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
информационной безопасности
(название кафедры)

Добржинский Ю.В.
(подпись) (Ф.И.О.)

«15» июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Философия информационной безопасности
Направление 10.03.01 Информационная безопасность
(Комплексная защита объектов информатизации)
Форма подготовки очная

курс 3 семестр 5
лекции 36 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 72 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 36 час.
в том числе на подготовку к экзамену 00 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет 5 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 от «15» июня 2019 г.

И.о. заведующего кафедрой: Добржинский Ю.В., с.н.с., к.т.н.
Составитель: Смирнов М.Е., ст. преподаватель.

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 «Философия информационной безопасности»

Рабочая программа по курсу «Философия информационной безопасности» разработана для студентов по направлению 10.03.01 «Информационная безопасность» в соответствии с требованиями ФГОС ВО.

Общая трудоемкость освоения дисциплины составляет 108 часов (3 з.е.). Учебным планом предусмотрены лекционные занятия (36 часов), практические занятия (36 часов), самостоятельная работа студентов (36 часов). Дисциплина реализуется на 3 курсе в 5 семестре. Форма контроля по дисциплине – зачет.

Цель дисциплины «Философия информационной безопасности» сформировать у студентов объёмные знания, касающиеся каждой области информационной безопасности, а также развить в процессе обучения системное мышление. Взглянуть на общую картину информационной безопасности и принять участие в решении актуальных проблем в режиме круглого стола.

Задачи:

-основные положения теории информации, принципы построения систем обработки и передачи информации, основы семантического подхода к анализу информационных процессов;

-принципы организации информационных систем в соответствии с требованиями информационной защищенности, в том числе в соответствии с требованиями по защите государственной тайны;

-принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

-методами организации и управления деятельностью служб защиты информации на предприятии;

-технологией проектирования, построения и эксплуатации комплексных систем защиты информации;

-методами научного исследования уязвимости и защищенности информационных процессов;

-методиками проверки защищенности объектов информатизации на соответствие требованиям;

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

Код и формулировка компетенции	**Этапы формирования компетенции**	
ОК-12 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	Знает	цели, задачи и принципы построения комплексной системы защиты информации.
	Умеет	определять состав защищаемой информации.
	Владеет	общими представлениями о защищенности информации.
ОПК-4способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Знает	этапы разработки комплексной системы защиты информации.
	Умеет	синтезировать структуру комплексной системы защиты информации.
	Владеет	знаниями, что должна включать в себя комплексная защита информации.
ПК-16 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Знает	перечень вопросов зи, требующих документационного закрепления
	Умеет	оценивать эффективность комплексной системы защиты информации.
	Владеет	знаниями оценить стабильность системы защиты информации.

Для формирования вышеуказанных компетенций в рамках дисциплины «Философия 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: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

МОДУЛЬ 1. Проблемы обеспечения информационной безопасности (13 час.)

Раздел I. Проблемы обеспечения информационной безопасности (6 час.)

Тема 1. Определение и место информационной безопасности в общей совокупности информационных проблем современного общества (3 час.)

Предмет, задачи и содержание курса. Терминология курса. Место курса среди других дисциплин. Структура курса. Методика аудиторной и самостоятельной работы студентов по изучению курса. Основные источники информации. Научная и учебная литература. Периодические издания.

Тема 2. Ретроспективный анализ развития подходов к защите информации(3 час.)

Исторические аспекты развития информационно безопасности. Развитие информационной безопасности в Российской Федерации. Особенность эмпирического подхода к защите информации.

Раздел II. Современная постановка задачи защиты информации (7 час.)

Тема 1. Современная постановка задачи защиты информации(3 час.)

Задача защиты информации в последнее десятилетие. Повышение значимости информации как общественного ресурса. Существенные

изменения в организации информационных технологий. Возможности решения всех проблем организации защитных процессов по отношению

к информации в рамках единой концепции.

Тема 2. Сущность, необходимость, пути и условия перехода к интенсивным способам защиты информации(4 час.)

Понятия интенсивный способ защиты информации. Целенаправленная реализация всех достижений теории и практики. Трудности формирования баз исходных данных.

МОДУЛЬ 2. Основы теории защиты информации (11 час.)

Раздел I. Основы теории защиты информации (5 час.)

Тема 1. Особенности и состав научно-методологического базиса решения задач защиты информации(2 час.)

Понятия теории защиты информации. Задачи теории защиты информации. Методы решения задач информационной безопасности.

Тема 2. Общеметодологические принципы формирования теории защиты информации(3 час.)

Построение адекватных моделей изучаемых систем и процессов. Унификация разрабатываемых решений. Максимальная структуризация изучаемых систем и разрабатываемых решений. Радикальная эволюция в реализации разработанных концепций.

Раздел II. Методологический базис теории защиты информации (6 час.)

Тема 1. Методологический базис теории защиты информации (4 час.)

Методы теории нечетких множеств. Методы теории лингвистических переменных. Неформальные методы оценивания. Неформальные методы поиска оптимальных решений.

Тема 2. Принципы автоформализации профессиональных знаний эксперта-аналитика(2 час.)

Последовательность и взаимосвязь этапов автоформализации знаний. Функциональная структура процесса принятия решения. Сложность формирования базы моделей.

МОДУЛЬ 3. Угрозы и оценка уязвимости информации. (12 час.)

Раздел I. Угрозы и оценка уязвимости информации(6 час.)

Тема 1. Понятие угрозы безопасности информации. Ретроспективный анализ подходов к формированию множества угроз(3 час.)

История развития подходов к решению проблем обеспечения информационной безопасности. Интенсификация процессов защиты информации как основа теоретико-концептуального подхода.

Тема 2. Системная классификация угроз безопасности информации (3 час.)

Системная классификация угроз информации. Происхождение угроз. Предпосылки появления угроз. Источники угроз.

Раздел II. Постановка задачи и анализ существующих методик (6 час.)

Тема 1. Постановка задачи и анализ существующих методик определения требований к защите информации (3 час.)

Переход от концепции создания инструментальных средств получения решений на инженерной основе к концепции создания методологического базиса и инструментальных средств. Проблема определения требований к защите информации, их характер рассмотрение организационного и технического аспекта.

Тема 2. Основные выводы и перспективы развития теории и практики защиты информации(3 час.)

Периоды: эмпирический, эмпирико-концептуальный и теоретико-концептуальный. Основы целостной теории защиты информации. Совершенствование теоретических основ защиты информации. Перевод защиты информации на индустриальную основу. Комплексное обеспечение

компьютерной безопасности. Комплексное обеспечение безопасности объекта. Обеспечение информационной безопасности.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (36час.)

Занятие 1. Моделирование проблем и решения организации защитных процессов по отношению к информации в рамках единой концепции.**(4час.)**

Занятие 2. Основное содержание теории защиты информации **(4час.)**

Занятие 3. Методы оценки уязвимости информации **(4час.)**

Занятие 4. Методы оценки достоверности информационной **(4час.)**

Занятие 5. Базы моделей прогнозирования значений показателей уязвимости информации **(4час.)**

Занятие 6. Модели оценки ущерба от реализации угроз безопасности информации **(4час.)**

Занятие 7. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты **(4час.)**

Занятие 8. Определение весов вариантов потенциально возможных условий защиты информации **(4час.)**

Занятие 9. Методы деления поля значений факторов на типовые классы **(4час.)**

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Философия 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 - наименование	
				текущий контроль	промежуточная аттестация
1	МОДУЛЬ 1. Проблемы обеспечения информационной безопасности.	ОК-12 ОПК-4 ПК-16	Знает	ПР-4	1-8
			Умеет	ПР-4	1-8
			Владеет	ПР-4	1-8
2	МОДУЛЬ 2. Основы теории защиты информации.	ОК-12 ОПК-4 ПК-16	Знает	ПР-7	9-17
			Умеет	ПР-7	9-17
			Владеет	ПР-7	9-17
3	МОДУЛЬ 3. Угрозы и оценка уязвимости информации.	ОК-12 ОПК-4 ПК-16	Знает	ПР-7	18-25
			Умеет	ПР-7	18-25
			Владеет	ПР-7	18-25

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и 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. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 242 с.— Режим доступа: http://www.iprbookshop.ru/62945.html.— ЭБС «IPRbooks»

2. Защита информации ограниченного доступа от утечки по техническим каналам: Справочное пособие / Бузов Г.А. - М.:Гор. линия-Телеком, 2015. - 586 с.: 60x90 1/16 (Обложка) ISBN 978-5-9912-0424-8 - Режим доступа: http://znanium.com/catalog/product/895240

3. Никифоров С.Н. Защита информации [Электронный ресурс]: учебное пособие/ Никифоров С.Н.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2015.— 384 с.— Режим доступа: http://www.iprbookshop.ru/74365.html.— ЭБС «IPRbooks»

Дополнительная литература

1. Каторин Ю.Ф. Техническая защита информации [Электронный ресурс]: лабораторный практикум/ Каторин Ю.Ф., Разумовский А.В., Спивак А.И.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2013.— 113 с.— Режим доступа: http://www.iprbookshop.ru/68715.html.— ЭБС «IPRbooks»

2. Титов А.А. Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие/ Титов А.А.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2010.— 197 с.— Режим доступа: http://www.iprbookshop.ru/13931.html.— ЭБС «IPRbooks»

3. Голиков А.М. Защита информации от утечки по техническим каналам [Электронный ресурс]: учебное пособие/ Голиков А.М.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2015.— 256 с.— Режим доступа: http://www.iprbookshop.ru/72090.html.— ЭБС «IPRbooks»

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия

кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020 7) Dallas Lock. Поставщик Конфидент. Партнерское соглашение БП-8-16/576-16-ЦЗ/1 от 23.11.2016. Срок действия договора 23.11.2019. Лицензия до 23.11.2019

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для более эффективного освоения и усвоения материала рекомендуется ознакомиться с теоретическим материалом по той или иной теме до проведения семинарского занятия. Работу с теоретическим материалом по теме с использованием учебника или конспекта лекций можно проводить по следующей схеме:

- название темы;
- цели и задачи изучения темы;
- основные вопросы темы;
- характеристика основных понятий и определений, необходимых для усвоения данной темы;
- список рекомендуемой литературы;
- наиболее важные фрагменты текстов рекомендуемых источников, в том числе таблицы, рисунки, схемы и т.п.;
- краткие выводы, ориентирующие на определенную совокупность сведений, основных идей, ключевых положений, систему доказательств, которые необходимо усвоить.

В ходе работы над теоретическим материалом достигается:

- понимание понятийного аппарата рассматриваемой темы;
- воспроизведение фактического материала;
- раскрытие причинно-следственных, временных и других связей;
- обобщение и систематизация знаний по теме.

При подготовке к экзамену рекомендуется проработать вопросы, рассмотренные на лекционных и практических занятиях и представленные в рабочей программе, используя основную литературу, дополнительную литературу и интернет-ресурсы.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, 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 – 15) Оборудование: Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Электронная доска Poly Vision Walk-and-Talk WTL 1810 Мультимедийная аудитория: 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

Приложение 1 к рабочей программе учебной дисциплины

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 «Философия информационной безопасности»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «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	5 неделя	Задание по группам.	8	ПР-10
2	8 неделя	Реферат «Угрозы информационной безопасности»	6	ПР-4
3	10 неделя	Реферат «Актуальные методы защиты информации»	6	ПР-4
4	13 неделя	Ролевая игра «Защита - нападение»	8	ПР-10
5	19 неделя	Зачет	8	УО-1

Самостоятельная работа студентов включает:

– освоение лекционного материала;

– подготовку к ролевым игра, изучения основных законов информационной безопасности.

– выполнение индивидуального домашнего задания;

– оформление выполненного индивидуального домашнего задания;

– подготовку к защите выполненного индивидуального домашнего задания.

В отчет по индивидуальному домашнему заданию должны входить:

1) Условия задач (конкретное задание выдается преподавателем);

2) Согласование с преподавателем выполненного домашнего задания;

3) Выступление перед аудиторией.

Самостоятельная работа студентов по дисциплине складывается из времени, необходимого для освоения лекционного материала, освоения и совершенствования навыков решения задач и времени выполнения и оформления индивидуального домашнего задания.

Задачи, включенные в самостоятельные работы, ориентированы на выявление степени владения студентом техникой решения типовых задач,

умения находить нужный метод решения и уверенно применять его в условиях дефицита времени.

Приложение 2 к рабочей программе учебной дисциплины

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 «Философия информационной безопасности»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки - очная

Владивосток
2019

Обучающиеся должны выполнять индивидуальные задания. Задания должны быть выполнены в процессе изучения соответствующего раздела курса. При выполнении заданий возможно использование учебно-методической литературы и электронных лекций курса.

Вопросы к экзамену

1. История развития подходов к решению проблем обеспечения информационной безопасности. Интенсификация процессов защиты информации как основа теоретико-концептуального подхода.
2. Недостатки формальных методов исследования систем применительно к проблемам защиты информации. Необходимость разработки неформальной теории систем.
3. Основы методологии системного анализа. Понятие структуризации проблем.
4. Ретроспективный анализ развития подходов к обеспечению информационной безопасности, эмпирический, эмпирико-концептуальный и теоретико-концептуальный подходы.
5. Суть и основное содержание унифицированной концепции защиты информации.
6. Основное содержание компонентов унифицированной концепции защиты информации.
7. Современная постановка задачи защиты информации. Факторы, обуславливающие необходимость, и объективные предпосылки изменения постановки задачи в современных условиях.
8. Особенности перехода в современных условиях к интенсивным способам защиты информации.
9. Особенности и состав научно-методологического базиса теории защиты информации.
10. Общеметодологические принципы формирования теории защиты информации.

11. Теоретико-прикладные принципы формирования теории защиты информации.

12. Методологический базис теории защиты информации: теория нечетких множеств, теория лингвистических переменных, неформальные методы оценивания, неформальные методы поиска оптимальных решений.

13. Модели систем и процессов защиты информации. Системная классификация моделей.

14. Обобщенная модель процессов защиты информации.

15. Стратегии защиты информации. Критерии выбора стратегий.

16. Система показателей уязвимости информации, содержание показателей уязвимости.

17. Методы и модели оценки уязвимости информации.

18. Методы определения требований к защите информации.

19. Методы проектирования систем защиты информации

20. Методы обеспечения повседневной деятельности системы защиты информации.

21. Обобщенные итоги и перспективы развития теории и практики защиты информации.

22. Основные выводы из истории развития теории и практики защиты информации.

23. Перспективы развития теории и практики защиты информации.

24. Проблемы создания и организации работы центров защиты информации.

25. Проблемы кадрового обеспечения сферы информационной безопасности.