



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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»

Руководитель ОП

(подпись)

Варлатая С.К.

(Ф.И.О.)

«УТВЕРЖДАЮ»

И.о. заведующего кафедрой
информационной безопасности
(название кафедры)



(подпись)

Добржинский Ю.В.

(Ф.И.О.)

«15» июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организационное и правовое обеспечение информационной безопасности

Направление 10.03.01 Информационная безопасность

(Комплексная защита объектов информатизации)

Форма подготовки очная

курс 4 семестр 7

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 7 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 «Организационное и правовое обеспечение информационной безопасности»

Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» разработана для студентов 4 курса по специальности «Информационная безопасность» в соответствии с требованиями ФГОС ВО по данной специальности и положением об учебно-методических комплексах дисциплин образовательных программ высшего профессионального образования. Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к дисциплинам бакалавриата.

Общая трудоемкость освоения дисциплины составляет 108 часов (3 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (36 час.), самостоятельная работа студентов (36 час.). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – зачёт.

Дисциплина «Организационное и правовое обеспечение информационной безопасности» имеет целью обучить студентов принципам построения, средств и условий организационной и правовой защиты информации, порядок засекречивания и рассекречивания сведений, документов и продукции, допуск и доступ к конфиденциальной информации и документам, организацию внутри-объектового и пропускного режимов и организацию охраны на предприятиях, а так же показать студентам, что концепция организационного и правового обеспечения информационной безопасности стала определяющим фактором при создании эффективных систем обработки информации.

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к базовой части профессионального цикла. Знания и практические навыки, полученные из дисциплины «Организационное и правовое обеспечение информационной

безопасности», используются студентами при разработке выпускной квалификационной работы.

Цель: Дать основы устройства и принципов организационного и правового обеспечения информационной безопасности.

Задачи:

- Дать базовое представление об информационной безопасности;
- Дать основы средств и методов организационного и правового обеспечения информационной безопасности;
- Дать основные принципы построения защиты информации безопасности;
- Привить системный подход к проблеме защиты информации

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

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-5 способностью использовать нормативные правовые акты в профессиональной деятельности	Знает	требования к подсистеме аудита и политике аудита
	Умеет	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
	Владеет	методами формирования требований по защите информации
ПК-9 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знает	основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации
	Умеет	применять действующую законодательную базу в области обеспечения компьютерной безопасности
	Владеет	навыками организации и обеспечения режима секретности; методами организации и управления деятельностью служб защиты информации на предприятии

Для формирования вышеуказанных компетенций в рамках дисциплины «Организационное и правовое обеспечение 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. Основы организационного обеспечения ИБ (13ч)

Раздел 1. Организационное обеспечение ИБ (13 ч)

Тема 1. Принципы, силы, средства и условия организационной защиты информации (2ч)

Тема 2. Порядок засекречивания и рассекречивания сведений, документов и продукции (4ч)

Тема 3. Допуск и доступ к конфиденциальной информации и документам (3ч)

Тема 4. Организация внутри-объектового и пропускного режимов на предприятиях и в учреждениях; организация охраны на них (4ч)

Модуль 2. Организация ИБ (14ч)

Раздел 1. Организация защиты информации (14 ч)

Тема 1. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам (3ч)

Тема 2. Основные понятия информационной безопасности (3ч)

Тема 3. Организация защиты информации от утечки по техническим каналам(4ч)

Тема 4. Задачи и структура государственной системы инженерно-технической защиты информации (4ч)

Модуль 3. Методы обеспечения ИБ (9ч)

Раздел 1. Методология обеспечения защиты информации (9 ч)

Тема 1. Организация защиты информации на предприятиях (3ч)

Тема 2. Методическое обеспечение инженерно-технической защиты

информации (3ч)

Тема 3. Моделирование каналов несанкционированного доступа к информации(3ч)

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практическая работа(36ч)

Тема 1. Защита информации от копирования (6ч)

Тема 2. Защита программ от дисасемблирования(7ч)

Тема3. Защита программ от дисасемблирования. Архивирование программного кода (6ч)

Тема 4. Защита программ в оперативной памяти(9ч)

Тема5. Приемы работы с защищенными программами(8ч)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Организационное и правовое обеспечение 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	Коды и этапы формирования	Оценочные средства - наименование
-------	-------------------------------	---------------------------	-----------------------------------

	дисциплины	компетенций	текущий контроль	промежуточная аттестация	
1	Модуль 1. Основы организационного обеспечения ИБ	ОПК-5 ПК-9	Знает	ПР-1	1-7
			Умеет	ПР-4	1-7
			Владеет	ПР-7	1-7
2	Модуль 2. Организация ИБ	ОПК-5 ПК-9	Знает	ПР-1	8-21
			Умеет	ПР-4	8-21
			Владеет	ПР-7	8-21
3	Модуль 3. Методы обеспечения ИБ	ОПК-5 ПК-9	Знает	ПР-1	22-35
			Умеет	ПР-4	22-35
			Владеет	ПР-7	22-35

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. Кармановский, н.с. Организационно-правовое и методическое обеспечение информационной безопасности [электронный ресурс]: учебное пособие / н.с. Кармановский, о.в. Михайличенко, с.в. Савков. — электрон. Дан. — Санкт-Петербург: НИУ ИТМО, 2013. — 148 с. — режим доступа: https://e.lanbook.com/book/43579#book_name
2. Жигулин, Г.П. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебное пособие / Г.П. Жигулин. — Электрон. дан. — Санкт-Петербург: НИУ ИТМО, 2014. — 173 с. — Режим доступа: <https://e.lanbook.com/book/70952>

3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. — Режим доступа: <http://znanium.com/catalog/product/335362>
4. 1. Варлатая С.К., Шаханова М.В. Защита и обработка конфиденциальных документов : учебно-методический комплекс для вузов. Владивосток : Изд-во Дальневосточного технического университета, 2008. – 179 с. - <http://lib.dvfu.ru:8080/lib/item?id=chamo:384161&theme=FEFU>

Дополнительная литература

1. Ададунов С.Е. Информационная безопасность и защита информации на железнодорожном транспорте: В 2ч.Ч.1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте: Учебник / Ададунов С.Е.; Под ред. Корниенко А.А. - М.:УМЦ ЖДТ, 2014. - 440 с. — Режим доступа: <http://znanium.com/catalog/product/487777>
2. Карабутов, Н. Н. Построение и анализ информационного обеспечения в информационных системах на водном транспорте [Электронный ресурс] : Учебное пособие / Н. Н. Карабутов, П. Н. Карабутов, М. И. Иванов. — М. : Алтайр-МГАВТ, 2013. - 170 с. — Режим доступа: <http://znanium.com/catalog/product/476237>
3. Андрианов В.В. Обеспечение информационной безопасности бизнеса / Андрианов В.В., Зефирова С.Л., Голованов В.Б. - М.:ЦИПСИР, 2011. - 373 с. — Режим доступа: <http://znanium.com/catalog/product/556539>

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного,	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 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.
---	--

практического семинарского групповых индивидуальных консультаций, контроля промежуточной аттестации.	и и и и и	4) MathCad Education University 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.
--	-----------------------	---

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 зачету 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

<p>Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.</p>	<p>Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: "Компьютер DNS Office (автоматизированное рабочее место), Рабочее место сотрудников в составе: системный блок, клавиатура, мышь, монитор 17" Acer-173 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 EW330U, 3000 ANSI Lumen, 1280x800 Сетевая видеочкамера Multipix MP-HD718 Доска аудиторная</p>
--	--



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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

**УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ
РАБОТЫ ОБУЧАЮЩИХСЯ**

**по дисциплине «Организационное и правовое обеспечение
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	реферат	21	УО-1
2	12 неделя	зачет	15	УО-1

Самостоятельная работа студентов включает:

- освоение лекционного материала;
- выполнение индивидуального домашнего задания;
- оформление выполненного индивидуального домашнего задания;
- подготовку к защите выполненного индивидуального домашнего задания.



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 «Организационное и правовое обеспечение
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 зачету

1. Основные положения Концепции национальной безопасности Российской Федерации и Доктрины информационной безопасности Российской Федерации.

2. Определение понятия «государственная тайна». Перечень сведений, составляющих государственную тайну.

3. Правовые механизмы отнесения сведений к государственной тайне, рассекречивания сведений и их носителей.

4. Защита государственной тайны. Субъекты защиты государственной тайны, их функции в данной сфере. Контроль и надзор за обеспечением защиты государственной тайны.

5. Особенности правовой защиты сведений, составляющих государственную тайну.

6. Основные объекты института коммерческой тайны.

7. Субъекты информационных правоотношений, возникающих по поводу коммерческой тайны.

8. Правовой режим коммерческой тайны.

9. Защита прав на коммерческую тайну. Ответственность за нарушения при работе с коммерческой тайной.

10. Институты профессиональных тайн и их значение для обеспечения защиты прав и свобод человека и гражданина, коммерческих интересов организаций и учреждений.

11. Основные категории сведений, защищаемых в режиме профессиональной тайны.

12. Система правового регулирования отдельных институтов профессиональных тайн.

13. Понятие и характеристика правонарушений в информационной сфере.
14. Криминалистическая характеристика преступлений в сфере компьютерной информации.
15. Ответственность за правонарушения в сфере компьютерной информации. Понятие информационных угроз.
16. Информационные войны.
17. Информационные угрозы безопасности РФ. Доктрина информационной безопасности РФ.
18. Виды противников. Хакеры.
19. Компьютерные вирусы. История. Определение по УК РФ.
20. Виды, принципы действия вирусов, демаскирующие признаки.
21. Виды возможных нарушений информационной системы. Общая классификация информационных угроз.
22. Угрозы ресурсам компьютерной безопасности. Угрозы, реализуемые на уровне локальной компьютерной системы. Человеческий фактор.
23. Угрозы компьютерной информации, реализуемые на аппаратном уровне.
24. Удаленные атаки на компьютерные системы. Причины уязвимостей компьютерных сетей.
25. Правовое урегулирование защиты информации.
26. Роль, задачи и обязанности администратора безопасности КС.
27. Защита данных криптографическими методами. Методы шифрования.
28. Защита данных криптографическими методами. Алгоритмы шифрования.
29. Требования к шифрам. Сравнение DES и ГОСТ 28147-89
30. Типовые удаленные атаки с использованием уязвимостей сетевых протоколов. Классификация удаленных атак.

31. Политика безопасности и ее составляющие.
32. Модели защиты информации в КС.
33. Технологии защиты и разграничения доступа.
34. Стандарты ИБ.



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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по дисциплине «Организационное и правовое обеспечение
информационной безопасности»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки - очная

Владивосток
2019

Учебным планом на изучение дисциплины отводится один семестр. Промежуточной формы контроля не предусмотрено. В качестве итогового контроля предусмотрен экзамен.

Исходя из объема часов, выделяемых на изучение дисциплины, надо обратить особое внимание на организацию самостоятельной работы. Студентам необходимо прививать умение самостоятельного поиска решений в ходе выполнения заданий. Детальную проработку материала, связанного с разработкой программного обеспечения, следует оставить на самостоятельное изучение.

Следует отметить, что на лекциях приходится излагать достаточно большое количество материала технического характера, поэтому требуется уделить особое внимание вопросам подачи материала с использованием технических средств обучения. Кроме того, студентам необходимо заранее выдать требуемые лекционные и справочные материалы, а также методические указания и рекомендации. При изложении материала следует особо подчеркнуть связь излагаемых вопросов с практикой, в противном случае на практических занятиях может возникнуть большое количество дополнительных вопросов.

По основным разделам и темам дисциплины преподавателю важно придерживаться следующих методических рекомендаций.

Модуль «Основы организационного обеспечения ИБ» является большей частью теоретической, ее главная цель объяснить, что такое защита информации, зачем она нужна и какие принципы, силы, средства и условия существуют в настоящее время. Рассмотреть, как осуществляется порядок засекречивания и рассекречивания сведений, как реализуется допуск и доступ к конфиденциальной информации документам. Подробно рассмотреть Организация внутриобъективного и пропускного режимов на предприятиях и организации охраны на них. Дополнительно можно включить историческую составляющую.

Модуль «Организации ИБ» представляет самую важную и объемную часть курса. Обучаемые должны уяснить способы организации защиты информации по техническим каналам, основные задачи и структуру государственной системы инженерно-технической защиты информации, организацию подготовки и проведения совещаний и заседаний по конфиденциальной безопасности в соответствии с законодательством Российской Федерации.

Модуль «Методы обеспечения ИБ» является теоретически-практической. В ходе изучения данной темы, помимо практических упражнений, рекомендуется проводить занятия, на которых система будет рассматриваться в целом, будут моделироваться угрозы и методы и средства предотвращения их реализации.