МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Кубанский государственный университет»
Факультет компьютерных технологий и прикладной математики

УТВЕРЖДАЮ
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Хагуров Т.А.
подпись
«31» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.09 ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки **01.04.02 Прикладная математика и информатика**

Программа магистратуры Математические и информационные технологии в цифровой экономике

Форма обучения очная

Квалификация (степень) выпускника магистр

Краснодар 2024

Рабочая программа дисциплины «Защита информации» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 01.04.02 Прикладная математика и информатика, программа Математические и информационные технологии в цифровой экономике.

Программу составил: Савин В.Н.,
к.т.н., доцент кафедры прикладной математики

Рабочая программа дисциплины «Защита информации» утверждена на заседании кафедры прикладной математики
протокол № 10 от 20.05.2024 г.

И.о. заведующего кафедрой, к.ф.-м.н.,
А.В. Письменский

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики
протокол № 6 от 21.05.2024 г.

Председатель УМК факультета компьютерных технологий и прикладной математики УМК факультета
А.В. Коваленко, д.ф.-м.н, к.э.н., доцент

Рецензенты:

Шапошникова Татьяна Леонидовна.
Доктор педагогических наук, кандидат физико-математических наук, профессор. Почетный работник высшего профессионального образования РФ. Зав. каф. физики института фундаментальных наук (ИФН) ФГБОУ ВО «КубГТУ».

Марков Виталий Николаевич.
Доктор технических наук. Профессор кафедры информационных систем и программирования института компьютерных систем и информационной безопасности (ИКСиИБ) ФГБОУ ВО «КубГТУ».

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Цели изучения дисциплины определены государственным образовательным стандартом высшего образования и соотнесены с общими целями ООП ВО по направлению подготовки «Прикладная информатика», в рамках которой преподается дисциплина.

Целью дисциплины «Защита информации» является овладение основными методами защиты информации и их применения при решении задач информационной безопасности, умение самостоятельно расширять знания в области защиты информации.

1.2 Задачи дисциплины

- изучение основных понятий и методов решения типовых задач защиты информации;
- овладение практическими навыками в реализации алгоритмов криптографии;
- обучение основам проведения криптоанализа.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации» относится к обязательной части (Б1.О) учебного плана.

Для изучения данной учебной дисциплины (модуля) студент должен владеть обязательным минимумом содержания математической части ООП для данного направления:

знать/понимать

- основные понятия и методы математического анализа, аналитической геометрии, линейной алгебры, принципы алгоритмизации и программирования;
- основы информационной безопасности;

уметь

- применять математические методы для решения практических задач;
- составлять алгоритмы и компьютерные программы;

владеть

- методами решения алгебраических уравнений, аналитической геометрии, теории вероятностей;
- инструментальными средствами программирования.

Вышеуказанные знания, умения и навыки формируются предшествующими дисциплинами:

- Векторная алгебра.
- Математический анализ.
- Основы информационной безопасности.
- Основы программирования.

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся общепрофессиональных компетенций (ОПК):

№ п.п.	Код и наименование компетенции	Индикаторы достижения компетенции		
		знает	**умеет**	**владеет**
1.	ОПК-4 Способен комбинировать и адаптировать существующие информационно-	- основные понятия о погрешности и приближенных вычислениях;	обоснованно выбрать вычислительный метод, разработать алгоритм решения	инструментарием разработки программной реализации

№ п.п.	Код и наименование компетенции	Индикаторы достижения компетенции		
		знает	**умеет**	**владеет**
	коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	- основные требования, предъявляемые к вычислительным схемам: корректность, устойчивость, сходимость;	поставленной задачи в рамках теоретического и экспериментального исследования;	криптографических алгоритмов
2.	ПК-3 Способен эффективно применять алгоритмические и программные решения в области информационно-коммуникационных технологий, а также участвовать в их проектировании и разработке	- криптографические методы защиты информации; - протоколы безопасности	составить и отладить программу на алгоритмическом языке (Паскаль / C++/ Phyton/ Julia) для решения сложных задач (криптографических)	вычислительными методами решения задач линейной алгебры, теории чисел, методами дискретной математики

2 Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 4 зач.ед. (144 часов), их распределение по видам работ представлено в таблице

Вид учебной работы	Трудоемкость, часов
	2 семестр
Контактная работа, в том числе:	**20,3**
Аудиторные занятия:	**20**
Занятия лекционного типа (Л)	10
Занятия семинарского типа (семинары, практические занятия) (ПЗ)	–
Лабораторные работы (ЛР)	10
Иная контактная работа:	**0,3**
Контроль самостоятельной работы (КСР)	–
Промежуточная аттестация (ИКР)	0,3
Самостоятельная работа, в том числе:	**88**
Курсовой проект (КП), курсовая работа (КР)	–
Проработка учебного (теоретического) материала (ПМ)	68
Подготовка к текущему контролю (ПТК)	12
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)	–
Реферат (Р)	8
Контроль: подготовка к экзамену	**35,7**

Общая трудоемкость	**час.**	**144**
	зач. ед.	**4**

2.2 Структура учебной дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые во 2 семестре

№ раздела	Наименование разделов, *тем*	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Системы безопасности с особыми условиями: системы с открытым ключом, разделённый секрет, протокол с нулевым разглашением	46	6	-	6	34
2.	Методы атаки на системы защиты информации и способы противодействия им	42	4	-	4	34
	ИТОГО по разделам дисциплины:	**88**	**10**	**-**	**10**	**68**
	Промежуточная аттестация (ИКР)	0,3				
	Подготовка к текущему контролю (ПТК)	12				
	Реферат (Р)	8				
	Подготовка к текущему контролю	35,7				
	Общая трудоемкость по дисциплине	**144**				

Сокращения: Л – лекции, ПЗ – практические занятия, ЛР – лабораторные работы, СРС – самостоятельная работа студентов.

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Системы безопасности с особыми условиями: системы с открытым ключом, разделённый секрет, протокол с нулевым разглашением	Системы безопасности с особыми условиями: системы с открытым ключом, разделённый секрет, протокол с нулевым разглашением	Тестирование, написание реферата (по желанию)
2.	Методы атаки на системы защиты информации и способы противодействия им	Атака «человек посередине», атака повтором, атака на открытое сообщение, атака на ключи, атака грубой силой, уязвимости системы	Тестирование, написание реферата (по желанию)

2.3.2 Занятия семинарского типа

Семинарские занятия не предусмотрены учебным планом.

2.3.3 Лабораторные занятия

№	Наименование раздела	Содержание раздела (номера и наименования лабораторных работ)	Форма текущего контроля
1	2	3	4
1.	Системы безопасности с особыми условиями: системы с открытым ключом, разделённый секрет, протокол с нулевым разглашением	Системы безопасности с особыми условиями: системы с открытым ключом, разделённый секрет, протокол с нулевым разглашением	Защита ЛР
2.	Методы атаки на системы защиты информации и способы противодействия им	Атака «человек посередине», атака повтором, атака на открытое сообщение, атака на ключи, атака грубой силой, уязвимости системы	Защита ЛР

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены учебным планом.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающегося по дисциплине

Целью самостоятельной работы студента является углубление знаний, полученных в результате аудиторных занятий. Вырабатываются навыки самостоятельной работы. Закрепляются опыт и знания, полученные во время лабораторных занятий. Ниже представлен перечень учебно-методических материалов, которые помогают обучающемуся организовать самостоятельное изучение тем (вопросов) дисциплины по всем видам СРС.

№	Вид самостоятельной работы	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка и повторение лекционного материала, материала учебной и научной литературы, подготовка к семинарским занятиям	Методические указания для подготовки к лекционным и семинарским занятиям, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г. Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г.
2	Подготовка к лабораторным занятиям	Методические указания по выполнению лабораторных работ, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г.
3	Подготовка к решению задач и тестов	Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г.

№	Вид самостоятельной работы	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
4	Подготовка докладов	Методические указания для подготовки эссе, рефератов, курсовых работ, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть расширен и конкретизирован в зависимости от контингента обучающихся.

3 Образовательные технологии

Лекционные материалы реализуются с помощью электронных презентаций. При реализации учебной работы по дисциплине «Вычислительные методы» используются следующие образовательные технологии:

- интерактивная подача материала с мультимедийной системой;
- разбор конкретных исследовательских задач.

Объем интерактивных занятий – 20% от объема аудиторных занятий

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
4	*Л*	Интерактивная подача материала с мультимедийной системой. Обсуждение сложных и дискуссионных вопросов.	*2*
	ЛР	Компьютерные занятия в режимах взаимодействия «преподаватель - студент».	*2*
ИТОГО			*4*

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4 Оценочные и методические материалы

4.1 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Вычислительные методы».

Оценочные средства включает контрольные материалы для проведения текущего контроля в форме тестовых заданий для защиты лабораторных работ, промежуточной аттестации в форме вопросов и заданий к экзамену.

В качестве оценочных средств, используемых для текущего контроля успеваемости, предлагается перечень вопросов по выполненным лабораторным работам, которые прорабатываются в процессе освоения курса. Данный перечень охватывает все основные разделы курса, включая знания, получаемые во время самостоятельной работы. Кроме того, важным элементом технологии является самостоятельное решение студентами и сдача индивидуальных проектных заданий в конце курса. Студент демонстрирует свое решение преподавателю, отвечает на дополнительные вопросы.

4.1.1 Примерные задания для защиты лабораторных работ

1) Даны k точек по (k, n) пороговой схеме. Восстановить секретное число по заданным точкам.
2) Сгенерировать k-значное простое число (метод Миллера-Рабина).
3) Рассчитать открытый и закрытый ключ для RSA по следующим данным: p, q, e.
4) Найти ключ RSA с помощью одной из атак: повторным шифрованием, на основе китайской теоремы об остатках.
5) На эллиптической кривой $E_p(a,b): y^2 = x^3 + ax + b\ (mod\ p)$ сложить заданные точки.
6) Найти порядок эллиптической кривой.
7) Найти k P для заданной точки P эллиптической кривой.
8) Подготовить цифровые конверты для слепой подписи по следующим данным p,q,r,s.
9) Подписать «вслепую» чек на s руб. Подготовить цифровые конверты для слепой подписи по следующим данным: p, q, e, r, s. Предварительно нужно проверить одинаковость суммы во вскрытых конвертах.

Примеры задач:

1) Даны 7 точек по (4, 7) пороговой схеме:
{1, 21120}, {2, 23629}, {3, 2282}, {4, 10064}, {5, 12297}, {6, 3524}, {7, 7509}. Восстановить секретное число по точкам 1, 2, 4, 6
m=a[0]=212, a[1]=13678, a[2]=22750, a[3]=13701, a[4]=16027 – случайный секретный многочлен
По точкам 1, 2, 4, 6 составляем интерполяционный многочлен Лагранжа
L 1 = 26736+2196 x+8362 x^2+21149 x^3 ,
L 2 = 25177+28655 x+15231 x^2+18600 x^3 ,
L 3 = 15972+2114 x+27320 x^2+13036 x^3 ,
L 4 = 19779+25477 x+7529 x^2+5657 x^3 ,
f= 212+13678 x+22750 x^2+13701 x^3
Свободный член многочлена f является искомым секретом.
Ответ. 212.

2) Выполняется по алгоритму без исходных данных (достаточно длины числа), например,

сгенерировать 100-значное простое число.

3) Дано: (p,q,e)= (24329, 46817, 2027)
Находим (p,q,n,fi,e,d) = (24329, 46817, 1139010793, 1138939648, 2027, 909690819)
Ответ. Открытый ключ (e, n) = (2027, 1139010793),
закрытый ключ (d, n) = (909690819, 1139010793)

4) На эллиптической кривой $E_{5693}(3,5): y^2 = x^3 + 3x + 5\ (mod\ 5693)$ сложить точки (2709, 5404) и (4803, 5595). Ответ. (305, 2879)

5) Найти порядок кривой $E_{5693}(3,5)$. Ответ. 5662.

6) Также найти 327P для заданной точки P = $(3208,5364)$.
327P = 256P + 64P + 4P + 2P + P
2P=(3962, 5424), 4P=(4858, 3641), 8P=(5182, 3286), 16P=(2632, 2764), 32P=(2280, 4493), 64P=(73, 2906), 128P=(4288, 1078), 256P=(667, 4345), 3P=(1423, 3461), 7P=(1190, 5128), P71=(2820, 2725), P357=(1117, 1914) Ответ. 357 P = (1117, 1914).

7) Найти порядок заданной точки P = (2353, 466), зная, что порядок кривой $E_{5693}(2,5)$ равен 5687.
$5687 = 11^2 \cdot 47$. Делители: {1, 11, 47, 121, 517, 5687}

$$\frac{5687}{47} = 121, \frac{5687}{11} = 517, \qquad 121 = 1 + 8 + 16 + 32 + 64, \qquad 517 = 1 + 4 + 512$$

2P=(3565, 1484), 4P=2·2P=(4637, 2460), 8P=(5596, 1529), 16P=(1244, 1542), 32P=(3483, 1164), 64P=(2594, 1401), 128P=(2522, 771), 256P=(5514, 1728), 512P=(252, 5022), 5P=(3806, 773), 517P=(3375, 3442), 9P=(3326, 1599), 25P=(2139, 1805), 57P=(5627, 5416), 121P=(97, 4964).

8) (s,k,p,q,n,fi,e,d) = (5000 , 4 , 12347, 433, 5346251, 5333472, 751, 369295)
Случайные числа r={4887697, 5151826, 636226, 5233748}
Конверты y={ 4480105, 2324865, 3517314, 5259449}
Банк выбирает случайный конверт t = 2 и получает все случайные числа, кроме выбранного числа r={4887697, ?, 636226, 5233748} и проверяет, что в конверте зашифрована указанная сумма {5000, ?, 5000, 5000} после этого вслепую подписывает выбранный конверт f = 891939. Покупатель извлекает подписанный чек md=4334714. После этого банк при предъявлении подписанного чека проверяет его открытым ключом банка $md^e\ mod\ n\ =\ s$.

4.2 Фонд оценочных средств для проведения промежуточной аттестации

4.2.1 Примерный перечень вопросов к экзамену

1. Задачи защиты информации.
2. Методы защиты информации (правовые, математические, технические) и их практическая значимость.
3. Обмен ключами по открытым каналам связи (алгоритм Диффи-Хеллмана).
4. Практические аспекты использования шифрсистем с открытым ключом.
5. Генерация простых чисел. Метод Миллера-Рабина.
6. Система открытого шифрования RSA.
7. Атаки на RSA (методы взлома).
8. Система открытого шифрования на основе эллиптических кривых.
9. Алгоритмы цифровых подписей. Общие положения. Цифровые подписи на основе шифрсистем с открытым ключом. ГОСТ Р 34.10-2012

10. Система с разделением секрета.
11. Электронные деньги (подпись «вслепую»).
12. Аутентификация и идентификация
13. Протокол аутентификации с нулевым разглашением.
14. Хэширование. Радужные таблицы.
15. Квантовые алгоритмы шифрования.
16. О теоретико-информационном подходе в криптографии. Энтропия и количество информации. “Ненадёжность шифра”, “ложные ключи” и “расстояние единственности”. Практически стойкие шифры.
17. Типовые генераторы псевдослучайных последовательностей. Конгруэнтные генераторы. Генераторы Фибоначчи. Генераторы, основанные на сложнорешаемых задачах теории чисел.
18. Генераторы на основе линейных регистров сдвига и методы их взлома.
19. Линейные рекуррентные последовательности (ЛРП) над полем. Свойства ЛРП максимального периода. Линейная сложность псевдослучайной последовательности. Алгоритм Берлекемпа-Месси.
20. Методы усложнения ЛРП. Фильтрующие и комбинирующие генераторы, и их свойства. Композиции линейных регистров сдвига.

4.2.2 Критерии оценки

Оценка «отлично»:

– систематизированные, глубокие и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы;

– точное использование научной терминологии систематически грамотное и логически правильное изложение ответа на вопросы;

– безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач;

– выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации;

– полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине;

– умение ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин;

– творческая самостоятельная работа на практических/семинарских/лабораторных занятиях, активное участие в групповых обсуждениях, высокий уровень культуры исполнения заданий;

– высокий уровень сформированности заявленных в рабочей программе компетенций.

Оценка «хорошо»:

– достаточно полные и систематизированные знания по дисциплине;

– умение ориентироваться в основном теориях, концепциях и направлениях дисциплины и давать им критическую оценку;

– использование научной терминологии, лингвистически и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;

– владение инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач;

– усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине;

– самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий;

– средний уровень сформированности заявленных в рабочей программе компетенций.

Оценка «удовлетворительно»:

– достаточный минимальный объем знаний по дисциплине;

– усвоение основной литературы, рекомендованной учебной программой;

– умение ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку;

– использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок;

– владение инструментарием учебной дисциплины, умение его использовать в решении типовых задач;

– умение под руководством преподавателя решать стандартные задачи;

– работа под руководством преподавателя на практических занятиях, допустимый уровень культуры исполнения заданий;

– достаточный минимальный уровень сформированности заявленных в рабочей программе компетенций.

Оценка «неудовлетворительно»:

– фрагментарные знания по дисциплине;

– отказ от ответа (выполнения письменной работы);

– знание отдельных источников, рекомендованных учебной программой по дисциплине;

– неумение использовать научную терминологию;

– наличие грубых ошибок;

– низкий уровень культуры исполнения заданий;

– низкий уровень сформированности заявленных в рабочей программе компетенций.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть дополнен и конкретизирован в зависимости от контингента обучающихся.

5 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1 Основная литература

1. Фомичев, В. М. Криптография — наука о тайнописи: учебное пособие / В. М. Фомичев. - Москва: Прометей, 2020. - 66 с. - ISBN 978-5-00172-040-9. - Текст: электронный. - Режим доступа: https://znanium.com/read?id=389799

2. Бабаш, А. В. Криптографические методы защиты информации.Т.1:Уч.-метод.пос./Бабаш А. В., 2-е изд. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 413 с.: - (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст: электронный. - Режим доступа: https://znanium.com/read?id=334834

3. Нестеров С. А. Основы информационной безопасности: Учебное пособие. – 3е изд., стер. – СПб.: Издательство «Лань», 2017. – 324 с. – (Учебники для вузов. Специальная литература).ISBN 978-5-8114-2290-6.

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.2 Дополнительная литература

4. Криптографическая защита информации: учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. С.О. Крамарова. — Москва: РИОР: ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст: электронный. - Режим доступа: https://znanium.com/read?id=416723

6 Методические указания для обучающихся по освоению дисциплины

Учебная деятельность проходит в соответствии с графиком учебного процесса. Процесс самостоятельной работы контролируется во время аудиторных занятий и индивидуальных консультаций. Самостоятельная работа студентов проводится в форме изучения отдельных теоретических вопросов по предлагаемой литературе.

По желанию студента предлагается написание реферата на выбранную им тему (по согласованию с преподавателем). Для написания реферата необходимо подобрать литературу. Общее количество литературных источников, включая тексты из Интернета, (публикации в журналах), должно составлять не менее 10 наименований. Учебники, как правило, в литературные источники не входят.

Рефераты выполняют на листах формата А4. Страницы текста, рисунки, формулы нумеруют, рисунки снабжают порисуночными надписями. Текст следует печатать шрифтом №14 с интервалом между строками в 1,5 интервала, без недопустимых сокращений. В конце реферата должны быть сделаны выводы.

В конце работы приводят список использованных источников.

Реферат должен быть подписан студентом с указанием даты ее оформления.

Работы, выполненные без соблюдения перечисленных требований, возвращаются на доработку.

Выполненная студентом работа определяется на проверку преподавателю в установленные сроки. Если у преподавателя есть замечания, работа возвращается и после

исправлений либо вновь отправляется на проверку, если исправления существенные, либо предъявляется на ее защите.

Примерные темы рефератов:

1. Атаки по побочным данным.
2. Система шифрования с разделённым ключом.
3. Протоколы с нулевым разглашением.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

7.1 Перечень информационно-коммуникационных технологий

– Проверка домашних заданий и консультирование посредством ЭИОС, электронной почты и социальной сети «ВКонтакте».

– Использование электронных презентаций при проведении лекционных и лабораторных занятий.

7.2 Перечень лицензионного и свободно распространяемого программного обеспечения

1. Операционная система MS Windows.
2. Интегрированное офисное приложение MS Office.
3. Система программирования MS Visual Studio или Delphi.

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

1. Википедия, свободная энциклопедия – Wikipedia [Электронный ресурс]. - URL: http://ru.wikipedia.org.
2. Электронная библиотека КубГУ [Электронный ресурс]. - URL: http://www.kubsu.ru/ru/node/1145.
3. Электронная библиотечная система eLIBRARY.RU [Электронный ресурс]. - URL: http://www.elibrary.ru.
4. Профессиональная база данных zbMath [Электронный ресурс]. - URL: https://zbmath.org/.

8 Материально-техническое обеспечение по дисциплине

№	Вид работ	Материально-техническое обеспечение дисциплины и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук), соответствующим программным обеспечением, а также необходимой мебелью (доска, столы, стулья) (аудитории: 129, 131, 133, А305, А307)

2.	Лабораторные занятия	Лаборатория, укомплектованная специализированной мебелью, техническими средствами обучения (современными ПЭВМ на базе процессоров Intel или AMD, объединёнными локальной сетью) с выходом в глобальную сеть Интернет, а также современным лицензионным программным обеспечением (операционная система Windows 8/10, пакет Microsoft Office, среды программирования MS Visual Studio и Delphi) (аудитории: 101, 102, 105, 106, 107, А301а)
3.	Групповые (индивидуальные) консультации	Аудитория для семинарских занятий, групповых и индивидуальных консультаций, укомплектованные необходимой мебелью (доска, столы, стулья) (аудитории: 129, 131)
4.	Текущий контроль, промежуточная аттестация	Аудитория для семинарских занятий, текущего контроля и промежуточной аттестации, укомплектованная необходимой мебелью (доска, столы, стулья) (аудитории: 129, 131, 133, А305, А307, 147, 148, 149, 150, 100С, А3016, А512), компьютерами с лицензионным программным обеспечением и выходом в интернет (аудитории: 106, 106а. А301)
5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети Интернет, программой экранного увеличения, обеспеченный доступом в электронную информационно-образовательную среду университета, необходимой мебелью (доска, столы, стулья) (аудитория 102а, читальный зал).