

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,  
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»  
(СПбГУТ)

Кафедра \_\_\_\_\_  
Защищенных систем связи  
(полное наименование кафедры)

СПбГУТ))

Документ подписан простой  
электронной подписью

Сертификат: 009b47d8b89b08d0f6  
Владелец: Киричек Руслан Валентинович  
Действителен с 13.02.2023 по 12.02.2028



УТВЕРЖДАЮ

А.В. Абилов

2023

Регистрационный №\_23.05/566-Д

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Средства криптографической защиты информации

(наименование дисциплины)

образовательная программа высшего образования

11.05.04 Инфокоммуникационные технологии и системы  
специальной связи

(код и наименование направления подготовки / специальности)

Инженер

(квалификация)

Системы радиосвязи специального назначения

(направленность / профиль образовательной программы)

очная форма

(форма обучения)

Санкт-Петербург

Рабочая программа дисциплины составлена на основе требований Федерального государственного образовательного стандарта высшего образования по направлению (специальности) подготовки «11.05.04 Инфокоммуникационные технологии и системы специальной связи», утвержденного приказом Министерства образования и науки Российской Федерации от 02.04.2020 № 542 дсп, и в соответствии с рабочим учебным планом, утвержденным ректором университета.

## **1. Цели и задачи дисциплины**

Целью преподавания дисциплины «Средства криптографической защиты информации» является:

изучение вопросов основ криптографической защиты информации в телекоммуникационных системах. Дисциплина «Основы криптографии» должна обеспечивать формирование фундамента подготовки будущих специалистов в области инфокоммуникаций, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана.

Эта цель достигается путем решения следующих(ей) задач(и):

фундаментализации, интенсификации и индивидуализации процесса обучения путём внедрения и эффективного использования достижений криптографии, теории связи и информации. В результате изучения дисциплины у студентов должны сформироваться знания, умения и навыки, позволяющие проводить самостоятельный анализ предметной области.

## **2. Место дисциплины в структуре образовательной программы**

Дисциплина «Средства криптографической защиты информации» Б1.О.30 является одной из дисциплин обязательной части учебного плана подготовки специалиста по направлению «11.05.04 Инфокоммуникационные технологии и системы специальной связи». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Высшая математика».

## **3. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 1

<b>№ п/п</b>	<b>Код компетенции</b>	<b>Наименование компетенции</b>
1	ОПК-3	Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности
2	ПК-5	Способен оценивать параметры безопасности и защищать программное обеспечение и сетевые устройства администрируемой сети с помощью специальных средств управления безопасностью
3	ПК-21	Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

Индикаторы достижения компетенций

Таблица 2

ОПК-3.1	Знает основные закономерности передачи информации в инфокоммуникационных системах, основные виды сигналов, используемых в телекоммуникационных системах, особенности передачи различных сигналов по каналам и трактам телекоммуникационных систем
---------	---

ОПК-3.2	Знает принципы, основные алгоритмы и устройства цифровой обработки сигналов; принципы построения телекоммуникационных систем различных типов и способы распределения информации в сетях связи
ОПК-3.3	Умеет решать задачи обработки данных с помощью средств вычислительной техники
ОПК-3.4	Умеет строить вероятностные модели для конкретных процессов, проводить необходимые расчеты в рамках построенной модели
ОПК-3.5	Владеет методами и навыками обеспечения информационной безопасности
ПК-5.1	Знает архитектуру, протоколы и общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
ПК-5.2	Знает основные принципы, криптографические протоколы и программные средства обеспечения информационной безопасности сетевых устройств
ПК-5.3	Умеет применять программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа
ПК-5.4	Пользоваться нормативно-технической документацией в области обеспечения информационной безопасности инфокоммуникационных систем
ПК-5.5	Владеет навыками и средствами установки и управления специализированными программными средствами защиты сетевых устройств администрируемой сети от несанкционированного доступа
ПК-21.1	Знает общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
ПК-21.2	Умеет подключать и настраивать современные средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов); работать с контрольно-измерительными аппаратными и программными средствами
ПК-21.3	Владеет навыками установки дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация
ПК-21.4	Владеет навыками документирование настроек средств обеспечения безопасности удаленного доступа

#### 4. Объем дисциплины и виды учебной работы

Очная форма обучения

Таблица 3

Вид учебной работы	Всего часов	Семестры	
		7	-
Общая трудоемкость	6 ЗЕТ	216	216
<b>Контактная работа с обучающимися</b>	84.35	84.35	
в том числе:			
Лекции	32	32	
Практические занятия (ПЗ)	50	50	
Лабораторные работы (ЛР)		-	
Задача контрольной работы		-	
Задача курсовой работы		-	
Задача курсового проекта		-	
Промежуточная аттестация	2.35	2.35	
<b>Самостоятельная работа обучающихся (СРС)</b>	98	98	
в том числе:			
Курсовая работа		-	

Курсовой проект		-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала	98	98
Подготовка к промежуточной аттестации	33.65	33.65
<b>Вид промежуточной аттестации</b>		Экзамен

## 5. Содержание дисциплины

### 5.1. Содержание разделов дисциплины.

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела	№ семестра		
			очная	очно- заоч- ная	заоч- ная
1	Раздел 1. Введение в криптографию	Основные определения. История криптографии. Классификация криptoалгоритмов.	7		
2	Раздел 2. Математические основы криптографии.	Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Алгебраические структуры. Поля Галуа. Структура генератора псевдослучайных последовательностей (ГПСП). Алгоритмы генерации псевдослучайных последовательностей Криптографические стойкие ГПСП. Тестирование ГПСП	7		
3	Раздел 3. Симметричная криптография.	Стандарт шифрования DES. Режимы работы алгоритма DES. Стандарт шифрования AES. Стандарт шифрования ГОСТ Р 34.12-2015 (Магма и Кузнецик) Шифр одноразового блокнота. Принцип использования ГПСП при поточном шифровании. Шифр RC4.	7		
4	Раздел 4. Криптосистема RSA.	Принцип работы современных асимметричных криптосистем. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистема Рабина.	7		
5	Раздел 5. Криптосистемы на основе метода эллиптических кривых.	Эллиптические кривые в вещественных числах, эллиптические кривые в полях Галуа, криптография эллиптической кривой, моделирующая криптосистему Эль-Гамаля.	7		
6	Раздел 6. Криптографические хеш-функции.	Итеративные хеш-функции. Схема Меркеля-Дамгарда. Хеш-функции, основанные на блочных шифрах. Схема Рабина. Алгоритм безопасного хеширования SHA. Шифр Whirlpool. Российский стандарт хеширования ГОСТ Р 34.11-2012.	7		
7	Раздел 7. Электронная цифровая подпись.	Алгоритм формирования электронной цифровой подписи (ЭЦП). Схема ЭЦП RSA. ЭЦП Эль-Гамаля. ЭЦП Шнорра. Стандарт цифровой подписи DSS. Схема ЭЦП эллиптической кривой. Российский стандарт ЭЦП ГОСТ Р 34.10- 2012	7		

8	Раздел 8. Алгоритмы безопасного распределения ключей.	Стандарт ANSI. X9.17. Методы хранения ключевой информации. Прямой обмен ключами между пользователями. Система «запрос-ответ». Алгоритм Ниидома-Шредера. Алгоритм Диффи-Хеллмана. Использование Центра распределения ключей. Инфраструктура PKI. Стандарт X.509. Система Kerberos.	7		
9	Раздел 9. Основы современной стеганографии.	Цели стеганографии. Практическое применение стеганографии. Классификация алгоритмов стеганографии. Цифровые метки. Цифровые водяные знаки. Скрытая передача данных. Защита подлинности документов и авторских прав стеганографическими методами.	7		
10	Раздел 10. Основы криptoанализа.	Методы криptoанализа. Криptoанализ блочных шифров. Частотный криptoанализ. Дифференциальный криptoанализ. Линейный криptoанализ. Интерполяционный криptoанализ. Методы криptoанализа, основанные на слабости ключевых разверток.	7		

5.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

Таблица 5

№ п/п	Наименование обеспечиваемых (последующих) дисциплин
1	Системы радиосвязи специального назначения

5.3. Разделы дисциплин и виды занятий.

### Очная форма обучения

Таблица 6

№ п/п	Наименование раздела дисциплины	Лек- ции	Практ. занятия	Лаб. занятия	Семи- нары	СРС	Всего часов
1	Раздел 1. Введение в криптографию	2	4			7	13
2	Раздел 2. Математические основы криптографии.	4	6			15	25
3	Раздел 3. Симметричная криптография.	4	6			15	25
4	Раздел 4. Криптосистема RSA.	2	6			7	15
5	Раздел 5. Криптосистемы на основе метода эллиптических кривых.	2	4			10	16
6	Раздел 6. Криптографические хеш-функции.	4	4			10	18
7	Раздел 7. Электронная цифровая подпись.	2	6			10	18
8	Раздел 8. Алгоритмы безопасного распределения ключей.	4	6			8	18
9	Раздел 9. Основы современной стеганографии.	4	4			8	16

10	Раздел 10. Основы криптоанализа.	4	4			8	16
	Итого:	32	50	-	-	98	180

## 6. Лекции

Очная форма обучения

Таблица 7

№ п/п	Номер раздела	Тема лекции	Всего часов
1	1	История криптографии	2
2	2	Основы криптографии	2
3	2	Алгоритмы генерации псевдослучайных последовательностей Криптографические стойкие ГПСП	2
4	3	Симметричная криптография	2
5	3	Принцип использования ГПСП при поточном шифровании.	2
6	4	Принцип работы современных асимметричных криптосистем.	2
7	5	Криптография эллиптической кривой	2
8	6	Криптографические хеш-функции	2
9	6	Российский стандарт хеширования ГОСТ Р 34.11- 2012.	2
10	7	Алгоритм формирования электронной цифровой подписи (ЭЦП)	2
11	8	Методы хранения ключевой информации	2
12	8	Использование Центра распределения ключей.	2
13	9	Основы современной стеганографии.	2
14	9	Защита подлинности документов и авторских прав стеганографическими методами.	2
15	10	Методы криптоанализа.	2
16	10	Методы криптоанализа, основанные на слабости ключевых разверток.	2
		Итого:	32

## 7. Лабораторный практикум

Рабочим учебным планом не предусмотрено

## 8. Практические занятия (семинары)

Очная форма обучения

Таблица 8

№ п/п	Номер раздела	Тема занятия	Всего часов
1	1	Разработка классических криптоалгоритмов.	4
2	2	Генерация и тестирование псевдослучайных последовательностей.	2
3	2	Модульная арифметика: основы вычисления в классах вычетов.	4
4	3	Программные средства реализации современные симметричные криптосистемы.	2
5	3	Современные симметричные криптосистемы .	4
6	4	Изучение принципов работы асимметричных криптосистем	4
7	4	Изучение реализаций асимметричной криптографии в среде .NET Framework.	2
8	5	Шифрование открытого текста на основе эллиптических кривых.	4

9	6	Изучение реализаций хэш-функций и ЭЦП в среде .NET Framework.	4
10	7	Реализация существующих хэш-функций и алгоритмов ЭЦП.	4
11	7	Изучение методов формирования дайджеста сообщения (хэшфункции) и электронной цифровой подписи (ЭЦП)	2
12	8	Использование алгоритма шифрования RSA для безопасного распределения ключей симметричной криптосистемы.	4
13	8	Изучение методов безопасного распределения ключей в небезопасной среде.	2
14	9	Разработка системы для скрытой передачи сообщений.	4
15	10	Криптоанализ шифров табличной перестановки.	4
Итого:			50

## 9. Примерная тематика курсовых проектов (работ)

Рабочим учебным планом не предусмотрено

## 10. Самостоятельная работа

Очная форма обучения

Таблица 9

№ п/п	Номер раздела	Содержание самостоятельной работы	Форма контроля	Всего часов
1	1	Изучение материалов лекции	отчет	7
2	2	Изучение материалов лекции	отчет	15
3	3	Изучение материалов лекции	отчет	15
4	4	Изучение материалов лекции	отчет	7
5	5	Изучение материалов лекции	отчет	10
6	6	Изучение материалов лекции	отчет	10
7	7	Изучение материалов лекции		10
8	8	Изучение материалов лекции		8
9	9	Изучение материалов лекции		8
10	10	Изучение материалов лекции		8
Итого:				98

## 11. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Для самостоятельной работы по дисциплине рекомендовано следующее учебно-методическое обеспечение:

- Положение о самостоятельной работе студентов в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича;
- рекомендованная основная и дополнительная литература;
- конспект занятий по дисциплине;
- слайды-презентации и другой методический материал, используемый на занятиях;
- методические рекомендации по подготовке письменных работ, требования к их содержанию и оформлению (реферат, эссе, контрольная работа) ;
- фонды оценочных средств;

## **12. Фонд оценочных средств для проведения промежуточной аттестации обучающихся**

Фонд оценочных средств разрабатывается в соответствии с локальным актом университета "Положение о фонде оценочных средств" и является приложением (Приложение А) к рабочей программе дисциплины.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине включает в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- 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;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Для каждого результата обучения по дисциплине определяются показатели и критерии оценки сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

## **13. Перечень основной и дополнительной литературы, необходимой для освоений дисциплины**

### **12.1. Основная литература:**

#### **1. Коржик, Валерий Иванович.**

Криптографические методы и средства обеспечения информационной безопасности : учебное пособие / В. И. Коржик, Д. В. Кушнир ; рец. С. Е. Душин ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2012. - 89 с. : ил. - 90.54 р. - Текст : непосредственный.

#### **2. Коржик, Валерий Иванович.**

Основы криптографии : [Электронный ресурс] : учебное пособие / В. И. Коржик, В. П. Просихин, В. А. Яковлев ; рец.: Р. Р. Биккенен, Б. В. Изотов ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2014. - 277 с. : ил. - ISBN 978-5-89160-097-3 : Б. ц.

#### **3. Коржик, Валерий Иванович.**

Основы криптографии : учебное пособие / В. И. Коржик, В. А. Яковлев ; рец.: Р. Р. Биккенин, Б. В. Изотов. - СПб. : СПбГУТ, 2016. - 295 с. : ил., табл. - ISBN 978-5-

89160-097-3 : 600.00 р. - Текст : непосредственный.

4. Коржик, Валерий Иванович.

Lecture noyes in cryptography : [Электронный ресурс] : учебное пособие / В. И. Коржик, К. А. Ахрамеева ; рец.: В. А. Яковлев, Б. В. Изотов ; Федеральное агентство связи, Федеральное государственное бюджетное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2017. - 102 р. : ил. - ISBN 978-5-89160-152-9 : 596.14 р.

12.2. Дополнительная литература:

1. Введение в криптографию / В. В. Ященко [и др.] ; общ. ред. В. В. Ященко. - 2-е изд., испр. - М. : МЦНМО-ЧеРо, 1999. - 271 с. : ил. - (Новые математические дисциплины). - Библиогр. в конце глав. - ISBN 5-900916-40-5 (в пер.) : 91.00 р. - Текст : непосредственный.
2. Коржик, Валерий Иванович.  
Криптографические методы и средства обеспечения информационной безопасности : методические указания к лаб. работам / В. И. Коржик, Д. В. Кушнир ; рец. С. Е. Душин ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2012. - 23 с. : ил., табл. - Текст : непосредственный.

#### **14. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»**

- [www.sut.ru](http://www.sut.ru)
- [lib.spbgu.ru/jirbis2\\_spbgu](http://lib.spbgu.ru/jirbis2_spbgu)

#### **15. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем.**

15.1. Программное обеспечение дисциплины:

- Open Office
- Google Chrome

15.2. Информационно-справочные системы:

- ЭБС iBooks (<https://ibooks.ru>)
- ЭБС Лань (<https://e.lanbook.com/>)
- ЭБС СПбГУТ (<http://lib.spbgu.ru>)

## **16. Методические указания для обучающихся по освоению дисциплины**

### **15.1. Планирование и организация времени, необходимого для изучения дисциплины**

Важным условием успешного освоения дисциплины «Средства криптографической защиты информации» является создание системы правильной организации труда, позволяющей распределить учебную нагрузку равномерно в соответствии с графиком образовательного процесса. Большую помощь в этом может оказать составление плана работы на семестр, месяц, неделю, день. Его наличие позволит подчинить свободное время целям учебы, трудиться более успешно и эффективно. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Все задания, включая вынесенные на самостоятельную работу, рекомендуется выполнять непосредственно после соответствующего аудиторного занятия (лекции, практического занятия), что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях, систематизировать ранее пройденный материал, на его основе приступить к овладению новыми знаниями и навыками.

Система университетского обучения основывается на рациональном сочетании нескольких видов учебных занятий (в первую очередь, лекций и практических занятий), работа на которых обладает определенной спецификой.

### **15.2. Подготовка к лекциям**

Знакомство с дисциплиной происходит уже на первой лекции, где от студента требуется не просто внимание, но и самостоятельное оформление конспекта. При работе с конспектом лекций необходимо учитывать тот фактор, что одни лекции дают ответы на конкретные вопросы темы, другие – лишь выявляют взаимосвязи между явлениями, помогая студенту понять глубинные процессы развития изучаемого предмета, как в истории, так и в настоящее время.

Конспектирование лекций – сложный вид вузовской аудиторной работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем записать ее. Желательно запись осуществлять на одной странице листа или оставляя поля, на которых позднее, при самостоятельной работе с конспектом, можно сделать дополнительные записи, отметить непонятные места.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста. Работая над

конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

### 15.3. Подготовка к практическим занятиям

Тщательное продумывание и изучение вопросов плана основывается на проработке пройденного материала (материала лекций, практических занятий), а затем изучения обязательной и дополнительной литературы, рекомендованной к данной теме.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы практикума, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Необходимо понимать, что невозможно во время аудиторных занятий изложить весь материал из-за лимита аудиторных часов, и при изучении дисциплины недостаточно конспектов занятий. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме.

### 15.4. Рекомендации по работе с литературой

Работу с литературой целесообразно начать с изучения общих работ по теме, а также учебников и учебных пособий. Далее рекомендуется перейти к анализу монографий и статей, рассматривающих отдельные аспекты проблем, изучаемых в рамках курса, а также официальных материалов и неопубликованных документов (научно-исследовательские работы, диссертации), в которых могут содержаться основные вопросы изучаемой проблемы.

Работу с источниками надо начинать с ознакомительного чтения, т.е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения. В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание ученика на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет. Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не

сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции – это сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Если в литературе встречаются разные точки зрения по тому или иному вопросу из-за сложности прошедших событий и правовых явлений, нельзя их отвергать, не разобравшись. При наличии расхождений между авторами необходимо найти рациональное зерно у каждого из них, что позволит глубже усвоить предмет изучения и более критично оценивать изучаемые вопросы. Знакомясь с особыми позициями авторов, нужно определять их схожие суждения, аргументы, выводы, а затем сравнивать их между собой и применять из них ту, которая более убедительна.

Следующим этапом работы с литературными источниками является создание конспектов, фиксирующих основные тезисы и аргументы. Можно делать записи на отдельных листах, которые потом легко систематизировать по отдельным темам изучаемого курса. Другой способ – это ведение тематических тетрадей-конспектов по одной какой-либо теме. Большие специальные работы монографического характера целесообразно конспектировать в отдельных тетрадях. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы). Впоследствии эта информация может быть использована при написании текста реферата или другого задания.

Таким образом, при работе с источниками и литературой важно уметь:

- сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;
- обобщать полученную информацию, оценивать прослушанное и прочитанное;
- фиксировать основное содержание сообщений; формулировать, устно и письменно, основную идею сообщения; составлять план, формулировать тезисы;
- готовить и презентовать развернутые сообщения типа доклада;
- работать в разных режимах (индивидуально, в паре, в группе), взаимодействуя друг с другом;
- пользоваться реферативными и справочными материалами;
- контролировать свои действия и действия своих товарищей, объективно оценивать свои действия;
- обращаться за помощью, дополнительными разъяснениями к преподавателю, другим студентам;
- пользоваться лингвистической или контекстуальной догадкой, словарями различного характера, различного рода подсказками, опорами в тексте (ключевые слова, структура текста, предваряющая информация и др.);
- использовать при говорении и письме перифраз, синонимичные средства, слова-описания общих понятий, разъяснения, примеры, толкования, «словотворчество»
- повторять или перефразировать реплику собеседника в подтверждении понимания его высказывания или вопроса;

- обратиться за помощью к собеседнику (уточнить вопрос, переспросить и др.);
- использовать мимику, жесты (вообще и в тех случаях, когда языковых средств не хватает для выражения тех или иных коммуникативных намерений).

#### 15.5. Подготовка к промежуточной аттестации

При подготовке к промежуточной аттестации целесообразно:

- внимательно изучить перечень вопросов и определить, в каких источниках находятся сведения, необходимые для ответа на них;
- внимательно прочитать рекомендованную литературу;
- составить краткие конспекты ответов (планы ответов).

### 17. Материально-техническое обеспечение дисциплины

Таблица 10

№ п/п	Наименование специализированных аудиторий и лабораторий	Наименование оборудования
1	Лекционная аудитория	Аудио-видео комплекс
2	Аудитории для проведения групповых и практических занятий	Аудио-видео комплекс
3	Компьютерный класс	Персональные компьютеры
4	Аудитория для курсового и дипломного проектирования	Персональные компьютеры
5	Аудитория для самостоятельной работы	Компьютерная техника
6	Читальный зал	Персональные компьютеры

Лист изменений № 1 от 9 января 2020 г

Рабочая программа дисциплины  
«Средства криптографической защиты информации»

Код и наименование направления подготовки/специальности:

**11.05.04 Инфокоммуникационные технологии и системы специальной связи**

Направленность/профиль образовательной программы:

**Системы радиосвязи специального назначения**

Из п. 14.2 Информационно-справочные системы исключить с 08.01.2020 г.  
строку: ЭБС IPRbooks (<http://www.iprbookshop.ru>)

Основание: прекращение контракта № 4784/19 от 25.01.2019 г. на предоставление доступа к электронно-библиотечной системе IPRbooks.

Внесенные изменения утверждаю:

Начальник УМУ \_\_\_\_\_ Л.А. Васильева