ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

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)

Регистрационный № 20.05/401-Д

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы защиты информации в телекоммуникационных системах
(наименование дисциплины)

образовательная программа высшего образования

11.03.02 Инфокоммуникационные технологии и системы связи
(код и наименование направления подготовки / специальности)

бакалавр
(квалификация)

Инфокоммуникационные системы и технологии
(направленность / профиль образовательной программы)

очная форма, заочная форма
(форма обучения)

Санкт-Петербург

Рабочая программа дисциплины составлена на основе требований Федерального государственного образовательного стандарта высшего образования по направлению (специальности) подготовки «11.03.02 Инфокоммуникационные технологии и системы связи», утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 930, и в соответствии с рабочим учебным планом, утвержденным ректором университета.

1. Цели и задачи дисциплины

Целью преподавания дисциплины «Основы защиты информации в телекоммуникационных системах» является:

знакомство с основными угрозами и основами защиты информации, ознакомление со стандартами в сфере защиты информации.

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

развитие творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы защиты информации в телекоммуникационных системах» Б1.В.07 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «11.03.02 Инфокоммуникационные технологии и системы связи». Изучение дисциплины «Основы защиты информации в телекоммуникационных системах» опирается на знании дисциплин(ы) «Информатика и основы алгоритмизации».

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 1

№ п/п	Код компетенции	Наименование компетенции
1	ПК-14	Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)
2	ПК-24	Способен определять параметры безопасности и защиты программного обеспечения сетевых устройств

Индикаторы достижения компетенций

Таблица 2

ПК-14.1	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-14.2	Умеет подключать и настраивать современные средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов); работать с контрольно-измерительными аппаратными и программными средствами
ПК-14.3	Владеет навыками установки дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация
ПК-14.4	Владеет навыками документирование настроек средств обеспечения безопасности удаленного доступа

ПК-24.1	Умеет выяснять приемлемые для пользователей параметры работы сети в условиях нормальной (обычной) работы (базовые параметры)
ПК-24.10	Знает инструкции по установке администрируемых сетевых устройств
ПК-24.11	Знает инструкции по эксплуатации администрируемых сетевых устройств
ПК-24.12	Знает инструкции по установке администрируемого программного обеспечения
ПК-24.13	Знает инструкции по эксплуатации администрируемого программного обеспечения
ПК-24.14	Знает протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
ПК-24.15	Знает модель ISO для управления сетевым трафиком
ПК-24.16	Знает модели IEEE
ПК-24.17	Знает защищенные протоколы управления
ПК-24.18	Знает основные средства криптографии
ПК-24.19	Знает регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
ПК-24.2	Умеет применять аппаратные средства защиты сетевых устройств от несанкционированного доступа
ПК-24.20	Знает требования охраны труда при работе с сетевой аппаратурой администрируемой сети
ПК-24.21	Владеет навыками планирования защиты приложений от несанкционированного доступа
ПК-24.22	Владеет навыками оценки безопасности и защиты приложений от несанкционированного доступа
ПК-24.23	Владеет навыками планирования защиты операционных систем от несанкционированного доступа
ПК-24.24	Владеет навыками оценки защиты операционных систем от несанкционированного доступа
ПК-24.3	Умеет применять программные средства защиты сетевых устройств от несанкционированного доступа
ПК-24.4	Умеет применять программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа
ПК-24.5	Умеет пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
ПК-24.6	Знает общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
ПК-24.7	Знает архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети
ПК-24.8	Знает классификацию операционных систем согласно классам безопасности
ПК-24.9	Знает средства защиты от несанкционированного доступа операционных систем и систем управления базами данных

4. Объем дисциплины и виды учебной работы

Очная форма обучения

Таблица 3

Вид учебной работы		**Всего часов**	**Семестры**
			3
Общая трудоемкость	3 ЗЕТ	108	108
Контактная работа с обучающимися		50.25	50.25
в том числе:			
Лекции		20	20
Практические занятия (ПЗ)		16	16

Лабораторные работы (ЛР)	14	14
Защита контрольной работы		-
Защита курсовой работы		-
Защита курсового проекта		-
Промежуточная аттестация	0.25	0.25
Самостоятельная работа обучающихся (СРС)	57.75	57.75
в том числе:		
Курсовая работа		-
Курсовой проект		-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала.	49.75	49.75
Подготовка к промежуточной аттестации	8	8
Вид промежуточной аттестации		Зачет

Заочная форма обучения

Таблица 4

Вид учебной работы		**Всего часов**	**Семестры**	
			ус3	3
Общая трудоемкость	3 ЗЕТ	108	6	102
Контактная работа с обучающимися		10.55	6	4.55
в том числе:				
Лекции		4	4	-
Практические занятия (ПЗ)		4	-	4
Лабораторные работы (ЛР)		2	2	-
Защита контрольной работы		0.3	-	0.3
Защита курсовой работы			-	-
Защита курсового проекта			-	-
Промежуточная аттестация		0.25	-	0.25
Самостоятельная работа обучающихся (СРС)		93.45	-	93.45
в том числе:				
Курсовая работа			-	-
Курсовой проект			-	-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала.		93.45	-	93.45
Подготовка к промежуточной аттестации		4	-	4
Вид промежуточной аттестации			-	Зачет

5. Содержание дисциплины

5.1. Содержание разделов дисциплины.

Таблица 5

№ п/п	**Наименование раздела (темы) дисциплины**	**Содержание раздела**	**№ семестра**		
			очная	**очно-заоч-**	**заоч-ная**

1	Раздел 1. Введение	Концепции информационной безопасности. Основные угрозы информации. Основные направления обеспечения информационной безопасности. Классификация средств, инженерно-техническая защита.	3		3
2	Раздел 2. Симметричные криптосистемы	Развитие криптографии. Блочные шифры. Алгоритм DES. Стандарт IEEE 802.11. Угрозы, связанные с использованием беспроводных сетей.Основные системы блочного и потокового шифрования. Основы криптоанализа.	3		3
3	Раздел 3. Ассиметричное шифрование	Основы систем с открытым ключом, алгоритм RSA. Цифровая подпись. Управление ключами. Проверка подлинности.	3		3
4	Раздел 4. Стеганография	Основные термины и определения. Скрытая передача и хранение данных. Типичные примеры стегосистем. Классификация основных методов атак на стегосистемы.	3		3
5	Раздел 5. Технологии аутентификации	Классификация методов идентификации и аутентификации. Электронные ключи. Системы радиочастотной идентификации. Использование магнитных карт и штрих кодов. Использование биометрической информации. Использование паролей. Сравнение различных технологий.	3		3
6	Раздел 6. СКУД	Элементы СКУД. Классификация идентификаторов. Основные типы видеоисточников информации. Структура цифровой системы видеонаблюдения.	3		3
7	Раздел 7. Безопасность компьютерных систем	Классификация компьютерных систем. Угрозы безопасности информации в компьютерных системах. Несанкционированный доступ к информации. Базовый принцип обеспечения безопасности. Правовое регулирование в области информационной безопасности. Защита информации в сетях от несанкционированного доступа.	3		3
8	Раздел 8. Проблемы безопасности операционных систем	Сетевая операционная система. Политика безопасности. Управление доступом. Аутентификация и авторизация. Требования, предъявляемые к сетевым операционным системам. Основы информационной безопасности операционных систем (Windows, UNIX).	3		3
9	Раздел 9. Компьютерные вирусы	Классификация компьютерных вирусов. Примеры компьютерных вирусов, признаки заражения. Классификация антивирусов.	3		3
10	Раздел 10. Анализ информационной безопасности сети предприятия	Планирование анализа сетевой безопасности. Многоуровневая защита. Типы анализа безопасности. Сканирование уязвимостей. Противодействие информационной разведке. Противодействие атакам на отказ в обслуживании. Анализ сетевого трафика.	3		3

5.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

Таблица 6

№ п/п	Наименование обеспечиваемых (последующих) дисциплин
1	Защищенные операционные системы
2	Основы криптографии

5.3. Разделы дисциплин и виды занятий.

Очная форма обучения

Таблица 7

№ п/п	Наименование раздела (темы) дисциплин	Лекции	Практ. занятия	Лаб. занятия	Семинары	СРС	Всего часов
1	Раздел 1. Введение	2	2	3		5	12
2	Раздел 2. Симметричные криптосистемы	2	2	3		5	12
3	Раздел 3. Ассиметричное шифрование	2	2	4		5	13
4	Раздел 4. Стеганография	2	2	4		5	13
5	Раздел 5. Технологии аутентификации	2	2			5	9
6	Раздел 6. СКУД	2	2			5	9
7	Раздел 7. Безопасность компьютерных систем	2	2			5	9
8	Раздел 8. Проблемы безопасности операционных систем	2	2			5	9
9	Раздел 9. Компьютерные вирусы	2				5	7
10	Раздел 10. Анализ информационной безопасности сети предприятия	2				4.75	6.75
	Итого:	20	16	14	-	49.75	99.75

Заочная форма обучения

Таблица 8

№ п/п	Наименование раздела (темы) дисциплин	Лекции	Практ. занятия	Лаб. занятия	Семинары	СРС	Всего часов
1	Раздел 1. Введение	0.4	0.5	0.5		9	10.4
2	Раздел 2. Симметричные криптосистемы	0.4	0.5	0.5		9	10.4
3	Раздел 3. Ассиметричное шифрование	0.4	0.5	0.5		9	10.4
4	Раздел 4. Стеганография	0.4	0.5	0.5		9	10.4
5	Раздел 5. Технологии аутентификации	0.4	0.5			9	9.9

6	Раздел 6. СКУД	0.4	0.5			9	9.9
7	Раздел 7. Безопасность компьютерных систем	0.4	0.5			9	9.9
8	Раздел 8. Проблемы безопасности операционных систем	0.4	0.5			9	9.9
9	Раздел 9. Компьютерные вирусы	0.4				9.45	9.85
10	Раздел 10. Анализ информационной безопасности сети предприятия	0.4				12	12.4
	Итого:	4	4	2	-	93.45	103.45

6. Лабораторный практикум

Очная форма обучения

Таблица 9

№ п/п	Номер раздела (темы)	Наименование лабораторной работы	Всего часов
1	1	Работа с антивирусными программами.	3
2	2	Основные технологии стеганографии (на примере стеганографии в изображениях).	3
3	3	Работа с прибором имитации радио закладок.	4
4	4	Анализ уязвимостей.	4
		Итого:	14

Заочная форма обучения

Таблица 10

№ п/п	Номер раздела (темы)	Наименование лабораторной работы	Всего часов
1	1	Работа с антивирусными программами.	0.5
2	2	Основные технологии стеганографии (на примере стеганографии в изображениях).	0.5
3	3	Работа с прибором имитации радио закладок.	0.5
4	4	Анализ уязвимостей.	0.5
		Итого:	2

7. Практические занятия (семинары)

Очная форма обучения

Таблица 11

№ п/п	Номер раздела (темы)	Наименование практических занятий (семинаров)	Всего часов
1	1	Статические методы анализа шифров на основе шифра простой замены	2
2	2	Характеристики блоковых шифров	2

3	3	Характеристики потоковых шифров	2
4	4	Теория чисел применительно к построению криптосистем.	2
5	5	Ассиметричные системы шифрования (RSA)	2
6	6	Изучение основ СКУД	2
7	7	Основные технологии уязвимостей операционных систем	2
8	8	Технологии аутентификации в ОС	2
		Итого:	16

Заочная форма обучения

Таблица 12

№ п/п	Номер раздела (темы)	Наименование практических занятий (семинаров)	Всего часов
1	1	Статические методы анализа шифров на основе шифра простой замены	0.5
2	2	Характеристики блоковых шифров	0.5
3	3	Характеристики потоковых шифров	0.5
4	4	Теория чисел применительно к построению криптосистем.	0.5
5	5	Ассиметричные системы шифрования (RSA)	0.5
6	6	Изучение основ СКУД	0.5
7	7	Основные технологии уязвимостей операционных систем	0.5
8	8	Технологии аутентификации в ОС	0.5
		Итого:	4

8. Примерная тематика курсовых проектов (работ)

Рабочим учебным планом не предусмотрено

9. Самостоятельная работа

Очная форма обучения

Таблица 13

№ раздела дисципли-ны	Содержание СРС	Форма контроля	Всего часов
1	Изучение концепции информационной безопасности Введение в дисциплину.	Отчет	5
2	Изучение симметричных криптосистем. Подготовка к лабораторным работам.	Отчет	5
3	Изучение ассиметричного шифрования. Подготовка к лабораторным работам.	Отчет	5
4	Стеганография. Подготовка к лабораторным работам.	Отчет	5
5	Технологии аутентификации. Подготовка к лабораторным работам.	Отчет	5
6	СКУД. Подготовка к лабораторным работам.	Отчет	5
7	Безопасность компьютерных систем. Подготовка к лабораторным работам.	Отчет	5
8	Проблемы безопасности операционных систем. Подготовка к лабораторным работам.	Отчет	5

9	Компьютерные вирусы. Подготовка к лабораторным работам.	Отчет	5
10	Анализ информационной безопасности сети предприятия. Подготовка к лабораторным работам.	Отчет	4.75
		Итого:	49.75

Заочная форма обучения

Таблица 14

№ раздела дисциплины	Содержание СРС	Форма контроля	Всего часов
1	Изучение концепции информационной безопасности Введение в дисциплину.	Отчет	9
2	Изучение симметричных криптосистем. Подготовка к лабораторным работам.	Отчет	9
3	Изучение ассиметричного шифрования. Подготовка к лабораторным работам.	Отчет	9
4	Стеганография. Подготовка к лабораторным работам.	Отчет	9
5	Технологии аутентификации. Подготовка к лабораторным работам.	Отчет	9
6	СКУД. Подготовка к лабораторным работам.	Отчет	9
7	Безопасность компьютерных систем. Подготовка к лабораторным работам.	Отчет	9
8	Проблемы безопасности операционных систем. Подготовка к лабораторным работам.	Отчет	9
9	Компьютерные вирусы. Подготовка к лабораторным работам.	Отчет	9.45
10	Анализ информационной безопасности сети предприятия. Подготовка к лабораторным работам.	Отчет	12
		Итого:	93.45

10. 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;
- методические указания к выполнению лабораторных работ для студентов;

11. 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 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.

12. Перечень основной и дополнительной литературы, необходимой для освоений дисциплины

12.1. Основная литература:

1. Коржик, Валерий Иванович. Основы криптографии [Текст] : учебное пособие по спец. 210403 "Защищенные телекоммуникационные системы связи" / В. И. Коржик, В. П. Просихин ; рец.: Р. Р. Биккенин, Б. В. Изотов. - СПб. : Линк, 2008. - 256 с. : ил. - Библиогр. в конце частей. - ISBN 5-98595-012-3 : 300.00 р.
2. Основы информационной безопасности сетей и систем [Текст] : учебное пособие / Д. И. Кириллов [и др.] ; 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. Ч. 1. - 2012. - 63 с. : ил. - 206.91 р.
3. Основы информационной безопасности сетей и систем [Текст] : учебное пособие / Д. И. Кириллов [и др.] ; 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. Ч. 2. - 2012. - 65 с. : ил. - 206.91 р.
4. 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.
5. Коржик, Валерий Иванович. Основы криптографии [Текст] : учебное пособие / В. И. Коржик, В. П. Просихин, В. А. Яковлев ; рец.: Р. Р. Биккенин, 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". - 2-е изд. - СПб. : СПбГУТ, 2014. - 275 с. : ил., табл. - ISBN 978-5-89160-097-3 : 1579.51 р.
6. Коржик, Валерий Иванович. Основы криптографии [Текст] : учебное пособие / В. И. Коржик, В. А. Яковлев ; рец.: Р. Р. Биккенин, Б. В. Изотов. - СПб. : СПбГУТ, 2016. - 296 с. : ил., табл. - ISBN 978-5-89160-097-3 : 600.00 р.

12.2. Дополнительная литература:

1. Бабков, И. Н. Защита информации от утечки по техническим каналам в телекоммуникационных системах [Электронный ресурс] : учебное пособие по спец. 201800 / И. Н. Бабков, В. П. Просихин ; Министерство РФ по связи и информатизации, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. - СПб. : СПбГУТ, 2002. - 54 с. : ил. - 50.00 р.
2. Зубов, А. Ю. Криптографические методы защиты информации. Совершенные шифры [Текст] : учеб. пособие / А. Ю. Зубов ; рец.: В. Б. Алексеев, Э. А. Применко, А. Б. Лось. - М. : Гелиос АРВ, 2005. - 191 с. : ил. - Библиогр.: с. 187-189. - ISBN 5-85438-135-4 (в обл.) : 77.00 р.
3. Защита информации в системах мобильной связи [Текст] : учеб. пособие для вузов / А. А. Чекалин [и др.] ; науч. ред.: А. В. Заряев, С. В. Скрыля ; рец. Н. Н. Толстых. - 2-е изд., испр. и доп. - М. : Горячая линия-Телеком, 2005. - 171, [4] с. : ил. - Библиогр.: с. 167-168. - ISBN 5-93517-269-0 (в обл.) : 132.00 р.
4. Красов, Андрей Владимирович. Безопасность IP-телефонии [Текст] : методические указания к лабораторным работам 210403 / А. В. Красов, Д. И. Кириллов, В. В. Кондратьев ; рец. С. Е. Душин ; Федеральное агентство связи, СПбГУТ им. проф. М. А. Бонч-Бруевича. - СПб. : СПбГУТ, 2008. - 66 с. : ил + табл. - Библиогр. : с.65. - 97.75 р.
5. Коржик, Валерий Иванович. Основы криптографии [Электронный ресурс] : метод. указ. к лаб. работам / В. И. Коржик, К. А. Небаева ; Федер. агентство связи, Гос. образовательное учреждение высш. проф. образования "С.-Петерб. гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ. Ч. 1. - 2011. - 64 с. : ил. - Библиогр.: с. 64. - (в обл.) : 253.45 р.
6. Андрианов, В. И. Инновационное управление рисками информационной безопасности [Электронный ресурс] : учеб. пособие / В. И. Андрианов, А. В. Красов, В. А. Липатников ; рец.: С. Е. Душин, Е. В. Стельмашонок ; Федер. агентство связи, Федер. гос. образовательное бюдж. учреждение высш. проф.

образования "С.-Петерб. гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2012. - 396 с. : ил. - Библиогр.: с. 394-395. - ISBN 978-5-91891-092-4 (в обл.) : 320.00 р.

7. Основы информационной безопасности сетей и систем [Текст] : методические указания к лабораторным работам / Д. И. Кириллов [и др.] ; 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. - 42 с. : ил. - 169.86 р.
8. Красов, Андрей Владимирович. Основы защиты информации в телекоммуникационных системах [Электронный ресурс] : методические указания к лабораторным работам / А. В. Красов, М. В. Левин, И. А. Ушаков ; рец. В. В. Княжицкий ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2013. - 23 с. : ил. - 38.55 р.
9. Голиков, А. М. Сети и системы радиосвязи и средства их информационной защиты [Электронный ресурс] : учебное пособие / Голиков А. М. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2007. - 392 с. - ISBN 978-5-86889-393-3 : Б. ц. Книга находится в Премиум-версии ЭБС IPRbooks.
10. Организационно-техническое обеспечение устойчивости функционирования и безопасности сетей связи общего пользования [Электронный ресурс] : монография / М. В. Буйневич [и др.] ; рец.: П. В. Филиппов, С. И. Биденко, И. Г. Малыгин ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2013. - 144 с. : ил. - Б. ц.
11. Организационно-техническое обеспечение устойчивости функционирования и безопасности сетей связи общего пользования [Текст] : монография / М. В. Буйневич [и др.] ; рец.: И. П. Филиппов, С. И. Биденко, И. Г. Малыгин ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2013. - 143 с. : ил. - ISBN 978-5-89160-0874 : 706.00 р.
12. Милославская, Н. Г. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов [Электронный ресурс] / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М. : Горячая линия–Телеком, 2013. - 166 с. : ил. - ISBN 978-5-9912-0275-6 : Б. ц.
13. Чуянов Проблемы защищенности телекоммуникационных систем [Электронный ресурс] : учебное пособие / Чуянов. - Омск : Омская академия МВД России, 2015. - 164 с. - ISBN 978-5-88651-601-2 : Б. ц. Книга находится в Премиум-версии ЭБС

IPRbooks.

13. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Ресурсы информационно-телекоммуникационной сети «Интернет» из указанного перечня являются рекомендуемыми дополнительными (вспомогательными) источниками официальной информации, размещенной на легальных основаниях с открытым доступом. За полноту содержания и качество работу сайтов несет ответственность правообладатель.

Таблица 15

Наименование ресурса	Адрес
Поисковая система google.com	google.ru
Поисковая система	yandex.ru

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

14.1. Программное обеспечение дисциплины:

- Cisco Packet Tracer
- Linux
- Maxima
- Windows ИКСС

14.2. Информационно-справочные системы:

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

15. Методические указания для обучающихся по освоению дисциплины

15.1. Планирование и организация времени, необходимого для изучения дисциплины

Важным условием успешного освоения дисциплины «Основы защиты информации в телекоммуникационных системах» 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 информации 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).

16. Материально-техническое обеспечение дисциплины

Таблица 16

№ 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
7	Лаборатория "Цифровая обработка сигналов" компании Texas Instruments	Лабораторные стенды (установки) Контрольно-измерительные приборы
8	Лаборатория программно-аппаратных средств обеспечения информационной безопасности	Лабораторные стенды (установки) Контрольно-измерительные приборы
9	Лаборатория распределенных систем безопасности	Лабораторные стенды (установки) Контрольно-измерительные приборы