МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
Государственное образовательное учреждение высшего образования Московской области
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ОБЛАСТНОЙ УНИВЕРСИТЕТ
(МГОУ)
Физико-математический факультет
Кафедра вычислительной математики и методики преподавания информатики

Согласовано управлением организации и контроля качества образовательной деятельности
«08» мая 2020 г.
Начальник управления _____
/М.А. Миненкова /

Одобрено учебно-методическим советом
Протокол «10» мая 2020 г. № 07
Председатель _____
/Г.Е. Суслин /

Рабочая программа дисциплины
Математические основы защиты информации и информационной безопасности

Направление подготовки
44.04.01 Педагогическое образование

Программа подготовки:
Информатика в образовании

Квалификация
Магистр

Форма обучения
Очная

Согласовано учебно-методической комиссией физико-математического факультета:
Протокол «11» мая 2020 г. № 10
Председатель УМКом _____
/Н.Н. Барабанова/

Рекомендовано кафедрой вычислительной математики и методики преподавания информатики
Протокол от «20» мая 2020 г. № 10
Зав.кафедрой _____
/М.В. Шевчук /

Мытищи
2020

Авторы-составители:
Шевчук М. В. кандидат физико-математических наук, доцент
Шевченко В. Г. кандидат педагогических наук, доцент

Рабочая программа дисциплины «Математические основы защиты информации и информационной безопасности» составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 44.04.01 Педагогическое образование, утверждённого приказом МИНОБРНАУКИ России от 22.02.2018 г. № 126.

Дисциплина входит в Блок ФДТ «Факультативные дисциплины (модули)» и является факультативной дисциплиной.

Год начала подготовки (по учебному плану) 2020

СОДЕРЖАНИЕ

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

1.1. Цель и задачи дисциплины

Целью освоения дисциплины «Математические основы защиты информации и информационной безопасности» является изучение основных вопросов криптографии и стеганографии, необходимых для обеспечения компьютерной безопасности информации, защиты информации от несанкционированного допуска и обеспечения конфиденциальности обмена информацией в информационно-вычислительных системах, рассмотрение математических основ современных криптосистем и методов их криптоанализа.

Задачи дисциплины:

- формирование представлений о методах и алгоритмах шифрования;
- изучение математических основ криптографии;
- формирование и развитие компетенций, знаний, практических навыков и умений в области систем криптографии и шифрования;
- изучение стандартов, протоколов и алгоритмов шифрования.

1.2. Планируемые результаты обучения

В результате освоения данной дисциплины у обучающихся формируются следующие компетенции:

СПК-6. Способен самостоятельно осуществлять научное исследование и применять его результаты при решении конкретных научно-исследовательских задач.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в Блок ФДТ «Факультативные дисциплины (модули)» и является факультативной дисциплиной.

Компетенции, знания, навыки и умения, полученные в ходе изучения дисциплины, должны всесторонне использоваться и развиваться студентами в процессе последующей профессиональной деятельности при использовании языков программирования, системного и прикладного программного обеспечения для решения профессиональных задач.

3. ОБЪЕМ И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем дисциплины

Показатель объема дисциплины	Кол-во часов

	очная
Объем дисциплины в зачетных единицах	2
Объем дисциплины в часах	72
Контактная работа:	20,2
Лекции	4
Лабораторные занятия	16
Контактные часы на промежуточную аттестацию:	0,2
Зачет	0,2
Самостоятельная работа	44
Контроль	7,8

Форма промежуточной аттестации: зачет в 3 семестре.

3.2. Содержание дисциплины

Наименование разделов (тем) дисциплины с кратким содержанием	**Количество часов**	
	Лекции	**Лабораторные занятия**
Тема 1. Введение в информационную безопасность Информационная безопасность. Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность. Методы информационной безопасности: физические, организационно-правовые и технические средства защиты. Сервисы информационной безопасности: аутентификация, авторизация и аудит. Угрозы информационной безопасности. Классификация угроз информационной безопасности: по природе возникновения, по степени преднамеренности, по месторасположению, по степени вреда, наносимого информационной системе.	0,5	2
Тема 2. Основные понятия криптографии и криптографические протоколы Отправитель и получатель. Стенография. Сообщения и шифрование. Дешифрование. Криптография. Криптоанализ. Криптоаналитики. Алгоритмы и ключи. Криптосистема. Симметричные алгоритмы. Потоковые алгоритмы. Потоковые шифры. Блочные алгоритмы. Блочные шифры. Открытый ключ.	0,5	2

Закрытый ключ. Вскрытие ключа. Подстановочные и перестановочные шифры. Протокол. Криптографический протокол. Арбитражный протокол. Самодостаточный протокол. Передачи информации с использованием симметричной криптографии. Однонаправленные функции. Цифровые подписи. Обмен ключами. Удостоверение подписи. Криптографическая защита баз данных. Службы меток времени. Подписи по доверенности. Групповые подписи. Подписи с обнаружением подделки. Вычисления с зашифрованными данными. Электронная почта с подтверждением. Безопасные вычисления с несколькими участниками. Анонимная широковещательная передача сообщений. Электронные наличные.		
Тема 3. Криптографические методы и типы алгоритмов Классификация критографических методов защиты информации. Длина симметричного ключа. Длина открытого ключа. Сравнение длин симметричных и открытых ключей. Генерация ключей. Нелинейные пространства ключей. Передача ключей. Проверка ключей. Использование ключей. Обновление ключей. Хранение ключей. Резервные ключи. Время жизни ключей. Управление открытыми ключами. Режим электронной шифровальной книги. Повтор блока. Потоковые блоки. Самосинхронизирующиеся потоковые шифры. Режим обратной связи по шифру. Синхронные потоковые шифры. Режим выходной обратной связи. Режим счетчика. Выбор режима шифра. Выбор алгоритма. Шифрование коммуникационных каналов. Шифрование хранимых данных. Компрессия, кодирование и шифрование. Скрытие шифротекста в шифротексте.	0,5	2
Тема 4. Математические основы криптографии Энтропия и неопределенность. Норма языка. Избыточность. Безопасность криптосистемы. Расстояние уникальности. Практическое использование теории информации. Путаница и диффузия. Вычислительная сложность алгоритмов. Линейный алгоритм. Постоянный алгоритм. Полиномиальный алгоритм. Экспоненциальный алгоритм. Сложность проблем и классы сложности. Арифметика вычетов. Метод Монтгомери. Алгоритм Баррета. Дискретный логарифм. Наибольший общий делитель. Алгоритм Эвклида. Малая теорема Ферма. Функция Эйлера. Китайская теорема об остатках. Квадратичные вычеты. Вычисление в поле Галуа. Разложение на множители. Генерация простого числа. Дискретные логарифмы в конечном	0,5	2

поле.		
Тема 5. Стандарты шифрования данных DES Исторические этапы разработки и принятия стандартов шифрования. Блочный шифр DES. Схема алгоритма блочного шифра DES. Дешифрование DES. Аппаратные и программные реализации блочного шифра DES. Безопасность DES. Дифференциальный и линейный криптоанализ. Криптоанализ со связанными ключами. Реальные критерии проектирования. Варианты DES. Блочные шифры: LUCIFER, MADRYGA, REDOC, MMB, ГОСТ, CAST, BLOWFISH, CRAB, RC5.	0,5	2
Тема 6. Однонаправленные хэш-функции Устойчивость к столкновениям. Длины однонаправленых хэш-функций. Обзор однонаправленых хэш-функций. Однонаправленная хэш-функция Snefru. Алгоритм N-хэш. Однонаправленная хэш-функция MD4. Однонаправленная хэш-функция MD5. Алгоритм безопасного хэширования SHA. Однонаправленная хэш-функция переменно длины HAVAL. Однонаправленные хэш-функции, использующие симметричные блочные алгоритмы. Скорость хэширования. Выбор однонаправленной хэш-функции. Коды проверки подлинности сообщения.	0,5	2
Тема 7. Криптосистемы с открытым ключом и алгоритмы обмена ключами Алгоритм цифровой подписи DSA. Варианты DSA. Алгоритм цифровой подписи ГОСТ. Схемы цифровой подписи с использованием дискретных алгоритмов. Схема цифровой подписи ESIGN. Клеточные автоматы. Схемы идентификации: FEIGE-FIAT-SHAMIR, GUILLOU-QUISQUATER, SCHNORR. Преобразование схем идентификации в схемы подписи. Алгоритм с открытым ключом DIFFIE-HELLMAN. Обмен ключом без обмена ключом. Протокол «точка-точка». Трехпроходный протокол Шамира. Обмен зашифрованными ключами. Защищенные переговоры о ключе. Распределение ключа для конференции и секретная широковещательная передача.	0,5	2
Тема 8. Специальные алгоритмы для протоколов Криптография с несколькими открытыми ключами. Алгоритмы разделения секрета. Неотрицаемые цифровые подписи. Подписи, подтверждаемые доверенным лицом. Вычисления с зашифрованными данными. Честные и отказоустойчивые криптосистемы. Слепые подписи. Передача с забыванием.	0,5	2

Безопасные вычисления с несколькими участниками. Вероятностное шифрование. Квантовая криптография.		
Итого	4	16

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Темы для самостоятельного изучения	Изучаемые вопросы	Кол-во часов	Формы самостоятельной работы	Методические обеспечения	Формы отчетности
Классические криптосистемы.	Основные понятия. Области применения.	4	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
Блочные шифры.	Основные понятия. Области применения.	4	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
Элементы алгебраической геометрии.	Основные понятия. Области применения.	4	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
Системы RSA.	Основные понятия. Области применения.	4	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
Шифрование с открытым ключом.	Основные понятия. Области применения.	4	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
Электронно-цифровая подпись.	Основные понятия. Области применения.	4	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
Алгебраические методы криптоанализа.	Основные понятия. Области применения.	4	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
Итого		28			

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

5.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и наименование компетенции	Этапы формирования
СПК-6. Способен самостоятельно осуществлять научное исследование и применять его результаты при решении конкретных научно-исследовательских задач	1. Работа на учебных занятиях. 2. Самостоятельная работа.

5.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Оцениваемые компетенции	Уровень сформированности	Этап формирования	Описание показателей	Критерии оценивания	Шкала оценивания
СПК-6	Пороговый	1. Работа на учебных занятиях 2. Самостоятельная работа	Знать методы осуществления научных исследований Уметь самостоятельно осуществлять научное исследование и применять его результаты при решении конкретных научно-исследовательских задач	Тестирование, конспект	Шкала оценивания тестирования Шкала оценивания конспекта
	Продвинутый	1. Работа на учебных занятиях 2. Самостоятельная работа	Знать методы осуществления научных исследований Уметь самостоятельно осуществлять научное исследование и применять его результаты при решении конкретных научно-исследовательских задач Владеть умением самостоятельно осуществлять научное исследование и применять его результаты при решении конкретных научно-	Тестирование, конспект, лабораторные работы	Шкала оценивания тестирования Шкала оценивания конспекта Шкала оценивания практической работы

Оцениваемые компетенции	Уровень сформированности	Этап формирования	Описание показателей	Критерии оценивания	Шкала оценивания
			исследовательских задач		

Критерии и шкала оценивания практических работ

Критерий оценивания	Баллы
Задание выполнено полностью, оформлено по образцу, соответствует предъявляемым требованиям (к каждому заданию предъявляются свои требования, прописанные перед каждым заданием в электронном курсе)	3
Задание выполнено полностью, но есть неточности в оформлении материала или совсем не соответствует требованиям, предъявляемым к оформлению	2
Задание выполнено не полностью или есть неточности в выполнении, есть неточности в оформлении материала или совсем не соответствует требованиям, предъявляемым к оформлению	1
Максимальное количество баллов	3

Критерии и шкала оценивания конспекта

Критерии оценивания	Баллы
Текст конспекта логически выстроен и точно изложен, ясен весь ход рассуждения	1
Даны ответы на все поставленные вопросы, изложены научным языком, с применением терминологии	1
Ответ на каждый вопрос заканчиваться выводом, сокращения слов в тексте отсутствуют (или использованы общепринятые)	0,5
Оформление соответствует образцу. Представлены необходимые таблицы и схемы	0,5
Максимальное количество баллов	3

5.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для тестовых заданий

Выберите один правильный ответ.

1. Документ, в котором информация представлена в электронно-цифровой форме:
   a) электронная цифровая подпись
   b) быстрая цифровая подпись
   c) электронный документ

Выберите один правильный ответ.

2. Что входит в схему электронной подписи:
   a) алгоритм генерации ключевых пар пользователя
   b) функции обработки подписи
   c) функцию вычисления подписи
   d) функцию удаления подписи
   e) функцию проверки подписи

Выберите один правильный ответ.

3. Для чего в асимметричном методе шифрования используется несекретный
   a) расшифрования
   b) шифрования
   c) аутентификации
   d) конфиденциальности

4. *Соотнесите* понятия и определения:

1) Код	a) Операция, обратная кодированию, восстановление информации в первичном алфавите по полученной последовательности кодов.
2) Кодирование	b) Знаки вторичного алфавита, используемы для представления знаков или их сочетаний первичного алфавита
3) Декодирование	c) Перевод информации, представленной посредством первичного алфавита, в последовательность кодов.

Выберите один правильный ответ.

5. Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации _ это…
   a) электронный документ
   b) электронная цифровая подпись
   c) ключ электронной цифровой подписи

Выберите один правильный ответ.

6. Какие ключи используются в асимметричном методе шифрования:
   a) секретный
   b) несекретный
   c) секретный и несекретный

Выберите один правильный ответ.

7. Для чего в асимметричном методе шифрования используется секретный ключ:
   a) расшифрования
   b) шифрования
   c) аутентификации
   d) конфиденциальности

Выберите один правильный ответ.

8. 1 байт = ... бит.
   a) 8
   b) 16
   c) 4
   d) 32

Вставьте пропущенное слов.

9. _____ - раздел математики, в котором изучаются и разрабатываются системы изменения письма с целью сделать его непонятным для непосвященных лиц.

Примерный вариант практической работы

1. Создать контрольные суммы для любых пяти файлов, используя методы хеширования с помощью HashTab согласно варианту из таблицы заданий (стр. 87) и заполнить таблицу результатов:

	Алгоритм	Расшифровка	Значение хеш-сумм
Название_файла1.расширение			
Название_файла2.расширение			
Название_файла3.расширение			
Название_файла4.расширение			
Название_файла5.расширение			

2. Сравнить контрольные суммы MD5 пяти любых файлов, созданные с помощью HashTab и FreeCommander, результаты представить в таблице:

3.

№	Название файла с расширением	FreeCommander	HashTab

Примерные вопросы к зачету (проводится в устной форме)

1. Основные понятия криптографии.
2. Подстановочные шифры.
3. Перестановочные шифры.
4. Компьютерные алгоритмы.
5. Основные криптографические протоколы.
6. Передача информации с использованием симметричной криптографии.
7. Однонаправленные функции.
8. Передача информации с использованием криптографии с открытыми ключами.
9. Цифровые подписи.
10. Протокол обмена ключами.
11. Удостоверение подлинности и обмен ключами.
12. Формальный анализ протоколов проверки подлинности и обмена ключами.
13. Криптографическая защита баз данных.
14. Промежуточные протоколы.
15. Электронная почта с подтверждением.
16. Безопасные вычисления с несколькими участниками.
17. Анонимная широковещательная передача сообщений.
18. Длинна симметричного и открытого ключа.
19. Управление ключами.
20. Типы алгоритмов.
21. Криптографические режимы.
22. Выбор алгоритма.
23. Шифрование коммуникационных каналов.
24. Шифрование хранимых данных.
25. Компрессия, кодирование и шифрование.
26. Скрытие шифртекста в шифртексте.
27. Теория информации.
28. Теория сложности.
29. Теория чисел.
30. Разложение на множители.
31. Генерация простого числа.
32. Дискретные логарифмы в конечном поле.
33. Стандарт шифрования данных DES.
34. Блочные шифры: LUCIFER, MADRYGA, REDOC, RC2, MMB.
35. Блочные шифры: ГОСТ, CAST, BLOWFISH, RC5.
36. Использование однонаправленных хэш-функций.
37. Объединение блочных шифров.
38. Однонаправленные хэш-функции: Snefru, N-хэш, MD4, MD5.
39. Алгоритм безопасного хэширования SHA.

40. Алгоритм цифровой подписи DSA.
41. Клеточные автоматы.
42. Преобразование схем идентификации в схемы подписи.
43. Криптография с несколькими открытыми ключами.
44. Неотрицаемые цифровые подписи.
45. Честные и отказоустойчивые криптосистемы.

5.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура оценивания знаний и умений состоит из следующих составных элементов: учета посещаемости лекционных занятий, подготовки конспектов, выполнения практических работ, тестирования.

Требования к выполнению практических работ

Перед выполнением практической работы требуется получить вариант задания. Далее необходимо ознакомиться с заданием. Выполнение практической работы следует начать с изучения теоретических сведений, которые приводятся в соответствующих методических указаниях. Практическая работа считается выполненной, если: предоставлен отчет о результатах выполнения задания; проведена защита проделанной работы.

Защита работ проводится в два этапа: демонстрируются результаты выполнения задания, в случае лабораторной работы, предусматривающей разработку программного приложения при помощи тестового примера доказывается, что результат, получаемый при выполнении программы правильный, далее требуется ответить на ряд вопросов из перечня контрольных вопросов, который приводится в задании на работу.

Вариант задания выдается преподавателем, проводящим практические занятия. Отчет должен содержать следующие элементы: название работы, цель, задание, основную часть, вывод по работе. Требования к оформлению и выполнению работы определены в методических рекомендациях.

Требования к выполнению самостоятельных работ

Целью выполнения самостоятельных работ (конспектов по тематике курса) является проработка соответствующих разделов курса посредством самостоятельного решения каждой задачи.

Конспект считается выполненным, если он предоставлен в соответствии с требованиями, является полным и имеет план. Требования к оформлению и выполнению работы определены в методических рекомендациях.

Промежуточная аттестация по дисциплине учитывает уровень результатов обучения, общее качество работы, самостоятельность. Освоение дисциплины оценивается по балльной шкале.

Общее количество баллов по дисциплине - 100 баллов.

Максимальное количество баллов, которое можно набрать в течение семестра за посещаемость, выполнение практических работ и самостоятельных работ, тестирование - 86 баллов.

За посещение лекционных занятий и написание конспектов магистрант может набрать максимально до 4 баллов.

За выполнение практических работ магистрант может набрать максимально 18 баллов (всего 6 лабораторных работ, по 3 балла за одну работу).

За выполнение самостоятельных работ магистрант может набрать максимально 24 балла (всего 8 конспектов, по 3 балла за один конспект).

За тестирование магистрант может набрать максимально 40 баллов (20 вопросов по 2 балла за один вопрос).

Обучающийся, набравший 41 балл и более, допускается к зачету. Максимальная сумма баллов, которые магистрант может набрать при сдаче экзамена, составляет 14 баллов.

Требования к зачету

Для допуска к зачету по дисциплине необходимо выполнить все требуемые пункты отчетности. Существенным моментом является посещаемость занятий (в случае пропусков занятий предполагается более подробный опрос по темам пропущенных занятий). На зачет выносится материал, излагаемый в лекционном курсе и рассматриваемый на лабораторных занятиях. Для получения зачета необходимо правильно ответить на несколько поставленных вопросов. В затруднительных ситуациях (в отдельных случаях) допускается на зачете воспользоваться тетрадью с записью материалов лекций в присутствии преподавателя. При этом преподаватель может убедиться, в какой степени студент ориентируется в «своих» материалах, и по ряду дополнительных вопросов (по тетради).

Структура оценивания зачета

Критерии оценивания	Баллы
Ставится, если студент обнаруживает всестороннее, систематическое и глубокое знание программного материала по дисциплине; обстоятельно анализирует структурную взаимосвязь рассматриваемых тем и разделов дисциплины; усвоил основную и знаком с дополнительной литературой, рекомендованной программой, а также усвоил взаимосвязь основных понятий дисциплины в их значении для	20

Критерии оценивания	Баллы
приобретаемой профессии; проявил творческие способности в понимании, изложении и использовании учебного материала.	
Ставится, если студент, обнаруживает полное знание программного материала, успешно выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей образовательной деятельности.	10
Ставится, если студент обнаруживает знание основного программного материала в объеме, необходимом для дальнейшего обучения и профессиональной деятельности; справляется с выполнением заданий, предусмотренных программой; знаком с основной литературой, рекомендованной программой; допускает погрешности непринципиального характера в ответе на экзамене.	5
Ставится в том случае, если студент обнаруживает пробелы в знаниях основного программного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий.	0

Итоговая шкала оценивания результатов освоения дисциплины

Итоговая оценка по дисциплине формируется из суммы баллов по результатам текущего контроля и промежуточной аттестации и выставляется в соответствии с приведенной ниже таблицей.

Оценка по 100-балльной системе	Оценка по традиционной системе
81 – 100	зачтено
61 - 80	зачтено
41 - 60	зачтено
0 - 40	незачтено

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Основная литература

1. Гашков С.Б., Применко Э.А., Черепнев М.А., Криптографические методы защиты информации. [Текст] - М.: Издательство «Академия», 2010. – 304 с.

2. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И., Защита информации. Учебное пособие. [Текст] - М.: Издательство «РИОР», 2013. – 392 с.

3. Мельников В.П., Клейменов С.А., Петраков А.В., Информационная безопасность. [Текст] - М.: Издательство «Академия», 2013. – 336 с.

6.2. Дополнительная литература

1. Баричев С.Г., Гончаров В.В., Серов Р.Е., Основы современной криптографии. [Текст] - М.: Издательство «Горячая линия-Телеком», 2011. – 175 с.

2. Дождиков В.Г., Салтан М.И., Краткий энциклопедический словарь по информационной безопасности. [Текст] - М.: Издательство «Энергия», 2012. – 240 с.

3. Заика А.А., Компьютерная безопасность. [Текст] - М.: Издательство «Рипол КЛассик», 2010. – 304 с.

4. Малюк А., Теория защиты информации. [Текст] - М.: Издательство «Горячая линия-Телеком», 2012. – 184 с.

5. Музыкантский А.И., Фурин В.В., Лекции по криптографии. [Текст] - М.: Издательство «МЦНМО», 2011. – 68 с.

6. Рябко Б.Я., Фионов А.Н., Криптографические методы защиты информации. [Текст] - М.: Издательство «Горячая линия-Телеком», 2012. – 229 с.

7. Рябко Б.Я., Фионов А.Н., Основы современной криптографии и стеганографи. [Текст] - М.: Издательство «Горячая линия-Телеком», 2013. – 232 с.

8. Смирнов А.А., Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза. [Текст] - М.: Издательство «РИОР», 2012. – 159 с.

9. Таранников Ю.В., Комбинаторные свойства дискретных структур и приложения к криптологии. [Текст] - М.: Издательство «МЦНМО», 2011. – 152 с.

10. Чечета С., Введение в дискретную теорию информации и кодирования. Учебное пособие. [Текст] - М.: Издательство «МЦНМО», 2011. – 224 с.

6.3. Ресурсы информационно-телекоммуникационной сети «Интернет»

1. Интернет-Университет Информационных Технологий [Электронный ресурс]. - Режим доступа: http://www.intuit.ru

2. Информационно-образовательная среда «Открытый класс» [Электронный ресурс]. - Режим доступа: http://www.openclass.ru/

3. Конференция «Информационные технологии в образовании» [Электронный ресурс]. - Режим доступа: http://ito.bitpro.ru

4. Методология и технология электронного обучения (обзоры, статьи и др.) [Электронный ресурс]. - Режим доступа: http://cnit.ssau.ru/do/

5. Сайт Министерства образования и науки РФ [Электронный ресурс]. - Режим доступа: www.ed.gov.ru

6. Электронная версия журнала «Вестник образования» Электронный ресурс]. - Режим доступа: www.vestnik.edu.ru

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Методические рекомендации по организации самостоятельной работы магистрантов
2. Методические рекомендации по подготовке к практическим занятиям

8. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Лицензионное программное обеспечение:
Microsoft Windows
Microsoft Office
Kaspersky Endpoint Security
Информационные справочные системы:
Система ГАРАНТ
Система «КонсультантПлюс»
Профессиональные базы данных:
fgosvo.ru
pravo.gov.ru
www.edu.ru
Свободно распространяемое программное обеспечение, в том числе отечественного производства
ОМС Плеер (для воспроизведения Электронных Учебных Модулей)
7-zip
Google Chrome

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины включает в себя:

- учебные аудитории для проведения занятий лекционного и семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные учебной мебелью, доской, демонстрационным оборудованием.

- помещения для самостоятельной работы, укомплектованные учебной мебелью, персональными компьютерами с подключением к сети Интернет и обеспечением доступа к электронным библиотекам и в электронную информационно-образовательную среду МГОУ;

- помещения для хранения и профилактического обслуживания учебного оборудования, укомплектованные мебелью (шкафы/стеллажи), наборами демонстрационного оборудования и учебно-наглядными пособиями.