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

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:

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 оценки эффективности систем защиты информации, включая средства криптографической защиты информации

(СКЗИ), защищенные операционные системы и системы управления базами данных.

- основные положения и методы научных исследований, применяемые при разработке и анализе стойкости криптографических систем и протоколов.

- программные средства системного и прикладного назначения, включая отечественные криптографические пакеты, для решения задач профессиональной деятельности.

- принципы построения и архитектуру симметричных и асимметричных криптосистем (DES, AES, RSA, Эль-Гамаля), а также алгоритмов электронной цифровой подписи.

- классификацию, назначение и уязвимости криптографических протоколов (аутентификации, выработки ключа, разделения секрета, электронных платежей).

- принципы работы и свойства генераторов псевдослучайных последовательностей, включая регистры сдвига с линейной обратной связью (РСЛОС).

Уметь:

- выполнять работы по установке, настройке, администрированию и проверке работоспособности программно-аппаратных средств криптографической защиты информации.

- ставить и анализировать задачу при проведении разработок в области криптографии с точки зрения выбранных методов научных исследований.

- устанавливать причины, цели и условия изменения свойств криптографических алгоритмов и протоколов применительно к конкретным условиям эксплуатации.

- проектировать и разрабатывать компоненты защищенных автоматизированных систем с использованием криптографических методов и средств.

- проводить оценку эффективности реализации криптографических методов защиты информации и действующих политик безопасности в компьютерных системах.

- применять нормативные и методические документы (стандарты ГОСТ, рекомендации ФСТЭК/ФСБ) при разработке и эксплуатации средств криптографической защиты.

Владеть:

- навыками выбора методов научных исследований для решения конкретных задач обеспечения криптографической защиты информации.

- методами рационального выбора технологии, инструментальных средств и средств вычислительной техники при создании защищенных компьютерных систем с использованием криптографии.

- навыками работы с программно-аппаратными средствами криптографической защиты информации (СКЗИ), включая их установку, настройку и проверку работоспособности.

- основами разработки и реализации криптографических алгоритмов (симметричных, асимметричных, хеш-функций) на языках высокого и низкого уровня.

- методиками анализа и оценки стойкости криптографических протоколов, а также выявления их потенциальных уязвимостей (включая атаки типа "человек посередине").

- навыками применения нормативной и методической документации (национальные стандарты, рекомендации регуляторов) в области криптографической защиты информации при проектировании и эксплуатации компьютерных систем.

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):	176	96	80
В том числе:			
Занятия лекционного типа	96	48	48
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 184 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	Введение в криптографию. Рассматриваемые вопросы: - Роль криптографии в системе защиты информации. - Основные понятия и определения. - Структурная схема защищенной системы передачи информации.
2	Математические основы криптографии. Рассматриваемые вопросы: - Элементы теории чисел, конечные поля, вычеты. - Вычислительно сложные задачи математики (факторизация, дискретное логарифмирование).
3	Исторические шифры и их криптоанализ. Рассматриваемые вопросы: - Шифры перестановки и замены (Цезаря, Виженера, Сцитала). - Частотный криптоанализ. - Понятие о безусловно и вычислительно стойких шифрах (К. Шеннон).
4	Классическая симметричная криптография. Рассматриваемые вопросы: - Понятие симметричной шифросистемы. - Принципы Шеннона: рассеивание и перемешивание. - Лавинный эффект.
5	Блочные шифры и сети Фейстеля. Рассматриваемые вопросы: - Принципы построения блочных шифров. - Сети Фейстеля и SP-сети. - Алгоритм DES: структура, раундовые функции, режимы работы.
6	Современный стандарт симметричного шифрования AES. Рассматриваемые вопросы: - История создания. - Математический аппарат. - Структура алгоритма (SubBytes, ShiftRows, MixColumns, AddRoundKey).
7	Поточные шифры. Рассматриваемые вопросы: - Принципы построения поточных шифров.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Гаммирование. - Требования к генераторам ключевой последовательности.
8	Генераторы псевдослучайных последовательностей (ГПСП). Рассматриваемые вопросы: - Программные и аппаратные ГПСП. - Регистры сдвига с линейной обратной связью (РСЛОС). - Каскадирование РСЛОС.
9	Асимметричная криптография (криптосистемы с открытым ключом). Рассматриваемые вопросы: - Понятие асимметричной шифросистемы. - Односторонние функции. - Распределение открытых ключей.
10	Криптосистема RSA. Рассматриваемые вопросы: - Алгоритм генерации ключей. - Шифрование и дешифрование. - Вычислительная сложность. - Атаки на RSA.
11	Криптосистема Эль-Гамаля. Рассматриваемые вопросы: - Алгоритм на основе задачи дискретного логарифмирования. - Шифрование и дешифрование. - Сравнение с RSA.
12	Протокол Диффи-Хеллмана. Рассматриваемые вопросы: - Протокол выработки общего секретного ключа. - Атака "man-in-the-middle". - Модификации протокола.
13	Криптосистема Шамира. Рассматриваемые вопросы: - Бесключевой протокол Шамира. - Принципы построения и практическое применение.
14	Хеш-функции в криптографии. Рассматриваемые вопросы: - Понятие и основные свойства хеш-функции. - Коллизии первого и второго рода. - Области применения (MD5, SHA-1, SHA-2, SHA-3).
15	Электронная цифровая подпись (ЭЦП). Рассматриваемые вопросы: - Назначение и классификация (простая, неквалифицированная, квалифицированная). - Общая схема формирования и проверки подписи.
16	Алгоритмы ЭЦП на основе RSA и Эль-Гамаля. Рассматриваемые вопросы: - Схемы подписи. - Особенности и сравнение.
17	Криптография на эллиптических кривых (ECC). Рассматриваемые вопросы: - Общие сведения об эллиптических кривых. - Операция композиции точек. - Выбор параметров кривой.

№ п/п	Тематика лекционных занятий / краткое содержание
18	Применение эллиптических кривых. Рассматриваемые вопросы: - Шифр Эль-Гамаля на эллиптической кривой. - Стандарт ЭЦП ГОСТ Р 34.10. - Преимущества ECC.
19	Криптографические протоколы. Рассматриваемые вопросы: - Понятие протокола, отличия от алгоритма. - Цели и предназначение. - Виды протоколов.
20	Протоколы аутентификации. Рассматриваемые вопросы: - Протокол Шнорра, протокол Блюма. - Аутентификация на основе паролей и сертификатов.
21	Протоколы с нулевым разглашением (Zero-Knowledge Proof). Рассматриваемые вопросы: - Принципы и практическое значение.
22	Протоколы разделения секрета и электронных платежей. Рассматриваемые вопросы: - Пороговые схемы (Шамира). - Протоколы голосования. - Электронные деньги и купюры.
23	Управление криптографическими ключами. Рассматриваемые вопросы: - Генерация, распределение, хранение и уничтожение ключей. - Инфраструктура открытых ключей (PKI). - Удостоверяющие центры.
24	Современные направления криптографии. Рассматриваемые вопросы: - Квантовая криптография. - Стеганография. - Нейрокриптография. - Обзор отечественных стандартов и СКЗИ.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Исторические шифры. Изучение и реализация шифров Цезаря, Виженера. Проведение частотного криптоанализа.
2	Вычислительно сложные задачи математики. Решение задач факторизации чисел и дискретного логарифмирования.
3	Криптосистема (бесключевой протокол) Шамира. Моделирование протокола передачи сообщения без предварительного обмена ключами.
4	Криптосистема Эль-Гамаля. Реализация алгоритмов генерации ключей, шифрования и дешифрования.

№ п/п	Тематика практических занятий/краткое содержание
5	Криптосистема RSA. Изучение алгоритма, расчет ключей, шифрование и дешифрование сообщений.
6	Изучение блочных шифров. Анализ архитектуры блочных шифров на примере учебных алгоритмов.
7	Алгоритм AES. Детальный разбор и реализация этапов шифрования (SubBytes, ShiftRows, MixColumns).
8	Поточные шифры. Исследование принципов гаммирования. Реализация простого поточного шифра.
9	Аналоговое скремблирование. Изучение методов инверсии спектра и частотной перестановки.
10	Программные и аппаратные генераторы ПСП. Изучение принципов работы генераторов псевдослучайных чисел.
11	Регистры РСЛОС. Построение и анализ регистров сдвига с линейной обратной связью.
12	Структуры генераторов ПСП на базе РСЛОС. Изучение каскадных и мажоритарных схем. Защита работ.
13	Понятие протокола, отличия от криптосистем. Анализ различий на практических примерах (сравнение RSA и протокола аутентификации).
14	Виды криптопротоколов. Классификация протоколов (аутентификации, выработки ключа, управления ключами).
15	Аутентификация в информационных системах. Изучение методов аутентификации на основе паролей, токенов, биометрии.
16	Протокол Диффи-Хеллмана. Моделирование протокола выработки общего ключа. Анализ уязвимости к атаке "человек посередине".
17	Протокол Блюма. Изучение протокола аутентификации с нулевым разглашением.
18	Электронная подпись RSA. Реализация формирования и проверки ЭЦП на основе алгоритма RSA.
19	Электронные деньги одного номинала. Изучение принципов построения анонимных платежных систем.
20	Электронные деньги разного номинала. Анализ схем, позволяющих осуществлять платежи разными суммами.
21	Разделение секрета. Реализация пороговой схемы разделения секрета Шамира.

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.

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	Криптография Часть II Донгак Ш. М. Практикум М.: МИРЭА - Российский технологический университет, - 64 с. , 2020	https://reader.lanbook.com/book/163935
2	Криптографические методы защиты информации: классическая криптография Борисова С. Н. Учебное пособие Пензенский	https://reader.lanbook.com/book/162235

	государственный университет, - 186 с. - ISBN 978-5-907102-51-4 , 2018	

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, д.н. кафедры
«Управление и защита
информации» И.Ф. Михалевич

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической
комиссии С.В. Володин