МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

Добржинский Ю.В
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

Добржинский Ю.В
(подпись) (Ф.И.О.)

« 15 » июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы информационной безопасности
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс 2 семестр 3
лекции 54 час.
практические занятия 36 час.
лабораторные работы 00 час.
в том числе с использованием МАО лек. 9 / пр. 18 / лаб. 00 час.
в том числе в электронной форме лек. 00 / пр. 00 / лаб. 00 час.
всего часов аудиторной нагрузки 90 час.
в том числе с использованием МАО 27 час.
в том числе в электронной форме 00 час.
самостоятельная работа 54 час.
в том числе на подготовку к экзамену 36 час.
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 3 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 01.12.2016 № 1512

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол № 10 от « 15 » июня 2019 г.

И.о. заведующего кафедрой: Добржинский Ю.В., к.т.н., с.н.с.
Составитель (ли): Корнюшин П.Н. д.ф.-м. н., профессор

Владивосток
2019

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

ABSTRACT

Specialist's degree in 10.05.01 Computer Security
Specialization "Mathematical Methods for Information Security"
Course title: *Basics of Information Security*
Basic part of Block 1, 4 credits
Instructor: *Kornyushin P.N.*
At the beginning of the course a student should be able to:
• *the ability to use the basics of legal knowledge in various fields of activity (GC-4).*
Learning outcomes:
(OPK-5) the ability to use regulatory legal acts in their professional activities
(OPK-9) the ability to self-build the algorithm, conduct its analysis and implementation in modern software systems
Course description:
Discipline is devoted to the study of the basics of information security, which is in its essence an introduction to the specialty "Computer Security". The discipline provides for the study of five educational topics united by a single concept. Views on information are set forth as an object of protection, highlighting the characteristic properties of the information being protected. On the basis of a unified approach, nine historical information protection directions are considered. The author describes the quality models of information protection developed or modified by the author. The discipline is being completed with two topics dedicated to the two most significant threats to information security - information crimes and information wars. Within the framework of these topics, information and computer crimes are classified, their reasons are explained, the criminal law characteristics of certain criminal acts are given, the main strategies of information wars and types of information weapons are considered.
Main course literature:
1. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 [Электронный ресурс] : учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 244 с. — Режим доступа: https://e.lanbook.com/book/5178
2. Кожуханов, Н.М. Обеспечение информационной безопасности таможенной деятельности на основе инноваций в праве [Электронный ресурс] : монография / Н.М. Кожуханов. — Электрон. дан. — Москва : РТА, 2010. — 92 с. — Режим доступа: https://e.lanbook.com/book/74056
3. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С.А. Нестеров. — Электрон. дан. — Санкт-Петербург : СПбГПУ, 2014. — 322 с. — Режим доступа: https://e.lanbook.com/book/64809
Form of final control: exam

Аннотация к рабочей программе дисциплины
«Основы информационной безопасности»

Данный курс предназначен студентам по направлению подготовки 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана с кодом Б1.Б.19.

Трудоемкость дисциплины в зачетных единицах составляет 4 з.е., в академических часах – 144 часов (лекции – 54 часа, практическая работа – 36 часов, самостоятельная работа – 54 часа, в том числе 36 часов на подготовку к экзамену). Дисциплина реализуется на 2 курсе в 3 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Основы информационной безопасности» базируется на предварительном изучении следующей дисциплины: «Правоведение».

Дисциплина посвящена изучению основ информационной безопасности, которая является по своей сути введением в специальность «Компьютерная безопасность». В дисциплине предусмотрено изучение пяти учебных тем, объединенных единым замыслом. Излагаются взгляды на информацию, как объект защиты с выделением характерных свойств защищаемой информации. На основе единого подхода рассматриваются девять исторически сложившихся направлений информационной защиты. Излагаются разработанные или модифицированные автором качественные модели информационной защиты. Завершается изучение дисциплины двумя темами, посвященными двум наиболее существенным угрозам информационной безопасности – информационным преступлениям и информационным войнам. В рамках указанных тем приводится классификация информационных и компьютерных преступлений, объясняются их причины, дается уголовно-правовая характеристика некоторых преступных деяний, рассматриваются основные стратегии информационных войн и виды информационного оружия.

Цель: обучить студентов принципам обеспечения информационной безопасности государства, организации, отдельного гражданина, подходам к анализу ее информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем.

Задачи:

- дать основы обеспечения информационной безопасности государства;
- дать основы методологии создания систем защиты информации;
- дать основы процессов сбора, передачи и накопления информации;
- дать основы методов и средств защищенности и обеспечения информационной безопасности компьютерных систем.

Для успешного изучения дисциплины «Основы информационной безопасности» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность использовать основы правовых знаний в различных сферах деятельности (ОК-4).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-5) способность использовать нормативные правовые акты в своей профессиональной деятельности	Знает	роль и место информационной безопасности в системе национальной безопасности страны.
	Умеет	действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма.
	Владеет	навыком анализа информационной инфраструктуры государства.
(ОПК-9) способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных	Знает	современные подходы к построению систем защиты информации.
	Умеет	выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации.

программных комплексах	Владеет	навыком работы с различными средствами программирования и отладки программного обеспечения.

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы информационной безопасности» применяются следующие методы активного/интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: конспект (ПР-7), собеседование (ОУ-1), коллоквиум (ОУ-2).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Лекции (54 часа)

Раздел I. Основные понятия информационной безопасности (3 час.)

Тема 1. Понятие национальной безопасности (1 час.)

Тема 2. Информационная безопасность в системе национальной безопасности РФ (2 час.)

Раздел II. Концепция информационной безопасности (6 час.)

Тема 1. Основные концептуальные положения системы защиты информации (2 час.)

Тема 2. Концептуальная модель информационной безопасности (2 час.)

Тема 3. Угрозы конфиденциальной информации (1 час.)

Тема 4. Действия, приводящие к неправомерному овладению конфиденциальной информацией. (1 час.)

Раздел III. Направления обеспечения информационной безопасности (6 час.)

Тема 1. Правовая защита (2 час.)

Тема 2. Организационная защита (2 час.)

Тема 3. Инженерно-техническая защита (2 час.)

Раздел IV. Выявление технических каналов утечки информации (12 час.)

Тема 1. Классификация технических каналов утечки информации (2 час.)

Тема 2. Классификация технических средств выявления каналов утечки информации (2 час.)

Тема 3. Индикаторы поля, интерсепторы и измерители частоты (2 час.)

Тема 4. Специальные сканирующие радиоприемники (1 час.)

Тема 5. Обнаружители диктофонов (1 час.)

Тема 6. Универсальные поисковые приборы (1 час.)

Тема 7. Программно-аппаратные поисковые комплексы (1 час.)

Тема 8. Нелинейные локаторы (1 час.)

Тема 9. Технические средства контроля двухпроводных линий (1 час.)

Раздел V. Защита информации от утечки по техническим каналам (6 час.)

Тема 1. Методы и средства защиты информации, обрабатываемой ТСПИ (2 час.)

Тема 2. Методы и средства защиты речевой информации в помещении (2 час.)

Тема 3. Методы и средства защиты телефонных линий (2 час.)

Раздел VI. Защита компьютерной информации от несанкционированного доступа (15 час.)

Тема 1. Угрозы безопасности информации в компьютерных системах (1 час.)

Тема 2. Программы-шпионы (3 час.)

Тема 3. Парольная защита операционных систем (3 час.)

Тема 4. Аппаратно-программные средства защиты информации от НСД (3 час.)

Тема 5. Проблемы обеспечения безопасности в глобальных сетях (3час.)

Тема 6. Построение комплексных систем защиты информации (4 час.)

Раздел VII. Стандарты и рекомендации в области информационной безопасности (6 час.)

Тема 1. Оранжевая книга (TCSEC) (1 час.)

Тема 2. Радужная серия (1 час.)

Тема 3. Гармонизированные критерии Европейских стандартов (IT-SEC) (1 час.)

Тема 4. Рекомендации X.800 (1 час.)

Тема 5. Концепция защиты от НСД ФСТЭК РФ (Гостехкомиссии при Президенте РФ). (2 час.)

Основное содержание теоретической части курса с тестами приведено в пособии «Корнюшин П.Н., Костерин С.С. Информационная безопасность. Электронное пособие. – Владивосток: Изд-во ДВГУ, 2003».

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (36 часов)

Занятие 1. Доктрина информационной безопасности (4 час.)

1. Методы обеспечения информационной безопасности.
2. Информационная безопасность в Российской Федерации

Занятие 2. Закон об информации, информационных технологиях и защите информации (6 час.)

1. Основные положения.
2. Область применения.
3. Право на доступ к информации.
4. Ограничение на доступ.

Занятие 3. Закон о государственной тайне (4 час.)

1. Классификация государственной тайны.
2. Законы, регулирующие государственную тайну.

Занятие 4. Закон о коммерческой тайне (4 час.)

1. Определение.
2. Режим коммерческой тайны.

Занятие 5. Закон об электронной цифровой подписи (6 час.)

1. Порядок выдачи цифровой подписи.
2. Использование цифровой подписи.

Занятие 6. Закон о персональных данных (12 час.)

1. Закон о персональных данных, кем регулируется.
2. Применение закона о ПДн в разных областях.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Основы информационной безопасности» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Основные понятия информационной безопасности	ОПК-5 ОПК-9	знает	конспект (ПР-7)	1-7
			умеет	собеседование (ОУ-1)	1-7
			владеет	коллоквиум (ОУ-2)	1-7
2	Раздел II. Концепция информационной безопасности	ОПК-5 ОПК-9	знает	конспект (ПР-7)	8-10
			умеет	собеседование (ОУ-1)	8-10
			владеет	коллоквиум (ОУ-2)	8-10
3	Раздел III. Направления обеспечения информационной безопасности	ОПК-5 ОПК-9	знает	конспект (ПР-7)	11-19
			умеет	собеседование (ОУ-1)	11-19
			владеет	коллоквиум (ОУ-2)	11-19
4	Раздел IV. Выявление технических каналов утечки информации	ОПК-5 ОПК-9	знает	конспект (ПР-7)	20-23
			умеет	собеседование (ОУ-1)	20-23
			владеет	коллоквиум (ОУ-2)	20-23
5	Раздел V. Защита информации от утечки по техническим каналам	ОПК-5 ОПК-9	знает	конспект (ПР-7)	23-25
			умеет	собеседование (ОУ-1)	23-25
			владеет	коллоквиум (ОУ-2)	23-25
6	Раздел VI. Защита компьютерной информации от несанкционированного доступа	ОПК-5 ОПК-9	знает	конспект (ПР-7)	23-25
			умеет	собеседование (ОУ-1)	23-25
			владеет	коллоквиум (ОУ-2)	23-25
7	Раздел VII. Стандарты и рекомендации в области информационной безопасности	ОПК-5 ОПК-9	знает	конспект (ПР-7)	26-30
			умеет	собеседование (ОУ-1)	26-30
			владеет	коллоквиум (ОУ-2)	26-30

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 [Электронный ресурс] : учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 244 с. — Режим доступа: https://e.lanbook.com/book/5178
2. Кожуханов, Н.М. Обеспечение информационной безопасности таможенной деятельности на основе инноваций в праве [Электронный ресурс] : монография / Н.М. Кожуханов. — Электрон. дан. — Москва : РТА, 2010. — 92 с. — Режим доступа: https://e.lanbook.com/book/74056
3. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С.А. Нестеров. — Электрон. дан. — Санкт-Петербург : СПбГПУ, 2014. — 322 с. — Режим доступа: https://e.lanbook.com/book/64809

Дополнительная литература

1. Кожуханов, Н.М. Правовые основы информационной безопасности [Электронный ресурс] : учебное пособие / Н.М. Кожуханов, Е.С. Недосекова. — Электрон. дан. — Москва : РТА, 2013. — 88 с. — Режим доступа: https://e.lanbook.com/book/74237
2. Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс] : учебное пособие / В.К. Новиков. — Электрон. дан. — Москва : Горячая линия-Телеком, 2015. — 176 с. — Режим доступа: https://e.lanbook.com/book/94633
3. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс] : учебное пособие / Ю.И. Коваленко. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: https://e.lanbook.com/book/5163

Перечень ресурсов информационно-телекоммуникационной сети

«Интернет»

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/

2. Малюк, А.А. Введение в информационную безопасность [Электронный ресурс] : учебное пособие / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 288 с. — Режим доступа: https://e.lanbook.com/book/5171

3. ФСТЭК. Техническая защита информации. [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/103-tekhnicheskaya-zashchita-informatsii

Перечень информационных технологий и программного обеспечения

Для работы в литературой из списка необходимо наличие к студента аккаунтов в указанной электронно-библиотечных системах: «Лань» (https://e.lanbook.com/).

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Основы информационной безопасности», составляет 90 академических часов. На самостоятельную работу – 54 часов. При этом аудиторная нагрузка состоит из 54 лекционных часов и 36 часов практических занятий.

Обучающийся получает теоретические знания на лекционных занятиях, необходимые для последующего выполнения практических заданий. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Студенту рекомендуется предварительно готовиться к лекции, используя ресурсы из списка, приведённого в разделе V, для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю.

При подготовке к практическим занятиям также необходимо повторить теоретический материал.

Промежуточная форма аттестации по данной дисциплине – экзамен. Вопросы к зачету соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к зачету студенту необходимо воспользоваться конспектами лекций, а также иными источниками из списка литературы для более глубокого понимания материала.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

ДВРУНЦ

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Основы информационной безопасности»

Направление подготовки 10.05.01 Компьютерная безопасность

специализация «Математические методы защиты информации»

Форма подготовки очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-18 недели обучения	Подготовка практического задания (выполнение отчета к занятию)	18	Отчет о выполнении практического задания
8	Сессия	Подготовка и сдача экзамена	36	Экзамен

Рекомендации по самостоятельной работе студентов

При подготовке отчета о выполнении практического задания должны использоваться источники из списка учебной литературы, а также примеры, рассмотренные на лекционных и практических занятиях. Отчет должен содержать:

- титульный лист;
- содержание;
- описание задания;
- решение;
- выводы.

Методические указания к выполнению отчета по занятию

Для получения **«зачтено»** отчет должен содержать основные пункты: титульный лист, содержание, описание задания, решение, выводы. При представлении отчета к сдаче обучающийся последовательно излагает принцип выполненной работы.

Оценка **«незачтено»** выставляется в случае, если отчет не содержит решения или выводов; обучающийся не может объяснить решение, излагает материал непоследовательно, сбивчиво

Подготовка отчета к практическому заданию предполагает повторение лекционного материала и выполнение лабораторных работ по темам из Раздела II РПУД. В результате студент должен предоставить отчет о проделанной работе.

Самостоятельная работа при подготовке к зачету и включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по лабораторным работам.

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Основы информационной безопасности»
Направление подготовки 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-5) способность использовать нормативные правовые акты в своей профессиональной деятельности	Знает	роль и место информационной безопасности в системе национальной безопасности страны.
	Умеет	действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма.
	Владеет	навыком анализа информационной инфраструктуры государства.
(ОПК-9) способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Знает	современные подходы к построению систем защиты информации.
	Умеет	выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации.
	Владеет	навыком работы с различными средствами программирования и отладки программного обеспечения.

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Основные понятия информационной безопасности	ОПК-5 ОПК-9	знает	конспект (ПР-7)	1-7
			умеет	собеседование (ОУ-1)	1-7
			владеет	коллоквиум (ОУ-2)	1-7
2	Раздел II. Концепция информационной безопасности	ОПК-5 ОПК-9	знает	конспект (ПР-7)	8-10
			умеет	собеседование (ОУ-1)	8-10
			владеет	коллоквиум (ОУ-2)	8-10
3	Раздел III. Направления обеспечения информационной безопасности	ОПК-5 ОПК-9	знает	конспект (ПР-7)	11-19
			умеет	собеседование (ОУ-1)	11-19
			владеет	коллоквиум (ОУ-2)	11-19
4	Раздел IV. Выявление технических каналов утечки информации	ОПК-5 ОПК-9	знает	конспект (ПР-7)	20-23
			умеет	собеседование (ОУ-1)	20-23
			владеет	коллоквиум (ОУ-2)	20-23
5	Раздел V. Защита информации от утеч-	ОПК-5 ОПК-9	знает	конспект (ПР-7)	23-25

	ки по техническим каналам		умеет	собеседование (ОУ-1)	23-25
			владеет	коллоквиум (ОУ-2)	23-25
6	Раздел VI. Защита компьютерной информации от несанкционированного доступа	ОПК-5 ОПК-9	знает	конспект (ПР-7)	23-25
			умеет	собеседование (ОУ-1)	23-25
			владеет	коллоквиум (ОУ-2)	23-25
7	Раздел VII. Стандарты и рекомендации в области информационной безопасности	ОПК-5 ОПК-9	знает	конспект (ПР-7)	26-30
			умеет	собеседование (ОУ-1)	26-30
			владеет	коллоквиум (ОУ-2)	26-30

Оценочные средства для промежуточной аттестации
Список вопросов на экзамен

1. Основные концептуальные положения системы защиты информации.

2. Концептуальная модель информационной безопасности.

3. Угрозы конфиденциальной информации.

4. Действия, приводящие к неправомерному овладению конфиденциальной информацией.

5. Правовая защита.

6. Организационная защита.

7. Инженерно-техническая защита.

8. Основные способы защиты информации.

9. Пресечение разглашения конфиденциальной информации.

10. Защита информации от утечки по визуально-оптическим каналам.

11. Защита информации от утечки по акустическим каналам.

12. Защита информации от утечки по электромагнитным каналам.

13. Защита информации от утечки по материально-вещественным каналам.

14. Способы несанкционированного доступа.

15. Защита от наблюдения и фотографирования.

16. Защита от подслушивания.

17. Противодействие незаконному подключению к линиям связи.

18. Защита от перехвата.

19. Защита в локальных сетях.

20. Защита в глобальных сетях.

21.Защита от утечки за счет электромагнитного излучения.

22.Защита от утечки за счет паразитной генерации.

23.Защита от утечки по цепям питания.

24.Защита от утечки по цепям заземления.

25.Противодействие подслушиванию посредством микрофонных схем.

26.Противодействие радиосистемам акустического подслушивания.

27.Обеспечение безопасности телефонных переговоров.

28.Противодействие лазерному подслушиванию.

29.Стандарты и рекомендации в области информационной безопасности.

30.Основные методы защиты операционных систем.

Критерии выставления оценки на экзамене

Оценка	Требования к сформированным компетенциям
«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач по методологии научных исследований.
«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«удовлетворительно»	Оценка «удовлетворительно» выставляется

	студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ
«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства для текущей аттестации

№ п/п	Код ОС	Наименование оценочного средства	Кроткая характеристика оценочного средства	Представление оценочного средства в фонде
1	ОУ-1	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определённому разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
2	ОУ-2	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
3	ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины