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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

_____ Добржинский Ю.В
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

_____ Добржинский Ю.В
(подпись) (Ф.И.О.)

« 15 » июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы построения защищенных компьютерных сетей
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс 5 семестр 9
лекции 36 час.
практические занятия 36 час.
лабораторные работы 00 час.
в том числе с использованием МАО лек. 9 / пр. 12 / лаб. 00 час.
в том числе в электронной форме лек. 00 / пр. 00 / лаб. 00 час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 21 час.
в том числе в электронной форме 00 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 27 час.
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 9 Семестр

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

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

И.о. заведующего кафедрой: Добржинский Ю.В., к.т.н., с.н.с.
Составитель (ли): Гордеев С.И. К.т.н., доцент, профессор

Владивосток
2019

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

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

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

II. Рабочая программа пересмотрена на заседании кафедры:

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

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

III. Рабочая программа пересмотрена на заседании кафедры:

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

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

IV. Рабочая программа пересмотрена на заседании кафедры:

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

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

ABSTRACT

Specialist's degree in 10.05.01 Computer Security
Specialization "Mathematical Methods for Information Security"
Course title: *Basics of building secure computer networks*
Basic part of Block 1, _4_credits
Instructor: *Gordeev S.I.*
At the beginning of the course a student should be able to:

• *ability to correctly apply the apparatus of mathematical analysis, geometry, algebra, discrete mathematics, mathematical logic, theory of algorithms, probability theory, mathematical statistics, information theory, number-theoretic methods (OPK-2) when solving professional problems;*

• *the ability to develop formal models of security policies, access control and information flow policies in computer systems, taking into account information security threats (OPK-9).*

Learning outcomes:

OPK-7 ability to take into account modern trends in the development of computer science and computer technology, computer technology in their professional activities, work with software tools for general and special purposes

OPK-8 ability to use programming languages and systems, tools for solving professional, research and applied tasks

PC-3 ability to analyze the security of computer systems for compliance with domestic and foreign standards in the field of computer security

Course description:

Discipline is basic for studying courses on telecommunication networks. Knowledge, skills and practical skills obtained as a result of studying the discipline "Basics of building secure computer networks" will allow students to base their professional activities on building, designing and operating software and hardware protection technologies for information transfer.

Main course literature:

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.— Режим доступа: http://www.iprbookshop.ru/52161.html

2. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс] : учебное пособие / А.М. Голиков. — Электрон. дан. — М.: ТУСУР, 2012. — 374 с. — Режим доступа: https://e.lanbook.com/book/11381

3. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс]: учебное пособие / М.А. Иванов, И.В. Чугунков. — Электрон. дан. — Москва : НИЯУ МИФИ, 2012. — 400 с. — Режим доступа: https://e.lanbook.com/book/75810

Form of final control: *exam*

Аннотация к рабочей программе дисциплины
«Основы построения защищенных компьютерных сетей»

Курс «Основы построения защищенных компьютерных сетей» предназначен студентам по направлению подготовки 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в базовую часть учебного плана Б1.Б.34.

Трудоёмкость дисциплины в зачетных единицах составляет 4 з.е., в академических часах – 144 часа (лекции – 36 часов, практическая работа – 36 часов, самостоятельная работа – 72 часа). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Основы построения защищенных компьютерных сетей» базируется на предварительном изучении следующих дисциплин: «Языки программирования», «Операционные системы», «Сети и системы передачи информации», «Основы информационной безопасности».

Дисциплина является базовой для изучения курсов по телекомуникационным сетям. Знания, умения и практические навыки, полученные в результате изучения дисциплины «Основы построения защищенных компьютерных сетей», позволят студентам основывать свою профессиональную деятельность на построении, проектировании и эксплуатации программно-аппаратных технологий защиты передачи информации.

Цель дисциплины: изучение методов и средств построения и эксплуатации беспроводных технологий для обеспечения информационной безопасности на объекте, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий защиты передачи информации в беспроводных коммуникациях.

Задачи:

- разработка проектов систем и подсистем защищенных компьютерных сетей в соответствии с техническим заданием;
- проведение инструментального мониторинга защищенности

объекта;

- поиск рациональных решений при разработке средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения;
- установка, настройка, эксплуатация и обслуживание аппаратно-программных средств защиты информации;
- обеспечение эффективного функционирования средств защиты информации с учетом требований по обеспечению защищенности компьютерной системы.

Для успешного изучения дисциплины «Основы построения защищенных компьютерных сетей» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);
- способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9).

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

Код и формулировка компетенции	**Этапы формирования компетенции**	
ОПК-7 способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с	Знает	Интернет-технологии для поиска информации.
	Умеет	Использовать пакеты прикладных программ для решения задач профессиональной деятельности.
	Владеет	Навыками работы с прикладными программами. Навыками анализа эффективности используемых прикладных программ.

программными средствами общего и специального назначения		
ОПК-8 способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Знает	Интернет-технологии для поиска информации.
	Умеет	Использовать пакеты прикладных программ для решения задач профессиональной деятельности.
	Владеет	Навыками работы с прикладными программами. Навыками анализа эффективности используемых прикладных программ.
ПК-3 способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знает	Методы сбора и анализа данных при проектировании системы защиты комьютерной сети.
	Умеет	Выявлять различные типы проблемных ситуаций.
	Владеет	Навыками анализа и составления отчетных документов.

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы построения защищенных компьютерных сетей» 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

Раздел I. Типовые угрозы сетевой безопасности (12 час.)

Тема 1. Сетевые атаки (4 час.)

Стадии проведения сетевой атаки. Классификации сетевых угроз, уязвимостей и атак. Атаки на реализации сетевых протоколов, отдельные узлы и службы. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI. Проблемы обеспечения конфиденциальности,

целостности и доступности информации на различных уровнях модели ISO/OSI.

Тема 2. Механизмы реализации атак в сетях (6 час.)

Удаленное определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP. Методы сканирования портов. Методы обнаружения пакетных сниферов. Методы обхода МЭ.

Тема 3. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак (2 час.)

Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации. Технические меры защиты от сетевых атак.

Раздел II. Криптографические методы защиты информации в компьютерных сетях (18 час.)

Тема 1. Криптографические протоколы обеспечения безопасности (6 час.)

Протоколы аутентификации на прикладном уровне. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.

Тема 2. Защита виртуальных частных сетей (4 час.)

Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IPSEC в туннельном и транспортном режимах. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей

Тема 3. Разработка защищенных сетевых приложений (8 час.)

Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. Программный интерфейс OpenSSL.

Раздел III. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях (6 час.)

Тема 1. Средства защиты локальных сетей при подключении к Интернет (4 час.)

Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности. Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ. Достоинства и недостатки МЭ. Построение правил фильтрации. Методы сетевой трансляции адресов (NAT). Шлюзы уровня

приложений. Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.

Тема 2. Защита серверов и рабочих станций (2 час.)

Средства и методы предотвращения и обнаружения вторжений. Системы обнаружения вторжений (СОВ). Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности. Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Способы противодействия вторжениям. Системы виртуальных ловушек (Honey Pot и Padded Cell)

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия. (36 часов)

Занятие 1. Модель OSI. (2 час.)

1. Физический, канальный, сетевой уровни
2. Транспортный, сеансовый, представительский, прикладной

Занятие 2. Сетевые протоколы. (4 час.)

1. FTP, telnet, HTTP, SSH, SMTP, IMAP, DNS
2. TCP, UDP, RIP
3. IPv4, IPv6
4. ARP, Ethernet, PPP, IEEE 802.22

Занятие 3. Классификация угроз (6 час.)

1. Характер угроз, цель атаки.
2. Пассивная и активная атаки.

Занятие 4. Способы аутентификации на различных уровнях OSI (4 час.)

1. SSL/TLS
2. IPSec
3. PGP

Занятие 5. Построение защищенной VPN (6 час.)

1. L2TP VPN
2. PPTP VPN
3. MPLS VPN

Занятие 6. Межсетевые экраны (6 час.)

1. Классификация межсетевых экранов

2. Принципы настройки межсетевых экранов
3. NAT
3. Существующие продукты на рынке

Занятие 7. СОВ (4 час.)

1. Виды СОВ
2. Существующие продукты на рынке

Занятие 8. Honeypot (4 час.)

1. Виды Honeypot
2. Honeypot в локальной сети

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Основы построения защищенных компьютерных сетей» 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. Типовые угрозы сетевой безопасности	ОПК-7, ОПК-8, ПК-3	знает	конспект (ПР-7)	1-7
			умеет	устный опрос (УО-1)	1-7
			владеет	устный опрос (УО-1)	1-7
2	Раздел II. Криптографические методы защиты информации в	ОПК-7, ОПК-8, ПК-3	знает	конспект (ПР-7)	8-10
			умеет	устный опрос (УО-1)	8-10
			владеет	устный опрос (УО-1)	8-10

	компьютерных сетях				
3	Раздел III. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях	ОПК-7, ОПК-8, ПК-3	знает	конспект (ПР-7)	11-19
			умеет	устный опрос (УО-1)	11-19
			владеет	устный опрос (УО-1)	11-19

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 ИНОФОМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.— Режим доступа: http://www.iprbookshop.ru/52161.html
2. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс] : учебное пособие / А.М. Голиков. — Электрон. дан. — М.: ТУСУР, 2012. — 374 с. — Режим доступа: https://e.lanbook.com/book/11381
3. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс]: учебное пособие / М.А. Иванов, И.В. Чугунков. — Электрон. дан. — Москва : НИЯУ МИФИ, 2012. — 400 с. — Режим доступа: https://e.lanbook.com/book/75810

Дополнительная литература

(печатные и электронные издания)

1. Чекмарев, Ю.В. Локальные вычислительные сети [Электронный ресурс] : учебное пособие / Ю.В. Чекмарев. — Электрон. дан. — М.: ДМК Пресс, 2010. — 200 с. — Режим доступа: https://e.lanbook.com/book/1147

2. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс]: учебное пособие / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов, Э.Р. Газизова ; под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 550 с. — Режим доступа: https://e.lanbook.com/book/5114
3. Агеев, Е.Ю. Основы компьютерных сетевых технологий [Электронный ресурс] / Е.Ю. Агеев. — Электрон. дан. — Москва : ТУСУР, 2011. — 83 с. — Режим доступа: https://e.lanbook.com/book/11484
4. Варлатая С.К., Шаханова М.В. Защита информационных процессов в компьютерных сетях : учебно-методический комплекс для вузов - Владивосток : Изд-во Дальневосточного технического университета, 2008. – 216 с. - http://lib.dvfu.ru:8080/lib/item?id=chamo:384163&theme=FEFU

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Национальная библиотека им. Н. Э. Баумана Bauman National Library [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://ru.bmstu.wiki/IP-%D1%81%D0%B5%D1%82%D0%B8_-_%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B82

2. Лекция 9: Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе TCP/IP [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.intuit.ru/studies/courses/2291/591/lecture/12691?page=2

3. Microsoft «Защита клиентских компьютеров от сетевых атак» [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://technet.microsoft.com/ru-ru/library/cc875823.aspx

Перечень информационных технологий и программного обеспечения

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

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Основы построения защищенных компьютерных сетей», составляет 72 академических часа. На самостоятельную работу отведено 72 часа (включая 27 часов на подготовку к экзамену). 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 экзамену соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к экзамену 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 D, ауд. D 734, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа,	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: "Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF

групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	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

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 построения защищенных компьютерных сетей»
Направление подготовки 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-18 неделя обучения	Подготовка практического задания (выполнение отчета к занятию)	45	Отчет о выполнении практического задания
2	Сессия	Подготовка и сдача экзамена	27	Экзамен

Рекомендации по самостоятельной работе студентов

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

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

Методические указания к выполнению отчета по занятию

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

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

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 построения защищенных компьютерных сетей»
Направление подготовки 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-7 способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Знает	Интернет-технологии для поиска информации.
	Умеет	Использовать пакеты прикладных программ для решения задач профессиональной деятельности.
	Владеет	Навыками работы с прикладными программами. Навыками анализа эффективности используемых прикладных программ.
ОПК-8 способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Знает	Интернет-технологии для поиска информации.
	Умеет	Использовать пакеты прикладных программ для решения задач профессиональной деятельности.
	Владеет	Навыками работы с прикладными программами. Навыками анализа эффективности используемых прикладных программ.
ПК-3 способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знает	Методы сбора и анализа данных при проектировании системы защиты комьютерной сети.
	Умеет	Выявлять различные типы проблемных ситуаций.
	Владеет	Навыками анализа и составления отчетных документов.

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Типовые угрозы сетевой безопасности	ОПК-7, ОПК-8, ПК-3	знает	конспект (ПР-7)	1-7
			умеет	устный опрос (УО-1)	1-7
			владеет	устный опрос (УО-1)	1-7
2	Раздел II. Криптографические методы защиты информации в компьютерных	ОПК-7, ОПК-8, ПК-3	знает	конспект (ПР-7)	8-10
			умеет	устный опрос (УО-1)	8-10
			владеет	устный опрос (УО-1)	8-10

	сетях				
3	Раздел III. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях	ОПК-7, ОПК-8, ПК-3	знает	конспект (ПР-7)	11-19
			умеет	устный опрос (УО-1)	11-19
			владеет	устный опрос (УО-1)	11-19

Список вопросов на экзамен

1. Модель OSI
2. Основные сетевые протоколы
3. Основные атаки на прикладном уровне
4. Отказ в обслуживании
5. Сетевые угрозы
6. Сниффер
7. DMZ и VPN
8. PGP
9. SSL
10. IPSec
11. Обнаружение вторжений
12. NAT
13. OpenSSL
14. Построение защищенной сети
15. Аудит прикладных служб
16. Honeypot
17. COB
18. Межсетевой экран

Критерии выставления оценки на экзамене

Оценка	Требования к сформированным компетенциям
«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении

	заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач по методологии научных исследований.
«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ
«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства для текущей аттестации

№ п/п	Код ОС	Наименование оценочного средства	Кроткая характеристика оценочного средства	Представление оценочного средства в фонде
1	ОУ-1	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определённому разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины

2	ОУ-2	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
4	ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины