

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 № 19.05/2148-Д

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические методы защиты информации
(наименование дисциплины)

образовательная программа высшего образования

12.03.03 Фотоника и оптоинформатика

(код и наименование направления подготовки / специальности)

бакалавр

(квалификация)

Фотоника в инфокоммуникациях

(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 «12.03.03 Фотоника и оптоинформатика», утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 949, и в соответствии с рабочим учебным планом, утвержденным ректором университета.

1. Цели и задачи дисциплины

Целью преподавания дисциплины «Криптографические методы защиты информации» является:

Целью дисциплины является формирование у обучаемых знаний в области принципов криптографических преобразований, типовые программно-аппаратных средств криптографической защиты информации и инфокоммуникаций от несанкционированного доступа.

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

В результате изучения дисциплины у студентов должны сформироваться знания, умения и навыки, позволяющие проводить самостоятельный криптографический анализ информационных процессов, формируемых в системах инфокоммуникаций, как изучаемых в настоящей дисциплине, так и находящихся за ее рамками. В результате изучения настоящей дисциплины студенты должны получить знания, имеющие не только самостоятельное значение, но и обеспечивающие базовую подготовку для усвоения ряда последующих дисциплин в области программно-защищенных инфокоммуникаций.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Криптографические методы защиты информации» Б1.В.26 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «12.03.03 Фотоника и оптоинформатика». Изучение дисциплины «Криптографические методы защиты информации» опирается на знания дисциплин(ы) «Высшая математика».

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	ОПК-4	Способен использовать современные информационные технологии и программное обеспечение при решении задач профессиональной деятельности, соблюдая требования информационной безопасности

Индикаторы достижения компетенций

Таблица 2

ОПК-4.1	Использует современные информационные технологии и программное обеспечение при решении задач профессиональной деятельности
ОПК-4.2	Соблюдает требования информационной безопасности при использовании современных информационных технологий и программного обеспечения

4. Объем дисциплины и виды учебной работы

Очная форма обучения

Таблица 3

Вид учебной работы		Всего часов	Семестры
			8
Общая трудоемкость	4 ЗЕТ	144	144
Контактная работа с обучающимися		52.35	52.35
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		2.35	2.35
Самостоятельная работа обучающихся (СРС)		58	58
в том числе:			
Курсовая работа			-
Курсовой проект			-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала.		58	58
Подготовка к промежуточной аттестации		33.65	33.65
Вид промежуточной аттестации			Экзамен

5. Содержание дисциплины

5.1. Содержание разделов дисциплины.

Таблица 4

№ п/п	Наименование раздела (темы) дисциплины	Содержание раздела	№ семестра		
			очная	очно-заочная	заочная
1	Раздел 1. Методы и средства криптографии в инфокоммуникациях	История криптографии. Основные понятия и определения. Требования к криптографическим системам. Исторические шифры. Современные методы и средства криптографии.	8		
2	Раздел 2. Симметричные криптографические системы, использующие блочные шифры.	Основные классы симметричных криптосистем. Общие сведения о блочных шифрах. Примеры алгоритмов блочного шифрования: DES и его модификации, AES (Rijndael), RC5, Российский стандарт ГОСТ28147-89. Режимы использования блочных шифров. Многократное шифрование	8		
3	Раздел 3. Симметричные криптографические системы использующие потоковые шифры.	Особенности потоковых шифров. Свойства линейного рекуррентного регистра. Нелинейные узлы усложнения. Примеры алгоритмов потокового шифрования: RC4, A5/1.	8		

4	Раздел 4. Симметричные криптографические системы использующие потоковые шифры.	Классификации систем аутентификации и характеристики их эффективности. Безусловно стойкие системы аутентификации. Вычислительно стойкие системы аутентификации. Использование модификаций блочных шифров. Примеры систем аутентификаций , использующих блочные шифры (ГОСТ28147 и др.)	8		
5	Раздел 5. Основные принципы построения несимметричных криптосистем (криптосистем с открытым ключом).	Основные требования , предъявляемые к криптосистемам с открытым ключом. Основы теории чисел и теории конечных полей. Свойства эллиптических кривых.	8		
6	Раздел 6. Примеры построения криптосистем с открытым ключом	Криптосистемы : РША , Рабина, Эль-Гамала, Диффи-Хеллмана , Мак-Элис. Построение криптосистем на основе теории эллиптических кривых. Использование сертификатов.	8		
7	Раздел 7. Электронные (цифровые подписи) и криптографические протоколы..	Принцип построения цифровых подписей (ЦП) на основе использования криптосистем с открытым ключом. Определение и свойства криптографических хеш-функций. Примеры построения ЦП :DSA, ГОСТ Р 3410-94. Понятие о криптографических протоколах. Примеры криптографических протоколов : разделение секретов , идентификация , совместные вычисления , тайное голосование. Методы формирования и распределения аутентифицированных ключей.	8		

5.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

Таблица 5

№ п/п	Наименование обеспечиваемых (последующих) дисциплин
1	Квантовая электроника

5.3. Разделы дисциплин и виды занятий.

Очная форма обучения

Таблица 6

№ п/п	Наименование раздела (темы) дисциплин	Лек-ции	Практ. занятия	Лаб. занятия	Семи-нары	СРС	Всего часов
1	Раздел 1. Методы и средства криптографии в инфокоммуникациях	2	4	2		12	20
2	Раздел 2. Симметричные криптографические системы , использующие блочные шифры.	2	2	2		12	18

3	Раздел 3. Симметричные криптографические системы использующие потоковые шифры.	2	4	2		12	20
4	Раздел 4. Симметричные криптографические системы использующие потоковые шифры.	4	2	2		12	20
5	Раздел 5. Основные принципы построения несимметричных криптосистем (криптосистем с открытым ключом).	2	2	2		10	16
6	Раздел 6. Примеры построения криптосистем с открытым ключом	2	2	4			8
7	Раздел 7. Электронные (цифровые подписи) и криптографические протоколы..	6					6
Итого:		20	16	14	-	58	108

6. Лабораторный практикум

Очная форма обучения

Таблица 7

№ п/п	Номер раздела (темы)	Наименование лабораторной работы	Всего часов
1	1	Изучение блочного шифра AES	2
2	2	Исследование модификаций блочных шифров	2
3	3	Изучение потокового шифра A5/1.	2
4	4	Исследование безусловно стойкой системы аутентификации	2
5	5	Элементы теории эллиптических кривых.	2
6	6	Изучение криптосистемы Мак-Элис	4
Итого:			14

7. Практические занятия (семинары)

Очная форма обучения

Таблица 8

№ п/п	Номер раздела (темы)	Наименование практических занятий (семинаров)	Всего часов
1	1	Изучение свойств идеального шифра	4
2	2	Изучение блочного шифра ГОСТ 28147-89	2
3	3	Исследование основных атак на потоковые шифры.	4
4	4	Исследование безусловно стойкой системы аутентификации.	2
5	5	Элементы теории чисел	2
6	6	Изучение криптосистемы RSA	2
Итого:			16

8. Примерная тематика курсовых проектов (работ)

Рабочим учебным планом не предусмотрено

9. Самостоятельная работа

Очная форма обучения

Таблица 9

№ раздела дисциплины	Содержание СРС	Форма контроля	Всего часов
1	Теоретико-информационные основы КСЗИ. Подготовка к лабораторной работе.	Отчет	12
2	Симметричные КСЗИ. Подготовка к лабораторной работе.	Отчет	12
3	Асимметричные КСЗИ. Подготовка к лабораторной работе.	Отчет	12
4	Управление криптографическими ключами. Подготовка к лабораторной работе.	Отчет	12
5	Электронные (цифровые) подписи и криптопротоколы. Подготовка к лабораторной работе.	Отчет	10
Итого:			58

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 (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.

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

12.1. Основная литература:

1. Коржик, Валерий Иванович. Криптографические методы и средства обеспечения информационной безопасности [Текст] : 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.
2. Коржик, Валерий Иванович. Основы криптографии [Электронный ресурс] : 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". - СПб. : СПбГУТ, 2014. - 277 с. : ил. - ISBN 978-5-89160-097-3 : Б. ц.
3. Рябко, Б. Я. Криптографические методы защиты информации: Учебное пособие [Электронный ресурс] / Б. Я. Рябко, А. Н. Фионов. - М. : Горячая линия-Телеком, 2012. - 229 с. : ил. - ISBN 978-5-9912-0286-2 : Б. ц.
4. 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. Введение в криптографию [Текст] / 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.
2. 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. -

13. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

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

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:

- Maxima
- SciLab
- 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 «Криптографические методы 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).

16. 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