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 Безопасности информационных систем
(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
Первый проректор – проректор по учебной работе
_____ А.В. Абилов
«23» 06 2023 г.

Регистрационный №_23.02/341-Д

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографическая защита информации
(наименование дисциплины)

образовательная программа высшего образования

09.03.02 Информационные системы и технологии
(код и наименование направления подготовки / специальности)

бакалавр
(квалификация)

Технологии проектирования защищенных систем обработки данных
(направленность / профиль образовательной программы)

очная форма, очно-заочная форма
(форма обучения)

Санкт-Петербург

Рабочая программа дисциплины составлена на основе требований Федерального государственного образовательного стандарта высшего образования по направлению (специальности) подготовки «09.03.02 Информационные системы и технологии», утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 926, и в соответствии с рабочим учебным планом, утвержденным ректором университета.

1. Цели и задачи дисциплины

Целью преподавания дисциплины «Криптографическая защита информации» является:

формирование системы теоретических знаний и практических навыков в области информационной безопасности и криптографической защиты информации как фундаментальной базы информационной культуры высокообразованной личности, а также создание необходимой базы (знаний) для успешного овладения последующих специальных дисциплин учебного плана; должна способствовать развитию творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания.

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

изучением основных алгоритмов шифрования; умением производить элементарные операции над шифрами, работать с алгоритмами шифрования; освоением основных криптографических методов и средств защиты информации; освоением простейших методов криптоанализа и методов оценки стойкости криптографических алгоритмов.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Криптографическая защита информации» Б1.В.10 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «09.03.02 Информационные системы и технологии». Изучение дисциплины «Криптографическая защита информации» опирается на знании дисциплин(ы) «Введение в профессию»; «Дискретная математика»; «Методы и средства защиты информации».

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-31	Способность обеспечивать информационную безопасность хранилищ и баз данных, баз знаний
2	УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

Индикаторы достижения компетенций

Таблица 2

ПК-31.1	Знать: угрозы и мероприятия по обеспечению информационной безопасности хранилищ и баз данных, баз знаний
ПК-31.2	Уметь: выявлять угрозы и разрабатывать мероприятия по обеспечению информационной безопасности хранилищ и баз данных, баз знаний

ПК-31.3	Иметь навыки: идентификации угроз и реализации мероприятий по обеспечению информационной безопасности хранилищ и баз данных, баз знаний
УК-1.1	Знать: методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа.
УК-1.2	Уметь: применять методики поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач.
УК-1.3	Владеть: методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач.

4. Объем дисциплины и виды учебной работы

Очная форма обучения

Таблица 3

Вид учебной работы		**Всего часов**	**Семестры**
			3
Общая трудоемкость	4 ЗЕТ	144	144
Контактная работа с обучающимися		50.25	50.25
в том числе:			
Лекции		20	20
Практические занятия (ПЗ)		30	30
Лабораторные работы (ЛР)			-
Защита контрольной работы			-
Защита курсовой работы			-
Защита курсового проекта			-
Промежуточная аттестация		0.25	0.25
Самостоятельная работа обучающихся (СРС)		93.75	93.75
в том числе:			
Курсовая работа			-
Курсовой проект			-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала		85.75	85.75
Подготовка к промежуточной аттестации		8	8
Вид промежуточной аттестации			Зачет

Очно-заочная форма обучения

Таблица 4

Вид учебной работы		**Всего часов**	**Семестры**
			4
Общая трудоемкость	4 ЗЕТ	144	144
Контактная работа с обучающимися		36.25	36.25
в том числе:			
Лекции		12	12
Практические занятия (ПЗ)		24	24
Лабораторные работы (ЛР)			-
Защита контрольной работы			-
Защита курсовой работы			-
Защита курсового проекта			-

Промежуточная аттестация	0.25	0.25
Самостоятельная работа обучающихся (СРС)	107.75	107.75
в том числе:		
Курсовая работа		-
Курсовой проект		-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала	99.75	99.75
Подготовка к промежуточной аттестации	8	8
Вид промежуточной аттестации		Зачет

5. Содержание дисциплины

5.1. Содержание разделов дисциплины.

Таблица 5

№ п/п	Наименование раздела дисциплины	Содержание раздела	№ семестра		
			очная	очно-заочная	заочная
1	Раздел 1. Основные понятия и задачи криптографии	Основные понятия криптографии и криптоанализа: криптографическое преобразование информации, отправитель и получатель информации, канал связи, открытое сообщение, криптографический ключ, процессы шифрования и расшифрования, криптограмма, криптографическая система, противник и его атаки. Методы криптографической защиты информации и роль криптографии в обеспечении безопасности информации. Основные задачи криптографии: обеспечение установленного режима доступа к информации, обеспечение целостности информации, аутентификация автора сообщения. История криптографии. Классические шифры. Шифры замены и перестановки. Классические шифры перестановки: «Сцитала», табличные перестановки, поворотные решетки. Криптоанализ простых шифров перестановки.	3	4	
2	Раздел 2. Шифры. Симметричные криптосистемы	Блочные и потоковые шифры. Классификация шифров замены. Шифры одноалфавитной (простой) замены. Криптосистема Цезаря. Частотный анализ шифров простой замены. Перестановки. Моноалфавитные и многоалфавитные подстановки. Системы шифрования Виженера. Псевдослучайные генераторы. Гаммирование. Стандарты шифрования AES и ГОСТ. Моноалфавитные и многоалфавитные подстановки. Системы шифрования Виженера. Псевдослучайные генераторы. Алгоритмы гаммирования. Стандарты шифрования.	3	4	

3	Раздел 3. Модели асимметричных криптосистем.	Двух-ключевые системы шифрации. Системы шифрования с открытым ключом. Однонаправленные функции. Алгоритм RSA. Криптографические хэш функции. Криптосистемы на эллиптических ключах. Изучение асимметричных криптосистем, процедур аутентификации и ЭЦП. Криптосистемы без передачи ключей.	3	4	
4	Раздел 4. Электронная подпись	Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012. DSS. Инфраструктура открытого ключа.	3	4	
5	Раздел 5. Криптографические протоколы	Основные понятия. Понятие криптографического протокола. Свойства, характеризующие безопасность протоколов. Виды криптографических протоколов. Основные атаки на безопасность протоколов. Протоколы сертификации ключей, протоколы распределения ключей.	3	4	
6	Раздел 6. Основы стеганографии	Стеганография в XXI веке. Цели. Практическое применение. Актуальность. Способы встраивания стеганографмческий информации. Методы обнаружения.	3	4	

5.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

Таблица 6

№ п/п	Наименование обеспечиваемых (последующих) дисциплин
1	Методы и средства проектирования информационных систем и технологий
2	Системы ведения хранилищ данных
3	Управление ИТ-проектами

5.3. Разделы дисциплин и виды занятий.

Очная форма обучения

Таблица 7

№ п/п	Наименование раздела дисциплины	Лекции	Практ. занятия	Лаб. занятия	Семинары	СРС	Всего часов
1	Раздел 1. Основные понятия и задачи криптографии	4				10	14
2	Раздел 2. Шифры. Симметричные криптосистемы	4	14			22	40
3	Раздел 3. Модели асимметричных криптосистем.	4	4			18	26
4	Раздел 4. Электронная подпись	2	2			10	14
5	Раздел 5. Криптографические протоколы	2	2			10.75	14.75
6	Раздел 6. Основы стеганографии	4	8			15	27
	Итого:	20	30	-	-	85.75	135.75

Очно-заочная форма обучения

Таблица 8

№ п/п	Наименование раздела дисциплины	Лек-ции	Практ. занятия	Лаб. занятия	Семи-нары	СРС	Всего часов
1	Раздел 1. Основные понятия и задачи криптографии	2				14	16
2	Раздел 2. Шифры. Симметричные криптосистемы	2	14			22	38
3	Раздел 3. Модели асимметричных криптосистем.	2	2			19	23
4	Раздел 4. Электронная подпись	2	2			14	18
5	Раздел 5. Криптографические протоколы	2	2			14.75	18.75
6	Раздел 6. Основы стеганографии	2	4			16	22
Итого:		12	24	-	-	99.75	135.75

6. Лекции

Очная форма обучения

Таблица 9

№ п/п	Номер раздела	Тема лекции	Всего часов
1	1	Основные понятия криптографии и криптоанализа: криптографическое преобразование информации, криптографический ключ, противник и его атаки. Методы криптографической защиты информации и роль криптографии в обеспечении безопасности информации. История криптографии. Классические шифры.	2
2	1	Основные задачи криптографии: обеспечение установленного режима доступа к информации, обеспечение целостности информации, аутентификация автора сообщения. Криптоанализ простых шифров перестановки.	2
3	2	Блочные и потоковые шифры. Классификация шифров замены. Шифры одноалфавитной (простой) замены. Криптосистема Цезаря. Частотный анализ шифров простой замены.	2
4	2	Моноалфавитные и многоалфавитные подстановки. Системы шифрования Виженера. Псевдослучайные генераторы. Алгоритмы гаммирования. Стандарты шифрования DES и ГОСТ.	2
5	3	Двух-ключевые системы шифрации. Однонаправленные функции. Алгоритм RSA. Криптографические хэш функции.	2
6	3	Криптосистемы на эллиптических ключах. Изучение асимметричных криптосистем, процедур аутентификации и ЭЦП. Криптосистемы без передачи ключей.	2
7	4	Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012. DSS. Инфраструктура открытого ключа.. Основы стеганографии.	2
8	5	Понятие криптографического протокола. Свойства, характеризующие безопасность протоколов. Виды криптографических протоколов. Основные атаки на безопасность протоколов. Протоколы сертификации ключей, протоколы распределения ключей.	2
9	6	Стеганография в XXI веке. Цели. Практическое применение. Актуальность.	2
10	6	Способы встраивания стеганографмческий информации. Методы обнаружения.	2

Итого:	20

Очно-заочная форма обучения

Таблица 10

№ п/п	Номер раздела	Тема лекции	Всего часов
1	1	Основные понятия криптографии и криптоанализа: криптографическое преобразование информации, криптографический ключ, противник и его атаки. Методы криптографической защиты информации и роль криптографии в обеспечении безопасности информации. История криптографии. Классические шифры. Основные задачи криптографии: обеспечение установленного режима доступа к информации, обеспечение целостности информации, аутентификация автора сообщения. Криптоанализ простых шифров перестановки.	2
2	2	Блочные и потоковые шифры. Классификация шифров замены. Шифры одноалфавитной (простой) замены. Криптосистема Цезаря. Частотный анализ шифров простой замены. Моноалфавитные и многоалфавитные подстановки. Системы шифрования Виженера. Псевдослучайные генераторы. Гаммирование. Стандарты шифрования DES и ГОСТ.	2
3	3	Двух-ключевые системы шифрации. Однонаправленные функции. Алгоритм RSA. Криптографические хэш функции. Криптосистемы на эллиптических ключах. Изучение асимметричных криптосистем, процедур аутентификации и ЭЦП. Криптосистемы без передачи ключей.	2
4	4	Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012. DSS. Инфраструктура открытого ключа.. Основы стеганографии.	2
5	5	Основные понятия. Понятие криптографического протокола. Свойства, характеризующие безопасность протоколов. Виды криптографических протоколов. Основные атаки на безопасность протоколов. Протоколы сертификации ключей, протоколы распределения ключей.	2
6	6	Стеганография в XXI веке. Цели. Практическое применение. Актуальность. Способы встраивания стеганографмческий информации. Методы обнаружения.	2
		Итого:	12

7. Лабораторный практикум

Рабочим учебным планом не предусмотрено

8. Практические занятия (семинары)

Очная форма обучения

Таблица 11

№ п/п	Номер раздела	Тема занятия	Всего часов
1	2	Реализация и исследование простейших алгоритмов шифрования в ручном режиме	2
2	2	Реализация и исследование алгоритма шифрования по таблице Виженера	4
3	2	Алгоритм шифрования AES	4

4	2	Слайдовая атака алгоритмов блочного шифрования	4
5	3	Алгоритм шифрования RSA	4
6	4	Исследование алгоритмов ЦЭП. Электронная подпись. ГОСТ Р 34.10-2012, DSS.	2
7	5	Исследование основных криптографических протоколов	2
8	6	Применение стеганографии для защиты конфиденциальной информации	4
9	6	Разработка программы для извлечения (встраивания) стеганографического сообщения	4
		Итого:	30

Очно-заочная форма обучения

Таблица 12

№ п/п	Номер раздела	Тема занятия	Всего часов
1	2	Реализация и исследование простейших алгоритмов шифрования в ручном режиме	2
2	2	Реализация и исследование алгоритма шифрования по таблице Виженера	4
3	2	Алгоритм шифрования AES	4
4	2	Слайдовая атака алгоритмов блочного шифрования	4
5	3	Алгоритм шифрования RSA	2
6	4	Исследование алгоритмов ЦЭП. Электронная подпись. ГОСТ Р 34.10-2012, DSS.	2
7	5	Исследование основных криптографических протоколов	2
8	6	Применение стеганографии для защиты конфиденциальной информации	2
9	6	Разработка программы для извлечения (встраивания) стеганографического сообщения	2
		Итого:	24

9. Примерная тематика курсовых проектов (работ)

Рабочим учебным планом не предусмотрено

10. Самостоятельная работа

Очная форма обучения

Таблица 13

№ п/п	Номер раздела	Содержание самостоятельной работы	Форма контроля	Всего часов
1	1	Основные понятия и задачи криптографии	Оценка работы на занятии. Выполнение задания.	10
2	2	Шифры. Симметричные криптосистемы	Оценка работы на занятии. Выполнение задания.	22
3	3	Модели асимметричных криптосистем.	Оценка работы на занятии. Выполнение задания.	18

4	4	Электронная подпись	Оценка работы на занятии. Выполнение задания.	10
5	5	Криптографические протоколы	Оценка работы на занятии. Выполнение задания.	10.75
6	6	Основы стеганографии.	Оценка работы на занятии. Выполнение задания.	15
			Итого:	85.75

Очно-заочная форма обучения

Таблица 14

№ п/п	Номер раздела	Содержание самостоятельной работы	Форма контроля	Всего часов
1	1	Основные понятия и задачи криптографии	Оценка работы на занятии. Выполнение задания.	14
2	2	Шифры. Симметричные криптосистемы	Оценка работы на занятии. Выполнение задания.	22
3	3	Модели асимметричных криптосистем.	Оценка работы на занятии. Выполнение задания.	19
4	4	Электронная подпись	Оценка работы на занятии. Выполнение задания.	14
5	5	Криптографические протоколы	Оценка работы на занятии. Выполнение задания.	14.75
6	6	Основы стеганографии.	Оценка работы на занятии. Выполнение задания.	16
			Итого:	99.75

11. Перечень учебно-методического обеспечения 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 освоения дисциплины

13.1. Основная литература:

1. Молдовян, А. А.
   Криптография : учебник для вузов / А. А. Молдовян, Н. А. Молдовян, Б. Я. Советов. - СПб. : Лань, 2001. - 218 с. : ил. - (Учебники для вузов. Специальная литература). - ISBN 5-8114-0246-5 : 60.50 р. - Текст : непосредственный.
2. 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.
3. Басалова, Г. В.
   Основы криптографии : [Электронный ресурс] : учебное пособие / Г. В. Басалова. - 2-е изд. - М. : ИНТУИТ, 2016. - 282 с. - URL: https://e.lanbook.com/book/100302. - Б. ц. Книга из коллекции ИНТУИТ - Информатика
4. Грибунин, В. Г.
   Цифровая стеганография : [Электронный ресурс] : учебное пособие / В. Г.

Грибунин, И. Н. Оков, И. В. Туринцев. - М. : СОЛОН-Пресс, 2017. - 262 с. - URL: https://e.lanbook.com/book/119110. - ISBN 978-5-91359-173-9 : Б. ц. Книга из коллекции СОЛОН-Пресс - Информатика . - [Б. м. : б. и.]. - https://e.lanbook.com/book/13655

5. Шаньгин, В. Ф.
Информационная безопасность компьютерных систем и сетей : [Электронный ресурс] : учебное пособие / Шаньгин В. Ф. - М. : ФОРУМ ; М. : ИНФРА-М, 2021. - 416 с. - URL: http://ibooks.ru/reading.php?productid=361273. - ISBN 978-5-8199-0754-2 : Б. ц.
6. Нестеров, С. А.
Основы информационной безопасности : [Электронный ресурс] : учебное пособие / С. А. Нестеров. - 5-е изд., стер. - Санкт-Петербург : Лань, 2022. - 324 с. - URL: https://e.lanbook.com/book/206279. - ISBN 978-5-8114-4067-2 : Б. ц. Книга из коллекции Лань - Информатика Предыдущее издание:Нестеров С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров, 2019. - 324 с. . - [Б. м. : б. и.]. - https://e.lanbook.com/book/114688

13.2. Дополнительная литература:

1. Коржик, Валерий Иванович. Основы криптографии : 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.
2. Коржик, Валерий Иванович.
Основы криптографии : учеб. пособие по спец. 210403 "Защищенные телекоммуникационные системы связи" / В. И. Коржик, В. П. Просихин ; рец.: Р. Р. Биккенин, Б. В. Изотов. - СПб. : Линк, 2008. - 249, [6] с. : ил. - Библиогр. в конце частей. - ISBN 5-98595-012-3 (в пер.) : 300.00 р. - Текст : непосредственный.
3. Коржик, Валерий Иванович.
Основы стеганографии : [Электронный ресурс] : учебно-методическое пособие по выполнению практических заданий / В. И. Коржик, К. А. Небаева ; рец. Р. Р. Биккенин ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2015. - 20 с. : табл. - 207.93 р.
4. Цифровая стеганография и цифровые водяные знаки : в 2 ч. / Федер. агентство связи, Федер. гос. бюдж. образовательное учреждение высш. образования "С.-Петерб. гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича"; общ. ред. В. И. Коржик. - СПб. : СПбГУТ, 2016 - 2017. - ISBN 978-5-89160-125-3. Ч. 1 : Цифровая стеганография / В. И. Коржик, К. А. Небаева, Е. Ю. Герлинг [и др.]. - 2016. - 225 с. : ил. - Библиогр. в конце разд. - ISBN 978-5-89160-136-9 (в обл.) : 1375.17 р.

5. Нормативное обеспечение эксплуатации средств защиты информации : [Электронный ресурс] : учеб. пособие / А. В. Красов, И. И. Лившиц, Д. В. Юркин [и

др.] ; рец.: А. А. Молдовян, Л. Б. Бузюков ; Федер. агентство связи, Федер. гос. бюдж. образовательное учреждение высш. образования "С.-Петерб. гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2017. - 67 с. : ил. - 325.20 р.
6. Цифровая стеганография и цифровые водяные знаки : в 2 ч. / Федер. агентство связи, Федер. гос. бюдж. образовательное учреждение высш. образования "С.-Петерб. гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича"; общ. ред. В. И. Коржик. - СПб. : СПбГУТ, 2016 - 2017. - ISBN 978-5-89160-125-3. Ч. 2 : Цифровые водяные знаки / В. И. Коржик, С. О. Анфиногенов, А. И. Кочкарев [и др.]. - 2017. - 197 с. : ил. - Библиогр. в конце разд. - ISBN 978-5-89160-153-6 (в обл.) : 1394.17 р.
7. Нестеров, С. А.
Основы интеллектуального анализа данных. Лабораторный практикум : [Электронный ресурс] : учебное пособие / С. А. Нестеров. - Санкт-Петербург : Лань, 2020. - 40 с. - URL: https://e.lanbook.com/book/130181. - ISBN 978-5-8114-4509-7. Книга из коллекции Лань - Информатика
8. Рацеев, С. М.
Математические методы защиты информации и их основы. Сборник задач : [Электронный ресурс] : учебное пособие / С. М. Рацеев. - СПб. : Лань, 2023. - 140 с. - (Высшее образование). - URL: https://e.lanbook.com/book/292913. - ISBN 978-5-507-45197-5 : Б. ц.

14. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

- www.sut.ru
- lib.spbgut.ru/jirbis2_spbgut

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.spbgut.ru)

15.3. Дополнительные источники

- ИНТУИТ (https://intuit.ru)

16. Методические указания для обучающихся по освоению дисциплины

16.1. Планирование и организация времени, необходимого для изучения дисциплины

Важным условием успешного освоения дисциплины «Криптографическая защита 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.

16.2. 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.

16.3. 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.

16.4. 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 обучающегося 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 подтверждение 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).

16.5. 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 15

№ 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