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.ДВ.02.0 Технологии кибербезопасности 2**
Направление(я)	**38.03.05 Бизнес-информатика**
Направленность (и)	**Информационная архитектура предприятия**
Квалификация	**бакалавр**
Форма обучения	**очная**
Факультет	**Факультет бизнеса и социальных технологий**
Кафедра	**Менеджмент и информатика**
Учебный план	**2023_38.03.05.plx 38.03.05 Бизнес-информатика**
ФГОС ВО (3++) направления	**Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 38.03.05 Бизнес-информатика (приказ Минобрнауки России от 29.07.2020 г. № 838)**
Общая трудоемкость	**108 / 3 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.

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 **3 ЗЕТ**

Часов по учебному плану	108
в том числе:	
аудиторные занятия	42
самостоятельная работа	30
часов на контроль	36

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	13 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	14	14	14	14
Практические	28	14	28	14
Итого ауд.	42	42	42	42
Контактная работа	42	42	42	42
Сам. работа	30	30	30	30
Часы на контроль	36	36	36	36
Итого	108	108	108	108

Виды контроля в семестрах:

Экзамен	3	семестр
Расчетно-графическая работа	3	семестр

2. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
2.1	Целью освоения дисциплины является изучение основных направлений деятельности по обеспечению безопасности информационных систем, основных угроз, уязвимостей, рисков, а также технологий угроз сетевой безопасности и механизмов противодействия сетевым атакам.

3. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.ДВ.02
3.1	**Требования к предварительной подготовке обучающегося:**
3.1.1	Экономико-математические методы
3.1.2	Русский язык и культура речи
3.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
3.2.1	Информационные технологии в менеджменте
3.2.2	Менеджмент
3.2.3	Правовые основы предпринимательской деятельности
3.2.4	Технологическая (проектно-технологическая) практика
3.2.5	Научно-исследовательская работа
3.2.6	Бизнес-планирование
3.2.7	Методологическое обеспечение обучения пользователей ИС
3.2.8	Мультимедийные технологии
3.2.9	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)
3.2.10	Стратегический менеджмент
3.2.11	Экономика организации
3.2.12	IT-инфраструктура организации
3.2.13	Информационное обеспечение управления организационными системами
3.2.14	Управленческие решения в профессиональной деятельности
3.2.15	Финансовый менеджмент
3.2.16	Выполнение и защита выпускной квалификационной работы
3.2.17	Логистические системы и управление цепями поставок
3.2.18	Технологическая (проектно-технологическая) практика
3.2.19	Управление проектами

4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-4 : Способен управлять проектами в области ИТ на основе полученных планов, проектов в условиях, когда проект не выходит за пределы утвержденных параметров
ПК-4.1 : Способен производить сбор информации для инициации проекта в соответствии с полученным заданием
ПК-4.3 : Способен производить мониторинг и управление работами проекта в соответствии с установленными регламентами
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-2.2 : Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)							
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Индикаторы**	**Литература**	**Интеракт.**	**Примечание**
	Раздел 1. Кибербезопасность: основные понятия и определения						

1.1	Основные понятия кибербезопасности. Информационная безопасность и кибербезопасность. Причины киберпреступлений.Проблемы кибербезопасности. /Лек/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК1
1.2	Различные определения информационной безопасности, защиты информации, кибербезопасности, киберустойчивости. Современная постановка задачи защиты информации. Специалисты по обеспечению кмбербезопасности. Лицензирование деятельности по обеспечению информационной безопасности. /Пр/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК1, ТК1
1.3	Проработка изученного материала /Ср/	3	4	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК1, ТК1
	Раздел 2. Моделирование угроз кибербезопасности						
2.1	Анализ рисков как основа управления кибербезопасностью. Инструменты анализа и контроля информационных рисков. Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей. /Лек/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	ПК1
2.2	Общая характеристика анализа, оценки и управления рисками. Шкалы. Оценка на основе выявления слабого звена. Оценка рисков на основе рассмотрения этапов вторжения. Программные средства, используемые для анализа рисков. /Пр/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК1
2.3	Packet Tracer — Настройка WEP/WPA2 PSK/WPA2 RADIUS /Лаб/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ТК1

2.4	Вредоносное ПО и вирусные атаки. Кибермошенничество. Обзор антивирусных средств защиты при организации системы кибербезопасности. Антивирусная защита персональных компьютеров и мобильных устройств. Брандмауэры. Средства аппаратной защиты информации. Организация программно-аппаратных средств кибербезопасности. /Пр/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК1
2.5	Обнаружение угроз и уязвимостей /Лаб/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ТК1
2.6	Оценка средств средств обеспечения кибербезопасности. Экономическое обоснование расходов на обеспечение кибербезопасности. Обоснованный выбор мер и средств обеспечения кибербезопасности. Методика оценки экономической эффективности средств обеспечения кибербезопасности. /Пр/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК1
2.7	Проработка изученного материала. Работа над РГР. /Ср/	3	8	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК1, ТК1
	Раздел 3. Способы защиты секретной информации						
3.1	Криптографические алгоритмы. Обзор алгоритмов шифрования и тенденций развития криптографии. Круг задач, на решение которых ориентированы криптографические методы. Основные понятия и определения криптографии. Обзор современных методов криптоанализа. Перспективные технологии криптоанализа. /Лек/	3	4	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК2

3.2	Концепция криптосистемы с открытым ключом. Классификация криптографических алгоритмов. Алгоритмы шифрования с секретным ключом (симметричные). Блочные шифры. Поточные шифры. Алгоритмы шифрования с открытым ключом (асимметричные). Криптоалгоритмы с секретным ключом. Методы криптоанализа и их влияние на развитие криптографии. Предельные возможности по взлому шифров методом полного перебора ключей. /Пр/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК2
3.3	Изучение шифрования файлов и данных /Лаб/	3	4	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ТК2
3.4	Идентификация и аутентификация пользователей. Методы авторизации пользователя при работе в сети Интернет. Авторизация и аутентификация. Методы создания и хранения паролей. Электронная цифровая подпись. Методы формирования электронной цифровой подписи. /Лек/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК2
3.5	Современные методы идентификации и аутентификации пользователей. Метод паролей. Биометрическая аутентификация. Способы разграничения доступа, методы и средства их реализации. Краткая характеристика современных средств разграничения доступа. Математические модели управления доступом к информации. Субъектно-объектная модель доступа. Политика безопасности и модель доступа. Электронные ключи. Идентификационные карточки, брелоки. Типы карточек. Единая биометрическая система России. /Пр/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК2
3.6	Использование цифровых подписей. /Лаб/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ТК2

3.7	Проработка изученного материала. Работа над РГР. /Ср/	3	8	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК2, ТК2.
	Раздел 4. Основы безопасности сетевых технологий						
4.1	Введение в безопасность сетевых технологий. Принципы функционирования Internet и Intranet. Способы нападения на сети и защита от межсетевого доступа. Особенности для различных уровней модели ISO/OSI. Технологии межсетевых экранов. Функции МЭ. Формирование политики межсетевого взаимодействия. Критерии оценки межсетевых экранов. /Лек/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК2
4.2	Построение защищенных виртуальных сетей VPN. Средства обеспечения безопасности VPN. Защита на канальном и сеансовом уровнях. Протоколы PPTP, L2TP, SSL/TLS, SOCKS. Защита на сетевом уровне. Протокол IPSEC /Пр/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК2
4.3	Packet Tracer — Межсетевые экраны на сервере и списки контроля доступа на маршрутизаторе /Лаб/	3	4	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ТК2
4.4	Проработка изученного материала. Работа над РГР. /Ср/	3	4	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК2, ТК2
	Раздел 5. Организационно-правовое обеспечение кибербезопасности						

5.1	Сущность и роль организационно-правовых аспектов кибербезопасности. Нормативная правовая база информационной безопасности. Виды и категории информации ограниченного доступа: государственная и другие виды тайн. Государственная система лицензирования и сертификации деятельности в области защиты информации. Зарубежные стандарты информационной безопасности. Стандарты РФ. Стандарты информационной безопасности в Интернете (IETF, RFC). Сертификация и аттестация в области информационной безопасности. /Лек/	3	2	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК2
5.2	Проработка изученного материала. Подготовка отчета по РГР. /Ср/	3	6	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК2, ТК2
	Раздел 6. Подготовка к итоговому контролю						
6.1	Итоговая аттестация /Экзамен/	3	36	ПК-4.1 ПК-4.3 УК-2.2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ИК

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 два (ТК1-ТК2).

При выполнении заданий ТК1 требуется выполнение лабораторных работ по темам 1-2. При выполнении заданий ТК 2 требуется выполнение лабораторных работ по темам 3-5 и выполнение РГР. 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. Понятие кибербезопасности
2. Виды киберпреступлений
3. Различные определения информационной безопасности, защиты информации, кибербезопасности, киберустойчивости.
4. Современная постановка задачи защиты информации.
5. Специалисты по обеспечению кибербезопасности.
6. Виды информации с точки зрения информационной безопасности.
7. Интересы личности (общества, государства) в информационной сфере.
6. Лицензирование деятельности по обеспечению 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.
14. Общая характеристика анализа, оценки и управления рисками.
15. Программные средства, используемые для анализа рисков.
16. Анализ угроз информационной безопасности компьютерных систем
17. Современные методы и средства защиты информации

Вопросы ПК2:
1. Методы авторизации пользователя при работе в сети Интернет
2. Компьютерная система как объект информационного воздействия.
3. Электронная цифровая подпись
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. Обзор алгоритмов шифрования и тенденций развития криптографии. Круг задач, на решение которых ориентированы криптографические методы. Основные понятия и определения криптографии.
15. Криптографические алгоритмы.
16. Обзор современных методов криптоанализа
17. Идентификация и аутентификация пользователей
18. Способы нападения на сети и защита от межсетевого доступа. Особенности для различных уровней модели ISO/OSI.
19. Технологии межсетевых экранов. Функции МЭ.
20. Нормативная правовая база информационной безопасности

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

1. Понятие кибербезопасности
2. Виды киберпреступлений
3. Различные определения информационной безопасности, защиты информации, кибербезопасности, киберустойчивости.
4. Современная постановка задачи защиты информации.
5. Специалисты по обеспечению кибербезопасности.
6. Виды информации с точки зрения информационной безопасности.
7. Интересы личности (общества, государства) в информационной сфере.
6. Лицензирование деятельности по обеспечению 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.
14. Общая характеристика анализа, оценки и управления рисками.
15. Программные средства, используемые для анализа рисков.
16. Анализ угроз информационной безопасности компьютерных систем
17. Современные методы и средства защиты информации
18. Методы авторизации пользователя при работе в сети Интернет
19. Компьютерная система как объект информационного воздействия.
20. Электронная цифровая подпись
21. Отечественные и зарубежные стандарты в области информационной безопасности.
22. Криптология и основные этапы ее становления и развития.
23. Анализ современных подходов к построению систем защиты информации.
24. Критерии оценки защищенности компьютерных систем, методы и средства обеспечения их информационной безопасности.
25. Определение вредоносного ПО.
26. Виды вредоносного ПО.
27. Что такое компьютерный вирус?
28. Классификация компьютерных вирусов.

29. Антивирусное ПО.
30. Современные требования к криптографическим системам.
31. Обзор алгоритмов шифрования и тенденций развития криптографии. Круг задач, на решение которых ориентированы криптографические методы. Основные понятия и определения криптографии.
32. Криптографические алгоритмы.
33. Обзор современных методов криптоанализа
34. Идентификация и аутентификация пользователей
35. Способы нападения на сети и защита от межсетевого доступа. Особенности для различных уровней модели ISO/OSI.
36. Технологии межсетевых экранов. Функции МЭ.
37. Нормативная правовая база информационной безопасности

6.2. Темы письменных работ

Расчетно-графическая работа по теме "Построение системы информационной безопасности предприятия" включает следующие основные разделы:
1. Разработка политики обеспечения информационной безопасности
2. Законодательный уровень
3. Организационный уровень
4. Криптография
5. Программно-технический уровень

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 РГР 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	сост: Е. Р. Кирколуп, Ю.Г. Скурыдин, Е.М. Скурыдина	Информационная безопасность: учебное пособие	Барнаул: АлтГПУ, 2017, https://e.lanbook.com/book/112164

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
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	Dr.Web®DesktopSecuritySuiteАнтивирус КЗ+ ЦУ	Государственный (муниципальный) контракт № РЦА06150002 от 15.06.2021 г. на передачу неисключительных прав на использование программ для ЭВМ ООО «АЙТИ ЦЕНТ»
7.3.2	AdobeAcrobatReader DC	Лицензионный договор на программное обеспечение для персональных компьютеров Platform Clients_PC_WWEULA-ru_RU-20150407_1357 AdobeSystemsIncorporated (бессрочно).
7.3.3	Opera	
7.3.4	Googl Chrome	
7.3.5	Yandex browser	
7.3.6	7-Zip	
7.3.7	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»
7.3.8	MS Windows XP,7,8, 8.1, 10;	Сублицензионный договор №502 от 03.12.2020 г. АО «СофтЛайн Трейд»
7.3.9	MS Office professional;	Сублицензионный договор №502 от 03.12.2020 г. АО «СофтЛайн Трейд»
7.3.10	Microsoft Teams	Предоставляется бесплатно
7.3.11	GNU Privacy Guard 2.3.4	GNU GENERAL PUBLIC LICENSE Version 3, 29 June 2007
7.3.12	Snort 3.1.18.0	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 "Гросс Систем.Информация и решения"	http://www.гроссинфо.рф
7.4.3	Базы данных ООО "Региональный информационный индекс цитирования"	

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.