ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Проректор по УМР
_____ И. А. Дибиров
«31» _____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОПЦ.13 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА

Направление подготовки 09.02.01 Компьютерные системы и комплексы
Квалификация: специалист по компьютерным системам
Срок обучения по ОП: 3г 10мес (очное обучение)
Форма обучения: очная
Образовательный стандарт (ФГОС) № 362 от 25.05.2022

Махачкала 2023

Автор(ы) составитель(и): Дибирова К.С.

Программа утверждена на заседании учебно-методического совета ДГПУ (протокол №3 от «28» апреля 2023г.

Председатель УМС ДГПУ д.ф.н, профессор
Дибиров И.А. _____
подпись

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

1.1. Место дисциплины в структуре основной профессиональнойобразовательной программы:

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности **09.02.01** Компьютерные системы и комплексы

Учебная дисциплина "Инженерная компьютерная графика" относится к общепрофессиональному циклу основной профессиональной образовательной программы. Дисциплина **ОПЦ.13 «**Информационная безопасность и защита информации**»** относится к **общепрофессиональному циклу** учебного плана (основной профессиональной образовательной программы) подготовки студентов по направлению 09.02.01 Компьютерные системы и комплексы

1.2. Требования к результатам освоения МДК:

В результате освоения учебной дисциплины обучающийся должен **уметь:**

- Формулировать тему, проблему, ставить цель и задачи, обосновывать актуальностьпроблемы, определять гипотезу, доказывать или опровергать ее.
- Изготовлять продукт исследовательской деятельности.
- Составлять содержание работы и план своих действий на каждом этапе.
- Составлять структуру своего исследования.
- Проводить исследование и делать вывод по его результатам.
- Работать с различными источниками информации, используя разные формы защитыинформации.
- Выявлять вирусы.
- Использовать современные средства защиты информации.

В результате освоения учебной дисциплины обучающийся должен **знать:**

- Современные методы защиты информации;
- Основные виды угроз;
- Виды продуктов вирусов;
- Формы защиты информации в сети ЭВМ;
- Требования к защите информации, критерии оценки угроз.

В результате освоения дисциплины формируются следующие *общие* и *профессиональных компетенции:*

- **ОК 04.** Эффективно взаимодействовать и работать в коллективе и команде;
- **ОК 05.** Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
- **ОК09.**Пользоваться профессиональной документацией на государственном и иностранном языках.

- **ПК 1.3** Оформлять техническую документацию на проектируемые устройства
- **ПК 2.1** Проектировать, разрабатывать и отлаживать программный код модулейуправляющих программ.
- **ПК 2.2** Владеть методами командной разработки программных продуктов.

1.3. Количество часов на освоение программы:

Максимальная учебная нагрузка - 340 часов, в том числе:

Вариативная часть - 340 часов.

Объём практической подготовки - 112 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	*Объем часов*
Максимальная учебная нагрузка (всего)	**340**
Обязательная аудиторная учебная нагрузка (всего)	**314**
в том числе:	
лекции	92
лабораторные занятия	94
практические занятия	132
Самостоятельная работа обучающегося	**22**
В т. ч. внеаудиторная самостоятельная работа	22
Промежуточная аттестация 5 и 6 семестр	зачет
Итоговая аттестация в форме 7 семестр:	**дифференцированного зачета**

2.2. Тематический план и содержание учебной дисциплины: Информационная безопасность и защита информации

Наименование разделов и тем	Содержание учебного материала, лекции и практические занятия, самостоятельная работа обучающихся.	Объем часов	Уровень освоения
1	2	3	4
Семестр 4		**164**	
Раздел 1. Общие вопросы информационный безопасности.		**63**	
Тема 1.1. Международные стандарты информационного обмена	**Содержание учебного материала** 1. Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. 2. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. 3. Защита информации, тайна, средства защиты информации. 4. Международные стандарты информационного обмена. 5. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защитеинформации. 6. Комплексность защиты информации: инструментальная, структурная, функциональная, временная.	**12**	**1**
	Лабораторные работы: 1. Основные правовые документы об информационной безопасности. 2. Сравнительный анализ законодательства в сфере информационной безопасности двух государств.	**8**	**1**
	Практические занятия: 1. Защита документооборота в вычислительных системах 2. Криптографические методы защиты 3. Шифрование методом IDEA	**12**	**2**
	Самостоятельная работа обучающихся: 1. Проведение анализа информационной системы. 2. Доклад на тему «Защита информации, тайна»	**4**	**3**
Тема 1.2 Понятия и угрозы.	**Содержание учебного материала** 7. Основные понятия. Механизмы безопасности. Классы безопасности. 8. Основные определения и критерии классификации угроз	**4**	**1**

	Лабораторные работы: 3. Разработка политики безопасности объекта. 4. Некоторых примеры исторических систем счисления	**8**	**2**
	Практическая работа 4. Шифрование методом RC6 5. Шифрование методом SAFER K-64 6. Параметры безопасности программы Microsoft Outlook	**12**	**2**
	Самостоятельная работа обучающихся: 3. Выявление угроз и уязвимостей, каналов утечки информации 4. Презентация по теме «Основные угрозы»	**3**	**3**
Раздел 2. Государственная система информационной безопасности		**35**	
Тема 2.1 Информационная безопасность в условиях функционирования в России глобальных сетей.	**Содержание учебного материала**	**12**	1
	9. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно справочные документы. 10. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. 11. Структура государственной системы информационной безопасности. 12. Структура законодательной базы по вопросам информационной безопасности. 13. Лицензирование исертификация в области защиты информации. 14. Место информационной безопасности экономических систем в национальной безопасности страны, опасности страны.		
	Лабораторные работы: 5. Непозиционной системы счисления. 6. Изучить арифметику систем счисления для целых чисел.	**8**	
	Практические занятия: 7. Права на использование директории для определенного пользователя 8. Проверка компьютера на предмет наличия уязвимостей 9. Исследование угроз доступности	**12**	**2**
	Самостоятельная работа обучающихся: 5. Краткий конспект по теме «Концепция информационной безопасности.» 6. Исследовательская работа	**3**	**3**
Раздел 3. Угрозы безопасности		**33**	
Тема 3.1	**Содержание учебного материала**	**10**	**1**

Угрозы безопасности.	15. Понятие угрозы. Виды противников или «нарушителей». 16. Классификация угроз информационной безопасности. Виды угроз. 17. Характер происхождения угроз (умышленные и естественные факторы). 18. Источники угроз. Предпосылки появления угроз. 19. Классы каналов несанкционированного получения информации		
	Лабораторные работы: 7. Произведение в системах счисления. 8. Деление в системах счисления .	**8**	
	Практические занятия: 10. Использование средств администрирования Windows для анализа и настройки безопасности 11. Использование шифрующей файловой системы 12. Аварийное восстановление информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.	**12**	**2**
	Самостоятельная работа обучающегося: 7. Виды противников или «нарушителей». Понятие о видах вируса 8. Краткий конспект по теме «Причины нарушения целостности информации.»	**3**	**3**
Раздел 4. Теоретические основы методов защиты информационных систем		**33**	
Тема 4.1 Теоретические основы методов защиты информационных систем	**Содержание учебного материала**		
	20. Основные положения теории информационной безопасности информационных систем. 21. Модели безопасности и их применение. Формальные модели безопасности 22. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. 23. Модель распространения прав доступа Take-Grant. Мандатная модель Белла- ЛаПадулы. 24. Ролевая политика безопасности. Ограничения на области применения формальных моделей	**10**	**1**
	Лабораторные работы: 9. Арифметика систем счисления для десятичных дробей. 10. Хранение отрицательных чисел в различных форматах в компьютере.	8	**2**
	Практические занятия: 13. Защита и восстановление данных на компьютере, используя систему архивации 14. Исследование реестра, на предмет возможных уязвимостей для вирусов 15. Использование брандмауэра для анализа трафика между двумя сетями.	**12**	**2**
	Самостоятельная работа обучающегося: 9. Три вида возможных нарушений информационной системы. 10. Доклад по теме «Права доступа Take-Grant»	3	**2**

Семестр 5 (зачет)		**88**	
Раздел 5. Методы защиты средств вычислительной техники		**43**	
Тема 5.1 Методы защитысредств вычислительной техники	**Содержание учебного материала** 1. Использование защищенных компьютерных систем. 2. Аппаратные и программныесредства для защиты компьютерных систем от НСД. 3. Средства операционной системы. Средства резервирования данных. 4. Проверкацелостности. Способы и средства восстановления работоспособности.	**8**	**1**
	Лабораторные работы: 1. Хранение чисел с плавающей запятой в компьютере 2. Хранение текстовой информации в компьютере. 3. Хранение графической информации в компьютере. 4. Хранение мультимедийной информации в компьютере.	**16**	**2**
	Практические занятия: 1. Криптосистема Эль-Гамаля 2. Шифрование методом Вернам 3. Использование классических крипто-алгоритмов подстановки и перестановки для защиты текстовой информации 4. Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей. 5. Стандарт симметричного шифрования AES RIJNDAEL.	**18**	**2**
	Самостоятельная работа обучающегося 1. Презентация по теме «Методы защиты средств вычислительной техники»	**1**	**3**
Раздел 6. Основы криптографии		**45**	
Тема 6.1 Основы криптографии	**Содержание учебного материала** 5. Методы криптографии. Симметричное и асимметричное шифрование. 6. Алгоритмышифрования. 7. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. 8. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. 9. Обеспечиваемая шифром степень защиты. Криптанализ и атаки на криптосистемы.	**10**	**1**
	Лабораторные работы: 5. Способ измерения количества информации по методу Хартли.	**18**	**2**

	6. Способ измерения количества информации по методу Шеннона. 7. Модель двоичного симметричного канала связи. 8. Историю развития сетевых технологий. 9. Стеки протоколов коммуникации в сети		
	Практические занятия 10. Генерация простых чисел, используемых в асимметричных системах шифрования 11. Электронная цифровая подпись. 12. Шифрование методом скользящей перестановки. 13. Шифрование на языке программирования TPascal	**16**	**2**
	Самостоятельная работа обучающегося: 2. Презентация по теме «Электронно-цифровая подпись»	**1**	**3**

Семестр 6 (зачет)		**38**	
Раздел 7.Архитектура защитных экономических систем		**38**	
Тема 7.1 Архитектура защитных экономических систем	**Содержание учебного материала**	**8**	**2**
	1. Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. 2. Классы задач защиты информации. Архитектура систем защиты информации. 3. Ядро и ресурсы средств защиты информации. Стратегии защиты информации. 4. Особенности экономических информационных систем.		
	Лабораторные работы: 1. Структура и назначение протокола IP 2. Проблема перехода к новой версии протокола IP. 3. Антивирусные средства защиты персонального компьютера 4. Соблюдение норм кибернетической гигиены в жизни	**10**	**2**
	Практические занятия 1. Шифрование методом аналитических преобразований 2. Протоколирование и аудит в ОС Windows 8. 3. Межсетевой экран – брандмауэр в ОС Windows 8. 4. Корректирующие коды для контроля целостности информации. Коды Хэмминга. Циклические кода 5. Методы сжатия по Шеннону и Хаффмену. LZW-сжатие.	**18**	**3**
	Самостоятельная работа обучающегося: 1. Краткий конспект «Функции защиты информации» 2. Доклад на тему «Стратегии защиты информации»	**2**	**3**
Семестр 7 (диф. зачет)		**50**	
Раздел 8. Алгоритмы и привязки программного обеспечения к аппаратному окружению		**30**	
Тема 8.1 Алгоритмы и привязки программного обеспечения к аппаратному окружению	**Содержание учебного материала**	**12**	**1**
	1. Индивидуальные параметры вычислительной системы. 2. Блок проверки аппаратного окружения. Дискета как средство привязки. 3. Технология HASP, эмуляторы. Временныеметки и запись в реестр. 4. Обеспечение требуемого количества запусков (trial version). 5. Технология spyware.Виды распространения программного обеспечения. 6. Шифрование и запутывание исполняемого кода		

	Лабораторные работы: 1. Кодирования информации в цифровой среде. 2. Условие Фано.	**5**	**3**
	Практические занятия 1. Сокрытие информации методом стеганографии 2. Антивирусная программа Dr.Web 3. Антивирус Касперского.	**12**	**2**
	Самостоятельная работа обучающегося: 1. Презентация на тему «Технология spyware»	**1**	**3**
Раздел 9. Алгоритмы и привязки программного обеспечения к аппаратному окружению		**20**	
Тема 9.1 Алгоритмы безопасности в компьютерных сетях	**Содержание учебного материала**	**6**	**1**
	1. Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты. 2. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». 3. Сетевые защищенные протоколы. Протоколирование.		
	Лабораторные работы: 3. Кодирование Хаффмана. 4. Кодирование Шеннона-Фано.	**5**	**3**
	Практические занятия 4. Сокрытие информации методом стеганографии 5. Рассмотрение распространенных антивирусных программ	**8**	**2**
	Самостоятельная работа обучающегося: 1. Составить алгоритм безопасности	**1**	**3**
ВСЕГО		**340**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 – ознакомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия учебного кабинета.
Оборудование учебного кабинета:

- сетевой компьютерный класс с выходом в Интернет;
- комплекты «столы-стулья» (2 к 1) в количестве не менее 15 шт.;
- шкафы для методической литературы;
- огнетушитель;
- информационные стенды

Технические средства обучения:

- интерактивная доска;
- проектор;
- компьютерное рабочее место для преподавателя;
- принтер;
- сканер.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, интернет ресурсов, дополнительной литературы

Основные источники:

1) Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ. - 3-е изд. (эл.). - М. : БИНОМ, 2015. - (Программисту). - http://www.studentlibrary.ru/book/ISBN9785996329526.html
   Электронное издание на основе: Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ.-3-е изд. (эл.).-Электрон. текстовые дан. (1 файл pdf : 482 с.).- М. : БИНОМ. Лаборатория знаний, 2015.- (Программисту).-Систем. требования: Adobe Reader XI ; экран 10". - ISBN 978-5-9963-2952-6.
2) Интеллектуальные системы защиты информации [Электронный ресурс] : учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - http://www.studentlibrary.ru/book/ISBN9785942756673.html
   Электронное издание на основе: Интеллектуальные системы защиты информации: учеб. пособие/ В. И. Васильев. 2-е изд., испр. и доп. - М.: Машиностроение, 2013.- 172 с. - ISBN 978-5-94275-667-3.

3) Информатика 2015 [Электронный ресурс] : учебное пособие / Алексеев А.П. - М. : СОЛОН-ПРЕСС, 2015. - http://www.studentlibrary.ru/book/ISBN9785913591586.html Электронное издание на основе: Информатика 2015: учебное пособие/ Алексеев А.П.- 2015. - 400 с., илл. - ISBN 978-5-91359-158-6.

Дополнительные источники:

1) Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. - Ростов-на-Дону: Издательство СКНЦ ВШ, 2012.

2) Соколов А. В., Степанюк О. М. Защита от компьютерного терроризма. Справоч-ное пособие. - СПб.: БХВ - Петербург, Арлит, 2012.- 496с.:ил.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения

Программа составлена в соответствии с требованиями ФГОС СПО для специальностей технического профиля

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
1. выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;	Выполнение и защита заданий по практическим работам.
2. осуществлять диагностику и поиск неисправностей технических средств;	Выполнение и защита заданий по практическим работам.
3. тестировать кабели и коммуникационные устройства;	Выполнение и защита заданий по практическим работам.
4. правильно оформлять техническую документацию;	Выполнение и защита заданий по практическим работам.
5. наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;	Выполнение и защита заданий по практическим работам.
6. устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	Выполнение и защита заданий по практическим работам.