Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ИНСТИТУТ ЭКОНОМИКИ, МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АНАЛИЗА ДАННЫХ
ОТДЕЛЕНИЕ ПРИКЛАДНОЙ ИНФОРМАТИКИ

кафедра системного анализа и информатики

УТВЕРЖДЕНА

решением кафедры системного анализа и информатики

Протокол №6 от «2» сентября 2019г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.09.01 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

направление подготовки
09.03.03 «Прикладная информатика»
направленность (профиль)
«Прикладная информатика в информационной безопасности»
квалификация
бакалавр
очная форма обучения

Год набора – 2020

Москва, 2020 г.

Автор–составитель: к.т.н.
доцент кафедры Системного анализа и информатики Каширская Е.Н.

Заведующий кафедрой
Системного анализа и информатики Маруев С.А

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина «Криптографические методы защиты информации» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-8	способен программировать приложения и создавать программные прототипы решения прикладных задач	ПК-8.1	Способен анализировать, выбирать, использовать и модифицировать алгоритмы при решении прикладных задач
ПК-22	способен анализировать рынок программно-технических средств, информационных продуктов и услуг для создания и модификации информационных систем	ПК-22.1	Способен выбирать операционные системы, системы управления базами данных, прикладное программное обеспечение, прочие услуги для функционирования ИС в соответствии с заданными требованиями

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Код этапа освоения компетенции	Результаты обучения
ПК-8.1	на уровне знаний: знать положений технологии программирования в части реализации и тестирования программных средств;
	на уровне умений: уметь осуществлять анализ и обоснованный выбор алгоритмов, а также их модификацию при решении прикладных задач;
	на уровне навыков: иметь навыки анализа, выбора, использования и модификации алгоритмов при решении прикладных задач;
ПК-22.1	на уровне знаний: знать актуальных на момент исследования операционных систем, систем управления базами данных, прикладного программного обеспечение;
	на уровне умений: уметь принимать решения по использованию в процессе разработки или модификации ИС тех или иных программных продуктов;
	на уровне навыков: иметь навык выбора поставщиков необходимого программного обеспечения и услуг.

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Объем дисциплины в ЗЕ и академических/астрономических часах – 4 ЗЕ (144/108 ч).
Количество академических/астрономических часов, выделенных на контактную работу по очной форме обучения – 48/36 часов (в т.ч. лекц. - 16 ч., практ.-32 ч.); на самостоятельную работу обучающихся на очной форме – 60/45 часов.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.ДВ.09.01 «Криптографические методы защиты информации» относится к дисциплинам по выбору вариативной части учебного плана по направлению подготовки 09.03.03 Прикладная информатика.
Дисциплина изучается на 4 курсе в 7 семестре (очная форма обучения).
Дисциплина опирается на объём знаний, полученных при изучении таких дисциплин, как Информатика, Программирование и алгоритмизация, Операционные системы, Информационные системы и технологии, Информационная безопасность, Программно-аппаратные средства защиты информации.
Форма промежуточной аттестации –курсовая работа (КР).

3. Содержание и структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Тема 1	Введение в криптографию	7	1		2		4	Д, О
Тема 2	Имитостойкость и помехоустойчивость шифров	15	3		4		8	Д, О

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Тема 3	Принципы построения и реализации крипто-графических алгоритмов	19	3		6		10	Д, О
Тема 4	Шифрование с открытым ключом	19	3		6		10	Д, О
Тема 5	Криптографические протоколы	26	4		8		14	Д, О
Тема 6	Криптосистемы на базе ЭВМ	23	3		6		14	
Промежуточная аттестация		КР 36ч.						КР
Всего академ./астроном.часов:		**108/81**	**16/12**		**32/24**		**60/45**	**36/27**

Примечание: * – формы текущего контроля успеваемости: доклад(ы) (Д), опрос (О).

Содержание дисциплины

№ п/п	Название темы	Основные вопросы и положения, раскрывающие содержание темы
Тема 1	**Введение в криптографию**	Содержание и задачи дисциплины. Ее особенности и связь с другими дисциплинами. Методические рекомендации по ее изучению и требования, предъявляемые при проверке знаний. Общая характеристика процессов защиты информации. Требования к защите, методология разработки и анализа средств зашиты. Классические модели защиты информации. Краткий исторический очерк развития криптографии. Исторические примеры: шифр Цезаря, квадрат Полибия, шифр Виженера, решетка Кардано, книжный шифр и др. Понятие о криптоанализе. Открытые сообщения. Частотные характеристики открытых сообщений. Математические модели открытых сообщений и критерии на открытый текст. Способы представления информации, подлежащей шифрованию. Основные понятия криптографии. Определение шифра и его математические модели. Ручные и машинные шифры. Ключевая система и основные требования к шифрам. Понятие криптосистемы.
Тема 2	**Имитостойкость и помехоустойчивост**	Шифры перестановки. Маршрутные и вертикальные перестановки, решетки и лабиринты.

	ь шифров	Шифры замены. Одноалфавитные и многоалфавитные шифры замены. Поточные и блочные шифры замены. Шифры гаммирования. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Теоретико-информационный подход к оценке стойкости шифров. Надежность ключей. Совершенные шифры. Стойкость шифра и избыточность языка. Имитостойкость и ее характеристики. Методы обеспечения имитостойкости. Помехоустойчивое кодирование. Характеристики помехоустойчивости
Тема 3	**Принципы построения и реализации криптографически х алгоритмов**	Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним. Датчики псевдослучайных последовательностей (регистры сдвига, линейный конгруэнтный метод, линейные рекуррентные последовательности, мультиплексорные методы). Периодичность случайных последовательностей. Распределение элементов в псевдослучайных последовательностях. Основные узлы и блоки криптосистем. Методы анализа криптографических алгоритмов. Алгоритмические, аналитические и статистические методы анализа поточных шифров.
Тема 4	**Шифрование с открытым ключом**	Системы шифрования с открытым ключом. Понятие односторонней функции. Криптосистемы RSA и Эль-Гамаля. Проблема факторизации целых чисел в конечных полях. Криптосистемы с открытым ключом на базе задаче о рюкзаке и линейных кодов. Асимметричные системы шифрования и их преимущества. Хэш-функции и их использование в криптографии.
Тема 5	**Криптографически е протоколы**	Понятие криптографического протокола. Связь стойкости 8 протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Цифровая подпись. Стандарты цифровой подписи Протоколы аутентификации и их связь с цифровой подписью. Протоколы сертификации и предварительного распределения ключей.
Тема 6	**Криптосистемы на базе ЭВМ**	Особенности реализации криптосистем на базе вычислительной техники. Криптографические интерфейсы. Применение смарт-карт в системах электронных платежей. Компьютерная стеганография - метод, дополняющий традиционные криптографические методы. “Полное” скрытие данных. Типы файл-контейнеров (графические, звуковые). Алгоритмы “упаковки” данных (регулярные, псевдослучайные, комбинированные).

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости.

4.1.1. В ходе реализации дисциплины «Криптографические методы защиты информации» используются следующие методы текущего контроля успеваемости обучающихся:

Тема (раздел)	Методы текущего контроля успеваемости
Тема 1	Доклады с презентацией, опрос на практическом занятии
Тема 2	Доклады с презентацией, опрос на практическом занятии
Тема 3	Доклады с презентацией, опрос на практическом занятии
Тема 4	Доклады с презентацией, опрос на практическом занятии
Тема 5	Доклады с презентацией, опрос на практическом занятии
Тема 6	Доклады с презентацией, опрос на практическом занятии

4.1.2. Зачет с оценкой проводится в форме устного ответа на билеты (по 2 вопроса в билете).

4.2. Материалы текущего контроля успеваемости обучающихся

Текущий контроль успеваемости осуществляется непрерывно, на протяжении всего курса. Прежде всего, это устный опрос по ходу лекции, выполняемый для оперативной активизации внимания обучающихся и оценки их уровня восприятия. Помимо этого, контроль самостоятельной работы обучающихся осуществляется при опросе на практических занятиях, докладах с презентацией.

<u>Тема 1.</u> Введение в криптографию

Вопросы для подготовки обучающихся к практическим занятиям
Освоение процесса зашифрования и расшифрования для простейших шифров.
Анализ шифров замены с использованием статистических закономерностей открытых сообщений

<u>Тема 2.</u> Имитостойкость и помехоустойчивость шифров

Вопросы для подготовки обучающихся к практическим занятиям
Шифр Виженера. Шифр Вернама

<u>Тема 3.</u> Принципы построения и реализации криптографических алгоритмов

Вопросы для подготовки обучающихся к практическим занятиям
Расчет мощности ключевой системы различных шифров
Расчет характеристик имитостойкости шифров

<u>Тема 4.</u> Шифрование с открытым ключом

Вопросы для подготовки обучающихся к практическим занятиям
Расчет характеристик помехоустойчивости шифров
Вычисление характеристик датчиков псевдослучайных чисел
Анализ некоторых алгоритмов выработки хэш-функций

<u>Тема 5.</u> Криптографические протоколы

Вопросы для подготовки обучающихся к практическим занятиям
Исследование криптографического
протокола

Тема 6. Криптосистемы на базе ЭВМ

Вопросы для подготовки обучающихся к практическим занятиям
Программная реализация криптографической системы

4.3. Оценочные средства для промежуточной аттестации

4.3.1. Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-8	способен программировать приложения и создавать программные прототипы решения прикладных задач	ПК-8.1	Способен анализировать, выбирать, использовать и модифицировать алгоритмы при решении прикладных задач
ПК-22	способен анализировать рынок программно-технических средств, информационных продуктов и услуг для создания и модификации информационных систем	ПК-22.1	Способен выбирать операционные системы, системы управления базами данных, прикладное программное обеспечение, прочие услуги для функционирования ИС в соответствии с заданными требованиями

4.3.2. Типовые оценочные средства

Промежуточный контроль проводится в форме зачета и предусматривает устный ответ на вопросы по билету.

Код и содержание этапа освоения компетенции	Результаты обучения	Оценочное средство
ПК-8.1 Способен анализировать, выбирать, использовать и модифицировать алгоритмы при решении прикладных задач	на уровне знаний: знать положения технологии программирования в части реализации и тестирования программных средств;	устный опрос
	на уровне умений: уметь осуществлять анализ и обоснованный выбор алгоритмов, а также их модификацию при решении прикладных задач;	устный опрос
	на уровне навыков: иметь навыки анализа, выбора, использования и модификации алгоритмов при решении прикладных задач;	устный опрос
ПК-22.1	на уровне знаний: знать актуальные на момент исследования операционные	устный

Способен выбирать операционные системы, системы управления базами данных, прикладное программное обеспечение, прочие услуги для функционирования ИС в соответствии с заданными требованиями	системы, системы управления базами данных, прикладного программного обеспечения;	опрос
	на уровне умений: уметь принимать решения по использованию в процессе разработки или модификации ИС тех или иных программных продуктов;	устный опрос
	на уровне навыков: иметь навык выбора поставщиков необходимого программного обеспечения и услуг.	устный опрос

Перечень вопросов к экзамену

1. Основные понятия и определения криптографии.
2. Виды криптосистем. Задачи, решаемые методами криптографии.
3. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.
4. История криптографии. Основные этапы становления науки криптографии.
5. Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски.
6. Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ.
7. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу.
8. Композиции шифров. Enigma. Шифр Хейглина.
9. Математическая модель шифра.
10. Атаки и угрозы шифрам.
11. Блочные шифры и их ключевая система. Замены и перестановки. S-P-сеть.
12. Сеть Файстеля. Шифр ГОСТ 28147-89.
13. Конечные кольца и поля многочленов.
14. Шифр SQUARE.
15. Шифр AES
16. Режимы шифрования.
17. Многократное шифрование. Композиция блочных шифров.
18. Совершенные шифры. Пример совершенного шифра.
19. Энтропийные характеристики шифров. Идеальные шифры.
20. Избыточность языка.
21. Оценка числа ложных ключей и расстояние единственности.
22. Безусловно стойкие и вычислительно стойкие шифры.
23. Псевдослучайные последовательности (ПСП). Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ.
24. Поточные шифры. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры.
25. Регистры сдвига с обратной линейной связью (РСЛОС).
26. ПСГ на основе РСЛОС.
27. Шифр Trivium.
28. Нелинейные регистры сдвига.
29. Шифр RC4.
30. Теория имитостойкости Симмонса. Имитация и подмена сообщения. Характеристики имитостойкости. Совершенная имитостойкость.

31. Коды аутентификации сообщений.
32. Защитные контрольные суммы.
33. Криптографические хэш-функции и требования к ним.
34. Подходы к проектированию хэш-функций.
35. Хэш-функции на основе блочного шифра.
36. Схема Меркла-Дамгарда и ГОСТ Р 34.11-2012.
37. Схема «губка» и SHA-3.
38. Коды аутентификации сообщений.
39. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.
40. Криптосистема Диффи-Хэллмана. Пример.
41. Криптосистема RSA. Пример.
42. Криптосистема Эль-Гамаля. Пример.
43. Криптосистема Рабина. Пример.
44. Криптосистема Гольдвассер-Микали. Пример.
45. Криптосистема Блюма-Гольдвассер. Пример.
46. Рюкзачные шифры. Криптосистема Меркла-Хэллмана.
47. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.
48. Подпись RSA, Эль-Гамаля.
49. Подпись Фиата-Шамира.
50. Подпись Онга-Шнорра-Шамира.
51. Неотрицаемая подпись Шаума-ван-Антверпена.
52. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.
53. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка.
54. Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра (ЭЦП) в Z_p к шифру (ЭЦП) на эллиптической кривой.
55. Шифр Эль-Гамаля на эллиптической кривой.
56. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001 (2012), ECDSA.

4.4. Методические материалы

4.4.1. Методические материалы, определяющие процедуру оценивания ответов обучающихся на вопросы на понимание лекционного материала

Критериями оценки ответа обучающихся на лекционном занятии выступают:

- правильность ответов на вопросы преподавателя по изученному материалу;
- полнота и лаконичность ответа;
- степень понимания тематики предмета;
- логика и аргументированность изложения материала;
- приведение примеров, демонстрирующих умение и владение полученными знаниями по темам предмета в раскрытии поставленных вопросов.

4.4.2. Методические материалы, определяющие процедуру оценивания при

проведении опроса на практическом занятии

Оценки **«отлично»** заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание вопроса, умение свободно ориентироваться в теме, усвоивший основную, и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка «отлично» выставляется обучающимся, усвоившим взаимосвязь основных понятий в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

Оценки **«хорошо»** заслуживает обучающийся, обнаруживший полное знание темы, успешно выполняющий предусмотренные программой задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка «хорошо» выставляется обучающимся, показавшим систематический характер знаний по пройденному материалу и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности;

Оценки **«удовлетворительно»** заслуживает обучающийся, обнаруживший знание основного материала в объеме, необходимом для дальнейшего усвоения материала и предстоящей работы по профессии, знакомый с основной литературой, рекомендованной программой.

Оценка **«неудовлетворительно»** выставляется обучающемуся, обнаружившему пробелы в знаниях основного материала темы, допустившему принципиальные ошибки в понимании и изложении учебного материала.

4.4.3. Методические материалы, определяющие процедуру оценивания промежуточной аттестации по дисциплине

Экзамен принимается в устной форме, по билетам. Задание для экзамена включает два теоретических вопроса. Оценка знаний обучающегося на экзамене носит комплексный характер и определяется его:

- ответом на экзамене;
- учебными достижениями в семестровый период.

Знания, умения, навыки обучающегося на зачете оцениваются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой.

Оценивание студента на экзамене по дисциплине
«Криптографические методы защиты информации»

Оценка	Требования к знаниям
Отлично	Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает на зачете, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение. Учебные достижения в семестровый период демонстрируют высокую степень овладения программным материалом.
Хорошо	Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская

	существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. Учебные достижения в семестровый период демонстрируют хорошую степень овладения программным материалом.
Удовлетво-рительно	Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ. Учебные достижения в семестровый период демонстрируют достаточную (удовлетворительную) степень овладения программным материалом.
Неудовлет-ворительно	Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. Учебные достижения в семестровый период не демонстрировали достаточную степень овладения программным материалом на пороговом уровне.

5. Методические указания для обучающихся по освоению дисциплины

5.1. Методические указания по вопросам на понимание лекционного материала

На лекциях рекомендуется слушать предлагаемый лектором материал, при этом параллельно конспектировать основные положения, поскольку это дает наибольший результат в усвоении материала. Предоставляется возможность задавать вопросы на уточнение понимания темы и принимать участие в ее обсуждении.

Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо постоянно разбирать материалы лекций по конспектам и учебным пособиям. Во время самостоятельной проработки лекционного материала особое внимание следует уделять возникшим вопросам, непонятным терминам, спорным точкам зрения. Все такие моменты следует выделить или выписать отдельно для дальнейшего обсуждения на практическом занятии. В случае необходимости следует обращаться к преподавателю за консультацией. Полный список литературы по дисциплине приведен в разделе 6 настоящей программы.

5.2. Методические указания по подготовке вопросов для самостоятельного изучения к занятиям практического (семинарского) типов

Подготовка обучающегося к практическому занятию осуществляется на основании плана раскрытия темы практического занятия, которое разрабатывается преподавателем на основе рабочей программы и доводится до сведения обучающегося своевременно.

При подготовке к практическому занятию обучающемуся необходимо изучить внимательно основные вопросы темы семинара. Важным условием успешной подготовки к практическому занятию является четкая организация самостоятельной работы студентов по изучению учебной и дополнительной литературы. Умение анализировать и применять для ответов на вопросы и решения задач и заданий полученные знания при самостоятельной подготовке в значительной степени определяет успешность освоения материала по дисциплине и формирование у обучающихся соответствующих компетенций.

Подготовка вопросов для самостоятельного изучения включает: изучение

необходимой литературы (обязательной, дополнительной литературы, специальных периодических изданий, Интернет-ресурсов), подготовку конспекта ответа, ответы на вопросы.

При подготовке к практическим занятиям важно:

– использовать достаточно широкий диапазон массива информации, провести обзор литературы и специальных изданий, составить каталог Интернет-ресурсов;

– представить различные подходы, четко и полно определить рассматриваемые понятия, выявить взаимосвязи понятий и явлений, взаимозависимости и связи с другими вопросами;

– грамотно структурировать материал, ясно, четко и логично его излагать, приводить соответствующие примеры из практики, для иллюстрации положений, тезисов и выводов использовать таблицы, схемы, графики, диаграммы.

Вопросы для самостоятельной подготовки к занятиям практического (семинарского) типа указаны в разделе 4.2.

5.2.1. Учебно-методическое обеспечение самостоятельной работы.

Самостоятельная работа студентом осуществляется для закрепления изученного материала после практических занятий для выполнения домашних заданий, для подготовки к контрольным работам, для изучения дополнительных материалов.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет, включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

1. Бабенко Л.К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л.К. Бабенко, Е.А. Ищукова. — М.: Издательство Юрайт, 2017. — 220 с. — (Серия: Университеты России). — ISBN 978-5-9916-9244-1.
2. Лось А.Б. Криптографические методы защиты информации: учебник для академического бакалавриата / А.Б. Лось, А.Ю. Нестеренко, М.И. Рожков. — 2-е изд., испр. — М.: Издательство Юрайт, 2017. — 473 с. — (Серия: Бакалавр. Академический курс). — ISBN 978-5-534-01530-0.
3. Фомичёв В.М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата / В. М. Фомичёв, Д.А. Мельников ; под ред. В. М. Фомичёва. — М.: Издательство Юрайт, 2017. — 245 с. — (Серия: Бакалавр. Академический курс). — ISBN 978-5-534-01794-6.
4. Васильева, И.Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата / И.Н. Васильева. — М.: Издательство Юрайт, 2017. — 349 с. — (Серия: Бакалавр. Академический курс). — ISBN 978-5-534-02883-6.

6.2. Дополнительная литература

1. Щеглов А.Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А.Ю. Щеглов, К.А. Щеглов. — М. : Издательство Юрайт, 2017. — 309 с. — (Серия: Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5.
2. Запечников С.В. Криптографические методы защиты информации: учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — М. : Издательство Юрайт, 2017. — 309 с. — (Серия: Бакалавр. Академический курс). — ISBN 978-5-534-02574-3.

3. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин М.В. Рудановский. - М.: Флинта, 2011. - 224 с. - 978-5-9765-1274-0. Режим доступа: http://biblioclub.ru/index.php?page=book&id=93351
4. Креопалов В.В. Технические средства и методы защиты информации. Практическое пособие - М.: Евразийский открытый институт, 2011. - 278 с. - 978-5-374-00507-3. Режим доступа: http://biblioclub.ru/index.php?page=book&id=90753
5. Лебеденко Ю. И. Биометрические системы безопасности - Тула: Издательство ТулГУ, 2012. - 159 с. - 978-5-7679-2377-9. Режим доступа: http://biblioclub.ru/index.php?page=book&id=134536

6.3. Учебно-методическое обеспечение самостоятельной работы.

Самостоятельная работа студентом осуществляется для закрепления изученного материала после практических занятий для выполнения домашних заданий, для подготовки к контрольным работам, для изучения дополнительных материалов.

6.4. Нормативные правовые документы.

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.07.2017) «Об информации, информационных технологиях и о защите информации». Статья 16. Защита информации. СПС Консультант.
2. Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности». СПС Консультант.
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». СПС Консультант.
4. Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи». СПС Консультант.
5. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». СПС Консультант.
6. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». СПС Консультант.
7. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации». СПС Консультант.
8. Федеральный закон от 21.07.93 № 5486–1 «О государственной тайне» http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=156018
9. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=160225
10. Федеральный закон от 6 апреля 2011 года N 63-ФЗ «Об электронной подписи» http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=165011

6.5. Интернет-ресурсы

- академические электронно-библиотечные системы учебной литературы.
- база научно-технической информации ВИНИТИ РАН
- доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru

-среды разработки на языках C#, C++, Pascal, Java;

6.6. Иные источники.

Не предусмотрены

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Название лаборатории/класса, оснащенного необходимым, в соответствии с требованиями ФГОС/ СУОС, оборудованием	Наименование оборудования	Перечень лицензионного программного обеспечения
учебная аудитория для проведения занятий лекционного типа, текущего контроля и промежуточной аттестации	Рабочие места студентов: столы и стулья – соответственно количеству студентов. Рабочее место для инвалида и лиц с ОВЗ: парта с телескопической столешницей на электромеханическом приводе - 1 шт., кресло-коляска для инвалидов 18" - 1 шт., индукционная петля - 1 шт., компьютер с версией для слабовидящих - 1 шт., кнопка вызова сотрудников - 1 шт. Рабочее место преподавателя: стол – 1 шт., стул – 1 шт, кафедра - 1 шт. Доска меловая и маркерная. Экран, ноутбук Lenovo ideapad 100/15, проектор	Мультимедийный проектор КонсультантПлюс
информационно-аналитическая лаборатория - учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций	Рабочие места: столы компьютерные – в соответствии с количеством студентов, кресло Престиж Profi -B-20 Самба бордо в рубчик - 15 шт., подставка для ног Fellowes FS-48121 Standard черный - 15 шт. Рабочее место преподавателя: стол компьютерный - 1 шт., стул - 1 шт. Доска меловая или маркерная Персональные компьютеры	Мультимедийный проектор КонсультантПлюс
библиотека - помещение для самостоятельной работы	Рабочие места: столы и стулья. Рабочее место преподавателя: стол – 1 шт., стул - 1 шт., кафедра библиотечная - 1 шт. Телефон – 1 шт., цифровой многофункциональный копир - 1 шт., копировальный аппарат МФУ – 1 шт., принтер - 1 шт., сканер – 1 шт. Шкаф – 7 шт, стеллаж-33 шт, библиотечная стойка – 2 шт., стенд – 2 шт. Меловая или маркерная доска. Персональные компьютеры	Мультимедийный проектор КонсультантПлюс

Программное обеспечение:

В процессе лекционных и семинарских занятий используется следующее программное обеспечение:
- программы, обеспечивающие доступ в сеть Интернет (например, «Google chrome») и локальную сеть Академии;
- программы, демонстрации видео материалов (например, проигрыватель «Windows Media Player»);
- программы для демонстрации и создания презентаций (например, «Microsoft PowerPoint»).

Информационные справочные системы:
Информационно-правовой портал «Консультант плюс» (правовая база данных). [Электронный ресурс]. – URL: http://www.consultant.ru/
Информационно-правовой портал «Гарант» (правовая база данных). [Электронный ресурс]. – URL: http://www.garant.ru/