МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Физико-технический факультет

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Хагуров Т.А.
«___» _____ 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ФТД.02 МЕТОДЫ КРИПТОГРАФИИ И ЗАЩИТЫ ИНФОРМАЦИИ

(код и наименование дисциплины в соответствии с учебным планом)

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

Направленность (профиль) / специализация
Физика и техника радиоэлектронных и фотонных инфокоммуникаций
(наименование направленности (профиля) специализации)

Форма обучения очная
(очная, очно-заочная, заочная)

Квалификация бакалавр
(бакалавр, магистр, специалист)

Краснодар 2020

Рабочая программа дисциплины ФТД.02 «Методы криптографии и защиты информации» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи».

Программу составил:

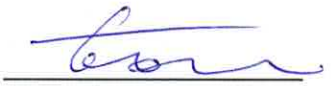
О.А. Кулиш, канд. физ.-мат. наук,
доцент кафедры оптоэлектроники

подпись

Рабочая программа дисциплины ФТД.02 «Методы криптографии и защиты информации» утверждена на заседании кафедры оптоэлектроники ФТФ, протокол № 10 от 17 апреля 2020 г.
Заведующий кафедрой оптоэлектроники
д-р техн. наук, профессор Яковенко Н.А.

подпись

Утверждена на заседании учебно-методической комиссии физико-технического факультета, протокол № 9 от 20 апреля 2020 г.
Председатель УМК ФТФ
д-р физ.-мат. наук, профессор Богатов Н.М.



подпись

Рецензенты:

Попов А.В., директор ООО "Партнер Телеком"

Скачедуб А.В., канд. физ.-мат. наук, доцент кафедры физики и информационных систем

1 Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины

Основная цель преподавания дисциплины магистрантам 1 курса по направлению подготовки 11.04.02 «Инфокоммуникационные технологии и системы связи» состоит в формировании профессиональных компетенций, востребованных при проектировании, создании и управлении защищенными системами связи.

1.2 Задачи дисциплины

Задачами освоения дисциплины «Зашита информации в связи» являются:

а) рассмотрение общетеоретических вопросов, связанных с понятиями:

- защита информации и информационная безопасность;
- защищенный канал связи;
- угрозы информационной безопасности;
- информация как экономический ресурс;
- модели оценки ценности информации;

б) рассмотрение различных методов и подходов к организации защиты конфиденциальной информации при передаче по каналам связи, оценке рисков и угроз информационной безопасности организации при использовании телекоммуникационных сетей, нормативным документам по обеспечению информационной безопасности, а также подходы к оценке стоимости конфиденциальной информации и финансовых затрат по обеспечению ее защиты.

в) получение практических навыков разработки проекта защищенной системы связи, научно-обоснованного выбора методов и технологий защиты конфиденциальной информации в соответствии с целями организации, расчета финансовых затрат на покупку, внедрение, обслуживание оборудования и проведение мероприятий по защите информации при передаче в сетях связи.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Б1.В.ДВ.01.02 «Зашита информации в связи» для магистратуры по направлению 11.04.02 Инфокоммуникационные технологии и системы связи (профиль: Оптические системы локации, связи и обработки информации) относится к дисциплинам по выбору вариативной части Блока 1 «Дисциплины (модули)» Б1 учебного плана.

Дисциплина логически и содержательно-методически связана с дисциплинами вариативной части блока 1. Для освоения данной дисциплины необходимо владеть методами линейной алгебры, уметь применять математические методы для решения практических задач.

В результате изучения настоящей дисциплины студенты должны получить знания, имеющие не только самостоятельное значение, но и обеспечивающие базовую подготовку для усвоения дисциплин вариативной части блока 1, обеспечивая согласованность и преемственность с этими дисциплинами при переходе к оптическим и цифровым технологиям.

Программа дисциплины «Защита информации в связи» согласуется со всеми учебными программами дисциплин базовой и вариативной частей блока 1 «Дисциплины (модули)» учебного плана.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся профессиональной компетенции: ПК-6, ПК-7.

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-6	способностью разрабатывать прогрессивные методы технической эксплуатации инфокоммуникационных систем, сетей и устройств	Понятия «защита информации», «информационная безопасность», «защищенный канал связи», «угроза информационной безопасности»	Выбирать модель оценки ценности защищаемой информации.	Навыками разработки проекта защищенной системы связи, научно-обоснованного выбора методов и технологий защиты конфиденциальной информации в зависимости от целей организации, расчета стоимости оборудования и мероприятий по обеспечению защиты информации в сетях связи
2.	ПК-7	готовностью к участию в осуществлении в установленном порядке деятельности по сертификации технических средств и услуг инфокоммуникаций	Нормативные документы, регламентирующие мероприятия по обеспечению информационной безопасности.	Оценивать риски и угрозы информационной безопасности при использовании различных каналов связи.	Навыками разработки установленного порядка деятельности по сертификации. Знаниями в сфере технических средств и услуг коммуникаций.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет _3_ зач.ед. (_108_ часов), их распределение по видам работ представлено в таблице *(для студентов ОФО)*.

Вид учебной работы		Всего часов	Семестры (часы)
			9
Контактная работа, в том числе:			
Аудиторные занятия (всего):		42	42
Занятия лекционного типа		14	14
Занятия семинарского типа (семинары, практические занятия)		-	-
Лабораторные занятия		28	28
Иная контактная работа:			
Промежуточная аттестация (ИКР)		0,3	0,3
Самостоятельная работа, в том числе:		39	39
Курсовая работа		-	-
Проработка учебного (теоретического) материала		23	23
Реферат		7	7
Подготовка к текущему контролю		9	9
Контроль:			
Подготовка к экзамену		26,7	26,7
Общая трудоемкость	**час.**	**108**	**108**
	в том числе контактная работа	**42,3**	**42,3**
	зач. ед.	**3**	**3**

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы (темы) дисциплины, изучаемые в _9_ семестре *(очная форма)*:

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Самостоятельная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Основные понятия в области технической защиты информации в связи.	22	4	-	-	12
2.	Криптографические методы защиты информации.	36	6	-	20	14
3.	Защита от изменений и контроль целостности информации.	23	4	-	8	13
	Подготовка к экзамену	26,7	-	-	-	-
	Промежуточная аттестация (ИКР)	0,3				
	Итого по дисциплине:	108	14	-	28	39

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента, ИКР – промежуточная аттестация .

2.3 Содержание разделов (тем) дисциплины:

2.3.1 Занятия лекционного типа

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1.	Основные понятия в области технической защиты информации в связи.	Концептуальные основы защиты информации. Система документов по технической защите информации. Органы технической защиты информации в РФ. Лицензирование деятельности в области ТЗИ. Классификация угроз и объектов защиты. Методы и средства защиты информации от утечки по техническим каналам.	Р
2.	Криптографические методы защиты информации.	Основные понятия и определения криптографии. Классические шифры. Современные системы криптографии. Атаки на алгоритмы шифрования. Построение сетей засекреченной связи.	ЛР, Р
3.	Защита от изменений и контроль целостности информации.	Способы обеспечения целостности информации. Криптографические и программные средства контроля целостности информации.	ЛР, Р

Примечание: ЛР-лабораторная работа, Р – реферат.

2.3.2 Занятия семинарского типа

Согласно учебному плану семинарские занятия по учебной дисциплине не предусмотрены.

2.3.3 Лабораторные занятия

№	Наименование разделов	Наименование лабораторных работ	Кол-во часов	Форма текущего контроля
1	Криптографические методы защиты информации.	Изучение классических шифров замены. Криптоанализ шифров табличной перестановки. Изучение методов генерации псевдослучайных чисел.	10	Отчет по лабораторной работе
		Изучение криптосистемы RSA.	10	Отчет по лабораторной работе
2	Защита от изменений и	Изучение системы цифровой	8	Отчет по

	контроль целостности информации.	подписи.		лабораторной работе
		Итого:	28	

Лабораторные работы выполняются в компьютерном классе в рамках Microsoft Office с использованием встроенных в эту систему средств Microsoft Excel.

В результате выполнения лабораторных работ у студентов формируются и оцениваются все требуемые ФГОС и ООП для направления 11.04.02 Инфокоммуникационные технологии и системы связи (профиль: Оптические системы локации, связи и обработки информации) компетенции: ПК-6, ПК-7.

2.3.4 Примерная тематика курсовых работ (проектов).

Согласно учебному плану курсовые работы (проекты) по данной дисциплине не предусмотрены.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю).

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Проработка учебного (теоретического) материала	Методические рекомендации по организации и выполнению самостоятельной работы студентов для бакалавров направления подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи» и магистров направления подготовки 11.04.02 «Инфокоммуникационные технологии и системы связи»
2	Реферат	
3	Подготовка к текущему контролю	

Перечень учебно-методического обеспечения дисциплины по темам программы для проработки теоретического материала

№	Наименование раздела	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1.	Основные понятия в области технической защиты информации в связи	1.Мельников В.П. Информационная безопасность и защита информации: учебное пособие для студентов вузов / Мельников, Владимир Павлович, С. А. Клейменов, А. М. Петраков ; В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 5-е изд., стер. – М.: Академия, 2011. – 331 с.: ил. – (Высшее профессиональное образование, Информатика и вычислительная техника) (Учебное пособие). – Библиогр: с. 327-328. 2. Рябко, Борис Яковлевич. Основы современной криптографии и стеганографии/ Б. Я. Рябко, А. Н. Фионов. - М: Горячая линия-Телеком, 2010. - 232 с.: ил. - Библиогр.: с. 225-229. **http://biblioclub.ru/index.php?page=book&id=438331**

2.	Криптографические методы защиты информации.	1.Васильева И.Н. Криптографические методы защиты информации. Учебник и практикум для академического бакалавриата / Васильева, Ирина Николаевна; И.Н. Васильева. – М.: ЮРАЙТ, 2016. – 369 с. **https://www.biblio-online.ru/book/59BABD78-5536-4ED4-BB9D-55E2F19F80B2**
3.	Защита от изменений и контроль целостности информации.	1. Прохорова, О.В.Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. - http://biblioclub.ru/index.php?page=book&id=438331.. 2.Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. - М.: Юрайт, 2017. - 309 с. **https://www.biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E**

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

В процессе преподавания дисциплины используются следующие методы:

– лекции;

– публичная защита лабораторных работ;

– написание реферата;

– консультации преподавателей;

– самостоятельная работа студентов (изучение теоретического материала, подготовка к лабораторным занятиям, выполнение домашних работ. подготовка к опросу и экзамену).

Для проведения всех лекционных занятий используются мультимедийные средства воспроизведения активного содержимого, позволяющего слушателю воспринимать особенности изучаемого материала, зачастую играющие решающую роль в понимании и восприятии, а также формировании профессиональных компетенций. Интерактивные аудиторные занятия с использованием мультимедийных систем позволяют активно и эффективно вовлекать учащихся в учебный процесс и осуществлять обратную связь. Помимо этого, становится возможным эффективное обсуждение сложных и дискуссионных вопросов и проблем.

По изучаемой дисциплине студентам предоставляется возможность открыто

пользоваться (в том числе копировать на личные носители информации) подготовленными ведущим данную дисциплину преподавателем материалами в виде **электронного комплекса сопровождения**, включающего в себя:

– электронные конспекты лекций;

– электронные варианты учебно-методических пособий для выполнения лабораторных заданий;

– списки контрольных вопросов к каждой теме изучаемого курса;

– разнообразную дополнительную литературу, относящуюся к изучаемой дисциплине в электронном виде.

Сопровождение самостоятельной работы студентов также организовано в следующих формах:

– усвоение, дополнение и вникание в разбираемые разделы дисциплины при помощи знаний, получаемых по средствам изучения рекомендуемой литературы и осуществляемое путем написания реферативных работ;

– консультации, организованные для разъяснения проблемных моментов при самостоятельном изучении тех или иных аспектов разделов усваиваемой информации в дисциплине.

Основные образовательные технологии, используемые в учебном процессе:

– интерактивная лекция с мультимедийной системой с активным вовлечением студентов в учебный процесс и обратной связью;

– лекции с проблемным изложением;

– обсуждение сложных и дискуссионных вопросов и проблем и разрешение проблем;

– компьютерные занятия в режимах взаимодействия «преподаватель – студент», «студент – преподаватель», «студент – студент»;

– технологии смешанного обучения: дистанционные задания и упражнения, составление глоссариев терминов и определений, групповые методы Wiki, интернет-тестирование и анкетирование.

Интерактивные образовательные технологии, используемые в аудиторных занятиях:

– технология развития критического мышления;

– лекции с проблемным изложением;

– использование средств мультимедиа;

– изучение и закрепление нового материала (интерактивная лекция, работа с наглядными пособиями, видео- и аудиоматериалами, использование вопросов, Сократический диалог);

– обсуждение сложных и дискуссионных вопросов и проблем («Займи позицию (шкала мнений)», проективные техники, «Один – вдвоем – все вместе», «Смени позицию», «Дискуссия в стиле телевизионного ток-шоу», дебаты, симпозиум);

– разрешение проблем («Дерево решений», «Мозговой штурм», «Анализ казусов»);

– творческие задания;

– работа в малых группах;

– использование средств мультимедиа (компьютерные классы).

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Занятия, проводимые с использованием интерактивных технологий

Семестр	Вид занятия(Л, ПЗ, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
9	Л	Интерактивная лекция с мультимедийной системой	14
9	ЛР	Индивидуальное выполнение лабораторных заданий	28
Итого:			42

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

В процессе подготовки и ответам на контрольные вопросы формируются и оцениваются все требуемые ФГОС и ООП для направления 11.04.02 Инфокоммуникационные технологии и системы связи (профиль: «Оптические системы локации, связи и обработки информации») компетенции: ПК-6, ПК-7.

Ниже приводится перечень и примеры из фонда оценочных средств. Полный комплект оценочных средств приводится в ФОС дисциплины Б1.В.ДВ.01.02 «Защита информации в связи».

4.1 Фонд оценочных средств для проведения текущего контроля.

Текущий контроль организован в виде лабораторных занятий путем оценки активности студента и результативности его действий

Контрольных вопросов при защите лабораторных работ и для самостоятельной подготовки.

Ниже приводятся примеры контрольных вопросов для разделов рабочей программы.

Раздел 1.

1. Основные понятия в области защиты информации в связи.
2. Законодательные и иные правовые акты в области защиты информации в связи.
3. Классификация технических каналов утечки информации.
4. Классификация методов и средств защиты информации от утечки по техническим каналам.
5. Методы экранирования технических средств.
6. Фильтрация информационных сигналов.
7. Пространственное и линейное зашумление.

Раздел 2.

1. Основные понятия классической криптографии.
2. Шифры замены и перестановки.
3. Блочные и потоковые шифры.
4. Шифры простой замены.
5. Шифр Виженера.
6. Одноразовый шифровальный блокнот.

7. Шифры гаммирования.
8. Шифры колонной замены.
9. Основы теории Шеннона.
10. Алгоритм шифрования DES.
11. Алгоритм ГОСТ 28147-89.
12. Вычислительная стойкость криптоалгоритмов.
13. Атаки на алгоритмы шифрования.
14. Имитостойкость и помехоустойчивость шифров.
15. Управление криптографическими ключами.
16. Симметричные и асимметричные шифры.
17. Система Диффи-Хеллмана.
18. Шифр RSA.

Раздел 3.

19. Функции хэширования
20. Цифровая подпись
21. Криптография на эллиптических кривых
22. Цифровая подпись на эллиптических кривых

Перечень компетенций (части компетенций), проверяемых оценочным средством:

ПК-6 - способностью разрабатывать прогрессивные методы технической эксплуатации инфокоммуникационных систем, сетей и устройств: знать Понятия «защита информации», «информационная безопасность», «защищенный канал связи», «угроза информационной безопасности».

Критерии оценивания ответов студентов:

С целью контроля и подготовки студентов к изучению новой темы вначале каждой практического занятия преподавателем проводится индивидуальный или фронтальный устный (письменный) опрос по выполненным заданиям предыдущей темы. Критерии оценки: – правильность ответа по содержанию задания (учитывается количество и характер ошибок при ответе):
– полнота и глубина ответа (учитывается количество усвоенных фактов, понятий и т.п.);
– сознательность ответа (учитывается понимание излагаемого материала);
– логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией);
– своевременность и эффективность использования наглядных пособий и технических средств при ответе (учитывается грамотно и с пользой применять наглядность и демонстрационный опыт при устном ответе);
– использование дополнительного материала (обязательное условие);
– рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения задания, устного ответа во времени, с учетом индивидуальных особенностей студентов).

Темы рефератов по учебной программе

В процессе подготовки и написания реферата у студентов формируются и оцениваются требуемые ФГОС и ООП по направлению 11.04.02 Инфокоммуникационные технологии и системы связи (профиль: Оптические системы локации, связи и обработки

информации) компетенции: ПК-6, ПК-7.

1. Композиции шифров.
2. Режимы работы блочных шифров.
3. Вычислительная стойкость криптоалгоритмов.
4. Методы криптоанализа блочных шифров.
5. Построение сетей засекреченной связи.
6. Система Диффи-Хэллмана.
7. Функции хэширования.

Перечень компетенций (части компетенций), проверяемых оценочным средством:

П-8 - готовностью к участию в осуществлении в установленном порядке деятельности по сертификации технических средств и услуг инфокоммуникаций: знать нормативные документы, регламентирующие мероприятия по обеспечению информационной безопасности.

Критерии оценки рефератов:

- Оценка «отлично» – выполнены все требования к написанию и представления реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.
- Оценка «хорошо» – основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.
- Оценка «удовлетворительно» – имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.
- Оценка «неудовлетворительно» – тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Вопросы, выносимые на экзамен в 9 семестре по дисциплине «Зашита информации в связи» по направлению 11.04.02 Инфокоммуникационные технологии и системы связи(профиль: «Оптические системы локации, связи и обработки информации»).

1. Основные понятия в области защиты информации в связи
2. Законодательные и иные правовые акты в области защиты информации в связи
3. Классификация технических каналов утечки информации

4. Классификация методов и средств защиты информации от утечки по техническим каналам
5. Методы экранирования технических средств
6. Фильтрация информационных сигналов
7. Пространственное и линейное зашумление
8. Основные понятия классической криптографии
9. Шифры замены и перестановки
10. Блочные и потоковые шифры
11. Шифры простой замены
12. Шифр Виженера
13. Одноразовый шифровальный блокнот
14. Шифры гаммирования
15. Шифры колонной замены
16. Основы теории Шеннона
17. Алгоритм шифрования DES
18. Алгоритм ГОСТ 28147-89
19. Вычислительная стойкость криптоалгоритмов
20. Атаки на алгоритмы шифрования
21. Имитостойкость и помехоустойчивость шифров
22. Управление криптографическими ключами
23. Симметричные и асимметричные шифры
24. Система Диффи-Хеллмана
25. Шифр RSA
26. Функции хэширования
27. Цифровая подпись
28. Криптография на эллиптических кривых
29. Цифровая подпись на эллиптических кривых

Перечень компетенций (части компетенций), проверяемых оценочным средством:

ПК-6 - способностью разрабатывать прогрессивные методы технической эксплуатации инфокоммуникационных систем, сетей и устройств: знать Понятия «защита информации», «информационная безопасность», «защищенный канал связи», «угроза информационной безопасности»; уметь выбирать модель оценки ценности защищаемой информации; владеть навыками разработки проекта защищенной системы связи, научно-обоснованного выбора методов и технологий защиты конфиденциальной информации в зависимости от целей организации, расчета стоимости оборудования и мероприятий по обеспечению защиты информации в сетях связи. П-8 - готовностью к участию в осуществлении в установленном порядке деятельности по сертификации технических средств и услуг инфокоммуникаций: знать нормативные документы, регламентирующие мероприятия по обеспечению информационной безопасности; уметь оценивать риски и угрозы информационной безопасности при использовании различных каналов связи; владеть навыками разработки установленного порядка деятельности по сертификации. Знаниями в сфере технических средств и услуг коммуникаций.

Оценивание результатов устных и письменных опросов на экзамене:

Уровень знаний определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» - студент показывает полные и глубокие знания программного материала, логично и аргументировано отвечает на поставленный вопрос, а также дополнительные вопросы, показывает высокий уровень теоретических знаний.

Оценка «хорошо» - студент показывает глубокие знания программного материала, грамотно его излагает, достаточно полно отвечает на поставленный вопрос и дополнительные вопросы, умело формулирует выводы. В тоже время при ответе допускает несущественные погрешности.

Оценка «удовлетворительно» - студент показывает достаточные, но не глубокие знания программного материала; при ответе не допускает грубых ошибок или противоречий, однако в формулировании ответа отсутствует должная связь между анализом, аргументацией и выводами. Для получения правильного ответа требуется уточняющие вопросы.

Оценка «неудовлетворительно» - студент показывает недостаточные знания программного материала, не способен аргументировано и последовательно его излагать, допускается грубые ошибки в ответах, неправильно отвечает на поставленный вопрос или затрудняется с ответом.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:

1. Васильева И.Н. Криптографические методы защиты информации. Учебник и практикум для академического бакалавриата / Васильева, Ирина Николаевна; И.Н.

Васильева. – М.: ЮРАЙТ, 2016. – 369 с. **https://www.biblio-online.ru/book/59BABD78-5536-4ED4-BB9D-55E2F19F80B2**

2. Мельников В.П. Информационная безопасность и защита информации: учебное пособие для студентов вузов / Мельников, Владимир Павлович, С. А. Клейменов, А. М. Петраков ; В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 5-е изд., стер. – М.: Академия, 2011. – 331 с.: ил. – (Высшее профессиональное образование, Информатика и вычислительная техника) (Учебное пособие). – Библиогр.: с. 327-328.

3. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. - М. : Юрайт, 2017. - 309 с. **https://www.biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E**

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.2 Дополнительная литература:

1.Баранова, Е.К.Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш . - 3-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2017.322 с. - http://znanium.com/catalog.php?bookinfo=763644

2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. - http://biblioclub.ru/index.php?page=book&id=438331.

3. Рябко, Борис Яковлевич. Основы современной криптографии и стеганографии/ Б. Я. Рябко, А. Н. Фионов. - М. : Горячая линия-Телеком, 2010. - 232 с. : ил. - Библиогр. : с. 225-229. **http://biblioclub.ru/index.php?page=book&id=438331**

5.3. Периодические издания:

1. Вопросы защиты информации.
2. Защита информации.
3. Защита информации. Инсайд.
4. Специальная техника.
5. Специальная техника и связь
6. Безопасность. Достоверность. Информация.
7. Мир и безопасность.

6. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины (модуля).

1. Информационная система «Единое окно доступа к образовательным ресурсам»: http://window.edu.ru/window
2. Библиотека электронных учебников: http://www.book-ua.org/
3. Федеральный образовательный портал: http://www.edu.ru/db/portal/sites/res_page.htm
4. Каталог научных ресурсов: http://www.scintific.narod.ru/literature.htm
5. Большая научная библиотека: http://www.sci-lib.com/
6. Учебно-образовательная физико-математическая библиотека сайта EqWorld: http://eqworld.ipmnet.ru/ru/library/physics/

7. Техническая библиотека:
http://techlibrary.ru/

7. Методические указания для обучающихся по освоению дисциплины (модуля).

На самостоятельную работу студентов, согласно требованиям ФГОС ВО по направлению 11.04.02 Инфокоммуникационные технологии и системы связи (профиль: Оптические системы локации, связи и обработки информации), отводится около 43 % времени (39 час. срс) от общей трудоемкости дисциплины (108 час.). Сопровождение самостоятельной работы студентов может быть организовано в следующих формах:

– составлением индивидуальных планов самостоятельной работы каждого из студентов с указанием темы и видов занятий, форм и сроков представления результатов;

– проведением консультаций (индивидуальных или групповых), в том числе с применением дистанционной среды обучения.

Критерий оценки эффективности самостоятельной работы студентов формируется в ходе промежуточного контроля процесса выполнения заданий и осуществляется на основе различных способов взаимодействия в открытой информационной среде и отражается в процессе формирования так называемого «электронного портфеля студента».

В соответствии с этим при проведении оперативного контроля могут использоваться контрольные вопросы к соответствующим разделам основной дисциплины «Защита информации в связи».

Сопровождение самостоятельной работы студентов также организовано в следующих формах:

– усвоение, дополнение и вникание в разбираемые разделы дисциплины при помощи знаний, получаемых по средствам изучения рекомендуемой литературы и осуществляемое путем написания реферативных работ;

– консультации, организованные для разъяснения проблемных моментов при самостоятельном изучении тех или иных аспектов разделов усваиваемой информации в дисциплине.

К средствам обеспечения освоения дисциплины «Защита информации в связи» относятся электронные варианты дополнительных учебных, научно-популярных и научных изданий по данной дисциплине.

Рекомендуется следующий график и календарный план самостоятельной работы студентов по учебным неделям (15 недель):

Рекомендуемый график самостоятельной работы студентов в 9-м семестре по дисциплине «Защита информации в связи»

№ п/п	Наименование раздела	Содержание самостоятельной работы	Примерный бюджет времени на выполнение уч. час. (СР)	Сроки выполнения задания (номер учебной недели семестра)	Форма отчетности по заданию	Форма контроля
1	Композиции шифров.	Проработка учебного (теоретического материала) подготовка к текущей и промежуточной аттестации	5	1-2	Реферат	текстовый документ, устный опрос
		Подготовка к ЛР	1	1-2	ЛР	устный опрос
2	Режимы работы блочных шифров.	Проработка учебного (теоретического материала) подготовка к текущей и промежуточной аттестации	5	3-4	Реферат	текстовый документ, устный опрос
		Подготовка к ЛР	1	3-4	ЛР	устный опрос
3	Вычислительная стойкость криптоалгоритмов	Проработка учебного (теоретического материала) подготовка к текущей и промежуточной аттестации	5	5-6	Реферат	текстовый документ, устный опрос
		Подготовка к ЛР	1	5-6	ЛР	устный опрос
4	Методы криптоанализа блочных шифров.	Проработка учебного (теоретического материала) подготовка к текущей и промежуточной аттестации	6	7-9	Реферат	текстовый документ, устный опрос
		Подготовка к ЛР	2	7-9	ЛР	устный опрос
5	Построение сетей засекреченной связи.	Проработка учебного (теоретического материала) подготовка к текущей и промежуточной аттестации	3,2	9-11	Реферат	текстовый документ, устный опрос
		Подготовка к ЛР	1	9-11	ЛР	устный опрос

6	Система Диффи-Хэллмана.	Проработка учебного (теоретического материала) подготовка к текущей и промежуточной аттестации	2,8	11-12	Реферат	текстовый документ, устный опрос
		Подготовка к ЛР	2	11-12	ЛР	устный опрос
7	Практическое применение криптосистем.	Проработка учебного (теоретического материала) подготовка к текущей и промежуточной аттестации	3	12-15	Реферат	текстовый документ, устный опрос
		Подготовка к ЛР	1	12-15	ЛР	устный опрос
		Итого:	39			

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю).

8.1 Перечень информационных технологий.

– Консультирование посредством электронной почты.

–Использование электронных презентаций на сайте Moodle Кубгу.

8.2 Перечень необходимого программного обеспечения.

1. Операционная система Microsoft семейства Windows (7/8/10), в рамках программы компании Microsoft “Enrollment for Education Solutions” для компьютеров и серверов Кубанского государственного университета и его филиалов.

2. Офисный пакет приложений MS Office

8.3 Перечень информационных справочных систем:

1. Справочно-правовая система «Консультант Плюс»:
http://www.consultant.ru
2. Электронная библиотечная система eLIBRARY.RU:
http://www.elibrary.ru
3. Информационная система «Единое окно доступа к образовательным ресурсам»:
http://window.edu.ru/window

4. Рубрикон – крупнейший энциклопедический ресурс Интернета:
http://www.rubricon.com/
5. Каталог научных ресурсов:
http://www.scintific.narod.ru/literature.htm
6. Большая научная библиотека:
http://www.sci-lib.com/
7. Техническая библиотека:
http://techlibrary.ru/
8. Академик – Словари и энциклопедии на Академике:
http://dic.academic.ru/dic.nsf/enc_physics/

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю).

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Учебные аудитории для проведения занятий лекционного типа – ауд. 212, корп. С (ул. Ставропольская, 149)
2.	Лабораторные занятия	Учебные аудитории для проведения лабораторных работ – ауд. 212, корп. С (ул. Ставропольская, 149)
3.	Текущий контроль, промежуточная аттестация	Учебные аудитории для проведения промежуточной аттестации– ауд. 212, корп. С (ул. Ставропольская, 149)
4.	Самостоятельная работа	Аудитория для самостоятельной работы – ауд. 208, корп. С (ул. Ставропольская, 149)

«Мультимедийный класс специальных дисциплин» ауд. 205С		
Лабораторные занятия по дисциплине: «Защита информации в связи»	Оборудование и программно-техническое оснащение учебно-научной лаборатории:	Кол-во
	Персональные электронно-вычислительные машины: CPU с частотой более 2,4 ГГц , LCD	12
	Microsoft Office 2003, 2013	12
	Kaspersky Endpoint Security 10 Антивирусная программа	12
	Windows XP, 7 Операционная система	12
	Соединительные модули, шнуры, кабели	~
	Проектор SANYO PLC-SW20A	1
	Парта (рабочий стол)	16
	Экран проекционный 153х140	1
	Доска белая маркерная	3
	Стулья	25