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
10.03.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Теоретические основы защиты информации

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

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: 23.04.2024

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Теоретические основы защиты информации» является формирование профессиональных компетенций по основным разделам дисциплины.

Основными задачами дисциплины являются:

- освоение студентами математических методов криптографии, базовых методов и средств защиты информации;
- ознакомление с законодательством и стандартами в этой области;
- студенты должны изучить теоретические основы защиты информации 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 использовать необходимые математические методы для решения задач профессиональной деятельности.

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

Знать:

- виды защиты информации;
- типы атак и методы противодействия атакам;
- математические основы криптографии и методы шифрования;
- службы и механизмы безопасности;
- информационный процесс управления криптографическими ключами;
- виды и алгоритмы электронной подписи (ЭП).

Уметь:

- применять на практике методы противодействия атакам;
- использовать на практике службы и механизмы безопасности;
- применять математические методы для решения задач профессиональной деятельности.

Владеть:

- навыками использования полученных теоретических знаний на практике;
- навыками использования полученных теоретических знаний при изучении последующих дисциплин профессионального цикла, связанных с защитой 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 1
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
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 96 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	УГРОЗЫ И ПУТИ ИХ РЕАЛИЗАЦИИ Рассматриваемые вопросы: - классификация угроз - пути реализации угроз;

№ п/п	Тематика лекционных занятий / краткое содержание
	- службы и механизмы безопасности.
2	ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ Рассматриваемые вопросы: - правовая, техническая, физическая и криптографическая защита информации; - законодательные меры защиты информации, стандарты.
3	СЛУЖБЫ БЕЗОПАСНОСТИ Рассматриваемые вопросы: - аутентификация (подтверждение подлинности); - обеспечение целостности и засекречивание данных; - контроль доступа и защита от отказов.
4	МЕХАНИЗМЫ БЕЗОПАСНОСТИ Рассматриваемые вопросы: - шифрование и ЭП; - подстановка трафика и управления маршрутизацией; - арбитраж, или освидетельствование.
5	ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ В КРИПТОГРАФИИ - множества и отображения; - основная теорема арифметики; - первообразные корни и индексы.
6	МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ - алгоритм Евклида, соотношение Безу; - Диофантовы линейные уравнения; - первообразные корни и индексы.
7	МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ. ВЫЧЕТЫ, СРАВНЕНИЯ - сравнения; - классы вычетов; - теорема Ферма, функция и теорема Эйлера; - квадратичные вычеты, символы Лежандра и Якоби.
8	АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: ГРУППЫ, КОЛЬЦА Рассматриваемые вопросы: - группы, морфизмы групп; - делимость в кольцах; - кольцо многочленов.
9	АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: ПОЛЯ Рассматриваемые вопросы: - поля Галуа или конечные поля; - способы представления элементов конечных полей; - задача дискретного логарифмирования в конечных полях.
10	ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ - понятие эллиптической кривой над полем; - порядок эллиптической кривой; - применение эллиптических кривых в криптографии.
11	СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ Рассматриваемые вопросы: - виды шифров, требования к шифрам, методы шифрования.

№ п/п	Тематика лекционных занятий / краткое содержание
	- стандарты шифрования данных (симметричные криптосистемы); - Российский стандарт крипто- и имитозащиты сообщений; - концепция криптосистемы с открытым ключом.
12	КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ Рассматриваемые вопросы: - управление криптографическими ключами (виды ключей, процедуры управления ключами); - генерация ключей; - хранение ключей; - распределение ключей.
13	ЭЛЕКТРОННАЯ ПОДПИСЬ Рассматриваемые вопросы: - проблема аутентификации данных; - подписи с дополнительными функциональными свойствами.
14	АЛГОРИТМЫ ЭП Рассматриваемые вопросы: - алгоритмы электронной подписи (назначение и виды, классификация, подделка ЭП); - слепая ЭП, быстрая, неоспоримая.
15	ХЭШ-ФУНКЦИИ Рассматриваемые вопросы: - виды; - хэш-функции - использование в ЭП, стандарты хэш-функций.
16	СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ Рассматриваемые вопросы: - криптографические средства создания защищенных виртуальных сетей; - криптографическая защита удаленного доступа к сети; - СКЗИ для передачи данных в локальных сетях; - сетевые протоколы криптографической защиты.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ Результат работы – получение практических навыков решения задач.
2	АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: ГРУППЫ Результат работы – получение практических навыков решения задач.
3	АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: КОЛЬЦА, ПОЛЯ Результат работы – получение практических навыков решения задач.
4	ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ, ПРИМЕНЕНИЕ В КРИПТОГРАФИИ Результат работы – получение практических навыков решения задач.
5	ИССЛЕДОВАНИЕ И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДОВ ШИФРОВАНИЯ Результатом работы является отлаженная программа, реализующая предложенный студентом алгоритм шифрования.
6	КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ

№ п/п	Тематика практических занятий/краткое содержание
	Студент получит навыки управления криптографическими ключами.
7	ЭЛЕКТРОННАЯ ПОДПИСЬ Студент получит навыки применения соответствующих стандартов, будет знать процессы формирования и проверки ЭП.
8	ХЭШ-ФУНКЦИЯ Студент получит навыки применения соответствующих стандартов, будет знать особенности использования функции хэширования в схемах ЭП.

4.3. Самостоятельная работа обучающихся.

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

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

№ п/п	Библиографическое описание	Место доступа
1	Вострецов, 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: 03.03.2024).-Текст:электронный.
2	Казарин О. В. , Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального	Образовательная платформа Юрайт [сайт].URL: https://urait.ru/bcode/497433 (дата обращения: 03.03.2024). - Текст: электронный

	образования / О. В. Казарин, А. С. Забабурин. Москва: Издательство Юрайт, 2022. 312 с. (Профессиональное образование). ISBN 978-5-534-13221-2.	
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.	https://e.lanbook.com/book/110336 (дата обращения: 03.03.2024). — 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 978-5-8114-4067-2.	Лань: э.https://e.lanbook.com/book/206279 (дата обращения: 03.03.2024). Режим доступа: для авториз. пользователей.Текст: электронный
5	Лось А. Б., Нестеренко А. Ю., Рожко 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: 18.03.2024). — 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;

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

9. Форма промежуточной аттестации:

Зачет 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