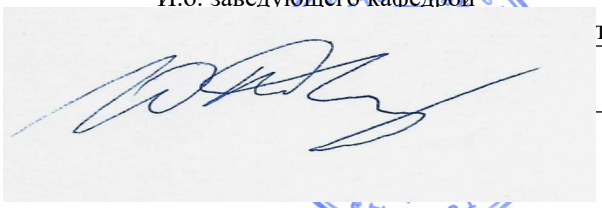
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

Варлатая С.К.
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой



ти

Ю.В.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Основы управления информационной безопасностью»
Направление подготовки 10.03.01 Информационная безопасность
(Комплексная защита объектов информатизации)
Форма подготовки очная

Школа естественных наук
Кафедра информационной безопасности
курс 3 семестр 6
лекции 18 час.
практические занятия 36 час.
лабораторные работы 00 час.
в том числе с использованием МАО лек. 00 / пр. 00 / лаб. 00 час.
всего часов аудиторной нагрузки 54 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 126 час.
в том числе на подготовку к экзамену 00 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет 6 семестр
экзамен не предусмотрен

Рабочая программа составлена в соответствии с требованиями образовательного стандарта, самостоятельно устанавливаемого ДВФУ, утвержденного приказом ректора от 20.07.2017 №12-13-1479.

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол 10 о « 15 » июня 2019 г.
№ ____ т ____ _____

И.о. заведующего кафедрой : Добржинский Ю.В., к.т.н., с.н.с.
Составитель (ли): Смирнов М.Е.

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)

Аннотация к рабочей программе дисциплины
«Основы управления информационной безопасностью»

Курс учебной дисциплины «Основы управления информационной безопасностью» предназначен для обучения студентов направления 10.03.01 «Информационная безопасность», профиль «Комплексная защита объектов информатизации» и входит в состав базовых дисциплин учебного плана Б1.Б.12.06.

Общая трудоемкость освоения дисциплины составляет 180 часов (5 з.е.). Учебным планом предусмотрены лекционные занятия (18 час.), практические занятия (36 час.), самостоятельная работа (126 час.). Дисциплина реализуется на 3 курсе в 6 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Основы управления информационной безопасностью» логически и содержательно связана с такими курсами, как «Основы информационной безопасности», «Основы проектной деятельности».

Содержание дисциплины охватывает следующий круг вопросов: понятие ИБ, основные составляющие, важные проблемы, законодательный уровень ИБ, риски в области ИБ, управление рисками, организация комплексной системы защиты информации.

Цель: изучение основ информационной безопасности, формирование у студентов информационного мировоззрения на основе знания принципов защиты информации; воспитание информационной культуры для эффективного применения полученных знаний в профессиональной деятельности, развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры;

Задачи:

- изучение структур и тенденций развития концептуальных,

методологических и организационных основ и современных принципов

защиты информации для обеспечения информационной безопасности государства;

- формирование основных теоретических и практических знаний,

раскрывающих сущность и значение национальной безопасности и защиты информации в условиях локальных и глобальных вычислительных сетей, автоматизированных информационных систем и систем телекоммуникаций;

- изучить основные положения Доктрины информационной

безопасности РФ;

- изучить основы комплексной системы защиты информации;

- изучить основы организационно-правового обеспечения защиты

информации;

- изучить методы и средства ведения информационных войн;

- изучить методологии создания систем защиты информации.

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

- способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-12);

- способность оценивать уязвимости информационных систем, разрабатывать требования и критерии оценки информационной безопасности, согласованных со стратегией развития информационных систем (ПК-10);

- способность разрабатывать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, проводить выбор необходимых технологий и технических средств, организовать внедрение и последующее сопровождение (ПСК-3.3).

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОК-3) способностью проявлять инициативу и принимать ответственные решения, осознавая ответственность за результаты своей профессиональной деятельности	Знает	особенности организации профессиональной работы структур, учреждений, функционирующих в сфере международных связей
	Умеет	применять знания о деятельности организаций, занимающихся вопросами международных отношений при решении профессиональных задач
	Владеет	навыками аналитического оценивания изучаемых проблем, навыками решения проблем, применяя профессиональные навыки и умения
(ПК-16) способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Знает	Правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны
	Умеет	Анализировать и оценивать угрозы информационной безопасности объекта
	Владеет	Методами формирования требований по защите информации
(ПК-17) способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Знает	Методы и принципы организационной защиты информации на предприятии
	Умеет	Формулировать и настраивать политику безопасности распространенных систем, а также локальных вычислительных сетей, построенных на их основе
	Владеет	Методами формирования требований по защите информации на предприятии
(ПК-18) способностью организовывать и выполнять работы по созданию, монтажу, наладке, испытанию и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности	Знает	основные факты о системах с открытым ключом
	Умеет	строить и изучать математические модели криптоалгоритмов
	Владеет	основным криптографическим инструментарием, необходимым для построение защищенных информационных систем

(ПК-19) способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Знает	первоочередные мероприятия по обеспечению безопасности информации АС организации
	Умеет	Пользоваться нормативными документами по защите информации
	Владеет	Методиками проверки защищенности объектов информации на соответствие требований нормативных документов

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

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Модуль I (18 час.)

Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации (4 час.)

Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.

Раздел 2. Информационная война, методы и средства ее ведения (8 час.)

Тема 1. Национальные интересы и угрозы информационной безопасности Российской Федерации (4 час.)

Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение.

Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России. Угрозы информационному обеспечению государственной политики Российской Федерации. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности.

Тема 2. Содержание информационного противоборства на межгосударственном уровне (2 час.)

Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного

противоборства. Информационное оружие, его классификация и возможности.

Тема 3. Содержание информационного противоборства на военном уровне (2 час.)

Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.

Раздел 3. Критерии защищенности телекоммуникационных систем (4 час.)

Тема 1. Методы и средства обеспечения информационной безопасности телекоммуникационных систем (2 час.)

Телекоммуникационная система как объект информационной безопасности. Общая характеристика методов и средств защиты информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.

Тема 2. Методы оценки защищенности телекоммуникационных систем от НСД (2 час.)

Модели, стратегии и системы обеспечения информационной безопасности.

Раздел 4. Защита информации, обрабатываемой в телекоммуникационных системах, от технических разведок (1 час.)

Тема 1. Классификация и возможности технических разведок (1 час.)

Радиоэлектронная разведка. Технические каналы утечки информации при эксплуатации телекоммуникационных систем. Методы защиты информации, обрабатываемой в телекоммуникационных системах, от технических разведок.

Раздел 5. Защита телекоммуникационных систем от внешнего электромагнитного воздействия (1 час.)

Тема 1. Генераторы электромагнитных импульсов (1 час.)

Эффекты, возникающие от внешнего электромагнитного воздействия на телекоммуникационные системы. Методы защиты телекоммуникационных систем от внешнего электромагнитного воздействия.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (36 час.)

Занятие 1 (8 час.)

1. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие.
2. Виды информации и основные методы ее защиты.

Занятие 2 (8 час.)

1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.
2. Виды угроз информационной безопасности Российской Федерации.
3. Источники угроз информационной безопасности Российской Федерации.
4. Анализ информационной инфраструктуры государства.
5. Информационное оружие, его классификация и возможности.
6. Цели информационной войны в мирное и военное время.
7. Объекты информационного воздействия в информационной войне

Занятие 3 (8 час.)

1. Формальная постановка и решение задачи обеспечения информационной безопасности телекоммуникационных систем.
2. Анализ факторов, определяющих безопасность телекоммуникационных систем.
3. Концепция защиты телекоммуникационных систем от НСД к информации.
4. Критерии оценки защищенности телекоммуникационных систем, методы и средства обеспечения их информационной безопасности.
5. Особенности обеспечения информационной безопасности телекоммуникационных систем при обработке информации, составляющей государственную тайну.

Занятие 4 (4 час.)

1. Классификация и возможности технических разведок. Радиоэлектронная разведка.
2. Технические каналы утечки информации при эксплуатации телекоммуникационных систем и их защита.

Занятие 5 (4 час.)

1. Защита телекоммуникационных систем от внешнего электромагнитного воздействия.

Занятие 6 (4 час.)

1. Контрольная работа по пройденному материалу.
2. Зачет

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Основы управления информационной безопасностью» 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 ДОСТИЖЕНИЙ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые модули/ разделы/ темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				Текущий контроль	Промежуточная аттестация
1	Модуль 1, Разделы 1, 2, 3, 4, 5	ОПК-2	Знает	ПР-7	1-6
			Умеет	ОУ-2	1-6
			Владеет	ОУ-1	1-6

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 ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 [Электронный ресурс] : учебное пособие / А.П. Курило [и др.]. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 244 с. https://e.lanbook.com/book/5178
2. Добровольский, В.С. Управление интеллектуальной безопасностью: организационные и правовые основы информационной безопасности [Электронный ресурс] : учебное пособие / В.С. Добровольский. — Электрон. дан. — Москва : МИСИС, 2014. — 224 с. https://e.lanbook.com/book/117438
3. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 c. http://www.iprbookshop.ru/6991.html

Дополнительная литература

(печатные и электронные издания)

1. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 c. http://www.iprbookshop.ru/52182.html
2. Шелупанов А.А. Информатика. Базовый курс. Часть 1. Общие вопросы информатики и программирование на Ассемблере [Электронный ресурс]: учебник/ Шелупанов А.А., Кирнос В.Н.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, В-Спектр, 2007.— 190 c. http://www.iprbookshop.ru/14012.html
3. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft [Электронный ресурс]/ Нестеров С.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 250 c. http://www.iprbookshop.ru/52141.html

Перечень информационных технологий и программного обеспечения

Программное обеспечение - не предусмотрено

Базы данных, информационно-справочные и поисковые системы - не предусмотрены

Материально-техническое обеспечение дисциплины: не предусмотрено

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Примерным учебным планом на изучение дисциплины отводится один семестр. В конце семестра, в качестве итогового контроля, предусмотрен зачет.

При изучении дисциплины учитывается междисциплинарный характер формируемых компетенций:

общекультурных компетенций (ОК):

способностью действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма (ОК-1) - формируется дисциплинами (помимо дисциплины Основы информационной безопасности): Философия, История, Правоведение, Организационное и правовое обеспечение информационной безопасности;

способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-5)- Философия, Правоведение, Безопасность жизнедеятельности, Криптографические методы защиты информации;

способностью к логически-правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания (ОК-9) - Философия, Иностранный язык, Экономика, Правоведение, Информатика.

профессиональных компетенций (ПК):

способностью понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных

системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-3) - Философия, Информатика, Теория информации и кодирования, Сети и системы передачи информации;

способностью использовать нормативные правовые документы в своей профессиональной деятельности (ПК - 6) - Иностранный язык, Правоведение, Организационное и правовое обеспечение информационной безопасности;

способностью осуществлять подбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-11) - Философия, Иностранный язык, Правоведение, Криптографические методы защиты информации, Организационное и правовое обеспечение информационной безопасности, Техническая защита информации;

способностью прогнозировать, ранжировать, моделировать информационные угрозы телекоммуникационных систем и оценивать уровни риска (ПК-21) -Информационная безопасность телекоммуникационных систем, Программно-аппаратные средства обеспечения информационной безопасности.

При преподавании дисциплины методически целесообразно в каждом разделе дисциплины выделить наиболее важные моменты и акцентировать на них внимание обучаемых.

Логика построения дисциплины основывается на изучении в начале курса общих вопросов безопасности с последующим переходом к изучению вопросов безопасности технических систем.

При изучении первого раздела программы следует обратить внимание обучаемых на возрастающую роль информационной безопасности в общей системе национальной безопасности Российской Федерации, а также на то, что информационная безопасность, имея и самостоятельное значение, входит составной частью в другие виды безопасности: экономическую,

внутриполитическую, социальную, международную, военную, пограничную, экологическую и другие.

При изучении второго раздела необходимо обратить внимание обучаемых на содержание национальных интересов Российской Федерации в информационной сфере и путях их обеспечения, а также на видах и источниках угроз информационной безопасности Российской Федерации. При этом целесообразно рассматривать информационную безопасность как некоторое состояние системы, которое достигается в результате информационного противоборства. В этом же разделе рекомендуется рассмотреть вопросы обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны, доведя до слушателей основные направления обеспечения информационной безопасности.

В третьем разделе изучение методов и средств обеспечения информационной безопасности объектов информационной сферы государства следует начинать с общих вопросов, а затем рассматривать методы и средства обеспечения информационной безопасности телекоммуникационных систем. При этом необходимо довести до слушателей модели, стратегии и системы обеспечения информационной безопасности телекоммуникационных систем.

В четвертом разделе изучаются вопросы защиты информации, обрабатываемой в телекоммуникационных системах, от технических разведок. Здесь целесообразно привести существующие классификации и возможности технических разведок. Отдельно рассмотреть такой вид разведки как радиоэлектронная разведка. Отдельным вопросом рассмотреть технические каналы утечки информации при эксплуатации телекоммуникационных систем.

Защита телекоммуникационных систем от внешнего электромагнитного воздействия изучается в пятом разделе. Особенностью при анализе данного воздействия является отсутствие нормативно-

методических документов по защите. При изложении данного материала особое внимание следует уделить эффектам, возникающим при внешнем электромагнитном воздействии на телекоммуникационную систему, и методам защиты от внешнего электромагнитного воздействия.

В разделе шесть подводятся итоги изучения курса и даются методические рекомендации по применению полученных знаний, умений и навыков при изучении последующих курсов.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 50) Оборудование: "Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор, Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718" Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.

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 управления информационной безопасностью»
Направление подготовки 10.03.01 Информационная безопасность
(Комплексная защита объектов информатизации)
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	2 неделя	Работа с конспектом	27 часов	ОУ-1 ОУ-2
2	6 неделя	Работа с конспектом	27 часов	ОУ-1 ОУ-2
3	8 неделя	Работа с конспектом	27 часов	ОУ-1 ОУ-2
4	12 неделя	Работа с конспектом	27 часов	ОУ-1 ОУ-2
5	16 неделя	Зачет	18 часов	ОУ-1

Характеристика заданий для самостоятельной работы студентов и методические рекомендации по их выполнению

Самостоятельная работа помогает студентам:

1) овладеть знаниями:

- чтение текста (учебника, первоисточника, дополнительной литературы и т.д.);

- составление плана текста, графическое изображение структуры текста, конспектирование текста, выписки из текста и т.д.;

- работа со справочниками и др. справочной литературой;

- использование компьютерной техники и Интернета и др.;

2) закреплять и систематизировать знания:

- работа с конспектом лекции;

- обработка текста, повторная работа над учебным материалом учебника, первоисточника, дополнительной литературы, аудио и видеозаписей;

- подготовка плана;

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности и уровня умений студентов.

Контроль результатов самостоятельной работы студентов должен осуществляться в пределах времени, отведенного на обязательные учебные занятия и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Работа с литературными источниками

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой.

Требования к представлению и оформлению результатов самостоятельной работы

Требования к конспекту для практических занятий:

1. Должен быть в отдельной тетради, подписанный.

2. Обязательно писать план занятия с указанием темы, вопросов, списка литературы и источников.

3. Отражать проблематику всех поставленных вопросов (анализ источника, литературы).

4. Иметь по ним аргументированные выводы. Слово «аргументированные» является ключевым. Главное - доказуемость выводов.

Критерии оценки выполнения самостоятельной работы

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;

- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы:

- Устный опрос.
- Зачет.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентов учебного материала;
- сформированность общеучебных умений;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности, варианты действий;
- умение сформировать свою позицию, оценку и аргументировать ее.

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 управления информационной безопасностью»
Направление подготовки 10.03.01 Информационная безопасность
(Комплексная защита объектов информатизации)
Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

Код и формулировка компетенции	Этапы формирования компетенции	
(ОК-3) способностью проявлять инициативу и принимать ответственные решения, осознавая ответственность за результаты своей профессиональной деятельности	Знает	особенности организации профессиональной работы структур, учреждений, функционирующих в сфере международных связей
	Умеет	применять знания о деятельности организаций, занимающихся вопросами международных отношений при решении профессиональных задач
	Владеет	навыками аналитического оценивания изучаемых проблем, навыками решения проблем, применяя профессиональные навыки и умения
(ПК-16) способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Знает	Правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны
	Умеет	Анализировать и оценивать угрозы информационной безопасности объекта
	Владеет	Методами формирования требований по защите информации
(ПК-17) способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Знает	Методы и принципы организационной защиты информации на предприятии
	Умеет	Формулировать и настраивать политику безопасности распространенных систем, а также локальных вычислительных сетей, построенных на их основе
	Владеет	Методами формирования требований по защите информации на предприятии
(ПК-18) способностью организовывать и выполнять работы по	Знает	основные факты о системах с открытым ключом
	Умеет	строить и изучать математические модели криптоалгоритмов

созданию, монтажу, наладке, испытанию и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности	Владеет	основным криптографическим инструментарием, необходимым для построение защищенных информационных систем
(ПК-19) способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Знает	первоочередные мероприятия по обеспечению безопасности информации АС организации
	Умеет	Пользоваться нормативными документами по защите информации
	Владеет	Методиками проверки защищенности объектов информации на соответствие требований нормативных документов

Контроль достижения целей курса

№ п/п	Контролируемые модули/ разделы/ темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				Текущий контроль	Промежуточная аттестация
1	Модуль 1, Разделы 1, 2, 3, 4, 5	ОПК-2	Знает	ПР-7	1-6
			Умеет	ОУ-2	1-6
			Владеет	ОУ-1	1-6

Критерии оценки:

86-100 баллов выставляется студенту, если решение задач показывает глубокое и систематическое знание всего программного материала, а также основного содержания лекционного курса; студент демонстрирует владение концептуально-понятийным аппаратом, научным языком и терминологией дискретной математики, логически корректное решение задач.

76-85 баллов – если студент показывает знание узловых проблем программы и основного содержания лекционного курса, умение пользоваться

концептуально-понятийным аппаратом в процессе решения задач в рамках данной темы, в целом логически корректное, но не всегда правильное аргументированное решение задач.

61-75 баллов – если студент показывает фрагментарное, поверхностное знание важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии дискретной математики; частичные затруднения с выполнением заданий, демонстрирует стремление логически обоснованно и последовательно изложить решение задачи.

50-60 баллов – если студент показывает незнание, либо отрывочное представление о данной проблеме в рамках учебно-программного материала, неумение использовать понятийный аппарат дискретной математики; отсутствие логики в решении задач.

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Текущая аттестация студентов

Текущая аттестация студентов по дисциплине «Основы управления информационной безопасностью» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация студентов по дисциплине «Основы управления информационной безопасностью» проводится в форме контрольных мероприятий (защиты индивидуальных заданий, контрольных работ и коллоквиумов) по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

- учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);

- степень усвоения теоретических знаний;

- уровень овладения практическими умениями и навыками по всем видам учебной работы;

- результаты самостоятельной работы.

Промежуточная аттестация студентов

Промежуточная аттестация студентов по дисциплине «Основы управления информационной безопасностью» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Промежуточная аттестация студентов по дисциплине «Основы управления информационной безопасностью» проводится в виде зачета в виде устного опроса в форме собеседования.

Вопросы к зачету.

1. Дать определение понятию национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Виды защищаемой информации.
4. Основные понятия и общеметодологические принципы теории информационной безопасности.
5. Роль информационной безопасности в обеспечении национальной безопасности государства.
6. Интересы личности в информационной сфере.
7. Интересы общества в информационной сфере.
8. Интересы государства в информационной сфере.
9. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
10. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности,

индивидуальному, групповому и общественному сознанию, духовному возрождению России.

11. Угрозы информационному обеспечению государственной политики Российской Федерации.
12. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.
13. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.
14. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства.
15. Содержание информационного противоборства на межгосударственном уровне
16. Информационная безопасность и информационное противоборство.
17. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства.
18. Информационное оружие, его классификация и возможности.
19. Телекоммуникационная система как объект информационного воздействия.
20. Телекоммуникационная система как объект информационной безопасности.

21. Общая характеристика методов и средств защиты информации.
22. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.
23. Программно-аппаратные средства обеспечения информационной безопасности.
24. Методы оценки защищенности телекоммуникационных систем от НСД.
25. Классификация и возможности технических разведок.
26. Радиоэлектронная разведка, ее объекты и содержание.
27. Технические каналы утечки информации при эксплуатации телекоммуникационных систем.
28. Методы защиты информации, обрабатываемой в телекоммуникационных системах, от технических разведок.
29. Эффекты, возникающие при внешнем электромагнитного воздействия на телекоммуникационные системы. Методы защиты от внешнего электромагнитного воздействия.

Критерии выставления оценки студенту на зачете по дисциплине «Основы управления информационной безопасностью»

Баллы (рейтинговой оценки)	**Оценка экзамена** (стандартная)	**Требования к сформированным компетенциям**
91-100	«зачтено»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал дисциплины «Основы управления информационной безопасностью», 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; способен анализировать и обобщать полученные знания, способен выбирать оптимальное решение, поставленной задачи.
76-90	«зачтено»	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; умеет строить дискретные модели при решении профессиональных задач, используя соответствующий математический аппарат решать типовые задачи, анализировать поставленную задачу, находить методы ее решения, проводить анализ полученного решения.
56-75	«зачтено»	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.
¿55	«не зачтено»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала дисциплины «Основы управления информационной безопасностью», допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, поэтому не может продолжить обучение без дополнительных занятий по данной дисциплине.

Приложение 3

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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по дисциплине «Основы управления информационной безопасностью»
Направление подготовки 10.03.01 Информационная безопасность
(Комплексная защита объектов информатизации)
Форма подготовки очная

Владивосток
2019

Методические указания по освоению дисциплины

На изучение дисциплины «Основы управления информационной безопасностью» отводится 180 часов, 54 часа из которых приходится на аудиторное обучение. Рекомендуется посещать все лекционные и практические занятия, во время которых составлять подробный конспект теоретического и практического изучаемого материала. Во время самостоятельной работы необходимо сначала прочитать конспекты лекций и практических занятий и потом приступить к выполнению индивидуального задания. При подготовке к контрольной работе необходимо выучить основные определения и формулы из конспекта лекций и просмотреть решение примеров по теме контрольной работы. При подготовке к зачету необходимо руководствуясь списком вопросов выучить перечисленные темы, пользуясь конспектом лекций и основной литературой. Для более глубокого изучения дисциплины можно использовать дополнительную литературу.