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

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 ассиметричных 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	МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ Рассматриваемые вопросы: - виды защиты информации; - методы защиты компьютерной информации; - законодательные меры защиты информации (нормативные правовые акты РФ в области защиты информации).
2	СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ Рассматриваемые вопросы: - средства защиты компьютерной информации; - криптографические средства защиты информации; - стандарты (оценочные стандарты и технические спецификации).
3	УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ Рассматриваемые вопросы: - классификация и характеристики угроз; - способы несанкционированного доступа; - основные способы и каналы утечки информации; - преодоление программных средств защиты.
4	СЛУЖБЫ И МЕХАНИЗМЫ ИБ Рассматриваемые вопросы: - виды служб и механизмов безопасности; - взаимосвязь между службами и реализующими их механизмами; - комплекс требований к системе компьютерной безопасности.
5	МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

№ п/п	Тематика лекционных занятий / краткое содержание
	Рассматриваемые вопросы: - серия международных стандартов 27000; - рекомендации X.800; - общие критерии оценки безопасности информационных технологий, ISO/IEC 27000:2018 и другие.
6	НАЦИОНАЛЬНЫЕ СТАНДАРТЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ Рассматриваемые вопросы: - обзор стандартов; - TCSEC; - CTCPEC; - ГОСТы; - ITSEC и другие.
7	ФЕДЕРАЛЬНЫЕ СТАНДАРТЫ ОЦЕНКИ БЕЗОПАСНОСТИ КС Рассматриваемые вопросы: - критерии, ГОСТы, руководящие и нормативные документы; - защита автоматизированных систем и средств вычислительной техники: классификация, требования по защите информации от НСД, классы защищенности; - стандарты безопасности в сети Internet: МЭ, протоколы защищенной передачи информации.
8	АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ Рассматриваемые вопросы: - основные средства защиты компьютерной информации и их функции (Zecurion Zgate; Secret Disk; КриптоПро CSP; другие разработки); - криптопроцессоры; - защита от изменения потока сообщений и прерывания передачи, защита от навязывания ложных сообщений в каналы связи; - межсетевые экраны.
9	БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ Рассматриваемые вопросы: - формальные методы доказательства правильности программ и их спецификаций; - методы и средства анализа безопасности ПО; - контрольно-испытательные и логико-аналитические методы.
10	БЕЗОПАСНОСТЬ ТЕХНИЧЕСКИХ СРЕДСТВ Рассматриваемые вопросы: - требования к техническим средствам; - анализ безопасности технических средств; - подходы к оценке информационной безопасности.
11	СЕТЕВЫЕ КОНФИГУРАЦИИ Рассматриваемые вопросы: - требования к обеспечению конфиденциальности; - требования к обеспечению целостности информации в сетевых конфигурациях.
12	БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ Рассматриваемые вопросы: - подходы к оценке информационной безопасности в сетях; - типы сетевых атак; - методы противодействия атакам; - защита от несанкционированного доступа (основные принципы системы AAA, методы аутентификации); - управление доступом к ресурсам (задачи, требования и модели доступа).

№ п/п	Тематика лекционных занятий / краткое содержание
13	ПОРЯДОК ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КС 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	ПОЛИТИКА БЕЗОПАСНОСТИ Рассматриваемые вопросы: - политика безопасности; - аксиомы политики безопасности; - политика дискреционного доступа; - политика мандатного доступа; - политика тематического разграничения доступа.
15	КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ 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	КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ Рассматриваемые вопросы: - управление криптографическими ключами (виды ключей, процедуры управления ключами); - генерация ключей; - хранение ключей; - распределение ключей.
17	СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ 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 Гамаля, комбинированный метод шифрования.
18	ХЭШ-ФУНКЦИИ Рассматриваемые вопросы: - виды; - хэш-функции - использование в ЭП, стандарты хэш-функций.
19	ЭЛЕКТРОННАЯ ПОДПИСЬ Рассматриваемые вопросы: - проблема аутентификации данных; - подписи с дополнительными функциональными свойствами.
20	АЛГОРИТМЫ ЭП Рассматриваемые вопросы: - алгоритмы электронной подписи (назначение и виды, классификация, подделка ЭП); - слепая ЭП, быстрая, неоспоримая.
21	АНАЛИЗ РИСКОВ

№ п/п	Тематика лекционных занятий / краткое содержание
	Рассматриваемые вопросы: - анализ рисков информационной безопасности; - планирование и практическая реализация процессов, направленных на минимизацию рисков.
22	КОМПЛЕКСНЫЙ ПОДХОД К ОЦЕНКИ БЕЗОПАСНОСТИ 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 оценки защищенности каналов обмена информацией и безопасности транзакций.
23	ПРОЕКТИРОВАНИЕ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Рассматриваемые вопросы: - принципы построения систем защиты конфиденциальной информации; - основы политики безопасности (понятие политики безопасности, реализация политики безопасности, модели безопасности); - основные этапы.
24	АНАЛИЗ СИСТЕМ ОБЕСПЕЧЕНИЯ ИБ 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	АНАЛИЗ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В результате выполнения лабораторной работы студент получит знания о наиболее востребованных инженерно-технических средствах защиты информации.
2	ОЦЕНКА БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ Результат работы – список угроз и мер по разработке безопасного ПО, согласно ГОСТ Р 58412-2019.
3	РЕКОМЕНДАЦИИ X.800 ДЛЯ РАСПРЕДЕЛЕННЫХ СИСТЕМ В результате выполнения лабораторной работы студент получит навыки применения рекомендаций X.800.
4	ПОЛОЖЕНИЯ ISO 15408 («COMMON CRITERIA») Студент получит навыки применения «Common Criteria» при формировании политики безопасности и системы оценок эффективности, а также при проведении комплексных испытаний защищенности объекта информатизации.
5	МЕЖСЕТЕВЫЕ ЭКРАНЫ В результате работы студент получит навыки применения МЭ.
6	ЗАЩИТА СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

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

- 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/	Библиографическое описание	Место доступа

п		
1	Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019.- 204 с. - ISBN 978-5-7996-2677-8.	https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf(дата обращения: 16.02.2024). - Текст:электронный.
2	Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2.	https://book-pc.ru/bezopasnost/1882-programmno-apparatnye-sredstva-zaschity-informacii.html(дата обращения: 16.02.2024). - Текст:электронный.
3	Голиков А. М. Защита информации в инфокоммуникационн ых системах и сетях: учебное пособие / А. М. Голиков. — Москва: ТУСУР, 2015. — 284 с. // Лань: электронно-библиотечная система.	https://e.lanbook.com/book/110336 (дата обращения: 16.02.2024). — Режим доступа: для авториз. пользователей. — Текст: электронный
4	Нестеров, С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург: Лань, 2022. — 324 с. — ISBN 978-	https://www.litres.ru/book/s-a-nesterov/osnovy-informacionnoy-bezopasnosti-66007377/(дата обращения: 16.02.2024). — Режим доступа: для авториз. пользователей. Текст: электронный.

	5-8114-4067-2. Текст: электронный	
5	Лось А. Б., Нестеренко А. Ю., Рожков М. И. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М.: Издательство Юрайт, 2019. — 473 с. — (Серия: Бакалавр. Академический курс). - ISBN 978-5-534-12474-3.	https://azon.market/image/catalog/v_1/product/pdf/378/3777079.pdf(дата обращения: 16.02.2024). — Режим доступа: для авториз. пользователей.—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:

-рабочие 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:

профессор, доцент, д.н. кафедры
«Вычислительные системы, сети и
информационная безопасность» И.Е. Сафонова

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова