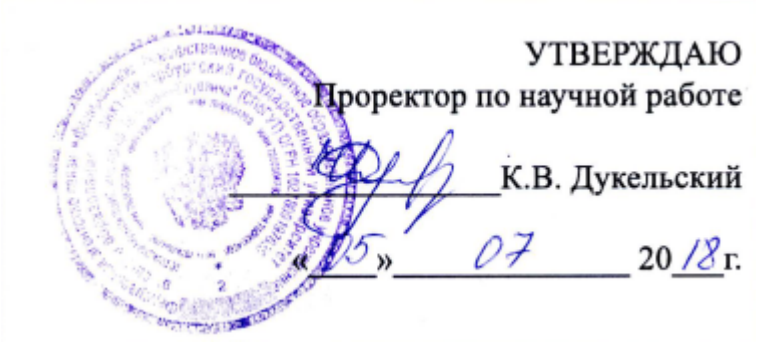
ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

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 №_19.05/21-Д

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и системы защиты информации, информационная безопасность
(наименование дисциплины)

образовательная программа высшего образования

10.06.01 Информационная безопасность
(код и наименование направления подготовки / специальности)

Исследователь. Преподаватель-исследователь
(квалификация)

Методы и системы защиты информации, информационная безопасность
(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 «10.06.01 Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 30.07.2014 № 874, и в соответствии с рабочим учебным планом, утвержденным ректором университета.

1. Цели и задачи дисциплины

Целью преподавания дисциплины «Методы и системы защиты информации, информационная безопасность» является:

формирование у аспирантов необходимых навыков для грамотного выбора средств и методик защиты информации.

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

Исследование методов разработки математических моделей, реализуемых в средствах защиты информации, а также технических заданий, эскизных, технических и рабочих проектов работ по защите информации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Методы и системы защиты информации, информационная безопасность» Б1.В.05 является обязательной дисциплиной вариативной части блока 1 учебного плана подготовки аспирантуры по направлению «10.06.01 Информационная безопасность». Изучение дисциплины «Методы и системы защиты информации, информационная безопасность» опирается на знании дисциплин(ы) «Научно-исследовательская деятельность».

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Компетенции, установленные ФГОС ВО

Таблица 1

№ п/п	Код компетенции	Наименование компетенции
1	ОПК-1	способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность
2	ОПК-2	способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности

Планируемые результаты обучения

Таблица 2

Код компе-тенции	знать	уметь	владеть
ОПК-1	Криптографические алгоритмы и особенности их программной реализации;;	Проводить исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации;;	Разработка математических моделей, реализуемых в средствах защиты информации;;

ОПК-2	Методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях;;	Разрабатывать архитектуру средств защиты информации, процедуры восстановления работоспособности средств и систем защиты после сбоев.;	Выбор средств и методов защиты информации;;

Дополнительные компетенции

Таблица 3

№ п/п	Код компетенции	Наименование компетенции
1	ПК-1	способностью исследовать методы и средства противодействия угрозам информационной безопасности в открытых компьютерных сетях, включая интернет

Планируемые результаты обучения

Таблица 4

Код компе-тенции	знать	уметь	владеть
ПК-1	Методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях;;	Разрабатывать интерфейсы средств защиты информации, процедуры восстановления работоспособности средств и систем защиты после сбоев.;	Разработка средств защиты информации в соответствии с техническим заданием;;

4. Объем дисциплины и виды учебной работы

Очная форма обучения

Таблица 5

Вид учебной работы		Всего часов	Семестры
			6
Общая трудоемкость	3 ЗЕТ	108	108
Контактная работа с обучающимися		18	18
в том числе:			
Лекции		18	18
Практические занятия (ПЗ)			-
Лабораторные работы (ЛР)			-
Защита контрольной работы			-
Защита курсовой работы			-
Защита курсового проекта			-
Промежуточная аттестация			-
Самостоятельная работа обучающихся (СРС)		54	54
в том числе:			
Курсовая работа			-
Курсовой проект			-

И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала.	54	54
Подготовка к промежуточной аттестации	36	36
Вид промежуточной аттестации		Экзамен

5. Содержание дисциплины

5.1. Содержание разделов дисциплины.

Таблица 6

№ п/п	Наименование раздела (темы) дисциплины	Содержание раздела	№ семестра		
			очная	очно-заочная	заочная
1	Раздел 1. Основы криптографии	Шифры и их свойства; композиции шифров; системы шифрования. Модели шифров; основные требования к шифрам; совершенные шифры, криптографические хеш-функции.	6		
2	Раздел 2. Оценка стойкости и надежности криптографических методов защиты	Теоретико-информационный подход к оценке криптостойкости шифров; имитостой кость и помехоустойчивость шифров; принципы построения криптографических алгоритмов; различие между программными и аппаратными реализациями.	6		
3	Раздел 3. Криптографические протоколы	Криптографические протоколы и основные требования к ним; протоколы «рукопожатия»; протоколы установления подлинности; протоколы идентификации и аутентификации.	6		
4	Раздел 4. Парольные системы разграничения доступа.	Парольные системы разграничения доступа. Протоколы генерации ключей; протоколы распределения ключей; рекомендации X. Протоколы разделения секретов; протоколы с нулевым разглашением; доказательства нулевого разглашения; протоколы «игры в покер»	6		
5	Раздел 5. Теоретическая и практическая стойкость шифров	Криптографическая стойкость шифров. Активные и пассивные атаки на шифрсистемы, задачи криптоаналитика. Теоретически стойкие шифры. Практическая стойкость шифров, её основные характеристики (трудоёмкость и надёжность дешифрования, количество необходимого материала). Связь между временной и вычислительной сложностью дешифрования. Классификация методов криптографического анализа. Классификация шифрсистем с секретным ключом. Шифрсистемы поточного шифрования (синхронные и асинхронные)	6		

6	Раздел 6. Криптография с открытым ключом. Электронная цифровая подпись.	Схемы шифрования с открытым ключом и цифровой подписи. Схемы шифрования и подписи RSA и Рабина. Схемы открытого шифрования Эль Гамаля. Сравнение криптосистем с открытым и секретным ключом. Новые схемы шифрования. Электронная цифровая подпись. Основные понятия. Схемы цифровой подписи RSA и Рабина и их применение. Схема цифровой подписи Эль Гамаля и ее модификации. Способы ускорения процедур подписи и проверки. Стандарты цифровой подписи США (DSA) и России (ГОСТ Р 34.10). Методы генерации секретных параметров для стандартов цифровой подписи. Разновидности схем электронной цифровой подписи и их применение.	6		
7	Раздел 7. Основы защиты информации от утечки по техническим каналам и физическая защита.	Виды, источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники. Побочные электромагнитные излучения и наводки; структура, классификация и основные характеристики технических каналов утечки информации; классификация технической разведки; основные этапы и процедуры добывания информации технической разведкой; возможности видов технической разведки.	6		
8	Раздел 8. Методы и средства инженерной защиты и технической охраны объектов; скрытие объектов наблюдения	Скрытие речевой информации в каналах связи; энергетическое скрытие акустических информативных сигналов; обнаружение и локализация закладных устройств, подавление их сигналов; подавление опасных сигналов акустоэлектрических преобразователей. Экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания; подавление опасных сигналов.	6		
9	Раздел 9. Характеристика государственной системы противодействия технической разведке; нормативные документы.	Характеристика государственной системы противодействия технической разведке; нормативные документы по противодействию технической разведке. Основные положения методологии инженерно-технической защиты информации. Виды контроля эффективности защиты информации, методы расчета и инструментального контроля показателей защиты информации.	6		
10	Раздел 10. Средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа	Основные методы и средства защиты информации от утечки по техническим каналам. Основные методы и средства инженерной защиты и технической охраны объектов. Основные методы и средства защиты информации в каналах связи.	6		

5.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

Таблица 7

№ п/п	Наименование обеспечиваемых (последующих) дисциплин
1	Научно-исследовательская деятельность
2	Представление научного доклада об основных результатах диссертации

5.3. Разделы дисциплин и виды занятий.

Очная форма обучения

Таблица 8

№ п/п	Наименование раздела (темы) дисциплин	Лекции	Практ. занятия	Лаб. занятия	Семинары	СРС	Всего часов
1	Раздел 1. Основы криптографии	1				8	9
2	Раздел 2. Оценка стойкости и надежности криптографических методов защиты	1				8	9
3	Раздел 3. Криптографические протоколы	2				8	10
4	Раздел 4. Парольные системы разграничения доступа.	2				10	12
5	Раздел 5. Теоретическая и практическая стойкость шифров	2				10	12
6	Раздел 6. Криптография с открытым ключом. Электронная цифровая подпись.	2				10	12
7	Раздел 7. Основы защиты информации от утечки по техническим каналам и физическая защита.	2					2
8	Раздел 8. Методы и средства инженерной защиты и технической охраны объектов; скрытие объектов наблюдения	2					2
9	Раздел 9. Характеристика государственной системы противодействия технической разведке; нормативные документы.	2					2
10	Раздел 10. Средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа	2					2
	Итого:	18	-	-	-	54	72

6. Лабораторный практикум

Рабочим учебным планом не предусмотрено

7. Практические занятия (семинары)

Рабочим учебным планом не предусмотрено

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	Оценка стойкости криптографических методов защиты	реферат	8
2	Криптографические протоколы	реферат	8
3	Оценка надежности криптографических методов защиты	реферат	8
4	Криптография с открытым ключом.	доклад	10
5	Теоретическая и практическая стойкость шифров	реферат	10
6	Электронная цифровая подпись.	доклад	10
		Итого:	54

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;

11. Фонд оценочных средств для проведения промежуточной аттестации обучающихся

Фонд оценочных средств разрабатывается в соответствии с Методическими рекомендациями по формированию ФОС и приказом Минобрнауки России от 5 апреля 2017г. № 301, г. Москва "Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры" 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. Галатенко, В. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / В. А. Галатенко. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 с.

12.2. Дополнительная литература:

1. Аверченков, В. И. Мониторинг и системный анализ информации в сети Интернет [Электронный ресурс] / В. И. Аверченков, С. М. Рощин. - Брянск : Изд-во БГТУ, 2012. - 160 с.

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 10

Наименование ресурса	Адрес
2. ЭБС «Айбукс»	ibooks.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:

- Open Office
- Google Chrome

14.2. Информационно-справочные системы:

- ЭБС iBooks (https://ibooks.ru)
- ЭБС IPRbooks (http://www.iprbookshop.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 «Методы и системы защиты информации, информационная безопасность» 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 11

№ 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 программно-аппаратных средств обеспечения информационной безопасности	Лабораторные стенды (установки) Контрольно-измерительные приборы