
16	<b>КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ</b> Рассматриваемые вопросы: - управление криптографическими ключами (виды ключей, процедуры управления ключами); - генерация ключей; - хранение ключей; - распределение ключей.
17	<b>СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ</b> Рассматриваемые вопросы: - стандарты шифрования данных (алгоритм шифрования данных DES, Triple DES, AES, алгоритм Ривеста); - Российский стандарт крипто- и имитозащиты сообщений; - концепция криптосистемы с открытым ключом; - криптосистема шифрования данных RSA, схемы шифрования Полига-Хеллмана, Эль Гамала, комбинированный метод шифрования.
18	<b>ХЭШ-ФУНКЦИИ</b> Рассматриваемые вопросы: - виды; - хэш-функции - использование в ЭП, стандарты хэш-функций.
19	<b>ЭЛЕКТРОННАЯ ПОДПИСЬ</b> Рассматриваемые вопросы: - проблема аутентификации данных; - подписи с дополнительными функциональными свойствами.
20	<b>АЛГОРИТМЫ ЭП</b> Рассматриваемые вопросы: - алгоритмы электронной подписи (назначение и виды, классификация, подделка ЭП); - слепая ЭП, быстрая, неоспоримая.
21	<b>АНАЛИЗ РИСКОВ</b>

№ п/п	Тематика лекционных занятий / краткое содержание
	Рассматриваемые вопросы: - анализ рисков информационной безопасности; - планирование и практическая реализация процессов, направленных на минимизацию рисков.
22	<b>КОМПЛЕКСНЫЙ ПОДХОД К ОЦЕНКИ БЕЗОПАСНОСТИ</b> Рассматриваемые вопросы: - применение стандартов при формировании политики безопасности и системы оценок эффективности, при проведении комплексных испытаний защищенности вычислительных систем и сетей; - стандарты для реализации и оценки технического совершенства систем шифрования; - использование стандартов при оценке защищенности каналов обмена информацией и безопасности транзакций.
23	<b>ПРОЕКТИРОВАНИЕ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b> Рассматриваемые вопросы: - принципы построения систем защиты конфиденциальной информации; - основы политики безопасности (понятие политики безопасности, реализация политики безопасности, модели безопасности); - основные этапы.
24	<b>АНАЛИЗ СИСТЕМ ОБЕСПЕЧЕНИЯ ИБ</b> Рассматриваемые вопросы: - аудит безопасности, анализ рисков, разработка Концепции обеспечения ИБ; - анализ архитектуры и структуры системы защиты; - анализ политик, процедур, регламентов и т.п.; - анализ программных и технических средства защиты конфиденциальной информации.

#### 4.2. Занятия семинарского типа.

##### Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	<b>АНАЛИЗ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ</b> В результате выполнения лабораторной работы студент получит знания о наиболее востребованных инженерно-технических средствах защиты информации.
2	<b>ОЦЕНКА БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ</b> Результат работы – список угроз и мер по разработке безопасного ПО, согласно ГОСТ Р 58412-2019.
3	<b>РЕКОМЕНДАЦИИ X.800 ДЛЯ РАСПРЕДЕЛЕННЫХ СИСТЕМ</b> В результате выполнения лабораторной работы студент получит навыки применения рекомендаций X.800.
4	<b>ПОЛОЖЕНИЯ ISO 15408 («COMMON CRITERIA»)</b> Студент получит навыки применения «Common Criteria» при формировании политики безопасности и системы оценок эффективности, а также при проведении комплексных испытаний защищенности объекта информатизации.
5	<b>МЕЖСЕТЕВЫЕ ЭКРАНЫ</b> В результате работы студент получит навыки применения МЭ.
6	<b>ЗАЩИТА СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ</b>

№ п/п	Наименование лабораторных работ / краткое содержание
	Результат работы – навыки практического применения Руководящего документа.
7	<b>ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ</b> ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ
8	<b>ИЗУЧЕНИЕ МЕТОДОВ ШИФРОВАНИЯ</b> В результате выполнения лабораторной работы будут зашифрованы и расшифрованы сообщения.
9	<b>ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДОВ ШИФРОВАНИЯ</b> Результатом работы является отлаженная программа, реализующая предложенный студентом алгоритм шифрования.
10	<b>ЭЛЕКТРОННАЯ ПОДПИСЬ</b> Студент получит навыки применения соответствующих стандартов, будет знать процессы формирования и проверки ЭП.
11	<b>ФУНКЦИЯ ХЭШИРОВАНИЯ</b> Студент получит навыки применения соответствующих стандартов, будет знать особенности использования функции хэширования в схемах ЭП.
12	<b>ТИПЫ И КАТЕГОРИИ ВОЗМОЖНЫХ НАРУШИТЕЛЕЙ</b> Результат работы – классификация нарушителей по степени угроз для защищаемого объекта информатизации.
13	<b>ПОЛИТИКА БЕЗОПАСНОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ</b> В результате выполнения лабораторной работы будет разработана политика безопасности для объекта информатизации.
14	<b>ОЦЕНКА БЕЗОПАСНОСТИ СЕТИ</b> Результат работы – оценка безопасности и список рекомендаций по повышению безопасности сети.
15	<b>ОЦЕНКА БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СИСТЕМЫ</b> Результат работы – оценка безопасности и список рекомендаций по повышению безопасности КС.
16	<b>РАЗРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ</b> В результате выполнения лабораторной работы студент получит навыки по разработки системы защиты информации.

#### 4.3. Самостоятельная работа обучающихся.

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

#### 4.4. Примерный перечень тем курсовых работ



Курсовая работа «Современные симметричные и асимметричные криптосистемы» направлена на развитие у обучающихся навыков самостоятельной творческой деятельности.

Примерный перечень тем курсовых работ:

- Реализация алгоритма Ривеста.
- Реализация алгоритма DES – режим сцепления блоков в CBC шифре.
- Реализация алгоритма DES – режим работы ECB (электронный блокнот).
- Реализация алгоритма DES – режим работы CFB – обратная связь по шифротексту.
- Реализация алгоритма DES – OFB – обратная связь по выходу.
- Алгоритм федерального стандарта x9.9.
- Алгоритм криптографического преобразования – общий.
- Алгоритм криптографического преобразования в режиме простой замены.
- Алгоритм криптографического преобразования в режиме гаммирования с обратной связью
- Алгоритм криптографического преобразования в режиме имитовставки.
- Алгоритм, основанный на схеме шифрования Эль Гамала.
- Алгоритм, основанный на комбинированном методе шифрования
- Алгоритм открытого распределения ключей Диффи-Хеллмана
- Алгоритм электронной подписи RSA.
- Алгоритм электронной подписи DSA.
- Отечественный стандарт цифровой подписи ГОСТ Р34.10-94.
- Алгоритм цифровой подписи с дополнительными функциями по схеме «слепой подписи».
- Алгоритм цифровой подписи с дополнительными функциями по схеме «неоспоримой подписи».

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

№ п/п	Библиографическое описание	Место доступа
----------	----------------------------	---------------

1	Алексеев В.М. Разработка мер защиты информационных ресурсов в корпоративной сети с выходом в интернет: Учебно-методическое пособие по курсовой работе – М.: РУТ (МИИТ), 2017. – 9 с.	<a href="https://library.miit.ru/bookscatalog/metod/DC-435.pdf">https://library.miit.ru/bookscatalog/metod/DC-435.pdf</a> (дата обращения: 02.10.2024). - Текст:электронный.
2	Алексеев В.М. Защита программ и данных: Учебно-методическое пособие. – М.: РУТ (МИИТ). 2017. – 24 с.	<a href="https://library.miit.ru/bookscatalog/metod/DC-436.pdf">https://library.miit.ru/bookscatalog/metod/DC-436.pdf</a> (дата обращения: 02.10.2024). - Текст:электронный.
3	Голиков А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие / А. М. Голиков. — Москва: ТУСУР, 2015. — 284 с. // Лань: электронно-библиотечная система.	<a href="https://e.lanbook.com/book/110336">https://e.lanbook.com/book/110336</a> (дата обращения: 16.02.2024). — Режим доступа: для авториз. пользователей. — Текст: электронный
4	Сидоренко В.Г., Скоробогатова Н.Н. Аспекты информационной безопасности: Учебное пособие. – М.: РУТ (МИИТ). 2018. – 64 с.	<a href="https://library.miit.ru/bookscatalog/metod/DC-667.pdf">https://library.miit.ru/bookscatalog/metod/DC-667.pdf</a> (дата обращения: 02.10.2024). — Текст: электронный.
5	Привалов А.А. Обеспечение информационной безопасности, проектирования, создания, модернизации объектов информации на базе компьютерных систем в защищенном исполнении: Учебно-методическое пособие к курсовой работе. -М.: РУТ (МИИТ), 2018. – 48 с.	<a href="https://library.miit.ru/bookscatalog/metod/DC-741.pdf">https://library.miit.ru/bookscatalog/metod/DC-741.pdf</a> (дата обращения: 02.10.2024). — Текст:электронный

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

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

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

Поисковые системы: Yandex, Google, Mail.

Официальный сайт РУТ (МИИТ) (<https://www.miit.ru/>).

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

Образовательная платформа «Юрайт» (<https://urait.ru/>).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (<http://e.lanbook.com/>).

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

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

Специализированное программное обеспечение не требуется.

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

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования:

- рабочее место преподавателя с персональным компьютером, подключённым к INTERNET;

- специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской;

- рабочие места студентов в компьютерном классе, подключённые к сети INTERNET.

9. Форма промежуточной аттестации:

Зачет в 5 семестре.

Курсовая работа в 5 семестре.

10. Оценочные материалы.

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

Авторы:

И.Е. Сафонова

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической  
комиссии

Н.А. Андриянова