Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ
филиал ФГБОУ ВО «РГГМУ» в г. Туапсе

Кафедра «Экономики и управления на предприятии природопользования»

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Основная профессиональная образовательная программа
высшего образования программы бакалавриата по направлению подготовки

09.03.03 «Прикладная информатика»

Направленность (профиль):
Прикладные информационные системы и технологии

Уровень:
Бакалавриат

Форма обучения
Очная/заочная

Год набора 2021

Согласовано
Руководитель ОПОП
«Прикладная информатика»
_____ Майборода Е.В.

Утверждаю
Директор филиала ФГБОУ
ВО «РГГМУ» в г. Туапсе_____ Олейников С.А.

Рассмотрена и утверждена на заседании кафедры
14 июня 2023 г., протокол № 9

Руководитель кафедры _____ Майборода Е.В.

Авторы-разработчики:

_____ Сафонова Т.В.
_____

Туапсе 2023

Рассмотрена и рекомендована к использованию в учебном процессе на 2023/2024 учебный год без изменений*

Протокол заседания кафедры №9 от 14 июня 2023 г

Рассмотрено и рекомендовано к использованию в учебном процессе на _____/_____ учебный год с изменениями (см. лист изменений)**

Протокол заседания кафедры _____ от __.__.20__ №__

*Заполняется при ежегодном пересмотре программы, если в неё не внесены изменения

** Заполняется при ежегодном пересмотре программы, если в неё внесены изменения

1. Цель и задачи освоения дисциплины

Цель дисциплины – изучение студентами основных угроз безопасности сети Интернет, методов обеспечения информационной безопасности, приобретение навыков применения средств защиты информации

Основные задачи дисциплины:

− изучить угрозы информационной безопасности.

− ознакомится с основными методами обеспечения информационной безопасности.

− изучить технологии обеспечения информационной безопасности в локальных и распределенных сетях.

− овладеть программным обеспечением для защиты информации.

− ознакомится с современными инструментами защиты информации в России и в мире

То есть, задачами дисциплины является изучение понятийного аппарата дисциплины, основных теоретических положений и методов, формирование умений и привитие навыков применения теоретических знаний для решения практических и прикладных задач.

2. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Информационная безопасность в интернете» относится к дисциплинам по выбору. Изучение дисциплины требует входных компетенций, знаний, умений и навыков, предусмотренных следующими курсами:

- Информатика и программирование
- Операционные и телекоммуникационные системы
- Информационные системы и технологии

Параллельно с дисциплиной «Информационная безопасность в интернете» изучается дисциплина «Моделирование и статистическая обработка экспериментальных данных»

3. Перечень планируемых результатов обучения

Процесс изучения дисциплины направлен на формирование компетенции ПК-5; ПК-6

Таблица 1

Профессиональные компетенции

Код и наименование профессиональной компетенции	**Код и наименование индикатора достижения профессиональной компетенции**	**Результаты обучения**
ПК-5. Способен разрабатывать техническое задание на основе выявленных и согласованных требований к системе и подсистеме	ПК-5.1. Применять стандарты оформления технических заданий ПК-5.2. Разрабатывать и описывать порядок работ по созданию и сдаче системы ПК-5.3. Представлять и защищать технического задания на систему ПК-5.4. Описывать объект, автоматизируемой системой, общих требований к системе	Знать: стандарты оформления технических заданий; порядок работ по созданию и сдаче системы Уметь: представлять и защищать техническое задание на систему; описывать общие требования к системе; Владеть: методологией проверки качества разработанных требований к системе и

		подсистеме; навыками разработки технического задания на систему
ПК-6. Способен выявлять риски на основе проведенного анализа требований к системе	ПК-6.1 Проверять качество разработанных требований к системе и подсистеме ПК-6.2 Анализировать возможные позитивные и негативные события, последствия и обстоятельства ПК-6.3 Применять основы теории управления рисками	Знать: методы обеспечения информационной безопасности Уметь: анализировать возможные позитивные и негативные события, последствия и обстоятельства Владеть: основами теории управления рисками

4. Структура и содержание дисциплины

Объем дисциплины составляет 8 зачетных единиц, 288 академических часа.

Таблица 2

Объем дисциплины по видам учебных занятий в академических часах

Объём дисциплины	**очная форма обучения**	**заочная форма обучения**
Объем дисциплины	**288**	**288**
Контактная работа обучающихся с преподавателем (по видам аудиторных учебных занятий) – всего:	**112**	**30**
в том числе:	**-**	**-**
лекции	**56**	**14**
практические занятия	**56**	**16**
Самостоятельная работа (далее – СРС) – всего:	**176**	**258**
Вид промежуточной аттестации	**зачет/экзамен**	**экзамен**

4.2. Структура дисциплины

Таблица 3

Структура дисциплины для очной формы обучения

№	**Тема дисциплины**	**Семестр**	**Виды учебной работы, в т.ч. самостоятельная работа студентов, час.**			**Формы текущего контроля успеваемости**	**Формируемые компетенции**	**Индикаторы достижения компетенций**
			лекции	практические	СРС			
1	Локальные и глобальные сети	7	1	2	22	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.4 ПК-6.1
2	Теоретические основы информационной безопасности	7	1	2	22	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.1 ПК-6.2

3	Угрозы информационной безопасности в сети Интернет	7	2	4	22	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.3 ПК-6.2
4	Основы криптографии	7	2	4	22	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.3 ПК-6.3
5	Методы и абстрактные модели защиты информации	8	2	4	22	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.2 ПК-6.1
6	Защита информации в IP-сетях	8	2	4	22	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.2 ПК-6.2
7	Классические и новые протоколы верхних уровней для работы с мультимедийным траффиком в сети Интернет	8	2	4	22	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.4 ПК-6.1
8	Анализ и управление рисками в сфере информационной безопасности	8	2	4	22	Конспектирование Реферат (презентация) Практическая работа Итоговый тест	ПК-5 ПК-6	ПК-5.1 ПК-6.3
	Итого	-	**14**	**28**	**176**			

Таблица 3.1

Структура дисциплины для заочной формы обучения

№	**Тема дисциплины**	**Курс**	**Виды учебной работы, в т.ч. самостоятельная работа студентов, час.**			**Формы текущего контроля успеваемости**	**Формируемые компетенции**	**Индикаторы достижения компетенций**
			лекции	практические	СРС			
1	Локальные и глобальные сети	5	1	1	33	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.4 ПК-6.1

2	Теоретические основы информационной безопасности	5	2	2	33	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.1 ПК-6.2
3	Угрозы информационной безопасности в сети Интернет	5	1	1	32	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.3 ПК-6.2
4	Основы криптографии	5	3	4	32	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.3 ПК-6.3
5	Методы и абстрактные модели защиты информации	5	2	2	32	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.2 ПК-6.1
6	Защита информации в IP-сетях	5	2	2	32	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.2 ПК-6.2
7	Классические и новые протоколы верхних уровней для работы с мультимедийным траффиком в сети Интернет	5	1	2	32	Конспектирование Реферат (презентация) Практическая работа	ПК-5 ПК-6	ПК-5.4 ПК-6.1
8	Анализ и управление рисками в сфере информационной безопасности	5	2	2	32	Конспектирование Реферат (презентация) Практическая работа Итоговый тест	ПК-5 ПК-6	ПК-5.1 ПК-6.3
	Итого	-	**14**	**16**	**258**			

4.3. Содержание разделов дисциплины

Раздел 1. Локальные и глобальные сети

− Применение компьютерных сетей;
− Сетевое оборудование и программное обеспечение;
− Эталонные модели;
− Примеры сетей;
− Стандартизация сетей;

Раздел 2. Теоретические основы информационной безопасности

− Общая схема процесса обеспечения безопасности;
− Идентификация, аутентификация, управление доступом;
− Защита от несанкционированного доступа;
− Модели безопасности;
− Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408.

Раздел 3. Угрозы информационной безопасности в сети Интернет

− Классификация угроз безопасности;
− Интерпретация угрозы атаки;
− Понятие надежности безопасности, параметры и характеристики безопасности;
− Классификация угроз уязвимостей и уровней защиты (защищенности);
− Объекты защиты и объекты моделирования;

Раздел 4. Основы криптографии

− Основные понятия;
− Исторические шифры;
− Симметричные шифры;
− Управление криптографическими ключами для симметричных шифров;
− Асимметричные шифры;
− Хеш-функции;
− Инфраструктура открытых ключей. Цифровые сертификаты;

Раздел 5. Методы и абстрактные модели защиты информации

− Абстрактные модели контроля доступа к защищенным режимам обработки информации;
− Модели и методы ролевого и сессионного контроля доступа. Вопросы идентификации ролей и сессий;
− Задачи построения системы защиты информации;
− Альтернативные методы защиты информации;

Раздел 6. Защита информации в IP-сетях

− Протокол защиты электронной почты S/MIME;
− Протоколы SSL и TLS;
− Протоколы IPSec и распределение ключей;
− Межсетевые экраны;

Раздел 7. Классические и новые протоколы верхних уровней для работы с мультимедийным траффиком в сети Интернет

− Мультимедийный трафик и его классификация;
− Интерактивные потоковые аудио и видео приложения;
− Классические протоколы транспортного уровня;
− Управление потоком и перегрузками в протоколе TCP;

Раздел 8. Анализ и управление рисками в сфере информационной безопасности

− Введение в проблему;
− Управление рисками. Модель безопасности с полным перекрытием;
− Управление информационной безопасностью. Стандарты ISO/IEC 17799.27002 и 27001;

− Методики построения систем защиты информации;
− Методики и программные продукты для оценки рисков;
− Выбор проекта системы обеспечения информационной безопасности. Игровая модель конфликта «защитник-нарушитель»

4.4. Содержание занятий семинарского типа

Таблица 4

Содержание практических занятий для очной формы обучения

№ темы дисциплины	Тематика практических занятий	Всего часов
1	Работа с сетевыми утилитами Работа с анализатором протоколов wireshark	2
2	Управление доступом к файлам на NTFS Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer	2
3	Использование сканеров безопасности для получения информации о хостах в сети Встроенный межсетевой экран Windows Server	4
4	Шифры замены. Потоковые шифры	4
5	Использование цифровых сертификатов Создание центра сертификации в Windows Server	4
6	Шифрование данных при хранении Настройка протокола IPSec в Windows Server	4
7	Использование Microsoft Security Assessment Tool Матричный подход к анализу рисков	4
8	Разработка политики информационной безопасности организации Анализ рисков на основе ПО «Риск Детектор»	4

Таблица 4.1

Содержание практических занятий для заочной формы обучения

№ темы дисциплины	Тематика практических занятий	Всего часов
1	Работа с сетевыми утилитами Работа с анализатором протоколов wireshark	1
2	Управление доступом к файлам на NTFS Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer	2
3	Использование сканеров безопасности для получения информации о хостах в сети Встроенный межсетевой экран Windows Server	1
4	Шифры замены. Потоковые шифры	4
5	Использование цифровых сертификатов Создание центра сертификации в Windows Server	2
6	Шифрование данных при хранении Настройка протокола IPSec в Windows Server	2
7	Использование Microsoft Security Assessment Tool Матричный подход к анализу рисков	2
8	Разработка политики информационной безопасности организации Анализ рисков на основе ПО «Риск Детектор»	2

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Методические материалы по дисциплине представлены в Методических рекомендациях для обучающихся по освоению дисциплины «Информационная безопасность в интернете».

6. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

Учет успеваемости обучающегося по дисциплине осуществляется по 100-балльной шкале. Максимальное количество баллов по дисциплине за один семестр – 100:

- максимальное количество баллов за выполнение всех видов текущего контроля -60;
- максимальное количество баллов за посещение лекционных занятий - 10;
- максимальное количество баллов за прохождение промежуточной аттестации - 30;
- максимальное количество дополнительных баллов - 15

6.1. Текущий контроль

Текущий контроль проводиться в форме доклада и выполнения практических работ.

Типовые задания, методика выполнения и критерии оценивания текущего контроля по разделам дисциплины представлены в Фонде оценочных средств по данной дисциплине.

6.2. Промежуточная аттестация

Форма промежуточной аттестации по дисциплине – зачет/экзамен.

Форма проведения экзамена: устно по вопросам

Перечень вопросов для подготовки к зачету:

ПК-5, ПК-6

1) Что такое информация.
2) Государственная тайна
3) Коммерческая тайна
4) Персональные данные
5) Понятие автоматизированная система
6) Информационная безопасность и ее составляющие
7) Защита информации
8) Методы обеспечения информационной безопасности
9) Классификация угроз информационной безопасности
10) Структура системы защиты от угроз нарушения конфиденциальности информации
11) Организационные меры обеспечения информационной безопасности
12) Идентификация и аутентификация
13) Методы хранения паролей
14) Дискреционная модель разграничения доступа
15) Мандатная модель разграничения доступа
16) Симметричные криптосистемы
17) Ассиметричные криптосистемы
18) Межсетевое экранирование
19) Модель iso/osi
20) Классы межсетевых экранов

Перечень вопросов для подготовки к экзамену:

1) Абстрактные модели контроля доступа к защищенным режимам обработки информации

2) Модели и методы ролевого и сессионного контроля доступа. Вопросы идентификации ролей и сессий
3) Задачи построения системы защиты информации
4) Альтернативные методы защиты информации
5) Системы обнаружения вторжений
6) Протоколирование и аудит
7) Требования к регистрационным журналам
8) Принципы обеспечения целостности
9) Цифровая подпись
10) Хэш-функция
11) Методы резервного копирования информации
12) Мультимедийный трафик и его классификация;
13) Интерактивные потоковые аудио и видео приложения;
14) Классические протоколы транспортного уровня;
15) Управление потоком и перегрузками в протоколе TCP;
16) Управление рисками. Модель безопасности с полным перекрытием
17) Управление информационной безопасностью. Стандарты ISO/IEC 17799.27002 и 27001
18) Методики построения систем защиты информации
19) Методики и программные продукты для оценки рисков
20) Выбор проекта системы обеспечения информационной безопасности
21) Игровая модель конфликта «защитник-нарушитель»

6.3. Балльно-рейтинговая система оценивания

Таблица 5

Распределение баллов по видам учебной работы

Вид учебной работы, за которую ставятся баллы	**Баллы**
Посещение лекционных занятий	0-10
Выполнение практических работ	0-35
Реферат (презентация)	0-10
Конспект	0-5
Итоговый тест	0-10
Промежуточная аттестация	0-30
ИТОГО	**0-100**

Таблица 6

Распределение дополнительных баллов

Дополнительные баллы (баллы, которые могут быть добавлены до 100)	**Баллы**
Участие в НИРС	0-13
Активность на учебных занятиях	0-2
ИТОГО	**0-15**

Минимальное количество баллов для допуска до промежуточной аттестации составляет 40 баллов при условии выполнения всех видов текущего контроля.

Таблица 7

Балльная шкала итоговой оценки на зачете

Оценка	**Баллы**
Зачтено	40-100
Незачтено	0-39

Таблица 8

Балльная шкала итоговой оценки на экзамене

Оценка	**Баллы**
Отлично	85-100
Хорошо	65-84
Удовлетворительно	40-64
Неудовлетворительно	0-39

7. Методические указания для обучающихся по освоению дисциплины

Методические рекомендации ко всем видам аудиторных занятий, а также методические рекомендации по организации самостоятельной работы, в том числе по подготовке к текущему контролю и промежуточной аттестации представлены в Методических рекомендации для обучающихся по освоению дисциплины «Информационная безопасность в интернете».

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1) Нестеров С.А. Информационная безопасность: учебник и практикум для академического бакалавриата. – М.: Издательство Юрайт, 2019.[Электронный ресурс] - Режим доступа: https://biblio-online.ru/book/informacionnaya-bezopasnost-434171

2) Запечников С.В., Казарин О.В. Криптографические методы защиты информации: учеб. Пособие для академического бакалавриата – М.: Издательство Юрайт, 2019. -309с. Электронный ресурс. Режим доступа: https://biblio-online.ru/book/kriptograficheskie-metody-zaschity-informacii-433133

Дополнительная литература

3) Бабенко Л.К., Ищукова Е.А. Криптографическая защита информации: симметричное шифрование: учеб. Пособие для вузов – М. Издательство Юрайт, 2019. – 220 с. Электронный ресурс. Режим доступа: https://biblio-online.ru/book/kriptograficheskaya-zaschita-informacii-simmetrichnoe-shifrovanie-437667

4) Лось А.Б., Нестеренко А.Ю., Рожков М. И.. Криптографические методы защиты информации для изучающих компьютерную безопасность.: учебник для академического бакалавриата – М.: Издательство Юрайт, 2019 – 473 с. [Электронный ресурс]— Режим доступа: https://biblio-online.ru/book/kriptograficheskie-metody-zaschity-informacii-dlya-izuchayuschih-kompyuternuyu-bezopasnost-447581

8.2. Перечень программного обеспечения

1. Операционная система Windows XP, Microsoft Office 2007
2. Программы электронных таблиц Excel
3. Текстовый редактор Word
4. Программа для создания презентаций Power Point
5. Программа распознавания текста FineReader

8.3. Перечень информационных справочных систем

1. Консультант Плюс.

8.4. Электронные библиотечные ресурсы:

1. Электронно-библиотечная система ГидроМетеоОнлайн- http://elib.rshu.ru/
2. Информация электронной библиотечной системы http://znanium.com/
3. Электронный каталог библиотеки РГГМУ http://lib.rshu.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=108
4. Издательство ЮРАИТ https://biblio-online.ru/

8.5. Перечень профессиональных баз данных

1. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/defaultx.asp
2. Федеральная государственная информационная система Национальная электронная библиотека (НЭБ). https://rusneb.ru/
3. Мультидисциплинарная реферативная и наукометрическая база данных Scopus компании Elsevier https://www.scopus.com/search/form.uri?display=basic#basic
4. Политематическая реферативно-библиографическая и наукометрическая (библиометрическая) база данных Web of Science компании Clarivate Analytics http://apps.webofknowledge.com/WOS_GeneralSearch_input.do?product=WOS&search_mode=GeneralSearch&SID=F4DWwm8nvkgneH3Gu7t&preferencesSaved=

9. Материально-техническое обеспечение дисциплины

Материально-техническое обеспечение программы соответствует действующим санитарно-техническим и противопожарным правилам и нормам и обеспечивает проведение всех видов лекционных, практических занятий и самостоятельной работы бакалавров.

Учебный процесс обеспечен аудиториями, комплектом лицензионного программного обеспечения, доступом к электронно-библиотечным системам.

Учебная аудитория для проведения занятий практического типа - укомплектована специализированной мебелью (ученические столы, стулья, компьютерные столы), компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi), доской меловой, мультимедиа проектором, аудиоколонками, учебно-наглядными пособиями, программным обеспечением.

Учебная аудитория для групповых и индивидуальных консультаций– укомплектована специализированной мебелью (ученические столы, стулья), доской меловой, компьютером с доступом в сеть Интернет, мультимедиа проектором, аудиоколонками, учебно-наглядными пособиями.

Учебная аудитория для текущего контроля и промежуточной аттестации– укомплектована специализированной мебелью (ученические столы, стулья), доской меловой, компьютером с доступом в сеть Интернет, мультимедиа проектором, аудиоколонками, учебно-наглядными пособиями.

Помещение для самостоятельной работы укомплектовано специализированной мебелью (ученические столы, стулья, компьютерные столы), компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi), доской меловой, мультимедиа проектором, аудиоколонками, учебно-наглядными пособиями, программным обеспечением.

10. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом

учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

11. Возможность применения электронного обучения и дистанционных образовательных технологий

Дисциплина может реализовываться с применением электронного обучения и дистанционных образовательных технологий