МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ярославский государственный университет им. П.Г. Демидова

Кафедра теоретической информатики

УТВЕРЖДАЮ
Декан факультета ИВТ
_____ Д.Ю. Чалый
«_18_»____мая_____2020 г.

Рабочая программа дисциплины
«Математические методы защиты информации»

Направление подготовки
02.03.02 Фундаментальная информатика и информационные технологии

Профиль
«Информатика и компьютерные науки»

Квалификация выпускника
Бакалавр

Форма обучения
очная

Программа рассмотрена
на заседании кафедры
от 27 апреля 2020 г.,
протокол № 9

Программа одобрена НМК
факультета ИВТ
протокол № 7 от
17 мая 2020 г.

Ярославль
2020

1. Цели освоения дисциплины

Целями дисциплины «Математические методы защиты информации» являются приобретение знаний и умений в области защиты информации от несанкционированного доступа. Данный курс вырабатывает у студентов навыки использования математического аппарата, способствует развитию логического, эвристического и алгоритмического мышления и дает представление о месте и роли математики в современном мире

2. Место дисциплины в структуре ОП бакалавриата

Дисциплина «Математические методы защиты информации» относится к вариативной части (дисциплина по выбору) ОП бакалавриата.

Для освоения данной дисциплиной студенты должны владеть базовыми математическими знаниями и информационными технологиями. Полученные в курсе «Математические основы защиты информации и информационной безопасности» знания необходимы для продолжения обучения в магистратуре и для подготовки специалиста в области информационных технологий.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП бакалавриата

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Профессиональные компетенции		
ПК-1 Способен понимать, совершенствовать и применять современный математический аппарат и современные технологии, интерпретировать данные современных научных исследований	ПК-1.2 Владеет методами математического моделирования	**Знать:** – знать основные понятия информационной безопасности ; **Уметь**: – выполнять работы с компьютером как средством управления информацией; – использовать профессиональные навыки в научной и познавательной деятельности, а также в социальной сфере; – понимать и применять в исследовательской и прикладной деятельности современный математический аппарат; – - критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной деятельности; **Владеть навыками:** – работы с информационными и компьютерными технологиями; – - работы с информацией в глобальных компьютерных сетях; – - работы в коллективе и использования нормативных правовых документов в своей деятельности.

		- применять в профессиональной деятельности современные языки программирования. ….

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зач. ед., 144 акад. час.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Раздел 1 Введение. Идея криптосистем открытого ключа	6	1	2				4	Контрольная работа
2	Раздел 2. Модульная арифметика. Проверка чисел на простоту	6	3	4				8	Контрольная работа
3	Раздел 3. Системы открытого ключа	6	3	6				10	Контрольная работа
4	Раздел 4. Симметричные криптосистемы	6	2	6		1		10	Контрольная работа
5	Раздел 5. Электронная цифровая подпись	6	2	4		1		5	Зачет
6	Раздел 6. Способы передачи ключей	6	2	4		1		5	Зачет
7	Раздел 7. Потоковое кодирование	6	2	4		1		5	Зачет
8	Раздел 8. Разделение секрета, подсознательный канал.	6	2	4		1		5	зачет
	Всего за 6 семестр		**17**	**34**		**5**		**52**	зачет
	Всего		**17**	**34**		**5**		**52**	

Содержание разделов дисциплины:

Раздел 1.

Зачем защищать информацию. Общая схема системы защиты информации. Возможности шифрования и криптоанализа. История защиты информации. Исторические

системы (Цезарь, Хилл, аффинная), одно алфавитные и много алфавитные системы (система Плейфейра, Виженера, Бьюфорта)

Раздел 2.

Понятие полиномиального и неполиномиального алгоритма. Понятие NP полной задачи. Примеры задач, для которых нахождение $yy = ff(xx)$ является более легкой (полиномиальной) задачей, а обратная задача $xx = \eta\eta(yy)$ является труднорешаемой. Введение в модулярную арифметику. Нахождение мультипликативно обратного элемента.

Основная теорема об остатках. Проверка чисел на простоту(тест на основе теоремы Эйлера, тест Соловея-Штрассена, тест Миллира-Рабина). Примеры.

Раздел 3.

Рюкзачная криптосистема. Построение криптосистемы. Возможность криптоанализа. Примеры. Теория достижимости. Модификация рюкзачной криптосистемы. Примеры.

Криптосистема RSA. Построение криптосистемы. Криптоанализ и факторизация. Примеры.

Криптосистемы Эль-Гамаля, Рабина, Вильямса, Уильемса. Построение криптосистемы. Примеры.

Раздел 4.

DES. Построение криптосистемы.
IDEA. Построение криптосистемы.
Гост. Построение криптосистемы. и т.д.
О выборе плохих ключей.

Раздел 5.

Общая схема ЭЦП. Примеры.
Описание хэш функции. Примеры.
Схема ЭЦП RSA. Примеры.
Схема ЭЦП Эль-Гамаля. Примеры.
Схема ЭЦП DSA. Примеры.
Схема ГОСТ Р34.10-94. Примеры.
Подделка ЭЦП Примеры.

Раздел 6.

Diffie-Hellman. Примеры
Hughes. Примеры
протокол точка-точка.
трехпроходный протокол Шамира.
обмен зашифрованными ключами: базовый протокол EKE (реализация EKE с помощью RSA, Эль-Гамаля, Diffie-Hellman.) Примеры

Раздел 7.

Определения. Классификация поточных шифров (синхронные и самосинхронизирующиеся) Конгруэнтные генераторы и криптоанализ конгруэнтных генераторов. Регистры сдвига. Алгоритм A5. Алгоритм RC4. Алгоритм Seal. Алгоритм Wake. Примеры.

.

Раздел 8.

Криптография с несколькими открытыми ключами. Примеры
Схема интерполяционных многочленов Лагранжа. Примеры
Подсознательный канал (Ong-Schnorr-Shamir, Эль-Гамаль, DSA). Примеры
Доказательство с нулевым знанием и т.д.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости)

В процессе осуществления образовательного процесса используются:

– для формирования текстов материалов для промежуточной и текущей аттестации – программы Microsoft Office, издательская система LaTeX;

– компиляторы высокоуровневых языков программирования;

– для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная:

1. Математические методы защиты информации / Яросл. гос. ун-т. Ч. 3 : метод. указания для студентов, обучающихся по направлению Прикладная математика и информатика (сост. М. В. Краснов), Ярославль, ЯрГУ, 2013, 47с

2. Мельников, В. П., Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 4-е изд., стереотип., М., Академия, 2009, 331с

3. Математические методы защиты информации / Яросл. гос. ун-т. Ч. 2 [Электронный ресурс] : метод. указания (сост. М. В. Краснов), Ярославль, ЯрГУ, 2011, 44с

4. Математические методы защиты информации / Яросл. гос. ун-т. Ч. 2 : метод. указания (сост. М. В. Краснов), Ярославль, ЯрГУ, 2011, 44с

5. Математические методы защиты информации / Яросл. гос. ун-т. Ч. 3 [Электронный ресурс] : метод. указания для студентов, обучающихся по направлению Прикладная математика и информатика (сост. М. В. Краснов), Ярославль, ЯрГУ, 2013, 47с

б) дополнительная:

1. Смарт, Н., Криптография / Н. Смарт ; пер. с англ., М., Техносфера, 2006, 528с
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина - 2-е изд., перераб. и доп. - М.: Радио и связь, 2001.-376с
3. Введение в криптографию: Учебник / Под общ. ред. В.В. Ященко. - СПб.: Питер, 2001.-288с
4. Тимофеев Е.А. Защита информации в распределенных сетях: учебное пособие для вузов. - Ярославль.: ЯрГУ, 2001.-60с
5. Краснов М.В. Математические методы защиты информации: методические указания. - Ярославль.: ЯрГУ, 2004.-27с.
6. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие. - М.: Логос, 2001.-263с.
7. Ярочкин В.И. Информационная безопасность: Учебное пособие для студентов непрофильных вузов. - М.: Международные отноше, 2000.-400с.
8. Основы криптографии: Учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. - М.: Гелиос АРВ, 2001.-480с.
9. Петраков А.В. Основы практической защиты информации: Учебное пособие для вузов - 3-е изд. - М.: Радио и связь, 2001.-368с.

в) ресурсы сети «Интернет»

1. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).

2.Информационная система "Единое окно доступа к образовательным ресурсам" (http://www.edu.ru (раздел Учебно-методическая библиотека) или по прямой ссылке http://window.edu.ru/library).

3. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru).

4. www.wikipedia.org

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

-учебные аудитории для проведения занятий лекционного типа и практических занятий (семинаров);

- учебные аудитории для проведения групповых и индивидуальных консультаций,

- учебные аудитории для проведения текущего контроля и промежуточной аттестации;

-помещения для самостоятельной работы;

-помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, хранящиеся на

электронных носителях и обеспечивающие тематические иллюстрации, соответствующие рабочим программам дисциплин.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор(ы) :
д.ф.-м.н., профессор Е.А. Тимофеев

Приложение №1 к рабочей программе дисциплины
«Математические методы защиты информации»
Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1. Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Примерные задания к промежуточным контрольным работам:

Контрольная работа № 1:

Вариант 1.

1. Взломать рюкзачную криптосистему B=(10,6,11)
2. Использовать модификацию рюкзачной криптосистемы для создания эцп m=37 подписать a=11
3. Взломать аффинную криптосистему если известно, что 12 переходит в 15, а 11 переходит в 10 модуль равен 31
4. построить систему Хилла d=2
5. построить систему плотного рюкзака.

Вариант 2.

1. Взломать рюкзачную криптосистему B=(12,7,11)
2. Использовать модификацию рюкзачной криптосистемы для создания эцп m=41 подписать a=10
3. Взломать аффинную криптосистему если известно, что 11 переходит в 15, а 11 переходит в 21 модуль равен 31
4. построить систему Хилла d=3
5. построить четвертую модификацию рюкзака

Контрольная работа № 2:

Вариант 1.

1. Построить систему RSA p=11, q=13
2. Построить систему Уильемса
3. Привести пример системы доказательства с нулевым знанием
4. Схема ЭЦП ГОСТ Р34.10-94

Вариант 2.

1. Построить систему Эль-Гамаля p=7, q=13
2. Построить систему Рабина
3. Привести пример системы доказательства с нулевым знанием
4. Схема ЭЦП DSA.

Вопросы к зачету:

1 Введение в предмет ММЗИ.
2 Способы защиты информации.
3 Некоторые исторические алгоритмы (алгоритмы Цезаря, Вижнера).
4 Криптоанализ исторических алгоритмов (алгоритмы Цезаря, Вижнера).
5 Влияние длины блока на криптографическую стойкость алгоритма (алгоритмы Хилла и Пифнера).
6 Сравнение классических одноалфавитных и многоалфавитных систем.
7 Идея открытых ключей и преимущества их.

8 Рюкзачная криптоситема.
9 Криптоанализ рюкзачной криптосистемы.
10 Плотный рюкзак.
11 Крптосистема RSA.
12 Криптоанализ крптосистемы RSA.
13 Криптосистемы основанные на дискретных логарифмах.
14 Криптосистема Рабина.
15 Криптосистема Уильямса.
16 Криптосистема Эль-Гамеля.
17 Криптосистема Вильемса.
18 Способы передачи ключей.
19 Криптосистемы основанные на эллептических кривых.
20 Обзор потоковых кодов.
21. Симметричные криптосистемы
22. Доказательство с нулевым знанием
23. ЭЦП
24. Разделение секрета. Подсознательный канал

Задания для самостоятельной работы

Задания для самостоятельной работы:

Тимофеев Е.А. Защита информации в распределенных сетях: учебное пособие для вузов. - Ярославль.: ЯрГУ, 2001.-60с

Краснов М.В. Математические методы защиты информации: методические указания. - Ярославль.: ЯрГУ, 2004.-27с.

2. Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

2.1. Шкала оценивания сформированности компетенций и ее описание

Оценивание уровня сформированности компетенций в процессе освоения дисциплины осуществляется по следующей трехуровневой шкале:

Пороговый уровень - предполагает отражение тех ожидаемых результатов, которые определяют минимальный набор знаний и (или) умений и (или) навыков, полученных студентом в результате освоения дисциплины. Пороговый уровень является обязательным уровнем для студента к моменту завершения им освоения данной дисциплины.

Продвинутый уровень - предполагает способность студента использовать знания, умения, навыки и (или) опыт деятельности, полученные при освоении дисциплины, для решения профессиональных задач. Продвинутый уровень превосходит пороговый уровень по нескольким существенным признакам.

Высокий уровень - предполагает способность студента использовать потенциал интегрированных знаний, умений, навыков и (или) опыта деятельности, полученных при освоении дисциплины, для творческого решения профессиональных задач и самостоятельного поиска новых подходов в их решении путем комбинирования и использования известных способов решения применительно к конкретным условиям. Высокий уровень превосходит пороговый уровень по всем существенным признакам.

2.2. Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования

Код компе-тенции	Форма контроля	Этапы форми-рования (№ темы (раздела)	Показатели оценивания	Шкала и критерии оценивания компетенций на различных этапах их формирования		
				Пороговый уровень	Продвинутый уровень	Высокий уровень
Общепрофессиональные компетенции						
ОПК-4	Контрольные работы 1,2. Зачет.	1-4	**Знать** построение наиболее известных исторических криптосистем; целый класс криптосистем с открытым ключом целый класс схем для создания ЭЦП; способы проверки числа на простоту симметрических методах (DES,IDEA и т.д.); **Уметь** создавать ЭЦП для документа; передавать в секрете ключи; шифровать информацию с помощью различных криптосистем.	**Знание** основных понятий курса, современных подходов к защите информации, математических основ криптографических алгоритмов. **Умение** использовать средства для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; **Владеть** передавать в секрете ключи; шифровать информацию с	**Знание** основных понятий курса, современных подходов к защите информации, математических основ криптографических алгоритмов. **Умение** использовать средства для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; **Владеть** передавать в секрете ключи; шифровать информацию с помощью различных криптосистем. задавать псевдослучайную последовательность для потокового кодирования.	**Знание** основных понятий курса, современных подходов к защите информации, математических основ криптографических алгоритмов. **Умение** использовать средства для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; **Владеть** передавать в секрете ключи; шифровать информацию с помощью различных криптосистем. задавать псевдослучайную последовательность для потокового кодирования.

			задать псевдослучайную последовательность для потокового кодирования **Владеть** методами защиты информации от несанкционированного доступа методами создания ЭЦП для документа	помощью различных криптосистем. задавать псевдослучайную последовательность для потокового кодирования.		
Профессиональные компетенции						
ПК-1	Контрольные работы 1,2. Зачет.	1-4	**Знать:** целый класс схем для создания ЭЦП; способы проверки числа на простоту симметрических методах (DES,IDEA и т.д.); **Уметь:** проводить доказательства справедливости умозаключений в различных неклассических логиках высказываний; задать псевдослучайную последовательность	**Знание** основных понятий курса, современных подходов к защите информации. **Умение** использовать средства для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; **Владеть** передавать в секрете ключи; шифровать информацию с	**Знание** основных понятий курса, современных подходов к защите информации, математических основ криптографических алгоритмов. **Умение** использовать средства для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; **Владеть** передавать в секрете ключи; шифровать	**Знание** основных понятий курса, современных подходов к защите информации, математических основ криптографических алгоритмов. **Умение** использовать средства для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; **Владеть** передавать в секрете ключи; шифровать информацию с помощью различных криптосистем. задавать псевдослучайную последовательность для потокового кодирования.

			для потокового кодирования **Владеть:** табличной техникой доказательства справедливости логических выводов; методами защиты информации от несанкционированного доступа методами создания ЭЦП для документа.	помощью различных криптосистем. задавать псевдослучайную последовательность для потокового кодирования.	информацию с помощью различных криптосистем. задавать псевдослучайную последовательность для потокового кодирования.	

3. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

3.1 Критерии оценивания степени овладения знаниями, умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

- владение основным объемом знаний по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;
- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знание базовых теорий, концепций и направлений по изучаемой дисциплине;
- самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

- достаточно полные и систематизированные знания в объёме программы дисциплины;
- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;
- самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

- систематизированные, глубокие и полные знания по всем разделам дисциплины;
- точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;

- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;
- способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
- активная самостоятельная работа на практических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

3.2 Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка. Для дисциплин, изучаемых в течение нескольких семестров, оценка может выставляться не только по окончании ее освоения, но и в промежуточных семестрах. Вид оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно», «зачтено», «незачтено») определяется рабочей программой дисциплины в соответствии с учебным планом.

Оценка «отлично» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована на высоком уровне.

Оценка «хорошо» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на продвинутом уровне.

Оценка «удовлетворительно» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «неудовлетворительно» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Оценка «зачет» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «незачтено» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Приложение №2 к рабочей программе дисциплины
«Математические методы защиты информации»

Методические указания для студентов по освоению дисциплины

Формы изучения дисциплины « Математические основы защиты информации и информационной безопасности» традиционны. Это лекции, дополняемые практическими занятиями и самостоятельная работа студента по выполнению домашних работ, подготовке к контрольным работам и зачету. Для лучшего понимания можно сочетать коллективной работы группы с самостоятельной работой студентов, и работать небольшими группами по обсуждению серии взаимосвязанных вопросов и коллективного поиска ответов на них.

Как правило, студенты записывают в свои конспекты излагаемый на доске материал. Составление конспекта лекций и дальнейшая работа с ним при подготовке к занятиям выступает как значительная часть процесса обучения. Практические занятия обычно с лекциями дополняют друг друга. Проводятся в академических группах под руководством преподавателя. Основной целью является формирование у студентов понимания теоретического материала, изложенного на лекции, через решение упражнений и задач. Здесь преподавание строится на разумном для каждой темы сочетании коллективной работы группы с самостоятельной индивидуальной работой студентов. Допустима также работа в небольших группах по обсуждению серии взаимосвязанных вопросов обучаемым и коллективного поиска ответов на них.

Домашние задания подразделяются на текущие (задание к очередному практическому занятию или лекции) и долгосрочные, т.е. задания выдаются на длительный период с обязательным предъявлением результатов. К последним относятся задания, связанные с реализацией моделей на компьютере. Студенты регулярно получают задания по самостоятельному изучению некоторых вопросов курса, а также дополнительных его разделов, по чтению учебной литературы.

Групповые консультации проводятся перед контрольными мероприятиями (контрольные работы, зачетные работы, экзамены) для большой группы студентов с целью систематизации знаний и устранению имеющихся сложностей с пониманием материала общего характера.

Самостоятельная работа реализуется:

1. Непосредственно в процессе аудиторных занятий.
2. В контакте с преподавателем вне рамок расписания - на консультациях по учебным вопросам, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.
3. В библиотеке, дома, и т.д. при выполнении студентом учебных задач.

Перенос активности студентов на работу во внеаудиторное время связан с рядом трудностей, основная из которых - это неготовность к нему большинства студентов, особенно младших курсов. Поэтому на практических занятиях преподаватель старается приучить студента работать самостоятельно, отводя для этого около половины времени на самостоятельное решение задач. Практические занятия строятся следующим образом:

1. Формулировка целей занятия, основных вопросов, которые должны быть рассмотрены.
2. Опрос.
3. Решение нескольких типовых задач у доски.
4. Самостоятельное решение задач.
5. Разбор ошибок при решении (в конце текущего занятия или в начале следующего).

По результатам самостоятельного решения задач и по проверке подготовки студента к практическому занятию (письменный опрос по теории и проверка домашнего задания) студент получает оценку. По материалам темы проводится контрольная работа.

Результаты выполнения этих заданий формируют оценку работы студента в конце семестра, которая составляет часть итоговой оценки на экзамене.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

В качестве учебно-методического обеспечения рекомендуется использовать литературу, указанную в разделе № 7 данной рабочей программы

Также для подбора учебной литературы рекомендуется использовать широкий спектр интернет-ресурсов:

1. Личный кабинет (http://lib.uniyar.ac.ru/opac/bk_login.php) дает возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню «Электронный каталог»; пройти процедуру авторизации, выбрав вкладку «Авторизация», и заполнить представленные поля информации.

2. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

3. Электронная картотека «Книгообеспеченность» (http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php) раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.