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

Северо-Западный институт управления – филиал РАНХиГС

Кафедра бизнес-информатики

УТВЕРЖДЕНО

Директор СЗИУ РАНХиГС
А.Д. Хлутков

ПРОГРАММА МАГИСТРАТУРЫ
Аналитическое обеспечение информационной безопасности
(наименование образовательной программы)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,
реализуемой без применения электронного (онлайн) курса

Б1.В.03 Криптографические методы защиты информации
(код и наименование РПД)

38.04.05 Бизнес-информатика
(код,наименование направления подготовки)

очная
(форма обучения)

Год набора – 2024

Санкт-Петербург, 2024 г.

Автор–составитель:
Кандидат технических наук, доцент, доцент кафедры бизнес-информатики Зеленина Лариса Ивановна.

Заведующий кафедрой бизнес-информатики
Доктор военных наук, профессор Наумов Владимир Николаевич

РПД «Криптографические методы защиты информации» одобрена протоколом заседания кафедры бизнес-информатики № 6 от 06.03.2023 г.

СОДЕРЖАНИЕ

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

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

Таблица 1

Код компетенции	Наименование Компетенции	Код компонента компетенции	Наименование компонента компетенции
ПКС-2	Способен обосновывать подходы и требования к системе обеспечения информационной безопасности, оценивать уровни безопасности компьютерных систем и сетей	ПКС-2.3	Способен оценивать уровни безопасности компьютерных систем и сетей
ПКС-4	Способен управлять информационными сервисами, ресурсами ИТ и ИТ-инновациями. Управлять ИАС в защищенном исполнении, обслуживать системы защиты	ПКС-4.2	Способен управлять ИАС в защищенном исполнении

В результате освоения дисциплины у магистрантов должны быть сформированы компетенции:

Таблица 2

ОТФ/ТФ (при наличии профстандарта)/ профессиональные действия	Код компонента компетенции	Результаты обучения
Формирование требований к защите информации в автоматизированных системах	ПКС-2.3	на уровне знаний: Знать: – основные понятия и задачи криптографии; – основные требования к системам криптографической защиты; – основные алгоритмы криптографической защиты; – принципы построения современных шифрсистем
		на уровне умения: Уметь: - Выявлять специфику криптографических угроз информационной безопасности по ряду

		категорий информации - Выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации. Владеть: - навыками определения криптографической стойкости шифрсистем, - навыками использования инструментов криптографической защиты информации
Применение ИАС в защищенном исполнении в процессах АИАД	ПКС-4.2	на уровне знаний: Знать: - постановку задач криптоанализа и подходы к их решению - методы криптозащиты компьютерных систем и сетей
		на уровне умения: Уметь: - пользоваться программными средствами, реализующими основные криптографические функции Владеть: - навыками использования инструментов криптографической защиты информации

2.Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 академ. часов/81 астрон. час.

Таблица 3

Очная форма

Вид работы	Трудоемкость (акад/астр.часы)
Общая трудоемкость	108/96
Контактная работа с преподавателем	50/37,5
Лекции	20/15
Практические занятия	28/21
Консультации	2/1,5
Самостоятельная работа	58/43,5
Контроль	
Формы текущего контроля	УО,Зад,
Форма промежуточной аттестации	Зачет с оценкой

Место дисциплины в структуре образовательной программы

Дисциплина «Криптографические методы защиты информации» относится к части, формируемой участниками образовательных отношений. Преподавание дисциплины опирается на дисциплины «Моделирование бизнес-процессов и формирование требований

к информационным системам в защищенном исполнении», «Организационное и правовое обеспечение информационной безопасности», «Моделирование информационной безопасности. Управление рисками», «Управление информационной безопасностью». Дисциплина изучается во втором семестре второго года обучения.

В свою очередь она создаёт необходимые предпосылки для освоения программ таких дисциплин, как «Управление информационной инфраструктурой предприятий», «Информационная инфраструктура предприятия».

Знания, умения и навыки, полученные при изучении дисциплины, используются студентами при выполнении выпускных квалификационных работ.

3.Содержание и структура дисциплины

3.1. Структура дисциплины

№ п/п	Наименование тем	Объем дисциплины, час.						Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий			СР		
			Л/ДОТ	ПЗ/ДОТ	КСР	СРО	СП	
Тема 1	История криптографии. Классические шифры	20	4	6		10		УО/Зад
Тема 2	Современные системы симметричной криптографии	26	4	6		16		УО/Зад
Тема 3	Асимметричная криптография	30	6	8		16		УО/Зад
Тема 4	Криптографические протоколы	30	6	8		16		УО/Зад
Промежуточная аттестация					2*			Зачет с оценкой
Всего (акад./астр. часы):		108	20	28	2	58		

Примечание:

2* - консультация

Используемые сокращения:

Л – занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся) ;

ПЗ – практические занятия (виды занятия семинарского типа за исключением лабораторных работ) ;

КСР – индивидуальная работа обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации) ;

СР – самостоятельная работа, осуществляемая без участия педагогических работников организации и (или) лиц, привлекаемых организацией к реализации образовательных программ на иных условиях;

СП – самопроверка;

СРО – самостоятельная работа обучающегося

контрольные работы (К), опрос (О)

3.2. Содержание дисциплины

Тема 1. История криптографии. Классические шифры

Основные понятия и задачи криптографии. Основные понятия и определения криптографии. Основные задачи криптографии. Криптографические протоколы.

Исторические шифры. Простые шифры перестановки. Шифры простой замены. Криптоанализ простых шифров. Пропорциональные шифры замены Шифры сложной (многоалфавитной) замены.

Тема 2. Современные системы симметричной криптографии

Свойства современных криптосистем. Классификация и виды шифров. Формальные модели шифров. Криптостойкость и имитостойкость шифра.

Блочные шифры. Структура блочных шифров. Американские стандарты блочного шифрования. Российские стандарты блочного шифрования ГОСТ 28147-89 и ГОСТ Р 34.12-2015. Основные методы анализа блочных криптосистем.

Потоковые шифры. Общие свойства потоковых шифров. Линейный рекуррентный регистр сдвига. Основные методы анализа поточных криптосистем. Потоковые шифры сетей GSM

Хэш- функции. Общие сведения о хэш-функциях. Бесключевые хэш-функции. Одноключевые хэш-функции. Код аутентификации HMAC.

Тема 3. Асимметричная криптография

Общие сведения об асимметрических криптосистемах.

Система распределения ключей Диффи-Хеллмана (DH).

Системы шифрования с открытым ключом. Криптографическая система RSA. Криптографическая система Эль-Гамаля

Электронная цифровая подпись. Общие сведения о цифровой подписи. ЭЦП на основе RSA. ЭЦП на основе схемы Эль-Гамаля. Атаки на схемы электронной цифровой подписи. Цифровые сертификаты.

Тема 4. Криптографические протоколы

Особенности и специальные виды криптографических протоколов.

Протоколы, связанные с ЭЦП. Разрешение споров по ЭЦП (протокол с судейством). Особые схемы электронной подписи

Протоколы аутентификации и распределения ключей. Распределение ключей с помощью симметричных криптосистем и арбитра. Обмен ключами с помощью асимметричных криптосистем. Взаимная аутентификация с помощью асимметричных криптосистем (протокол Нидхема-Шредера).

Специальные криптографические протоколы. Протоколы разделения секрета (распределения ответственности). Протокол доказательства с нулевым разглашением конфиденциальной информации. Электронные деньги (электронная наличность). Создание скрытого канала

4.Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 4.1

Тема (раздел)	Формы текущего контроля успеваемости

Тема 1. История криптографии. Классические шифры	УО/Зад
Тема 2. Современные системы симметричной криптографии	УО/Зад
Тема 3. Асимметричная криптография	УО/Зад
Тема 4. Криптографические протоколы	УО/Зад

4. 2. Типовые материалы текущего контроля успеваемости обучающихся.

Типовые оценочные материалы по теме 1

Задания по теме 1

Задание 1.

Используя шифр перестановки «Поворотные решетки Кардано» создать свой трафарет для поворотной решетки размером 6×6. Зашифровать текст с помощью созданного трафарета. Расшифровать криптограмму, полученную с помощью поворотной решетки, если известен использованный для шифрования трафарет.

Задание2.

Дешифровать криптограммы, полученные методами столбцовой и двойной перестановки.

Задание 3.

Зашифровать слово с помощью шифра Цезаря. Расшифровать криптограмму, полученную с помощью шифра Цезаря.

Задание 4.

Зашифровать слово с помощью шифра Виженера. Расшифровать криптограмму, полученную с помощью шифра Виженера.

Задание 5.

Дешифровать криптограмму, полученную шифром простой замены. Символы криптограммы закодированы двузначными числами. В тексте криптограммы сохранены пробелы и пунктуация. Символ пробела и знаки препинания в нормативный алфавит не входят.

Типовые вопросы для опроса по теме 1

1. Сформулировать основные понятия криптографии.
2. Определить основные задачи криптографии.
3. Что относится к криптографическим протоколам.
4. Что понимается под термином «исторические шифры»
5. Суть простых шифров перестановки.
6. Как работают шифры простой замены.
7. Как выполняется криптоанализ простых шифров.

Типовые оценочные материалы по теме 2

Задания по теме 2

Задание 1.

Найти секретный ключ *K* учебного алгоритма с помощью с помощью обычной слайдовой атаки

Задание 2.

Выполнить «в ручную» операцию *MixColumns* для заданного столбца байтов. Столбец байтов для преобразования приведен в таблице 1 (см ниже).

Задание 3.

Зашифровать с помощью алгоритма AES-128 заданный фрагмент на заданном ключе (см таблица 1).

Задание 4.

Дешифровать заданную криптограмму, полученную шифром AES-128 на ключе из задания ***3***, получить открытый текст сообщения. Криптограмма для расшифровывания приведена в таблице 1.

Таблица 1.

Столбец байтов AD 41 87 AC	Блок текста: 38 AD C5 0F AC 3F C1 1B 4C 8E B2 80 57 90 23 2C Ключ: A4 83 01 77 CA 0F 68 EE AF 66 AB 45 A7 7B 89 08 Криптограмма: AB 0A 78 15 33 CC 17 49 18 74 F4 AA 2C 92 9F 07

Типовые вопросы для опроса по теме 2:

1. Охарактеризовать свойства современных криптосистем: классификация и виды шифров. Формальные модели шифров.
2. Что понимается под криптостойкостью и имитостойкостью шифра.
3. Каковы основные методы анализа блочных криптосистем. В чем их суть
4. Какие зарубежные и российские стандарты блочного шифрования вам известны. Сравните их.
5. Каковы свойства потоковых шифров.
6. Что такое линейный рекуррентный регистр сдвига.
7. Какие методы методы анализа поточных криптосистем вам известны. В чем их суть.
8. Описать потоковые шифры сетей GSM
9. Что такое хэш- функция, каково ее назначение.
10. Сравнить бесключевые и одноключевые хэш-функции.
11. Какую хэш-функцию использует код аутентификации HMAC

Типовые оценочные материалы по теме 3

Задания по теме 3

Задание 1.

Зашифровать клавиатурный символ с помощью криптосистемы Блюма-Гольдвассер, сгенерировав 8-битовую псевдослучайную последовательность.

Из таблицы 2 выбрать значения параметров BBS-генератора *p*, *q*, случайное число *s* и подлежащий зашифрованию символ *M* (символ – русскоязычный).

Таблица 2

p	q	s	Открытый текст M
883	367	65486	О

Задание 2.

Расшифровать криптограмму, полученную в криптосистеме Блюма-Гольдвассер. Известно, что использована эффективная реализация BBS-генератора с максимально допустимым числом младших битов.

Значения секретного ключа: чисел p и q, криптограмма C, состоящая из числа-подсказки x_6 и последовательности ASCII-кодов c_i символов зашифрованного текста представлены в таблице 3.

Таблица 3

p	q	Криптограмма C	
		x_6	c_i
439	491	123530	130;222;119

Типовые вопросы для опроса по теме 3:

1. Что относится к асимметрическим криптосистемам.
2. В чем суть системы распределения ключей Диффи-Хеллмана.
3. В чем отличие систем шифрования с открытым ключом от систем шифрования с закрытым ключом.
4. В чем отличие криптографической системы RSA от криптографической системы Эль-Гамаля
5. Что представляет электронная цифровая подпись. Задачи, решаемые при ее использовании.
6. В чем отличие ЭЦП на основе RSA от ЭЦП на основе схемы Эль-Гамаля.
7. Кие атаки на схемы электронной цифровой подписи вам знакомы.
8. Что такое цифровые сертификаты.

Типовые оценочные материалы по теме 4

Задания по теме 4

Задание 1.

Выполнить шифрование, проверку аутентичности и дешифрование по алгоритму RSA, зная только открытые ключи абонентов криптосистемы RSA.

По известным открытым ключам (N, e) абонентов криптосистемы RSA (табл. 4) и тому, что кодирование символов сообщения осуществляется с помощью таблицы 5 (буквы «е» и «ё» не различаются). Найти значение передаваемого между абонентами шифртекста Y.

Таблица 4. Справочник открытых ключей абонентов криптосистемы RSA

Абонент	Ключ (N, e)	Абонент	Ключ (N, e)	Абонент	Ключ (N, e)
A	(5017, 251)	F	(8809, 307)	K	(4553, 241)

B	(8471, 125)	G	(6077, 619)	L	(6757, 233)
C	(4559, 311)	H	(5513, 607)	P	(8413, 507)
D	(3403, 211)	I	(7747, 353)	Q	(6313, 749)
E	(5177, 179)	J	(5561, 433)	R	(9301, 387)

Таблица 5. Таблица кодирования символов открытого текста

Символ	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
код	11	12	13	14	15	16	17	18	19	21	22	23	24	25	26	27
Символ	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
код	28	29	31	32	33	34	35	36	37	38	39	41	42	43	44	45

Задание 2.

Абоненты криптосистемы RSA обмениваются открытыми сообщениями с подтверждением авторства. Проверить аутентичность сообщения, если известны открытые ключи (N, e) абонентов криптосистемы (табл. 4). Кодирование символов сообщения осуществляется с помощью таблицы 5 (буквы «е» и «ё» не различаются). Параметры передачи текста в системе RSA, передаваемый открытый текст и проверочный код приведены в таблице 6.

Таблица 6.

Передача текста	Подпись
R $\rightarrow$ A; акт	1019;8218

Задание 3.

При передаче между абонентами перехвачена криптограмма Y, полученная шифрованием по алгоритму RSA. Дешифровать Y, вычислив секретный ключ d. Известны открытые ключи абонентов (табл. 4). Кодирование символов сообщения осуществляется с помощью таблицы 5. Параметры шифра RSA и криптограмму $\boldsymbol{Y}$ указаны в табл. 7.

Таблица 7.

Абоненты	Криптограмма $\boldsymbol{Y}$
F $\rightarrow$ P	3872;5862

Задание 4.

Даны значения модуля шифрования N, открытого ключа e и шифртекста Y. Известно, что Y получен шифрованием на открытом ключе (N, e) по алгоритму RSA. Используя разложение модуля на простые числа методом Ферма, определить секретный ключ алгоритма RSA и дешифровать Y.

N = 65815671868057, e = 7423489, Y = 64938654445479.

Типовые вопросы для опроса по теме 4:

1. Каковы особенности криптографических протоколов.
2. Какие виды кпрптографических протоколов вам известны.
3. Охарактеризовать протоколы, связанные с ЭЦП.
4. Сравнить протоколы аутентификации и распределения ключей.
5. Как осуществляется распределение ключей с помощью симметричных

криптосистем и арбитра.

6. В чем суть обмена ключами с помощью асимметричных криптосистем.

7.Каким образом осуществляется взаимная аутентификация с помощью асимметричных криптосистем.

8. Что относится к специальным криптографическим протоколам.

9. Протоколы распределения ответственности.

10.Протокол доказательства с нулевым разглашением конфиденциальной информации.

11. Что понимается под электронной наличностью.

12. Каким образом осуществляется создание скрытого канала

5.Оценочные материалы промежуточной аттестации по дисциплине

5.1. Зачет проводится с применением следующих методов (средств): устный опрос, задание.

5.2. Оценочные материалы промежуточной аттестации

Показатели и критерии оценивания компетенций на различных этапах их формирования

Компонент компетенции	Промежуточный/ключевой индикатор	Критерий оценивания
ПКС-2.3	Использует криптографические методы защиты, информационные технологии, программный инструментарий в объеме, необходимом для решения задач бизнес-аналитики	Применяет криптографические методы защиты информации. Демонстрирует использование инструментов криптографической защиты информации.
ПКС-4.2	Управляет ИАС в защищенном исполнении, обслуживает системы защиты	Демонстрирует способность управления ИАС в защищенном исполнении и обслуживания систем защиты

Типовые вопросы, выносимые на зачет

1. Основные понятия криптографии.
2. Основные задачи криптографии.
3. Криптографические протоколы.
4. Простые шифры перестановки и шифры простой замены
5. Криптоанализ простых шифров.
6. Шифры сложной (многоалфавитной) замены.
7. Свойства современных криптосистем.
8. Классификация и виды шифров.
9. Криптостойкость и имитостойкость шифра.
10. Структура блочных шифров.
11. Анализ российских и зарубежных стандартов блочного шифрования.

12. Основные методы анализа блочных криптосистем.
13. Свойства потоковых шифров.
14. Основные методы анализа поточных криптосистем.
15. Потоковые шифры сетей GSM
16. Общие сведения о хэш-функциях.
17. Бесключевые и одноключевые хэш-функции
18. Код аутентификации HMAC.
19. Асимметрические криптосистемы.
20. Система распределения ключей DH.
21. Системы шифрования с открытым ключом.
22. Криптографическая система RSA.
23. Криптографическая система Эль-Гамаля
24. Электронная цифровая подпись.
25. ЭЦП на основе RSA и схемы Эль-Гамаля.
26. Атаки на схемы электронной цифровой подписи.
27. Особенности и специальные виды криптографических протоколов.
28. Протоколы, связанные с ЭЦП.
29. Протоколы аутентификации и распределения ключей.
30. Протоколы разделения секрета (распределения ответственности).
31. Протокол доказательства с нулевым разглашением конфиденциальной информации.
32. Электронные деньги

Шкала оценивания

Оценка результатов производится на основе Положения о текущем контроле успеваемости обучающихся и промежуточной аттестации обегающихся по образовательным программам среднего профессионального и высшего образования в федеральном государственном бюджетном образовательном учреждении высшего образования «Российская академии народною хозяйства и государственной службы при Президенте Российской Федерации», утвержденного Приказом Ректора РАНХиГС при Президенте РФ от 30.01.2018 г. № 02-66 (п.10 раздела 3 (первый абзац) и п.11), а также Решения Ученого совета Северо-западного института управления РАНХиГС при Президенте РФ от 19.06.2018, протокол № 11.

Зачет с оценкой

Оценка «отлично» выставляется в случае, если при устном ответе студент проявил (показал):

- глубокое и системное знание всего программного материала учебного курса, изложил ответ последовательно и убедительно;
- отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей дисциплины;
- умение правильно применять теоретические положения при решении практических вопросов и задач.

Оценки «хорошо» выставляется в случае, если при устном ответе студент проявил (показал):

- знание узловых проблем программы и основного содержания лекционного курса;
- умение пользоваться концептуально-понятийным аппаратом умение преимущественно правильно применять теоретические положения при решении практических вопросов и задач;
- умение выполнять предусмотренные программой задания;
- в целом логически корректное, но не всегда точное и аргументированное изложение ответа.

Оценка «удовлетворительно» выставляется в случае, если при устном ответе студент проявил (показал):
- фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса;
- затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины;
- затруднения с применением теоретических положений при решении практических вопросов и задач.

Оценка «неудовлетворительно» выставляется в случае, если при устном ответе студент проявил (показал):
- незнание либо отрывочное представление учебно-программного материала;
- неумение использовать научно-понятийный аппарат и терминологию учебной дисциплины;
- неумение применять теоретические положения при решении практических вопросов и задач,
- неумение выполнять предусмотренные программой задания.

6.Методические материалы для обучающихся по освоению дисциплины

Рабочей программой дисциплины предусмотрены следующие виды аудиторных занятий: лекции, практические занятия. На лекциях рассматриваются наиболее сложный материал дисциплины. На лекциях рассматривается наиболее сложный материал дисциплины. Лекция сопровождается презентациями, компьютерными текстами лекции, что позволяет магистранту самостоятельно работать над повторением и закреплением лекционного материала. Для этого магистранту должно быть предоставлено право самостоятельно работать в компьютерных классах в сети Интернет. Кроме того, часть теоретического материала предоставляется на самостоятельное изучение по рекомендованным источникам для формирования навыка самообучения.

Практические занятия предназначены для самостоятельной работы магистрантов по решению конкретных задач. Каждое практическое занятие сопровождается заданиями, выдаваемыми магистрантам для решения во внеаудиторное время. Для оказания помощи в решении задач имеются тексты практических заданий с условиями задач и вариантами их решения.

Для работы с печатными и электронными ресурсами СЗИУ имеется возможность доступа к электронным ресурсам. Организация работы магистрантов с электронной библиотекой указана на сайте института (странице сайта – «Научная библиотека»).

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

7.1. Основная литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. http://znanium.com/bookread.php?book=432654 Электронный ресурс
2. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. - (Высшее образование) ISBN 978-5-369-01450-9 - Режим доступа http://znanium.com/bookread2.php?book=495249
3. Баранова Е. К. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. http://znanium.com/bookread.php?book=476047 Электронный ресурс
4. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: http://znanium.com/bookread.php?book=474838 Электронный ресурс
5. Кирпичников А.П. Криптографические методы защиты компьютерной информации [Электронный ресурс] : учебное пособие / А.П. Кирпичников, З.М. Хайбуллина. — Электрон. текстовые данные. — Казань: Казанский национальный исследовательский технологический университет, 2016. — 100 с. — 978-5-7882-2052-9. — Режим доступа: http://www.iprbookshop.ru/79313.htm
6. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с. ISBN 978-5-8199-0331-5 - Режим доступа: http://znanium.com/catalog/product/423927

7.2 Дополнительная литература

1. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. - Режим доступа: http://znanium.com/bookread2.php?book=405313
2. Девянин П.Н., Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : Учебное пособие для вузов / Девянин П.Н. - 2-е изд., испр. и доп. - М. : Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991203289.html
3. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: НИЦ ИНФРА-М, 2016. - 118 с. - Режим доступа: http://znanium.com/bookread2.php?book=507334
4. Калмыков И.А. Криптографические методы защиты информации [Электронный ресурс] : лабораторный практикум / И.А. Калмыков, Д.О. Науменко, Т.А. Гиш. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 109 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63099.html
5. Молдовян Н. А. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - СПб.: БХВ-Петербург, 2010. - 293 с. - (Учебное пособие) http://znanium.com/bookread.php?book=351283 Электронный ресурс
6. Партыка Т. Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. http://znanium.com/bookrea,d.php?book=420047 Электронный ресурс
7. Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации [Электронный ресурс] / . — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 67 с. — 2227- 8397. — Режим доступа: http://www.iprbookshop.ru/61738.html

7.3.Нормативные правовые документы и иная правовая информация

Не используются.

7.4.Интернет-ресурсы

1. Глоссарий по криптографии - https://hpc.name/text/get/82/p1.html
2. Литература по криптографии - http://www.proklondike.com/books/crypto.html
3. Сайт лаборатории радиосистем (кафедра радиофизики) - http://radiosys.ksu.ru
4. Сайт по криптографии - http://kek.ksu.ru/Student/Crypto/Main.htm
5. Электронные книги по криптографии - http://www.knigka.info/kriptograf/
6. Электронно-образовательные ресурсы на сайте научной библиотеки СЗИУ РАНХиГС (http://nwipa.ru)
7. Электронные учебники электронно-библиотечной системы (ЭБС) «Айбукс» http://www.nwapa.spb.ru/index.php?page_id=76
8. Электронные учебники электронно-библиотечной системы (ЭБС) «Лань» http://www.nwapa.spb.ru/index.php?page_id=76
9. Электронные учебники электронно-библиотечной системы (ЭБС) «IPRbooks» http://www.nwapa.spb.ru/index.php?page_id=76
10. Электронные учебники электронно-библиотечной системы (ЭБС) «Юрайт»

7.5. Иные источники.

Не используются.

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

Учебная дисциплина включает использование программного обеспечения Microsoft Excel, Microsoft Word, для подготовки текстового и табличного материала, выполнения задачи по крпитографической защите информации.

Интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии, справочники, библиотеки, электронные учебные и учебно-методические материалы).

Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

№ п/п	Наименование
	Компьютерные классы с персональными ЭВМ, объединенными в локальные сети с выходом в Интернет
	Пакет Excel -2016, proffesional
	Мультимедийные средства в каждом компьютерном классе и в лекционной аудитории
	Браузер, сетевые коммуникационные средства для выхода в Интернет

Компьютерные классы из расчета 1 ПЭВМ для одного обучаемого. Каждому обучающемуся должна быть предоставлена возможность доступа к сетям типа Интернет в течение не менее 20% времени, отведенного на самостоятельную подготовку.