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 специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Криптографические методы защиты информации и протоколы

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе 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: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2023

1. Общие сведения о дисциплине (модуле).

Основной целью изучения дисциплины «Криптографические методы защиты информации и протоколы» является формирование у обучающегося компетенций для следующих видов деятельности: ? научно-исследовательская; ? проектная; ? контрольно-аналитическая;

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Научно-исследовательская деятельность: - сбор, обработка, анализ и систематизация научно-технической информации, отечествен-ного и зарубежного опыта по проблемам компьютерной безопасности;

Проектная деятельность: - разработка технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов; -разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием.

Контрольно-аналитическая деятельность: -предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей; применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты; -подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей.

Эксплуатационная деятельность: -установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения; -установка, наладка, тестирование и обслуживание аппаратно-программных средств обеспечения информационной безопасности компьютерных систем; -проверка технического состояния и профилактические осмотры технических средств защиты информации; -проведение аттестации технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты.

Задачи дисциплины: - изложение основополагающих принципов защиты информации с помощью криптографических методов и изучение их практического применения. -развитие у обучаемых системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами с помощью методов криптографии; -изучение принципов синтеза и анализа криптосистем, математических методов оценки их стойкости. - получение основополагающих знаний о свойствах,

характеризующих защищенность криптографических протоколов, об основных механизмах, применяемых для обеспечения выполнения того или иного свойства безопасности протокола, а также основных уязвимостях протоколов.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-2 - Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-7 - Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

ОПК-8 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

ОПК-12 - Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;

ПК-4 - Способен участвовать в разработке подсистемы информационной безопасности компьютерной (в том числе автоматизированной) системы включая разработку программно-аппаратных средств защиты информации, защищенных операционных систем, систем управления базами данных, компьютерных сетей, систем антивирусной защиты, средств криптографической защиты информации;

ПК-6 - Способен проводить оценку эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

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

Знать:

- методики и инструментарий, определяет критерии и осуществляет проверку эффективности систем защиты информации и действующих политик

безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

- разработки в области обеспечения безопасности компьютерных систем и сетей

- программные средства системного и прикладного назначения для решения профессиональных задач

Уметь:

- Выполняет работы по установке, настройке, администрированию и проверке работоспособности программно-аппаратные средства системного, прикладного и специального назначения в сфере профессиональной деятельности.

- ставить и анализировать задачу при проведении разработок в области обеспечения безопасности компьютерных систем и сетей с точки зрения выбранного методы научных исследований.

- Устанавливает причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям.

- Проектирует и разрабатывает компоненты защищенных автоматизированных систем в сфере профессиональной деятельности.

Владеть:

- навыками выбора методов научных исследований при решении конкретных задач.

- рациональный выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности, создаваемых защищенных компьютерных систем в сфере профессиональной деятельности.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 10 з.е. (360 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	
		№6	№7
Контактная работа при проведении учебных занятий (всего):	160	96	64
В том числе:			
Занятия лекционного типа	80	48	32
Занятия семинарского типа	80	48	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 200 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	Основы криптографии Рассматриваемые вопросы: - Введение в криптографию - Структурная схема защищённой си-стемы передачи информации. - Роль криптографических методов защиты в её структуре. - Понятия модуляции, кодирования, шифрования. - Основные задачи защиты информации криптографическими методами. - Понятие симметричной шифросисте-мы и её структурная схема. - Понятие асимметричной шифроси-стемы и её структурная схема - Исторические шифры, их примеры - Теоретические положения криптографии - Понятия алфавита, стандартной кодировки и шифротекста. - Лавинный эффект в шифровании. - Частотный криптоанализ - Классификация атак в криптографии. Основные понятия. - Вычислительно сложные задачи математики. - Понятие «односторонней» функции и «односторонней функции с секретом». - Элементы теории чисел.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Функция Эйлера и её особенности, теоремы Эйлера и Ферма.
2	Криптосистемы с открытым ключом Рассматриваемые вопросы: - Криптосистемы на базе задачи дискретного логарифмирования Криптосистема Диффи — Хеллмана Криптосистема (бесключевой протокол) Шамира Криптосистема Эль-Гамаля. - Криптосистемы на базе задачи факторизации Криптосистема RSA.
3	Электронно-цифровая подпись (ЭЦП) Рассматриваемые вопросы: - Общие сведения об ЭЦП Назначение и классификация (НЭП, ПЭП, КЭП) - Алгоритмы ЭЦП Алгоритм ЭЦП Эль-Гамаля Алгоритм ЭЦП RSA - Хеш-функции Понятие и основные свойства хеш-функции. Коллизии первого и второго рода.
4	Криптосистемы на эллиптических кривых Рассматриваемые вопросы: - Общие сведения об эллиптических кривых. - Экспоненциальная и субэкспоненциальная сложность алгоритмов. - Эллиптические кривые. - Понятие дискриминанта и сингулярности. - Операция композиции точек на кривой. - Свойства точек на эллиптической кривой. - Алгоритмы на эллиптических кривых. - Выбор параметров кривой. - Построение криптосистем на эллиптических кривых. - Шифр Эль-Гамаля на эллиптической кривой. - Стандарт ЭЦП ГОСТ Р 34.10
5	Обзор криптографических алгоритмов и средств Рассматриваемые вопросы: - Введение Классификация криптографических алгоритмов и средств защиты информации. - Блочные шифры. Основные особенности построения блочных шифров с использованием SP-сетей и сетей Фейстеля. - Алгоритм DES и его вариации. Описание алгоритма DES. - Алгоритм AES. Описание алгоритма AES. - Поточные шифры. Основные особенности построения поточных шифров. - Аппаратное шифрование и скрембли-рование. Виды скремблирования, особенности аппаратного шифрования. - Управление ключами Распределение ключей на базе алгоритма Диффи-Хеллмана. - Стеганография: история и современность. Обзор стеганографических методов защиты информации. - Аутентификация и идентификация. Криптографические основы аутентификации пользователей компьютерных систем. - Применение криптографии в радиосвязи. Системы радиосвязи с ППРЧ и с ис-пользованием шумоподобных сигналов, расширение спектра, стандарт APCO25. - Помехоусточивость шифров. Шифры, не размножающие искажений. - Современные криптосистемы с открытым ключом. Асимметричные криптосистемы, их особенности. - Современные криптосистемы с секретным ключом. Симметричные криптосистемы, их особенности.
6	Генераторы псевдослучайных последовательностей Рассматриваемые вопросы: - Общие сведения о генераторах псевдослучайных последовательностей. Основные понятия и свойства генера-торов ПСП. - Программные и аппаратные генераторы ПСП Принципы построения программных и аппаратных генераторов ПСП. - Регистры РСЛОС. Регистры сдвига с линейными обрат-ными связями как генераторы псевдо-

№ п/п	Тематика лекционных занятий / краткое содержание
	случайных последовательностей. - Структуры генераторов ПСП на базе РСЛОС Каскадирование РСЛОС и мажори-тарная структура на их базе. - Характеристики генераторов ПСП. Вероятностные характеристики РСЛОС, предсказуемость ПСП.
7	Понятие протокола, виды протоколов. Рассматриваемые вопросы: - Понятие протокола, отличия от криптосистем, примеры. - Цели и предназначение протоколов. - Криптостойкость протоколов. - Виды криптокпротоколов. - Протоколы с нулевым разглашением. - Аутентификация в информационных системах.
8	Стандарт. Криптопротоколы. Рассматриваемые вопросы: - Протокол Диффи-Хеллмана. - Протокол Блюма. - Протокол аутентификации Шнорра. - Электронная подпись RSA. - Крипт. хэш-функции. - Электронная подпись Шнорра.
9	Другие виды криптопротоколов. Рассматриваемые вопросы: - Протоколы, связанные с электронными платежами. - Электронные купюры. - Электронные деньги одного номинала. - Электронные деньги разного номинала. - Разделение секрета. - Протоколы голосования.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Практичесое занятие №1 Исторические шифры
2	Практическое занятие №2 Вычислительно сложные задачи математики
3	Практическое занятие №3 Криптосистема (бесключевой протокол) Шамира
4	Практическое занятие №4 Криптосистема Эль-Гамаля
5	Практическое занятие №5 Криптосистема RSA.
6	Практическое занятие №6 Изучение блочных шифров
7	Практическое занятие №7 Алгорит AES

№ п/п	Тематика практических занятий/краткое содержание
8	Практическое занятие №8 Поточные шифры
9	Практическое занятие №9 Аналоговое скремблирование
10	Практическое занятие №10 программные и аппаратные генераторы ПСП
11	Практическое занятие №11 Регистры РСЛОС
12	Практическое занятие №12 Структуры генераторов ПСП на базе РСЛОС, защита работ
13	Практическое занятие №13 Понятие протокола, отличия от криптосистем, примеры.
14	Практическое занятие №14 Виды криптокпротоколов
15	Практическое занятие №15 Аутентификация в информационных системах
16	Практическое занятие №16 Протокол Диффи-Хеллмана
17	Практическое занятие №17 Протокол Блюма
18	Практическое занятие №18 Электронная подпись RSA
19	Практическое занятие №19 Электронные деньги одного номинала
20	Практическое занятие №20 Электронные деньги разного номинала
21	Практическое занятие №21 Разделение секрета

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к практическим занятиям.
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.
6	Выполнение курсовой работы.
7	Подготовка к промежуточной аттестации.
8	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1. Исторические шифры и их криптоанализ;

2. Современные криптосистемы с открытым ключом;

3. Современные симметричные криптосистемы;

4. Аппаратное шифрование и скремблирование;

5. Применение криптографических методов защиты информации на различных уровнях модели OSI;

6. Алгоритм симметричного шифрования AES;

7. Алгоритмы вычисления хеш-функций в криптографических системах;

8. Искусственные нейронные сети и нейрокриптография;

9. Стеганография: история и современность;

10. Блочные шифры с использованием SP-сетей и сетей Фейстеля;

11. Поточные шифры;

12. Квантовая криптография;

13. Задача о ранце и её криптографическое использование;

14. Современные стандарты и системы электронно-цифровой подписи;

15. Технические средства защиты авторских прав;

16. Протокол HTTPS и защита информации в сети Интернет;

17. Идентификация, аутентификация и парольная защита;

18. Помехоусточивость шифров. Шифры, не размножающие искажений;

19. Криптографическая защита каналов радиосвязи. Стандарт APCO P25;

20. Системы радиосвязи с ППРЧ и с использованием шумоподобных сигналов.

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

№ п/п	Библиографическое описание	Место доступа
1	Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров; Ред. А.А. Корниенко; Под Ред. А.А. Корниенко Однотомное издание Маршрут , 2006	НТБ (ЭЭ); НТБ (уч.3); НТБ (фб.); НТБ (чз.2)
2	Основы современной криптографии С.Г. Баричев, В.В. Гончаров, Р.Е. Серов Однотомное издание Горячая линия - Телеком , 2002	НТБ (фб.); НТБ (чз.1); НТБ (чз.2)
3	Основы криптографии А.П. Алферов, А.Ю. Зубов, А.С.	НТБ (фб.); НТБ (чз.1);

	Кузьмин, А.В. Черемушкин Однотомное издание Гелиос АРВ , 2002	НТБ (чз.2)
1	Криптография Н. Смарт Однотомное издание Техносфера , 2006	НТБ (фб.)

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

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/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

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.

MathCAD 14.0 или другая система моделирования.

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.

9. Форма промежуточной аттестации:

Курсовая работа в 6 семестре.

Экзамен в 6, 7 семестрах.

10. Оценочные материалы.

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

Авторы:

доцент, старший научный сотрудник,
к.н. кафедры «Управление и защита
информации» И.Ф. Михалевич

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической
комиссии С.В. Володин