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

Корнюшин П.Н
(подпись) (Ф.И.О.)

«01» февраля 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 36 час.
практические занятия 36 час.
лабораторные работы 00 час.
в том числе с использованием МАО лек. 9 / пр. 00 / лаб. 18 час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 27 час.
самостоятельная работа 36 час.
в том числе на подготовку к экзамену 36 час.
контрольные работы (количество) не предусмотрены
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 № 5 от «01» февраля 2020 г.

И. о. заведующего кафедрой: Корнюшин П.Н., д.ф.-м.н., профессор.
Составитель: Добржинский Ю.В., д.ф.-м.н., профессор

Владивосток
2020

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: Fundamentals 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 understand the importance of information in the development of modern society, to apply the achievements of information technology to search and process information on the profile of activities in global computer networks, library collections and other sources of information (OPK-3);
- the ability to develop, analyze and justify the adequacy of mathematical models of the processes arising from the work of software and hardware information protection (PSK-2.4);
- the ability to conduct a comparative analysis and make an informed choice of software and hardware tools for protecting information, taking into account modern and promising mathematical methods for protecting information (PSK-2.5).

Learning outcomes:

- (ОПК-5) способностью использовать нормативные правовые акты в своей профессиональной деятельности
- (ОПК-9) способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации

Course description: This discipline is aimed at learning 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 ре-сурс] : 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 дея-тельности 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 учебной программе дисциплины «Основы информационной безопасности»

Курс учебной дисциплины «Основы информационной безопасности» предназначен для обучения студентов направления 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин базовой части учебного плана Б1.Б.11.01

Общая трудоемкость дисциплины составляет 144 часа (4 з.е.). Учебным планом предусмотрены лекционные занятия (36 часа, в том числе 9 часов в интерактивной форме), практическая работа (36 часов, в том числе 18 часов в интерактивной форме), самостоятельная работа (36 часов, 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» логически и содержательно связана с такими курсами, как «Информатика» и «Введение в специальность».

Данная дисциплина нацелена на изучение 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 изучения дисциплины «Основы информационной безопасности» заключается в обучении 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 понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);

- способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации (ПСК-2.4);

- способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации (ПСК-2.5).

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 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) способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	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

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 **(8 час.)**

Тема 1. Понятие национальной безопасности **(4 час.)**

Тема 2. Информационная безопасность в системе национальной безопасности РФ **(4 час.)**

Раздел II. Концепция информационной безопасности **(8 час.)**

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

Тема 2. Концептуальная модель информационной безопасн**ости (2 час.)**

Тема 3. Угрозы конфиденциальной информации **(2 час.)**

Тема 4. Действия, приводящие к неправомерному овладению конфиденциальной информацией**. (2 час.)**

Раздел III. Направления обеспечения информационной безопасности **(3 час.)**

Тема 1. Правовая защита **(1 час.)**

Тема 2. Организационная защита **(1 час.)**

Тема 3. Инженерно-техническая защита **(1 час.)**

Раздел IV. Выявление технических каналов утечки информации **(18 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 **(2 час.)**

Тема 5. Обнаружители диктофонов **(2 час.)**

Тема 6. Универсальные поисковые приборы **(2 час.)**

Тема 7. Программно-аппаратные поисковые комплексы **(2 час.)**

Тема 8. Нелинейные локаторы **(2 час.)**

Тема 9. Технические средства контроля двухпроводных линий **(2 час.)**

Раздел V. Защита информации от утечки по техническим каналам **(3 час.)**

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

Тема 2. Методы и средства защиты речевой информации в помещении **(1 час.)**

Тема 3. Методы и средства защиты телефонных линий **(1 час.)**

Раздел VI. Защита компьютерной информации от несанкционированного доступа **(6 час.)**

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

Тема 2. Программы-шпионы **(1 час.)**

Тема 3. Парольная защита операционных систем **(1 час.)**

Тема 4. Аппаратно-программные средства защиты информации от НСД **(1 час.)**

Тема 5. Проблемы обеспечения безопасности в глобальных сетях (1 час.)

Тема 6. Построение комплексных систем защиты информации **(1 час.)**

Раздел VII. Стандарты и рекомендации в области информационной безопасности **(8 час.)**

Тема 1. Оранжевая книга (TCSEC) **(2 час.)**

Тема 2. Радужная серия **(2 час.)**

Тема 3. Гармонизированные критерии Европейских стандартов (ITSEC) **(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 «Добржинский Ю.В., 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	собеседование (ОУ-1)	1-7
			умеет	коллоквиум (ОУ-2)	1-7
			владеет	конспект (ПР-7)	1-7
2	Раздел II. Концепция информационной безопасности	ОПК-5 ОПК-9	знает	собеседование (ОУ-1)	8-10
			умеет	коллоквиум (ОУ-2)	8-10
			владеет	конспект (ПР-7)	8-10
3	Раздел III. Направления обеспечения информационной безопасности	ОПК-5 ОПК-9	знает	собеседование (ОУ-1)	11-19
			умеет	коллоквиум (ОУ-2)	11-19
			владеет	конспект (ПР-7)	11-19
4	Раздел IV. Выявление технических каналов утечки информации	ОПК-5 ОПК-9	знает	собеседование (ОУ-1)	20-23
			умеет	коллоквиум (ОУ-2)	20-23
			владеет	конспект (ПР-7)	20-23
5	Раздел V. Защита информации от утечки по техническим каналам	ОПК-5 ОПК-9	знает	собеседование (ОУ-1)	23-25
			умеет	коллоквиум (ОУ-2)	23-25

			владеет	конспект (ПР-7)	23-25
6	Раздел VI. Защита компьютерной информации от несанкционированного доступа	ОПК-5 ОПК-9	знает	собеседование (ОУ-1)	23-25
			умеет	коллоквиум (ОУ-2)	23-25
			владеет	конспект (ПР-7)	23-25
7	Раздел VII. Стандарты и рекомендации в области информационной безопасности	ОПК-5 ОПК-9	знает	собеседование (ОУ-1)	26-30
			умеет	коллоквиум (ОУ-2)	26-30
			владеет	конспект (ПР-7)	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 ре-сурс] : 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 дея-тельности 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

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 633, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	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. 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.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Основы информационной безопасности», составляет 72 академических часов. На самостоятельную работу – 36 часов. При этом аудиторная нагрузка состоит из 36 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. Та-

ким 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

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 633, 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: 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 информационной безопасности»

Специальность 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	Выполнение практических занятий. (Отчет по практическим занятиям 1-9)	63	Отчет о выполнении
8	Сессия	Подготовка к экзамену	9	Экзамен

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»

Специальность 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) способностью 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) способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	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

Контроль достижений 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	собеседование (ОУ-1)	1-7
			умеет	коллоквиум (ОУ-2)	1-7
			владеет	конспект (ПР-7)	1-7
2	Раздел II. Концепция информационной безопасности	ОПК-5 ОПК-9	знает	собеседование (ОУ-1)	8-10
			умеет	коллоквиум (ОУ-2)	8-10
			владеет	конспект (ПР-7)	8-10
3	Раздел III. Направления обеспечения информационной безопасности	ОПК-5 ОПК-9	знает	собеседование (ОУ-1)	11-19
			умеет	коллоквиум (ОУ-2)	11-19
			владеет	конспект (ПР-7)	11-19
4	Раздел IV. Выявление технических каналов утечки информации	ОПК-5 ОПК-9	знает	собеседование (ОУ-1)	20-23
			умеет	коллоквиум (ОУ-2)	20-23
			владеет	конспект (ПР-7)	20-23

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

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
(ОПК-5) способностью использовать нормативные правовые акты в своей профессиональной деятельности	знает (пороговый уровень)	Роль и место информационной безопасности в системе национальной безопасности страны.	Полнота и системность знаний	Изложение полученных знаний полное, в соответствии с требованиями учебной программы;
	умеет (продвинутый)	Действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма.	Степень самостоятельности выполнения действия (умения)	Обучающийся способен самостоятельно действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма.
	владеет (высокий)	Навыком анализа информационной инфраструктуры государства.	Степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	Обучающийся владеет навыком анализа информационной инфраструктуры государства.
(ОПК-9) способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	знает (пороговый уровень)	Современные подходы к построению систем защиты информации.	Полнота и системность знаний	Изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.
	умеет (продвинутый)	Выбирать и анализировать показатели	Степень самостоятельности выпол-	Обучающийся способен самостоятельно выбирать и

		качества и критерии оценки систем и отдельных методов и средств защиты информации.	нения действия (умения)	анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации.
	владеет (высокий)	Навыком работы с различными средствами программирования и отладки программного обеспечения.	Степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	Обучающийся владеет навыком работы с различными средствами программирования и отладки программного обеспечения.

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

В 3 семестре экзамен выставляется на основании сдачи всех самостоятельных работ и сдачи экзаменационного билета.

Для подготовки к ответу на экзамене обучающийся получает 20 минут. В ходе подготовки обучающийся может составлять любые записи, однако оценивается прежде всего устный, а не письменный ответ.

При определении оценки ответа обучающегося как на экзамене, так и на практическом занятии учитываются:

- соблюдение норм литературной речи;
- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций и учебной литературы, актуальным сведениям из информационных ресурсов Интернет.

Для получения «зачтено» ответ студента должен соответствовать следующим минимальным требованиям: полный ответ на 1 вопрос или частичный ответ на 2 вопроса; допускаются нарушения в последовательности изложения; демонстрируются поверхностные знания вопроса; имеются затруднения с выводами; допускаются нарушения норм литературной речи.

Оценка **«не зачтено»** выставляется в случае, если: обучающийся не ответил полно ни на один вопрос; материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине; имеются заметные нарушения норм литературной речи.

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.

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются конспект (ПР-7).

Конспект является показателем сформированности компетенции на пороговом уровне. Темы конспектов соответствуют темам теоретической части курса из Раздела II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Содержание конспекта
Отлично	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы, а также содержит сведения из дополнительных источников.
Хорошо	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Удовлетворительно	Конспект содержит базовые понятия, термины, положения, изученные на лекции.
Неудовлетворительно	Конспект не содержит основных понятий, терминов, положений по данной теме.