




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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП


Добжинский Ю.В.
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности


Добжинский Ю.В.
(подпись) (Ф.И.О.)

« 15 » июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы построения защищенных компьютерных сетей
Направление подготовки 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.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 21 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 27 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрены
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: Добжинский Ю.В., к.т.н., с.н.с.
Составитель: Власов А.А.

**Владивосток
2019**

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от « ____ » _____ 20__ г. № _____

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

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от « ____ » _____ 20__ г. № _____

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

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от « ____ » _____ 20__ г. № _____

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

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от « ____ » _____ 20__ г. № _____

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

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

Данный курс учебной дисциплины предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.34.

Общая трудоемкость освоения дисциплины составляет 144 часа (4 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), практические занятия (36 час.), самостоятельная работа студентов (72 час., в том числе 27 часов на подготовку к экзамену). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина 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 телекоммуникационным 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 - 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 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 применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способностью использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);

- 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 и профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-7 способностью учитывать современные тенденции 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 компьютерной 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: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

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,	знает	ПР-7	1-7
			умеет	ОУ-1	1-7
			владеет	ОУ-2	1-7
2	Раздел II. Криптографические методы защиты информации в компьютерных сетях	ОПК-8	знает	ПР-7	8-10
			умеет	ОУ-1	8-10
			владеет	ОУ-2	8-10
3	Раздел III. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях	ПК-3	знает	ПР-7	11-19
			умеет	ОУ-1	11-19
			владеет	ОУ-2	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 ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — М.: ДМК Пресс, 2012. — 592 с. — Режим доступа: <https://e.lanbook.com/book/3032>
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 Vauman 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

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус Д, ауд. Д 818, 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.
---	---

	<p>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."</p> <p>6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.</p>
<p>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.</p>	<p>"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.</p> <p>2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно.</p> <p>3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно.</p> <p>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.</p> <p>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."</p> <p>6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.</p>

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 108 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 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 818, 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 – 38) Оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avergence CP355AF ЖК-панель 47", Full HD, LG M4716 CCBA Мультимедийный проектор
---	---

	<p>Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718", доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт</p>
<p>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.</p>	<p>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"</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 «Основы построения защищенных компьютерных сетей»
Направление подготовки 10.05.01 Компьютерная безопасность
(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)	45	УО-1
2	Сессия	Подготовка к экзамену	27	Экзамен

Подготовка отчета к практическому заданию предполагает повторение лекционного материала и выполнение практических заданий по темам из Раздела II РПУД. Подготовка обучающегося к занятию проверяется устным опросом на практическом занятии.

Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям



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
(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 компьютерной сети
	Умеет	выявлять различные типы проблемных ситуаций
	Владеет	навыками анализа и составления отчетных документов

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,	знает	ПР-7	1-7
			умеет	ОУ-1	1-7
			владеет	ОУ-2	1-7
2	Раздел II. Криптографическ	ОПК-8	знает	ПР-7	8-10
			умеет	ОУ-1	8-10

	ие методы защиты информации в компьютерных сетях		владеет	ОУ-2	8-10
3	Раздел III. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях	ПК-3	знает	ПР-7	11-19
			умеет	ОУ-1	11-19
			владеет	ОУ-2	11-19

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Каждый экзаменационный билет содержит два вопроса из списка ниже. Кроме того, для допуска к экзамену необходимо сдать все практические работы.

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. 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

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются устный опрос (УО-1) и конспект (ПР-7).

Конспект является показателем сформированности компетенции на пороговом уровне. Темы конспектов соответствуют темам теоретической части курса из Раздела I 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.

Для оценки продвинутого и высокого уровня сформированности компетенции проводятся устные опросы. Темы соответствуют темам практических занятий из Раздела II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Содержание ответа
Отлично	<p>Полные и точные ответы на все вопросы по теме занятия;</p> <p>Свободное владение основными терминами и понятиями курса;</p> <p>Последовательное и логичное изложение материала курса;</p> <p>Законченные выводы и обобщения по теме вопросов;</p> <p>Соблюдаются нормы литературной речи.</p>
Хорошо	<p>Полные и точные ответы на все вопросы по теме занятия;</p> <p>Знание основных терминов и понятий курса;</p> <p>Последовательное изложение материала курса;</p> <p>Умение формулировать некоторые обобщения по теме вопросов;</p> <p>Соблюдаются нормы литературной речи.</p>
Удовлетворительно	<p>Полные и точные ответы на часть вопросов;</p> <p>Удовлетворительное знание основных терминов и понятий курса;</p> <p>Удовлетворительное знание и владение методами и средствами решения поставленных задач;</p> <p>Недостаточно последовательное изложение материала курса;</p> <p>Умение формулировать отдельные выводы и обобщения по теме вопросов.</p>
Неудовлетворительно	<p>Полные и точные ответы на часть вопросов;</p> <p>Материал излагается непоследовательно, сбивчиво;</p>

	Имеются заметные нарушения норм литературной речи.
--	--

