МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

26 июня 2019 г.

Кафедра «Управление и защита информации»

Автор Алексеев Виктор Михайлович, д.т.н., профессор

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Теоретико-числовые методы в криптографии

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2019

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 25 июня 2019 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 21 24 июня 2019 г. Заведующий кафедрой  Л.А. Баранов

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина «Теоретико-числовые методы в криптографии» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 100501 « Компьютерная безопасность».
Дисциплина «Теоретико-числовые методы в криптографии» относится к числу профессиональных прикладных дисциплин в силу направленности материала по проблемам безопасности и его важности для подготовки специалиста.
Целью преподавания дисциплины «Теоретико-числовые методы в криптографии» является изложение слушателям основных принципов и методов защиты информации, комплексного проектирования и анализа защищенных компьютерных систем КС.
Задачами изучения дисциплины являются:
понятия и задачи решаемые в криптографии;
видах информации, подлежащей шифрованию, о методах криптографического синтеза и анализа;
применениях криптографии в решении задач аутентификации, построения систем цифровой подписи;
о методах криптозащиты компьютерных систем и сетей и основных подходах к изучению криптосистем.
Основной целью изучения учебной дисциплины «Теоретико-числовые методы в криптографии» является формирование у обучающегося компетенций для научно-исследовательского видав деятельности.
Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):
научно-исследовательская деятельность:
анализ состояния и динамики объектов деятельности с использованием необходимых методов и средств анализа, моделирование исследуемых явлений или процессов с использованием современных вычислительных машин и систем, а также компьютерных программ;
разработка программ и методик испытаний объектов защиты информации, разработка предложений по внедрению результатов научных исследований.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Теоретико-числовые методы в криптографии" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Криптографические методы защиты информации

2.2.2. Криптографические протоколы

2.2.3. Модели безопасности компьютерных систем

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ОПК-3 Способен на основании совокупности существующих математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач защиты информации	ОПК-3.1 Применяет систему фундаментальных знании? (математических, естественнонаучных и инженерных) для формулирования и решения проблем задач защиты информации. ОПК-3.2 Применяет методы математического моделирования для формализации содержательно отчетливо сформулированных проблем.
2	ОПК-8 Способен проводить анализ корректности реализации эффективных комбинаторных, теоретико-числовых и криптографических алгоритмов и протоколов применительно к конкретным условиям	ОПК-8.1 Строит, анализирует и реализует алгоритмы, в том числе криптографические, в современных программных комплексах. ОПК-8.2 Устанавливает причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. ОПК-8.3 Анализирует корректность комбинаторных, теоретико-числовых и криптографических алгоритмов в современных программных комплексах.
3	ПКО-2 Способен применять математические методы в области компьютерной безопасности	ПКО-2.1 Проводит анализ и разрабатывает под руководством квалифицированного специалиста математические модели безопасности компьютерных систем. ПКО-2.2 Применяет специальные математические методы, включая криптографические, для анализа и разработки защищенных компьютерных систем. ПКО-2.3 Применяет решения на основе специальных математических методов для обеспечения защищенной передачи данных в современных компьютерных сетях.
4	ПКР-1 Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	ПКР-1.1 Строит математические модели для оценки безопасности компьютерных систем. ПКР-1.2 Анализирует компоненты системы безопасности с использованием современных математических методов.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

5 зачетных единиц (180 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 5
Контактная работа	54	54,15
Аудиторные занятия (всего):	54	54
В том числе:		
лекции (Л)	36	36
практические (ПЗ) и семинарские (С)	18	18
Самостоятельная работа (всего)	90	90
Экзамен (при наличии)	36	36
ОБЩАЯ трудоемкость дисциплины, часы:	180	180
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	5.0	5.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЭК	ЭК

4.3. Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	5	Раздел 1 Основы теории чисел	18		2		30	50	
2	5	Тема 1.1 Теория делимости	2					2	
3	5	Тема 1.2 Функция Эйлера	4					4	
4	5	Тема 1.3 Теория сравнений	4					4	
5	5	Тема 1.4 Сравнения с одним неизвестным	2					2	
6	5	Тема 1.5 Теория квадратичных вычетов	2					2	
7	5	Тема 1.6 Первообразные корни и индексы	2					2	
8	5	Тема 1.7 Построение доказуемо простых чисел общего и специального вида	2					2	
9	5	Раздел 2 Алгебраические основы теории чисел	10		8		30	48	
10	5	Тема 2.1 Основные понятия алгебры	2					2	
11	5	Тема 2.2 Конечные поля и неприводимые многочлены	4					4	
12	5	Тема 2.3 Кольца многочленов	4					4	
13	5	Раздел 3 Алгоритмы в криптографии и криптоанализе	8		8		30	46	
14	5	Тема 3.1 Элементы теории сложности	4					4	
15	5	Тема 3.2 Алгоритмы факторизации	2					2	
16	5	Тема 3.3 Алгоритмы	2					2	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		дискретного логарифмирования							
17	5	Раздел 4 экзамен						36	ЭК
18		Всего:	36		18		90	180	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 18 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	5	РАЗДЕЛ 1 Основы теории чисел	ПЗ 1. Сеть Фейштеля	2
2	5	РАЗДЕЛ 2 Алгебраические основы теории чисел	ПЗ 2. Шифр простой замены, таблица Вижинера	2
3	5	РАЗДЕЛ 2 Алгебраические основы теории чисел	Обмен ключами по Диффи-Хелману	2
4	5	РАЗДЕЛ 2 Алгебраические основы теории чисел	Шифр RSA	2
5	5	РАЗДЕЛ 2 Алгебраические основы теории чисел	ПК1 - текущ. контроль по разделу 2. (ТЕСТ №1)	2
6	5	РАЗДЕЛ 3 Алгоритмы в криптографии и криптоанализе	ПЗ 6. Конечные поля и неприводимые многочлены	2
7	5	РАЗДЕЛ 3 Алгоритмы в криптографии и криптоанализе	Кольца многочленов	2
8	5	РАЗДЕЛ 3 Алгоритмы в криптографии и криптоанализе	Итоговое защита практических работ	2
9	5	РАЗДЕЛ 3 Алгоритмы в криптографии и криптоанализе	ПК2 - текущ. контроль по разделу 3. (ТЕСТ №2)	2
			ВСЕГО:	18 / 0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Теоретико-числовые методы в криптографии» осуществляется в форме лекций, лабораторных работ и практических занятий.
Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью являются традиционными классически-лекционными (объяснительно-иллюстративные) и с использованием интерактивных (диалоговых) технологий.
Практические занятия организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач). Остальная часть практического курса проводится с использованием интерактивных (диалоговые) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а так же использованием компьютерной тестирующей системы.
Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относиться отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.
Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 3 раздела, представляющих собой логически завершенный объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	5	РАЗДЕЛ 1 Основы теории чисел	Изучение: теоремы Поклингтона и доказуемо простые числа общего вида на основании частичного разложения (n—1). Числа Ферма. Теорема Пепина. Числа Мерсенна.	30
2	5	РАЗДЕЛ 2 Алгебраические основы теории чисел	Кольца многочленов. Кольцо многочленов Zp[x]. Конечные поля многочленов. Кольца многочленов	30
3	5	РАЗДЕЛ 3 Алгоритмы в криптографии и криптоанализе	Метод прямого поиска. Шаг младенца – шаг великана. Алгоритмы дискретного логарифмирования: Алгоритм Полига-Хеллмана. Алгоритмы дискретного логарифмирования: Алгоритм исчисления порядка (index-calculus algorithm)	30
			ВСЕГО:	90

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства)	А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров	М. : Маршрут, 2006., 2006	Все разделы
2	Криптография	Н. Смарт	М. : Техносфера, 2006	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
3	Криптография в упражнениях и задачах	В.О. Осипян,К.В. Осипян	МИИТ, 2011	Все разделы

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ.
http://elibrary.ru/ - научно-электронная библиотека.
http://robotosha.ru/
www.chipinfo.ru.
http://siblec.ru/
http://autex.ru/
http://www.intuit.ru
http://twirpx.com
http://habrahabr.ru
http://semestr.ru
htth://www.cisco.ru
Поисковые системы: Yandex, Google, Mail, база научно-технической информации ВИНИТИ РАН.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.
Для проведения практических занятий необходимы компьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами:
Microsoft Office или Work 9,
интегрированная среда разработки программного обеспечения для эиуляции сетевого

оборудования OmniGraffle;
среда разработки программного обеспечения HTML5 и PHP.
Для проведения практических занятий необходимо иметь комплекс программ для ПЭВМ, обеспечивающих возможность выполнения работ:
в области построения программных и аппаратных средств защиты информации в телекоммуникационных сетях (iOS15 Cisco и выше);
программные продукты Mac OS server, XSan.

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для проведения аудиторных занятий и самостоятельной работы требуется:
1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET.
2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.
3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANET
4. Для проведения практических занятий: компьютерный класс; компьютеры с минимальными требованиями – Core 5, ОЗУ 4 ГБ, HDD 300 ГБ, wifi, USB 2.0.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающимся необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе. Обучающийся должен быть нацелен на максимальное усвоение подаваемого лектором материала, после лекции и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы.
Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.
Главная задача лекционного курса – сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.
Основные функции лекций: 1. Познавательно-обучающая; 2. Развивающая; 3. Ориентирующе-направляющая; 4. Активизирующая; 5. Воспитательная; 6. Организующая; 7. информационная.
Выполнение практических заданий и лабораторных работ служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.
Проведение практических занятий и лабораторных работ не сводится только к органическому дополнению лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для

своевременного подтягивания отстающих обучающихся.
При подготовке специалиста важна не только серьезная теоретическая подготовка, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. Этому способствует форма обучения в виде практических занятий и и лабораторных работ. Задачи практических занятий и лабораторных работ: закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию и лабораторной работе должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.
Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.
Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтра. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что- то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.
Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к экзамену и тестовые материалы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания.
Фонд оценочных средств являются составной частью учебно-методического обеспечения процедуры оценки качества освоения образовательной программы и обеспечивает повышение качества образовательного процесса и входит, как приложение, в состав рабочей программы дисциплины.
Основные методические указания для обучающихся по дисциплине указаны в разделе основная и дополнительная литература.