Министерство сельского хозяйства Российской Федерации
Департамент научно-технологической политики и образования

Новочеркасский инженерно-мелиоративный институт им. А.К. Кортунова филиал ФГБОУ ВО Донской ГАУ

УТВЕРЖДАЮ

Декан факультета ФБиСТ

В.А. Губачев _____

"____" _____ 2023 г.

РАБОЧАЯ ПРОГРАММА

Дисциплины	**Б1.В.08 Информационная безопасность**
Направление(я)	**44.03.01 Педагогическое образование**
Направленность (и)	**Информатика и информационно-коммуникационные технологии (ИКТ)**
Квалификация	**бакалавр**
Форма обучения	**очная**
Факультет	**Факультет бизнеса и социальных технологий**
Кафедра	**Менеджмент и информатика**
Учебный план	**2022_44.03.01ikt.plx** **44.03.01 Педагогическое образование**
ФГОС ВО (3++) направления	**Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 44.03.01 Педагогическое образование (приказ Минобрнауки России от 22.02.2018 г. № 121)**
Общая трудоемкость	**144 / 4 ЗЕТ**
Разработчик (и):	**канд. с.-х. наук, доц., Пономарева Софья Александровна**

Рабочая программа одобрена на заседании кафедры **Менеджмент и информатика**

Заведующий кафедрой **Иванов Павел Вадимович**

Дата утверждения уч. советом от 26.04.2023 протокол № 8.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 03F24D8300D7AE5FBC4DEAFDF2821DE436
Владелец: Мельник Татьяна Владимировна
Действителен: с 19.07.2022 до 19.10.2023

Новочеркасск 2023 г.

1. ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану	144
в том числе:	
аудиторные занятия	42
самостоятельная работа	66
часов на контроль	36

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	14 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	14	14	14	14
Практические	28	28	28	28
Итого ауд.	42	42	42	42
Контактная работа	42	42	42	42
Сам. работа	66	66	66	66
Часы на контроль	36	36	36	36
Итого	144	144	144	144

Виды контроля в семестрах:

Экзамен	3	семестр

2. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
2.1	Цель изучения дисциплины «Информационная безопасность» - обучение основным принципам информационной
2.2	безопасности, подходам к анализу компьютерных систем с точки зрения информационной безопасности и решению задач
2.3	защиты информации

3. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
3.1	**Требования к предварительной подготовке обучающегося:**
3.1.1	Русский язык и культура речи
3.1.2	Информационные системы и технологии
3.1.3	Методы оптимальных решений
3.1.4	Правоведение
3.1.5	Экономико-математические методы
3.1.6	Информационные системы и технологии
3.1.7	Методы оптимальных решений
3.1.8	Правоведение
3.1.9	Информационные системы и технологии
3.1.10	Методы оптимальных решений
3.1.11	Правоведение
3.1.12	Информационные системы и технологии
3.1.13	Методы оптимальных решений
3.1.14	Правоведение
3.1.15	Информационные системы и технологии
3.1.16	Методы оптимальных решений
3.1.17	Правоведение
3.1.18	Информационные системы и технологии
3.1.19	Методы оптимальных решений
3.1.20	Правоведение
3.1.21	Информационные системы и технологии
3.1.22	Методы оптимальных решений
3.1.23	Правоведение
3.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
3.2.1	Информационные системы и технологии
3.2.2	Методы оптимальных решений
3.2.3	Правоведение
3.2.4	Информационные технологии в менеджменте
3.2.5	Менеджмент
3.2.6	Правовые основы предпринимательской деятельности
3.2.7	Технологическая (проектно-технологическая) практика
3.2.8	Методологическое обеспечение обучения пользователей ИС
3.2.9	Мультимедийные технологии
3.2.10	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)
3.2.11	Стратегический менеджмент
3.2.12	Экономика организации
3.2.13	Бизнес-планирование
3.2.14	Информационное обеспечение управления организационными системами
3.2.15	Логистические системы и управление цепями поставок
3.2.16	Научно-исследовательская работа
3.2.17	Управленческие решения в профессиональной деятельности
3.2.18	Финансовый менеджмент
3.2.19	Выполнение и защита выпускной квалификационной работы

3.2.20	Технологическая (проектно-технологическая) практика
3.2.21	Управление проектами
3.2.22	IT-инфраструктура организации
3.2.23	Общесистемное программное обеспечение
3.2.24	Проектирование информационных систем
3.2.25	Информационные технологии мобильных устройств

4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-1 : Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач

ПК-1.1 : Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета)

УК-1 : Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

УК-1.1 : Демонстрирует знание особенностей системного и критического мышления, аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение

УК-1.3 : Анализирует источники информации с целью выяснения их противоречий и поиска достоверных суждений

УК-2 : Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

УК-2.1 : Определяет совокупность взаимосвязанных задач и ресурсное обеспечение, условия достижения поставленной цели, исходя из действующих правовых норм

УК-2.2 : Оценивает вероятные риски и ограничения, определяет ожидаемые результаты решения поставленных задач

УК-8 : Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов

УК-8.1 : Оценивает факторы риска, умеет обеспечивать личную безопасность и безопасность окружающих в повседневной жизни и в профессиональной деятельности

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Индикаторы	Литература	Интеракт.	Примечание
	Раздел 1. Основные сведения об информационной безопасности						
1.1	Введение в информационную безопасность Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации. Общеметодологические принципы теории информационной безопасности. Информационная безопасность как часть национальной безопасности. Доктрина информационной безопасности РФ. / /Лек/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.1 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК1

1.2	Переработка лекционного материала /Ср/	3	8	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК1
1.3	Понятие и виды защищаемой информации. Понятие и сущность защищаемой информации. Права и обязанности обладателя информации. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. Перечень сведений конфиденциального характера. Понятие интеллектуальной собственности и особенности ее защиты. Государственные стандарты в сфере информационной безопасности. /Пр/	3	4	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ТК1
1.4	Защита персональных данных. Информация, относящаяся к ПД. Хранение ПД. Порядок уничтожения ПД. Электронный архив. /Пр/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ТК1
1.5	Правовой аспект информационной безопасности. Нормативно -правовые акты регулирующие деятельность в сфере информационной безопасности. Руководящие документы по защите информации от несанкционированного доступа ФСТЭК России /Лек/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК1
1.6	Переработка изученного материала /Ср/	3	8	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК1
1.7	Защита документа в MS Office /Пр/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ТК1
	Раздел 2. Организационные основы обеспечения информационной безопасности на предприятии						

2.1	Понятие и виды угроз информационной безопасности. Понятие угрозы информационной безопасности. Классификация и виды угроз информационной безопасности. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа. Основные элементы канала реализации угрозы безопасности информации. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации /Лек/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК1
2.2	Электронная подпись. /Пр/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ТК1
2.3	Переработка изученного материал /Ср/	3	10	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК1
2.4	Меры противодействия угрозам и обеспечения информационной безопасности. Политика информационной безопасности предприятия. Защита информации как комплекс мер. Категории мер обеспечения информационной безопасности. Правовая, техническая, криптографическая, физическая защита информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности. /Лек/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК1
2.5	Разработка политики информационной безопасности "Требования по обеспечению информационной безопасности". /Пр/	3	4	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2	0	ТК1

2.6	Подготовка к ПК1. Подготовка к сдаче отчетности по ТК1 /Ср/	3	12	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК1, ТК1
	Раздел 3. Защита информации в компьютерных системах						
3.1	Компьютерная система как объект информационной безопасности. Основы безопасности операционных систем. Основные возможности и фильтрация трафика. Сетевые угрозы и методы противодействия им. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит. Формальные модели безопасности автоматизированных систем /Лек/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК2
3.2	Методы и критерии оценки защищенности компьютерных систем. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Критерии безопасности компьютерных систем «Оранжевая книга». Общие критерии безопасности информационных технологий. Руководящие документы Гостехкомиссии (ФСТЭК) России. Стандарты по управлению информационной безопасностью ISO/IEC 27000. /Пр/	3	4	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ТК2
3.3	Переработка изученного материала /Ср/	3	10	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ТК2
3.4	Файловая система ОС Windows. Токен доступа процесса в ОС Windows. Фильтрованный токен доступа администратора. Безопасность файлов в ОС Windows. Управление доступом. Организация аудита через ССУД. Организация глобального аудита с помощью утилиты auditpol. Операции с пользователями и группами. /Пр/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ТК2

3.5	Безопасность локальных вычислительных сетей. MAC и IP адреса. Доступность узлов, фильтрация пакетов. Поиск уязвимостей. Настройка безопасности интернет-обозревателей. /Пр/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ТК2
3.6	Вредоносное программное обеспечение и меры противодействия. Классификация вредоносного ПО. Технологии и алгоритмы защиты от вредоносных программ. Антивирусное ПО. Мониторинг, отражение кибератак. Межсетевые экраны. /Лек/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК2
3.7	Исследование и настройка межсетевого экрана. Настройка правила брандмауэра /Пр/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ТК2
3.8	Подготовка к сдаче отчетности по ТК2. /Ср/	3	10	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ТК2
	Раздел 4. Основы криптографии						
4.1	Криптографические методы защиты информации. Модель криптографической системы. Виды криптосистем. Основные требования к криптографическим системам. Виды шифров. Криптография с открытым ключом. Современные российские стандарты шифрования. Криптографические протоколы /Лек/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК2
4.2	Применение криптографических систем. Исторические примеры шифров. Криптографическая система RSA. /Пр/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ТК3
4.3	GNU Privacy Guard - программа для шифрования информации и создания цифровой подписи. /Пр/	3	2	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ТК3
4.4	Подготовка к сдаче отчетности по ТК3. Подготовка к ПК2 /Ср/	3	8	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК2, ТК3

	Раздел 5. Подготовка к итоговому контролю						
5.1	Подготовка к итоговому контролю /Экзамен/	3	36	УК-1.1 УК-1.3 УК-2.1 УК-2.2 УК-8.1 ПК-1.1	Л1.2 Л1.3 Л1.4 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	Экз

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

1. КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ
Текущий контроль знаний студентов очной формы обучения проводится в соответствии с балльно-рейтинговой системой оценки знаний, включающей в себя проведение текущего (ТК) и промежуточного контроля (ПК) по дисциплине. Для контроля освоения практических знаний в течение семестра проводятся текущий контроль по результатам проведения практических занятий, лабораторных работ и самостоятельного выполнения разделов расчётно-графической работы.
Формами ТК являются: оценка выполненных индивидуальных заданий, разделов расчётно-графической работы, контрольные работы или тесты с использованием форм MicrosoftForms, содержащие задания и задачи по темам практических занятий. отчёт по лабораторным работам.
Количество текущих контролей по дисциплине в семестре определяется кафедрой и составляет три (ТК1-ТК3).
При выполнении заданий ТК1 требуется выполнение практических заданий (задач) по темам 1-5 практических занятий.
При выполнении заданий ТК 2 требуется выполнение практических заданий (задач) по темам 6-9 практического занятия.
При выполнении заданий ТК 3 требуется выполнение практических заданий (задач) по темам 10-11 практического занятия.
Карточки с заданиями для проведения ТК в бумажном виде хранятся на кафедре. В ходе промежуточного контроля (ПК) проверяются теоретические знания обучающихся. Данный контроль проводится по разделам (модулям) дисциплины 2 раза в течение семестра. Формами контроля являются тестирование или опрос.
Семестр 3
Вопросы ПК1:
1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
2. Информационная безопасность в системе национальной безопасности РФ.
3. Состав и содержание направлений информационной безопасности.
4. Правовая база обеспечения информационной безопасности личности (общества, государства).
5. Виды информации с точки зрения информационной безопасности.
6. Интересы личности (общества, государства) в информационной сфере.
7. Основные нормативно-правовые акты в области информационной безопасности.
9. Угрозы информационной безопасности и факторы, воздействующие на информацию.
10. Причины, виды, каналы утечки и искажение информации.
11. Информационное оружие, его классификация и возможности.
12. Методы нарушения конфиденциальности (целостности, доступности) информации.
13. Внутренние и внешние угрозы информационной безопасности.

Вопросы ПК2:
1. Анализ угроз информационной безопасности компьютерных систем
2. Компьютерная система как объект информационного воздействия.
3. Современные методы и средства защиты информации.
4. Отечественные и зарубежные стандарты в области информационной безопасности.
5. Криптология и основные этапы ее становления и развития.
6. Анализ современных подходов к построению систем защиты информации.
7. Критерии оценки защищенности компьютерных систем, методы и средства обеспечения их информационной безопасности.
8. Определение вредоносного ПО.
9. Виды вредоносного ПО.
10. Что такое компьютерный вирус?
11. Классификация компьютерных вирусов.
12. Антивирусное ПО.
13. Современные требования к криптографическим системам.
14. Виды шифров.

2. КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
Промежуточная аттестация проводится в форме итогового контроля (ИК) по дисциплине:
Семестр : 3
Форма: экзамен
Вопросы для проведения экзамена:

1. Основные понятия информационной безопасности.
2. Роль информационной безопасности в обеспечении национальной безопасности государства.
3. Законодательство в области информационной безопасности
4. Угрозы безопасности информационных и телекоммуникационных средств и систем.
5. Внешние и внутренние источники угроз информационной безопасности
6. Компьютерная система как объект информационной безопасности.
7. Общая характеристика методов и средств защиты информации.
8. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.
9. Современные требования к криптографическим системам.
10. Виды криптографических систем.
11. Исторические виды шифров.
12. Что принято понимать под удаленной атакой?
13. Классификация удаленных атак.
14. Какие программы являются вредоносными?
15. Классификация классических вирусов
16. Способы заражения компьютерными вирусами
17. Признаки заражения компьютера
18. Косвенные признаки заражения компьютера
19. Действия при появлении признаков заражения вредоносной программой
20. Источники компьютерных вирусов
21. Глобальные сети и электронная почта как источник компьютерных вирусов
22. Локальные сети как источник компьютерных вирусов
23. Основные правила защиты от компьютерных вирусов
24. Антивирусные программы
25. Виды антивирусных программ
26. Информационная безопасность в системе национальной безопасности РФ.
27. Состав и содержание направлений информационной безопасности.
28. Правовая база обеспечения информационной безопасности личности (общества, государства).
29. Угрозы информационной безопасности и факторы, воздействующие на информацию.
30. Причины, виды, каналы утечки и искажение информации.
31. Внутренние и внешние угрозы информационной безопасности.
32. Состав и содержание направлений информационной безопасности.
33. Правовая база обеспечения информационной безопасности личности (общества, государства).
34. Виды информации с точки зрения информационной безопасности.
35. Интересы личности (общества, государства) в информационной сфере.
36. Основные нормативно-правовые акты в области информационной безопасности.
37. Причины, виды, каналы утечки и искажение информации.
38. Информационное оружие, его классификация и возможности.
39. Методы нарушения конфиденциальности (целостности, доступности) информации.

6.2. Темы письменных работ

Темы письменных работ:
- по теме 1 "Защита персональных данных"
- по теме 2 "Процедура получения сертификата электронной подписи" "Разработка политики информационной безопасности "Требования к обеспечению информационной безопасности" (по индивидуальным заданиям)
- по теме3 "Методы и критерии оценки защищенности компьютерных систем"
- по теме 4 "Методы шифрования" (по индивидуальным заданиям)

6.3. Фонд оценочных средств

1. ПОКАЗАТЕЛИ, КРИТЕРИИ И ШКАЛЫ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Оценка сформированности компетенций у студентов НИМИ ДонГАУ и выставление оценки по отдельной дисциплине ведется следующим образом: для студентов очной формы обучения итоговая оценка по дисциплине выставляется по 100-балльной системе, а затем переводится в оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Высокий уровень освоения компетенций, итоговая оценка по дисциплине «отлично» (90-100 баллов): глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач. Системно и планомерно работает в течении семестра. Повышенный уровень освоения компетенций, итоговая оценка по дисциплине «хорошо» (75-89 баллов): твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. Системно и планомерно работает в течении семестра. Пороговый уровень освоения компетенций, итоговая оценка по дисциплине «удовлетворительно» (60-74 балла): имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ. Пороговый уровень освоения компетенций не сформирован, итоговая оценка по дисциплине «неудовлетворительно» (менее 60 баллов): не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут

продолжить обучение без дополнительных занятий по соответствующей дисциплине. Критерии оценки уровня сформированности компетенций и выставление баллов по расчетно-графической работе (до 10 баллов, зачтено/незачтено): соответствие содержания работы заданию; грамотность изложения и качество оформления работы; соответствие нормативным требованиям; самостоятельность выполнения работы, глубина проработки материала; использование рекомендованной и справочной литературы; правильность выполненных расчетов и графической части; обоснованность и доказательность выводов.

2. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИЕ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ
Общий порядок проведения процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, соответствие индикаторам достижения сформированности компетенций определен в следующих локальных нормативных актах: 1. Положение о текущей аттестации знаний обучающихся в НИМИ ДГАУ (в действующей редакции). 2. Положение о промежуточной аттестации обучающихся по программам высшего образования (в действующей редакции). Документы размещены в свободном доступе на официальном сайте НИМИ ДонГАУ https://ngma.su/ в разделе: Главная страница/Сведения об образовательной организации/Локальные нормативные акты.

6.4. Перечень видов оценочных средств

1. ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ:
- тесты и билеты для проведения промежуточного контроля (ПК) и текущего контроля (ТК). Хранятся в бумажном виде на соответствующей кафедре;
- разделы индивидуальных заданий (письменных работ) обучающихся;
- отчеты по лабораторным работам обучающихся;
- задачи и задания.

2. ОЦЕНОЧНЫЕ СРЕДСТВА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ:
- комплект билетов для экзамена. Хранится в бумажном виде на соответствующей кафедре. Подлежит ежегодному обновлению и переутверждению. Число вариантов билетов в комплекте не менее числа студентов на экзамене.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Мельников В.П., Клейменов С.А.	Информационная безопасность и защита информации: учебное пособие для вузов по специальности "Информационные системы и технологии"	Москва: Академия, 2012,
Л1.2	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва ; Берлин: Директ-Медиа, 2020, https://biblioclub.ru/index.php?page=book&id=571485
Л1.3	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019, https://biblioclub.ru/index.php?page=book&id=576726
Л1.4	Гродзенский Я. С.	Информационная безопасность: учебное пособие	Москва: Проспект, 2020, https://biblioclub.ru/index.php?page=book&id=607433
Л1.5	сост: Е. Р. Кирколуп, Ю.Г. Скурыдин, Е.М. Скурыдина	Информационная безопасность: учебное пособие	Барнаул: АлтГПУ, 2017, https://e.lanbook.com/book/112164
Л1.6	Исмагилова А. С., Салов И. В., Шагапов И. А., Корнилова А. А.	Информационная безопасность в цифровом обществе: учебное пособие	Уфа: Башкирский государственный университет, 2019, https://biblioclub.ru/index.php?page=book&id=611084

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника : информационная безопасность автоматизированных систем: учебно-методическое пособие	Йошкар-Ола: ПГТУ, 2019, https://biblioclub.ru/index.php?page=book&id=562246
Л2.2	Филиппов Б. И., Шерстнева О. Г.	Информационная безопасность. Основы надежности средств связи: учебник	Москва ; Берлин: Директ-Медиа, 2019, https://biblioclub.ru/index.php?page=book&id=499170

	Авторы, составители	Заглавие	Издательство, год
Л2.3	Басыня Е. А.	Системное администрирование и информационная безопасность: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2018, https://biblioclub.ru/index.php?page=book&id=575325

7.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Бабаш А.В., Баранова Е.К.	Информационная безопасность. Лабораторный практикум: учебное пособие	Москва: КНОРУС, 2012,
Л3.2		Информационная безопасность: лабораторный практикум	Пермь: ПГГПУ, 2018, https://e.lanbook.com/book/129509

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

7.2.1	Университетская библиотека онлайн : электронно-библиотечная система (ЭБС) / ООО ДиректмедиаПаблишинг. – URL: http://biblioclub.ru/. - Режим доступа: для зарегистр. читателей ЭБС Университетская библиотека онлайн. - Текст: электронный https	https://biblioclub.ru
7.2.2	Microsoft 365: сайт / Microsoft. - URL: https://www.microsoft.com/ru-ru/. - Режим доступа: свободный. - Текст, изображение : электронные https https	https://www.microsoft.com/ru-ru/
7.2.3	Электронная информационно-образовательная среда института - Официальный сайт НИМИ ФГБОУ ВО Донской ГАУ / НИМИ ФГБОУ ВО Донской ГАУ. - URL:www.ngma.su. - Режим доступа: по логину-паролю. - Текст, изображение электронные	http://www.ngma.su

7.3 Перечень программного обеспечения

7.3.1	AdobeAcrobatReader DC	Лицензионный договор на программное обеспечение для персональных компьютеров Platform Clients_PC_WWEULA-ru_RU-20150407_1357 AdobeSystemsIncorporated (бессрочно).
7.3.2	Opera	
7.3.3	Googl Chrome	
7.3.4	Yandex browser	
7.3.5	7-Zip	
7.3.6	Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат. ВУЗ» (интернет-версия);Модуль «Программный комплекс поиска текстовых заимствований в открытых источниках сети интернет»	Лицензионный договор № 6482 от 28.02.2023 г.. АО «Антиплагиат»
7.3.7	MS Windows XP,7,8, 8.1, 10;	Сублицензионный договор №502 от 03.12.2020 г. АО «СофтЛайн Трейд»
7.3.8	MS Office professional;	Сублицензионный договор №502 от 03.12.2020 г. АО «СофтЛайн Трейд»
7.3.9	Microsoft Teams	Предоставляется бесплатно
7.3.10	Snort 3.1.18.0	GNU GENERAL PUBLIC LICENSE Version 3, 29 June 2007
7.3.11	GNU Privacy Guard 2.3.4	GNU GENERAL PUBLIC LICENSE Version 3, 29 June 2007

7.4 Перечень информационных справочных систем

7.4.1	Базы данных ООО Научная электронная библиотека	http://elibrary.ru/
7.4.2	Базы данных ООО "Региональный информационный индекс цитирования"	

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)		
8.1	227	Специальное помещение укомплектовано специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории: Коммутатор сетевой; Компьютеры, объединённые в локальную сеть с доступом в сеть «Интернет» и электронную информационно-образовательную среду НИМИ Донской ГАУ: Системный блок – 20 шт., Монитор ЖК – 20 шт.; Интерактивная видеосистема; Экран настенный; Учебно-наглядные пособия; Доска; Рабочие места студентов; Рабочее место преподавателя.
8.2	233	Специальное помещение укомплектовано специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории: Коммутатор сетевой; Компьютеры, объединённые в локальную сеть с доступом в сеть «Интернет» и электронную информационно-образовательную среду НИМИ Донской ГАУ: Системный блок – 14 шт.; Монитор ЖК - 14 шт.; Проектор настенный; Экран настенный; Учебно-наглядные пособия; Доска; Рабочие места студентов; Рабочее место преподавателя.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Положение о промежуточной аттестации обучающихся по программам высшего образования (введено в действие приказом директора НИМИ Донской ГАУ №3-ОД от 18.01.2018 г.) /Новочерк. инж.-мелиор. ин-т Донской ГАУ. - Новочеркасск, 2018. - URL: http://ngma.su (дата обращения 26.08.2021). - Текст : электронный.
2. Положение о текущей аттестации обучающихся в НИМИ ДГАУ (введено в действие приказом директора №119 от 14 июля 2015 г.) / Новочерк. инж.-мелиор. ин-т Донской ГАУ. - Новочеркасск, 2015. - URL: http://ngma.su (дата обращения 26.08.2021). - Текст : электронный. 3.Типовые формы титульных листов текстовой документации, выполняемой студентами в учебном процессе / Новочерк. инж.-мелиор. ин-т Донской ГАУ.-
Новочеркасск, 2015. - URL: http://ngma.su (дата обращения 26.08.2021). - Текст : электронный.
4. Методические указания по самостоятельному изучению дисциплины (приняты учебно-методическим советом института, протокол № 3 от «30» августа 2017 г.) / Новочерк. инж.-мелиор. ин-т Донской ГАУ. - Новочеркасск, 2017.-URL: http://ngma.su (дата обращения: 26.08.2021). - Текст : электронный.