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 «Метеорологии, экологии и экономического обеспечения деятельности предприятий природопользования»

Рабочая программа по дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Основная профессиональная образовательная программа
высшего образования программы бакалавриата по направлению подготовки

09.03.03 «Прикладная информатика»

Направленность (профиль):
Прикладная геоинформатика

Квалификация:
Бакалавр

Форма обучения
Заочная

Год поступления 2018-2016

Согласовано
Руководитель ОПОИ
«Прикладная информатика»

_____ **Аракелов М.С.**

Утверждаю
Директор филиала ФГБОУ ВО «РГГМУ» в г. Туапсе _____ **Аракелов М.С.**

Рассмотрена и утверждена на заседании кафедры 31 августа 2020 г., протокол № 1

Зав. кафедрой _____ **Цай С.Н.**

Авторы-разработчики:

_____ **Богданов П.Ю.**

_____

Туапсе 2020

Заочное отделение

Курс	Всего по ФГОС Час/ ЗЕТ	Аудиторных Час	Лек-ций, Час	Практич. занятий, Час	Лаборат. работ, Час	СРС/ контроль Час	Форма промежуточной аттестации (экз./зачет)
3	252/7	20	8	-	12	223/9	экзамен
Итого	252/7	20	8	-	12	223/9	экзамен

Аннотация рабочей программы представлена в приложении 1.

1. Цели и задачи учебной дисциплины, ее место в учебном процессе

1.1. Цели и задачи изучения дисциплины

Цель курса – изучить теоретические основы информационной безопасности (ИБ) и методологические нормы системного обеспечения защиты информационных процессов в компьютерных системах.

Теория определяется как совокупность основных идей и общих принципов, объединенных в единую систему и обобщенно раскрывающих ту или другую область действительности.

Применительно к ИБ теорию следует рассматривать как систему основных идей и положений, общих принципов, необходимых для раскрытия сущности и значения ИБ и выработки методологии защиты информации (ЗИ) в компьютерных системах.

Методология ЗИ в компьютерных системах - это учение о структуре, логической организации системы ЗИ, видах, методах и средствах деятельности по обеспечению безопасности защищаемой информации в компьютерных системах.

Задачи курса:

1. Раскрытие понятийного аппарата в области ИБ и ЗИ в компьютерных системах.
2. Раскрытие содержательных базовых положений.
3. Раскрытие современной доктрины ИБ.
4. Определение целей и принципов ЗИ в компьютерных системах.
5. Установление факторов, влияющих на ЗИ.
6. Установление угроз информации в компьютерных системах.
7. Раскрытие направлений, видов, методов и особенностей деятельности злоумышленников в компьютерной сети и при наличии изолированного компьютера.
8. Раскрытие назначения, сущности и структуры системы ЗИ в компьютерных системах, системных вопросов защиты программ и данных.
9. Определение требований к программной и программно-аппаратной реализации средств ЗИ в компьютерных системах и к защите АСУ от несанкционированного доступа (НСД).

1.2. Краткая характеристика дисциплины

Курс Информационная безопасность обеспечивает преемственность и гармонизацию изучения информационных технологий. Полученные студентами знания, позволят более глубоко изучить смежные профилирующие дисциплины по специальности «Прикладная информатика»

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

2.1. Требования к уровню освоения дисциплины

В результате обучения по дисциплине (модулю) *студент должен:*

Знать:

- назначение и виды ИКТ;

- технологии сбора, накопления, обработки, передачи и распространения информации;
- виды угроз ИС и методы обеспечения информационной безопасности;

Уметь:

- выявлять угрозы информационной безопасности;
- обосновывать организационно-технические мероприятия по защите информации в ИС;

Владеть навыками:

- разработки технологической документации;
- использования функциональных и технологических стандартов ИС;
- работы с инструментальными средствами защиты информации

В процессе освоения данной дисциплины студент формирует и демонстрирует следующие общекультурные, общепрофессиональные и профессиональные компетенции при освоении ОПОП ВО, реализующей ФГОС ВО:

общекультурные

ОК-4 - способностью использовать основы правовых знаний в различных сферах деятельности

ОК-7 - способностью к самоорганизации и самообразованию

общепрофессиональные

ОПК-1 - способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий

профессиональные

ПК-6 - способностью собирать детальную информацию для формализации требований пользователей заказчика

ПК-9 - способностью составлять техническую документацию проектов автоматизации и информатизации прикладных процессов

ПК-18 - способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью

ПК-20 - способностью осуществлять и обосновывать выбор проектных решений по видам обеспечения информационных систем

ПК-22 - способностью анализировать рынок программно-технических средств, информационных продуктов и услуг для создания и модификации информационных систем

2.2. Место дисциплины в структуре ОПОП ВО

Дисциплина Информационная безопасность относится к базовым дисциплинам блока 1 учебного плана ОПОП ВО по направлению подготовки 09.03.03 «Прикладная информатика»

Необходимыми условиями для освоения дисциплины являются:

знание

- основных теоретических положений информатики,
- методов составления программ;
- физических основ компьютерной техники и средств передачи информации;
- принципов работы технических устройств ИКТ;
- основы архитектуры и процессов функционирования вычислительных систем, сетей и телекоммуникаций;
- теоретические основы построения и функционирования операционных систем, их назначение и функции;

- сетевые протоколы;

умения

- работать на компьютере и в сети Интернет;
- использовать прикладное программное обеспечение;
- разрабатывать программные коды на одном из языков высокого уровня;
- оценивать архитектуру вычислительных систем, сетей и систем телекоммуникаций и их подсистем;
- использовать различные операционные системы;

владение

- навыками работы в современной программно-технической среде в различных операционных системах.

Содержание дисциплины является логическим продолжением содержания дисциплин Информатика и программирование, Операционные и телекоммуникационные системы и служит основой для освоения дисциплин Распределенные вычисления и приложения, Производственная практика.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет _7_ зачетных единицы; _252_ часа. Контактная работа составляет _20_ часов, в том числе: 8 часов - лекции, 12 часов-лабораторные работы, на самостоятельную работу обучающихся _223_ часа, контроль – 9 часов.

Заочное отделение

№ модуля образовательной программы	№ раздела, темы	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
			Лекции	Практические занятия	Лабораторные работы	СРС	Всего часов
	1	Основные понятия и положения защиты информации	1	-	0	14	15
	2	Методы и средства защиты информации в компьютерных системах	3,5	-	6	94	103,5
	3	Построение и организация функционирования комплексных систем защиты информации в компьютерных системах	0,5	-	2	44	46,5
	4	Криптографические методы защиты информации	3	-	4	28	35
		Подготовка к экзамену		-		43	43
		Контроль		-			9
ИТОГО:			**8**	**-**	**12**	**223**	**252**

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1.Теоретический курс *(ОК-4; ОК-7; ОПК-1; ПК-6; ПК-9; ПК-18; ПК-20; ПК-22)*

Заочное отделение

№ п/п	Номер раздела дисциплины	Объем часов		Раздел, тема учебной дисциплины, содержание темы
		Лекции	СРС	
1	Раздел 1	0,5	4	**Предмет и объект защиты** Предмет защиты, объект защиты информации.
2		0,5	4	**Угрозы безопасности информации в компьютерных системах** Случайные угрозы. Преднамеренные угрозы.
3		0	6	**Правовые и организационные методы защиты информации в КС** Правовое регулирование в области безопасности информации. Общая характеристика организационных методов защиты информации в КС.
4	Раздел 2	1	4	**Защита информации в КС от случайных угроз** Дублирование информации. Повышение надежности КС. Создание отказоустойчивых КС. Блокировка ошибочных операций. Оптимизация взаимодействия пользователей и обслуживающего персонала с КС Минимизация ущерба от аварий и стихийных бедствий.
5		0	8	**Методы и средства защиты информации в КС от традиционного шпионажа и диверсий** Система охраны объекта КС. Организация работ с конфиденциальными информационными ресурсами на объектах КС. Противодействие наблюдению в оптическом диапазоне. Противодействие прослушиванию. Средства борьбы с закладными подслушивающими устройствами. Защита от злоумышленных действий обслуживающего персонала и пользователей.
6		0	8	**Методы защиты от несанкционированного изменения структур КС** Общие требования к защищенности КС от несанкционированного изменения структур. Защита от закладок при разработке программ. Защита от внедрения аппаратных закладок на этапе разработки и производства. Защита от несанкционированного изменения структур КС в процессе эксплуатации.
7		1	4	**Защита информации в КС от несанкционированного доступа** Система разграничения доступа к информации в

				КС. Система защиты программных средств от копирования и исследования.
8		1	4	**Компьютерные вирусы и механизмы борьбы с ними** Классификация компьютерных вирусов. Файловые вирусы. Загрузочные вирусы. Вирусы и операционные системы. Методы и средства борьбы с вирусами. Профилактика заражения вирусами компьютерных систем.
9		0,5	4	**Защита информации в распределенных КС** Архитектура распределенных КС. Особенности защиты информации в РКС. Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных КС. Защита информации на уровне подсистемы управления РКС. Защита информации в каналах связи. Подтверждение подлинности информации, получаемой по коммуникационной подсети. Особенности защиты информации в БД.
10	Раздел 3	0,5	4	**Построение комплексных систем защиты информации (КСЗИ).** Концепция создания защищенных КС. Этапы создания комплексной системы защиты информации. Моделирование КСЗИ. Выбор показателей эффективности и критериев оптимальности КСЗИ. Математическая постановка задачи разработки КСЗИ. Подходы к оценке эффективности КСЗИ. Создание организационной структуры КСЗИ.
11		0	4	**Организация функционирования комплексных систем защиты информации** Применение КСЗИ по назначению. Техническая эксплуатация КСЗИ.
12	Раздел 4	1	4	**Криптографические методы защиты информации** Классификация методов криптографического преобразования информации. Шифрование. Основные понятия. Стандарты шифрования.
13		1	4	**Простейшие методы шифрования с закрытым ключом.** Общая схема симметричного шифрования. Методы замены. Пропорциональные шифры. Многоалфавитные подставки. Методы гаммирования. Методы перестановки.
14		1	4	**Принципы построения блочных шифров с закрытым ключом.** Понятие композиционного шифра. Операции используемые в блочных алгоритмах симметричного шифрования. Структура блочного алгоритма симметричного шифрования. Требования к блочному алгоритму шифрования.

				Сеть Фейштеля.
15		0	12	**Алгоритмы шифрования DES и AES** Основные сведения. Шифрование. Расшифрование. Двухкратные DES и атака «встреча посередине». Трехкратный DES. Алгоритм AES. Режимы работы блочных алгоритмов.
Итого:		**8**	**78**	

4.2. Практические занятия

Практические работы учебным планом не предусмотрены

4.3. Лабораторные работы *(ОК-4; ОК-7; ОПК-1; ПК-6; ПК-9; ПК-18; ПК-20; ПК-22)*

Заочное отделение

№ п/п	Номер раздела дисциплины	Наименование лабораторной работы	Формы контроля выполнения работы	Объем часов	
				Аудиторных	СРС
4	Раздел 2	Разграничения доступа к информации в КС.	Отчет, защита лабораторной	2	4
6		Протоколы коммутируемых соединений PAP, CHAP, RADIUS, DIAMETER, IPSec	Самотестирование	0	10
7		Аутентификация пользователей в сетях. Система Kerberos	Самотестирование	0	10
8		Протоколы TCP/IзP. Атаки.	Отчет, защита лабораторной	2	4
9		Безопасность в глобальных сетях	Самотестирование	0	10
10		Классификация брандмауэров	Самотестирование	0	10
11		Средства ОС Microsoft Windows XP по обеспечению компьютерной безопасности при работе с Интернетом	Отчет, защита лабораторной	2	4
12		Профилактика заражения вирусами компьютерных систем.	Самотестирование	0	10
13	Раздел 3	Выбор показателей эффективности и критериев оптимальности КСЗИ.	Самотестирование	0	10
16		Определение оценки вероятности реализации угроз	Самотестирование	0	10
17		Обеспечение безопасности информационного объекта	Самотестирование	0	10
18		Оценка рисков информационной безопасности. Microsoft Assessment Tool	Отчет, защита лабораторной	2	6
19	Раздел 4	Простейшие методы шифрования	Отчет, защита лабораторной	2	2
20		Методы замены. Пропорциональные шифры.	Отчет, защита лабораторной	2	2
			Итого:	**12**	**102**

4.4. Курсовые работы по дисциплине

Курсовые работы (проекты) учебным планом не предусмотрены.

4.5. Самостоятельная работа студента *(ОК-4; ОК-7; ОПК-1; ПК-6; ПК-9; ПК-18; ПК-20; ПК-22)*

Раздел дисциплины	№ п/п	Вид СРС	Формы контроля	Трудоемкость, часов
Раздел 1		Проработка учебного материала	Самотестирование	14
Раздел 2		Проработка учебного материала	Самотестирование	32
		Подготовка к выполнению и сдаче лабораторных работ	Лабораторная работа	32
		Подготовка к тестированию	Тест	30
Раздел 3		Проработка учебного материала	Самотестирование	8
		Подготовка к выполнению и сдаче лабораторных работ	Лабораторная работа	18
		Подготовка к тестированию	Тест	18
Раздел 4		Проработка учебного материала	Самотестирование	24
		Подготовка к выполнению и сдаче лабораторных работ	Лабораторная работа	4
		Подготовка к экзамену	Экзамен	43
			Итого:	**223**
			Контроль	**9**

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Методические рекомендации по организации самостоятельной работы студентов включают:

- Методические рекомендации по написанию реферата
- Методические рекомендации по подготовке к тестам
- Методические рекомендации по подготовке к лабораторным работам
- Методические рекомендации по подготовке к экзамену

4.6. Рефераты *(ОК-4; ОК-7; ОПК-1; ПК-6; ПК-9; ПК-18; ПК-20; ПК-22)*

1. Алгоритм AES
2. Алгоритм Anubis
3. Алгоритм Blowfish
4. Алгоритм Camellia
5. Алгоритм Crypton
6. Алгоритм Feal
7. Алгоритм Frog
8. Алгоритм Grand Cru
9. Алгоритм Ice
10. Алгоритм Kasumi
11. Алгоритм Speed
12. Алгоритм Twofish

5. Образовательные технологии

Для обеспечения успешного освоения курса применяются следующие виды организации учебного процесса:

1. **Лекция** (Лк) – передача учебной информации от преподавателя к студентам, как правило с использованием компьютерных и технических средств, направленная в основном на приобретение студентами новых теоретических и фактических знаний.
2. **Лабораторная работа** (Лб. раб.)- практическая работа студента под руководством преподавателя, связанная с использованием учебного, научного или производственного оборудования (приборов, устройств и др.) с физическим моделированием и проведением экспериментов, направленная в основном на приобретение новых фактических знаний и практических умений.
3. **Самостоятельная работа** – (СР) – изучение студентами теоретического материала, подготовка к лекциям, лабораторным работам, практическим и семинарским занятиям, оформление конспектов лекций, написание рефератов, отчетов, курсовых работ, проектов, работа в электронной образовательной среде и др. для приобретения новых теоретических и фактических знаний, теоретических и практических умений.
4. **Консультация** (Конс.)_ - индивидуальное общение преподавателя со студентом, руководство его деятельностью с целью передачи опыта, углубления теоретических и фактических знаний, приобретенных студентом на лекциях, в результате самостоятельной работы, в процессе выполнения курсового проектирования и др.

Основные виды образовательных технологий

1. **Информационные технологии** – обучение в электронной образовательной среде с целью расширения доступа к образовательным ресурсам (теоретически к неограниченному объему и скорости доступа), увеличения контактного взаимодействия с преподавателем, построения индивидуальных траекторий подготовки и объективного контроля и мониторинга знаний студентов.
2. **Работа в команде** – совместная деятельность студентов в группе под руководством лидера, направленная на решение общей задачи путем творческого сложения результатов индивидуальной работы членов команды с делением полномочий и ответственности.
3. **Case-study** - анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений.
4. **Проблемное обучение** – стимулирование студентов к самостоятельному приобретению знаний, необходимых для решения конкретной проблемы.
5. **Междисциплинарное обучение** – использование знаний из разных областей, их группировка и концентрация в контексте решаемой задачи.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы (представлен в матрице компетенций ниже)

Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых в них общепрофессиональных, профессиональных и общекультурных компетенций как механизм выбора образовательных технологий и оценочных средств

Темы, разделы дисциплины	К-во часов	Компетенции								Общее кол-во компетенций	$t_{ср}$
	Л/ЛР/СРС	ОК-4	ОК-7	ОПК-1	ПК-6	ПК-9	ПК-18	ПК-20	ПК-22		
Раздел 1. Основные понятия и положения защиты информации	**1/-/14**										
Тема 1. Предмет и объект защиты	0,5/-/4		+				+	+		3	1,5
Тема 2. Угрозы безопасности информации в компьютерных системах	0,5/-/4		+		+		+	+		4	1,125
Тема 3. Правовые и организационные методы защиты информации в КС	-/-/6	+	+	+				+		4	1,5
Раздел 2. Методы и средства защиты информации в компьютерных системах	**3,5/6/94**										
Тема 1. Защита информации в КС от случайных угроз	1/2/8		+		+		+	+	+	5	2,2
Тема 2. Методы и средства защиты информации в КС от традиционного шпионажа и диверсий	-/-/18		+				+	+	+	4	4,5
Тема 3. Методы защиты от несанкционированного изменения структур КС	-/-/18		+				+	+	+	4	4,5
Тема 4. Защита информации в КС от несанкционированного доступа	1/2/18		+				+	+	+	4	5,25
Тема 5. Компьютерные вирусы и механизмы борьбы с ними	1/-/14		+				+	+	+	4	3,75

Тема 6. Защита информации в распределенных КС	0,5/2/18	+	+	+	+	+	+	+	+	4	5,125
Раздел 3. Построение и организация функционирования комплексных систем защиты информации в компьютерных системах	**0,5/2/44**										
Тема 1. Построение комплексных систем защиты информации (КСЗИ).	0,5/-/18		+	+	+	+	+	+	+	7	2,64
Тема 2. Организация функционирования комплексных систем защиты информации	-/2/18		+		+	+	+	+	+	6	2,33
Раздел 4. Криптографические методы защиты информации	**3/4/28**										
Тема 1. Криптографические методы защиты информации	1/2/6		+	+			+	+	+	5	1,4
Тема 2. Простейшие методы шифрования с закрытым ключом.	-/2/14		+				+	+	+	4	4
Тема 3. Принципы построения блочных шифров с закрытым ключом.	-/-/4		+				+	+	+	4	1
Тема 4. Алгоритмы шифрования DES и AES	-/-/4		+				+	+	+	4	1
Подготовка к экзамену	-/-/-43	+	+	+	+	+	+	+	+	8	5,375
Контроль	**-/-/-/-9**	+	+	+	+	+	+	+	+	8	1,125
Итого	**8/12/223/9**	2	16	4	5	3	15	16	13		
Трудоемкость формирования компетенций	**8/12/223/9**	**13,125**	**48,32**	**17,165**	**19,92**	**14,265**	**46,82**	**48,32**	**44,195**		**252**

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Текущий контроль студентов производится в дискретные временные интервалы лектором и преподавателем (ями), ведущими лабораторные работы и практические занятия по дисциплине в следующих формах:

- выполнение лабораторных работ;
- защита лабораторных работ (тестирование);

- отдельно оцениваются личностные качества студента (аккуратность, исполнительность, инициативность) – работа у доски, своевременная сдача тестов, отчетов к лабораторным работам и письменных домашних заданий.

Промежуточная аттестация по результатам семестрам по дисциплине проходит в форме экзамена (включает в себя ответ на теоретические вопросы и решение задач)

Контроль и оценка результатов обучения (в соответствии с Положением о балльно-рейтинговой оценке образовательных достижений обучающихся (БРС))

Показатели	Кол-во часов	Кол-во тестов, к/р	Баллы	ИТОГО
Входной рейтинг		-	-	-
Посещение в т.ч. лекции практические занятия лабораторные занятия	20 8 12		 3	 36
Тесты по модулям		2	10	20
Коллоквиумы		2	10	20
Практические работы		1	14	14
Итоговый тест		1	10	10
СРС	223			
ИТОГО	252			100

Критерии оценки уровня сформированности компетенций

Показатели	61-72 % «удовлетворительно»	73-85% «хорошо»	86-100% «отлично»

6.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные контрольные вопросы и задания для текущего контроля

Примерные тесты *(ОК-4, ОК-7, ОПК-1, ПК-6, ПК-9, ПК-18, ПК-20, ПК-22)*

1. **Какую цель преследуют хакеры – дилетанты:**
   a) добиться доступа к системе, чтобы выяснить ее назначение;
   b) модифицировать или стереть данные, а также оставить преднамеренный след, например, в виде непристойной записки;
   c) совершенствуют систему безопасности предприятия

2. **Что относится к техническим средствам НСД:**
   a) телефонные автонабиратели;
   b) логические бомбы;
   c) экранный имитатор;
   d) получение паролей.

3. **Пассивный перехват сообщений в ЛВС включает:**
   a) чтение информации;
   b) дублирование;
   c) удаление или неправомочное использование реквизитов;

d) анализ трафика (использование адресов, других данных заголовка, длины и частоты сообщений).

4. Что означает термин ИДЕНТИФИКАЦИЯ?

a) Это присвоение имени субъекту или объекту.
b) Это проверка подлинности субъекта или объекта.
c) Это проверка целостности информации, программы, документа и т.д.

5. Какие угрозы информации относятся к случайным?

a) проявление ошибок программно-аппаратных средств АС; некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности; неправомерное включение оборудования или изменение режимов работы устройств и программ; неумышленная порча носителей информации; пересылка данных по ошибочному адресу абонента (устройства).
b) несанкционированное чтение информации; несанкционированное изменение информации; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.
c) пересылка данных по ошибочному адресу абонента (устройства); ввод ошибочных данных; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.

6. Источником каких угроз информации являются санкционированные программно-аппаратные средства?

a) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.); возникновение отказа в работе операционной системы.
b) стихийные бедствия; магнитные бури; радиоактивное излучение.
c) внедрение агентов в число персонала системы; вербовка персонала или отдельных пользователей, имеющих определенные полномочия; угроза несанкционированного копирования секретных данных пользователем; разглашение, передача или утрата атрибутов разграничения доступа.
d) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях); заражение компьютера вирусами с деструктивными функциями.

7. Какими основными свойствами обладает компьютерный вирус?

e) способностью к созданию собственных копий; наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.
f) способностью к созданию собственных копий; способностью уничтожать информацию на дисках; способность создавать всевозможные видео и звуковые эффекты.
g) наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы; способностью оставлять в оперативной памяти свою резидентную часть; способностью вируса полностью или частично скрыть себя в системе.

8. На чем основан алгоритм работы резидентного вируса?

a) Вирус при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.

b) Использование этих алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов и затем вирусы либо временно лечат их, либо подставляют вместо себя незараженные участки информации.
c) Используются для того, чтобы максимально усложнить процедуру обнаружения вируса. Эти вирусы достаточно трудно поддаются обнаружению, они не имеют сигнатур, т.е. не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного и того же вируса не будут иметь ни одного совпадения.

9. На чем основан алгоритм работы вируса с использованием самошифрования и полиморфичности?

a) Используются для того, чтобы максимально усложнить процедуру обнаружения вируса. Эти вирусы достаточно трудно поддаются обнаружению, они не имеют сигнатур, т.е. не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного и того же вируса не будут иметь ни одного совпадения.
b) Вирус при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.
c) Использование этих алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов, затем вирусы либо временно лечат их, либо подставляют вместо себя незараженные участки информации.

10. В чем заключается метод защиты информации - разделение доступа (привилегий)?

a) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
b) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.
c) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.
d) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.
e) В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

Перечень вопросов к экзамену *(ОК-4, ОК-7, ОПК-1, ПК-6, ПК-9, ПК-18, ПК-20, ПК-22)*

1) Сущность и понятие информационной безопасности (ИБ);
2) Определение атак на уровне приложений и типа Man–in–the–Middle и характеристика основных средств защиты от них;
3) Биометрические средства идентификации и аутентификации пользователей.
4) Характеристика основных составляющих ИБ;
5) Основные методы и условия неавторизованного доступа к ЛВС;
6) Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.

7) Значение ИБ для субъектов информационных отношений;
8) Краткая характеристика основных условий НСД к ЛВС;
9) Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
10) Место ИБ в системе национальной безопасности;
11) Краткая характеристика основных условий раскрытия и подмены трафика ЛВС;
12) Принцип работы простейших алгоритмов с закрытым ключом. Примеры Основные принципы обеспечения ИБ;
13) Определение атак типа DoS («отказ в обслуживании») и характеристика основных средств защиты от них;
14) Принцип работы простейших алгоритмов с закрытым ключом. Примеры
15) Классификация угроз ИБ;
16) Требования к средствам управления ИБ;
17) Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
18) Состав и краткая характеристика внутренних и внешних источников угроз ИБ;
19) Общий состав требований к межсетевому экрану;
20) Место информационной безопасности экономических систем в национальной безопасности страны.
21) Концепция информационной безопасности.
22) Состав и краткая характеристика основных угроз доступности;
23) Способы защиты информации в КС от случайных угроз
24) Причины нарушения безопасности информации при ее обработке криптографическими средствами.
25) Состав и краткая характеристика основных угроз целостности;
26) Повышение надежности КС
27) Понятие атаки на систему информационной безопасности.
28) Особенности локальных атак.
29) Состав и краткая характеристика основных угроз конфиденциальности;
30) Средства защиты информации от традиционного шпионажа
31) Распределенные информационные системы.
32) Удаленные атаки на информационную

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Критерии оценки знаний студентов на экзамене

Оценки **«отлично»** заслуживает студент, *за реализацию всех необходимых компетенций* при ответах на вопросы экзаменационного билета: студент показал всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка «отлично» выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала. Правильно решена задача. Соблюдаются нормы литературной и профессиональной речи, *подтвердив своими ответами сформированность компетенций, предусмотренных ФГОС (высокий уровень).*

Оценки **«хорошо»** заслуживает студент обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания,

усвоивший основную литературу, рекомендованную в программе. Как правило, оценка «хорошо» выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности. Задача решена с несущественными ошибками в расчетах. Студент *подтвердил своими ответами сформированность компетенций, предусмотренных ФГОС, на достаточном уровне.*

Оценка «удовлетворительно». Допускаются нарушения в последовательности изложения. Имеются упоминания об отдельных базовых нормативно-правовых актах. Неполно раскрываются причинно-следственные связи между государственными, политическими и экономическими явлениями и событиями. Демонстрируются поверхностные знания вопроса, а имеющиеся практические навыки с трудом позволяют решать конкретные задачи с существенными ошибками в расчетах. Имеются затруднения с выводами. Допускаются нарушения норм литературной и профессиональной речи, демонстрируя тем самым *частичную (на среднем уровне) сформированность компетенций, предусмотренных ФГОС.*

Оценка «неудовлетворительно». Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по программному материалу. Не раскрываются причинно-следственные связи между государственными, политическими и экономическими явлениями и событиями. Задача решена не верно. Имеются заметные нарушения норм литературной и профессиональной речи, непонимание сущности излагаемых вопросов; неуверенные и неточные ответы на дополнительные вопросы, что *демонстрирует несформированность (низкий уровень) у выпускника соответствующих компетенций, предусмотренных ФГОС.*

Методические указания для обучающихся по освоению дисциплины (модуля)

По дисциплине «Информационная безопасность» рабочим учебным планом предусмотрены следующие виды учебных занятий: лекции, лабораторные работы, самостоятельная работа студентов.

Формы работы со студентами: опросы и тестирование в ходе лекционных и лабораторных занятий.

Лабораторные работы являются логическим продолжением изучения той или иной темы дисциплины. Поэтому при подготовке к ним важно повторить теоретический материал по теме занятия, используя материалы лекций, рекомендуемые учебники и учебные пособия. Без такой целенаправленной самостоятельной работы студентам затруднительно выполнять лабораторные работы.

Непременным условием успешной учебной деятельности студентов является не только активная работа в аудитории, но и целенаправленная **самостоятельная работа**, предусмотренная учебным планом. Она призвана способствовать более глубокому усвоению изучаемой дисциплины, формировать навыки информационно-эвристической и аналитической работы, а также ориентировать студентов на умение применять теоретические знания на практике. В ходе самостоятельной работы студентам важно выработать навыки самостоятельного поиска источников информации, умелого их использования при доработке конспектов лекций, подготовке к лабораторным работам и постепенно перейти от деятельности, выполняемой под руководством преподавателя, к деятельности, организуемой самостоятельно, к полной замене контроля со стороны преподавателя самоконтролем.

Самостоятельная работа студентов должна носить систематический характер.

Проработка учебного материала после проведенных лекционных занятий осуществляется по конспектам лекций с привлечением учебной и научной литературы, нормативных документов в соответствии со списком рекомендованной литературы к каждой изучаемой теме.

Первый шаг в самостоятельной работе студентов: после лекционного занятия в этот же день изучить конспект лекции и осмыслить прочитанное, выделить места,

вызывающие дополнительные вопросы. Затем, обратившись к перечню рекомендованной, основной и дополнительной литературы по данной теме, дополнить конспект лекции, сделать необходимые выписки из нормативных документов; с помощью опорных конспектов разобраться в примерах, приведенных в учебниках. В результате такой работы должно сложиться понимание основных вопросов темы.

На лабораторных работах, происходит углубление и расширение знаний, полученных на лекциях и в процессе самостоятельной работы, выясняются и все неясные вопросы. Самостоятельная работа не ограничивается только подготовкой к лабораторным работам. Она может продолжаться и их проведения. В этом случае она нацелена на более глубокое освоение учебной дисциплины «Информационная безопасность» сверх учебной программы.

7.Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

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

7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (Сайты)

Интернет-ресурсы:

1. http://econavt.ru
2. https://ohranatruda.ru
3. http://www.gosnadzor.ru
4. http://rospotrebnadzor.ru

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 ЮРАЙТ https://biblio-online.ru/

Современные профессиональные базы 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=

7.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Программное обеспечение:

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

Информационные справочные системы

1. Консультант Плюс.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные аудитории оборудованы видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном, персональным компьютером с выходом в сеть Интернет; помещения для проведения семинарских и практических занятий оборудованы учебной мебелью; библиотека имеет рабочие места для студентов; компьютерные классы оснащены видеопроекционным оборудованием, средствами звуковоспроизведения, экраном, персональными компьютерами с выходом в сеть Интернет.

9. 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.

Приложение 1

Аннотация рабочей программы
Информационная безопасность

Курс Информационная безопасность обеспечивает преемственность и гармонизацию изучения информационных технологий. Полученные студентами знания, позволят более глубоко изучить смежные профилирующие дисциплины по специальности «Прикладная информатика»

Дисциплина нацелена на формирование общекультурных ОК-4; ОК-7; общепрофессиональных ОПК-1; и профессиональных компетенций ПК-6; ПК-9; ПК-18; ПК-20; ПК-22 выпускника.

Содержание дисциплины.

Предмет и объект защиты

Предмет защиты, объект защиты информации.

Угрозы безопасности информации в компьютерных системах

Случайные угрозы. Преднамеренные угрозы.

Правовые и организационные методы защиты информации в КС

Правовое регулирование в области безопасности информации. Общая характеристика организационных методов защиты информации в КС.

Защита информации в КС от случайных угроз

Дублирование информации. Повышение надежности КС. Создание отказоустойчивых КС. Блокировка ошибочных операций. Оптимизация взаимодействия пользователей и обслуживающего персонала с КС Минимизация ущерба от аварий и стихийных бедствий.

Методы и средства защиты информации в КС от традиционного шпионажа и диверсий

Система охраны объекта КС. Организация работ с конфиденциальными информационными ресурсами на объектах КС. Противодействие наблюдению в оптическом диапазоне. Противодействие прослушиванию. Средства борьбы с закладными подслушивающими устройствами. Защита от злоумышленных действий обслуживающего персонала и пользователей.

Методы защиты от несанкционированного изменения структур КС

Общие требования к защищенности КС от несанкционированного изменения структур. Защита от закладок при разработке программ. Защита от внедрения аппаратных закладок на этапе разработки и производства. Защита от несанкционированного изменения структур КС в процессе эксплуатации.

Защита информации в КС от несанкционированного доступа

Система разграничения доступа к информации в КС. Система защиты программных средств от копирования и исследования.

Компьютерные вирусы и механизмы борьбы с ними

Классификация компьютерных вирусов. Файловые вирусы. Загрузочные вирусы. Вирусы и операционные системы. Методы и средства борьбы с вирусами. Профилактика заражения вирусами компьютерных систем.

Защита информации в распределенных КС

Архитектура распределенных КС. Особенности защиты информации в РКС. Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных КС. Защита информации на уровне подсистемы управления РКС. Защита информации в каналах связи. Подтверждение подлинности информации, получаемой по коммуникационной подсети. Особенности защиты информации в БД.

Построение комплексных систем защиты информации (КСЗИ).

Концепция создания защищенных КС. Этапы создания комплексной системы защиты информации. Моделирование КСЗИ. Выбор показателей эффективности и

критериев оптимальности КСЗИ. Математическая постановка задачи разработки КСЗИ. Подходы к оценке эффективности КСЗИ. Создание организационной структуры КСЗИ.

Организация функционирования комплексных систем защиты информации

Применение КСЗИ по назначению. Техническая эксплуатация КСЗИ.

Криптографические методы защиты информации

Классификация методов криптографического преобразования информации. Шифрование. Основные понятия. Стандарты шифрования.

Простейшие методы шифрования с закрытым ключом.

Общая схема симметричного шифрования. Методы замены. Пропорциональные шифры. Многоалфавитные подставки. Методы гаммирования. Методы перестановки.

Принципы построения блочных шифров с закрытым ключом.

Понятие композиционного шифра. Операции используемые в блочных алгоритмах симметричного шифрования. Структура блочного алгоритма симметричного шифрования. Требования к блочному алгоритму шифрования. Сеть Фейштеля.

Алгоритмы шифрования DES и AES

Основные сведения. Шифрование. Расшифрование. Двухкратные DES и атака «встреча посередине». Трехкратный DES. Алгоритм AES. Режимы работы блочных алгоритмов.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные занятия, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля/аттестации: практические работы, выполнение тестов (текущий контроль), экзамен (промежуточная аттестация).

Заочная форма обучения. Общая трудоемкость (объем) дисциплины составляет _7_ зачетных единицы; _252_ часа. Контактная работа составляет _20_ часов, в том числе: 8 часов - лекции, 12 часов- лабораторные работы, на самостоятельную работу обучающихся _223_ часа, контроль – 9 часов.