Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сочинский государственный университет»

СОГЛАСОВАНО
Декан СПФ _____ Иванов И.А.
«__» _____ 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность

Шифр и направление подготовки 44.03.05 Педагогическое образование с двумя профилями подготовки

Квалификация (степень) выпускника бакалавр

Профиль подготовки бакалавра Математика и информатика

Форма обучения Очная

Выпускающая кафедра Педагогического и психолого-педагогического образования

Кафедра-разработчик рабочей программы Прикладной математики и информатики

Семестр	Трудоем-кость (час./зет.)	Лекцион. занятий, (час.)	Практич. занятий, (час.)	Лаборат. занятий, (час.)	СРС, (час.)	КР/КП (час.)	КРЗ	Форма промежуточного контроля (экз./зачет)
ОФО								
8	**108/3**	**-**	**36**	**-**	**72**	**-**	**-**	**ЗачетО**
ИТОГО	**108/3**	**-**	**36**	**-**	**72**	**-**	**-**	**ЗачетО**

Сочи 2019 г.

Рабочая программа по дисциплине Б1.В.ДВ.02.02 Информационная безопасность составлена в соответствии с требованиями ФГОС ВО 3++ по направлению подготовки 44.03.05 Педагогическое образование с двумя профилями подготовки (утвержден Приказом Минобрнауки № 125 от 22.02.2018)

Рабочую программу составил: подпись Симаворян С.Ж.

РАБОЧАЯ ПРОГРАММА РАССМОТРЕНА И ОДОБРЕНА

на заседании кафедры Прикладной математики и информатики

Протокол № 1 от «29» 08 2019 г.

Заведующий кафедрой Макарова И.Л.

Руководитель ОПОП Иванов И.А.

Рабочая программа одобрена на заседании Учебно-методического совета направления 44.03.05 Педагогическое образование (с двумя профилями подготовки)

Протокол № 01 от «30» 08 2019 г.

Председатель УМСН Иванов И.А.

Структура рабочей программы соответствует предъявляемым требованиям

Отдел качества образования и методического обеспечения Васильченко В.В.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ РПД

Рабочая программа переутверждена на 2020/2021 учебный год, протокол № 1 заседания кафедры от «29» августа 2020 г. В программу внесены дополнения и (или) изменения:

5.3 Особенности преподавания дисциплины

5.4 Материально-техническое обеспечение дисциплины

Обновлен список литературы.

Заведующий кафедрой _____ Макарова И.Л.

подпись ФИО

Рабочая программа переутверждена на 2022/2023 учебный год, протокол №1 заседания кафедры от «30» августа 2022 г. В программу внесены дополнения и(или) изменения.

На основании распоряжения ректора № 243-р, от 06.07.22 г. в рабочую программу дисциплины внесены изменения – Профессиональные компетенции установленные вузом (ПКУВ) на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников считать Профессиональными компетенциями определенными организацией самостоятельно на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников (ПК).

ПКУВ-1 считать ПК-1.

Заведующий кафедрой _____ Макарова И.Л

Рабочая программа переутверждена на 20___/20___ учебный год, протокол №___ заседания кафедры от «__» _____ 20_____г. В программу внесены дополнения и(или) изменения.

_____

_____

Заведующий кафедрой _____ _____

подпись ФИО

СОДЕРЖАНИЕ

1 ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Информационная безопасность» является освоение основ информационной безопасности для студентов по направлению подготовки 44.03.05 «Математика и информатика»

Задачи дисциплины:
- овладение основными понятиями информационной безопасности и методами защиты данных, необходимыми для применения в профессиональной работе, для продолжения образования;
- интеллектуальное развитие студентов, формирование качеств мышления, необходимых для профессиональной деятельности;
- формирование представлений об идеях и методах информационной безопасности;
- формирование представлений об информационной безопасности как неотъемлемой части функционирования вычислительных систем и сетей, понимания значимости вопросов информационной безопасности для будущей профессиональной деятельности.

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП НАПРАВЛЕНИЯ (СПЕЦИАЛЬНОСТИ)

Дисциплина «Информационная безопасность» является относится к Блоку 1 «Дисциплины (модули)», и является вариативной дисциплиной.

Таблица 1

Наименование категории (группы) компетенций	**Код и наименование компетенции**	**Предшествующие дисциплины**	**Последующие дисциплины**
	ПКУВ-2 Способен разрабатывать методику обучения отдельным разделам информатики и программирования с применением компьютерных технологий	Б1.В.02 Программирование Б1.В.06 Компьютерное моделирование Б1.В.07 Программное обеспечение ЭВМ и практикум по решению задач на ЭВМ Б1.В.08 Компьютерные сети Б1.В.ДВ.02.01 Основы кибербезопасности	Б1.В.09 Методический модуль Б1.В.09.02 Теория и методика обучения информатике Б1.В.ДВ.03.02 Проектирование информационных систем Б1.В.ДВ.03.01 Системы управления базами данных

3 ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК – универсальные компетенции;
ОПК – общепрофессиональные компетенции;
ПК – профессиональные компетенции;
ПКО – профессиональные компетенции обязательные;

ПКР – профессиональные компетенции рекомендуемые;
ПКУВ – профессиональные компетенции, установленные вузом.

Таблица 2

Компетенции и индикаторы их достижения			В результате изучения дисциплины обучающиеся должны:
Категория компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	
	ПКУВ-2 Способен разрабатывать методику обучения отдельным разделам информатики и программирования с применением компьютерных технологий	ПКУВ-2.1 Анализирует и разрабатывает альтернативные варианты методики обучения информатике с применением компьютерных технологий	З.1-ПКУВ-2.1 Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной У.1-ПКУВ-2.1 Уметь решать стандартные задачи профессиональной деятельности на основе информационной. Н.1-ПКУВ-2.1 Владеть навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
		ПКУВ-2.2 Использует компьютерные технологии для разработки информационных моделей реальных процессов окружающего мира	З.1-ПКУВ-2.2 Знать основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. У.1-ПКУВ-2.2 Уметь применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. Н.1-ПКУВ-2.2 Владеть навыками составления технической документации по защите информации на различных этапах жизненного цикла информационной системы.

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Тематический план дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов,

	Наименование модуля (раздела, темы)	**ОФО**

	дисциплины	Всего часов	Виды учебной нагрузки и их трудоемкость, часы				
			Лекции	Практические занятия	Лабораторные работы	СРС	Контроль
1	Тема 1. Нормативно-правовые акты информационной безопасности в Российской Федерации	6	-	2	-	4	-
2	Тема 2. Доктрина информационной безопасности Российской Федерации	6	-	2	-	4	-
3	Тема 3. Определение и основные понятия теории информационной безопасности	6	-	2	-	4	-
4	Тема 4. Методологический базис теории информационной безопасности	6	-	2	-	4	-
5	Тема 5. Модели систем и процессов защиты информации	6	-	2	-	4	-
6	Тема 6. Унифицированная концепция информационной безопасности	6	-	2	-	4	-
7	Тема 7. Угрозы, каналы несанкционированного получения информации, их классификация	6	-	2	-	4	-
8	Тема 8. Определение системы показателей уязвимости информации	6	-	2	-	4	-
9	Тема 9. Методы и модели оценки уязвимости информации	6	-	2	-	4	-
10	Тема10. Определение, анализ и классификация функций защиты информации	6	-	2	-	4	-
11	Тема 11. Определение, анализ и классификация задач защиты информации	6	-	2	-	4	-
12	Тема 12. Определение, анализ и классификация средств защиты информации	6	-	2	-	4	-
13	Тема 13. Определение и общеметодологические принципов архитектурного построения систем защиты информации	6	-	2	-	4	-
14	Тема 14. Методы проектирования систем защиты информации	6	-	2	-	4	-
15	Тема 15. Управление процессами функционирования защиты информации	6	-	2	-	4	-
16	Тема 16. Особенности защиты в ПЭВМ.	6	-	2	-	4	-
17	Тема 17. Особенности защиты информации в сетях ЭВМ.	6	-	2	-	4	-
18	Тема 18. Организация и обеспечение работ по безопасности информации	6	-	2	-	4	-
	ЗачетО	-	-	-	-	-	-
	ИТОГО	108	-	36	-	72	-

4.1.1 Лекционные занятия

Учебным планом не предусмотрены.

4.1.2 Практические занятия

№ п/п	Наименование модуля, раздела дисциплины	Объем, часов	Краткое содержание	Формируемые ЗУН	Ссылки на литературу
1	Тема 1. Нормативно-правовые акты информационной безопасности в Российкой Федерации	2	Что такое законодательный уровень информационной безопасности и почему он важен Обзор российского законодательства в области информационной безопасности	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
2	Тема 2. Доктрина информационной безопасности Российской Федерации	2	Сущность и содержание Доктрины информационной безопасности Российской Федерации	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
3	Тема 3. Определение и основные понятия теории информационной безопасности	2	Понятие информационной безопасности Основные составляющие информационной безопасности Важность и сложность проблемы информационной безопасности	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
4	Тема 4. Методологический базис теории информационной безопасности	2	Цели и особенности моделирования систем защиты информации Классификация и общий анализ моделирования систем защиты информации	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
5	Тема 5. Модели систем и процессов защиты информации	2	Общая модель процесса защиты Модели общей оценки угроз информации	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
6	Тема 6. Унифицированная концепция информационной безопасности	2	Системно-концептуальный подход к моделированию систем защиты информации	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
7	Тема 7. Угрозы, каналы несанкционированного получения информации, их классификация	2	Наиболее распространенные угрозы доступности Некоторые примеры угроз доступности	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
8	Тема 8. Определение	2	Система показателей уязвимости	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1,	[1-10]

	системы показателей уязвимости информации		информации	З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	
9	Тема 9. Методы и модели оценки уязвимости информации	2	Аналитическая модель оценки защищённости информации Статистическая модель оценки защищенности информации	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
10	Тема10. Определение, анализ и классификация функций защиты информации	2	Определение, назначение и анализ понятия функций защиты информации Обоснование полного множества функций защиты информации Методология выбора функций защиты информации	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
11	Тема 11. Определение, анализ и классификация задач защиты информации	2	Определение, назначение и анализ и понятия задач защиты информации Обоснование полного множества задач защиты информации Классификация задач защиты информации Методология выбора задач защиты информации	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
12	Тема 12. Определение, анализ и классификация средств защиты информации	2	Определение, анализ понятия средств защиты информации Обоснование полного множества средств защиты информации Классификация средств защиты информации Методология выбора средств защиты информации	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
13	Тема 13. Определение и общеметодологические принципов архитектурного построения систем защиты информации	2	Система защиты информации и общеметодологические принципы ее построения Основы архитектурного построения систем защиты информации	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
14	Тема 14. Методы проектирования систем защиты информации	2	Классификация и анализ постановок задач проектирования систем защиты информации Последовательность и общее содержание проектирования систем защиты информации	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
15	Тема 15. Управление процессами функционирования защиты информации	2	Общая организация управления защитой информации Технология планирования защиты информации, основные макропроцессы управления защитой информации	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]

16	Тема 16. Особенности защиты в ПЭВМ.	2	Особенности защиты информации в персональных ЭВМ Угрозы информации в персональных ЭВМ Обеспечение целостности информации в ПЭВМ	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
17	Тема 17. Особенности защиты информации в сетях ЭВМ.	2	Основные положения концепции построения и использования сетей ЭВМ Цели, функции и задачи защиты информации в сетях ЭВМ	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
18	Тема 18. Организация и обеспечение работ по безопасности информации	2	Перечень и общее содержание основных вопросов организации и обеспечения работ по защите информации Структура и функции органов защиты информации Стандарты и спецификации в области информационной безопасности	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
	ИТОГО	36			

4.1.3 Лабораторные занятия

В учебном плане отсутствуют

4.1.4 Самостоятельная работа студента

№ п/п	Наименование модуля, раздела дисциплины	Объем, часов	Вид СРС	Формируемые ЗУН	Ссылки на литературу
1	Тема 1. Нормативно-правовые акты информационной безопасности в Российской Федерации	4	Изучение вопросов и задач практического занятия	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
2	Тема 2. Доктрина информационной безопасности Российской Федерации	4	Изучение вопросов и задач практического занятия	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
3	Тема 3. Определение и основные понятия теории информационной безопасности	4	Изучение вопросов и задач практического занятия	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
4	Тема 4. Методологический базис теории информационной безопасности	4	Изучение вопросов и задач практического занятия	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]

5	Тема 5. Модели систем и процессов защиты информации	4	Изучение вопросов и задач практического занятия	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
6	Тема 6. Унифицированная концепция информационной безопасности	4	Изучение вопросов и задач практического занятия	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
7	Тема 7. Угрозы, каналы несанкционированного получения информации, их классификация	4	Изучение вопросов и задач практического занятия	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
8	Тема 8. Определение системы показателей уязвимости информации	4	Изучение вопросов и задач практического занятия	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
9	Тема 9. Методы и модели оценки уязвимости информации	4	Изучение вопросов и задач практического занятия	З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2.	[1-10]
10	Тема10. Определение, анализ и классификация функций защиты информации	4		З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
11	Тема 11. Определение, анализ и классификация задач защиты информации	4		З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
12	Тема 12. Определение, анализ и классификация средств защиты информации	4		З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
13	Тема 13. Определение и общеметодологические принципов архитектурного построения систем	4		З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]

	защиты информации				
14	Тема 14. Методы проектирования систем защиты информации	4		З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
15	Тема 15. Управление процессами функционирования защиты информации	4		З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
16	Тема 16. Особенности защиты в ПЭВМ.	4		З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
17	Тема 17. Особенности защиты информации в сетях ЭВМ.	4		З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
18	Тема 18. Организация и обеспечение работ по безопасности информации	4		З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.1, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2	[1-10]
	ИТОГО	72			

4.1.5 Интерактивные формы занятий

В учебном плане отсутствуют

4.2 Учебно-методическое и информационное обеспечение дисциплины

4.2.1 Литература

1 Галатенко, В. А. Основы информационной безопасности [Электронный ресурс] / В. А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c. — 978-5-94774-821-5. — Режим доступа: http://www.iprbookshop.ru/52209.html

2 Артемов, А. В. Информационная безопасность [Электронный ресурс] : курс лекций / А. В. Артемов. — Электрон. текстовые данные. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/33430.html

3 Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Электрон. текстовые данные. — М. : Евразийский открытый институт, 2012. — 311 c. — 978-5-374-00301-7. — Режим доступа: http://www.iprbookshop.ru/10677.html

4 Голиков, А. М. Основы информационной безопасности [Электронный ресурс] : учебное пособие / А. М. Голиков. — Электрон. текстовые данные. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2007. — 288 c. — 978-5-868889-467-1. — Режим доступа: http://www.iprbookshop.ru/13957.html

5 Горюхина, Е. Ю. Информационная безопасность [Электронный ресурс] : учебное пособие / Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева. — Электрон. текстовые данные. — Воронеж : Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015. — 221 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/72672.html

6 Федин, Ф. О. Информационная безопасность [Электронный ресурс] : учебное пособие / Ф. О. Федин, В. П. Офицеров, Ф. Ф. Федин. — Электрон. текстовые данные. — М. : Московский городской педагогический университет, 2011. — 260 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/26486.html

7. Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 c. — ISBN 978-5-4497-0863-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/101992.html

8. Основы национальной безопасности: учебно-методическое пособие / составители С. Ю. Махов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2019. — 88 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/95409.html

9. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Москва, Вологда : Инфра-Инженерия, 2020. — 692 c. — ISBN 978-5-9729-0486-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/98349.html

10. Костин, В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 31 c. — ISBN 978-5-906953-53-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/98200.html

4.2.2 Современные профессиональные базы данных и информационные справочные системы

4.2.3 Нормативные документы

4.2.4 Интернет-ресурсы и другие электронные информационные источники

Общие Интернет-ресурсы, электронные библиотечные системы

1. Электронная библиотека Сочинского государственного университета: база данных. – Сочи, [2017-]. – URL: http://lib.sutr.ru/ (дата обращения: 10.07.2019). – Текст : электронный.

2. ScienceDirect: полнотекстовая база данных / издательство Elsevier. – URL: https://www.sciencedirect.com/ (дата обращения: 10.07.2019). – Режим доступа: для авториз. пользователей. – Текст : электронный.

3. SpringerNature : полнотекстовая база данных / Springer Nature Switzerland AG. Part of Springer Nature. – URL: https://link.springer.com/ (дата обращения: 10.07.2019). – Режим доступа: для авториз. пользователей. – Текст : электронный.

4. IPRbooks : электронно-библиотечная система / ЭБС IPRbooks ; ООО «Ай Пи Эр Медиа», электронное периодическое издание «www.iprbookshop.ru». – Саратов, [2010-]. – URL: http://www.iprbookshop.ru/ (дата обращения: 10.07.2019). – Режим доступа: для авториз. пользователей. – Текст : электронный.

5. Znanium.com : электронно-библиотечная система / ЭБС Znanium.com, ООО «Научно-издательский центр Инфра-М». –Москва, [2011-]. – URL: http://znanium.com/ (дата обращения: 10.07.2019). – Режим доступа: для авториз. пользователей. – Текст : электронный.

6. Национальная электронная библиотека (НЭБ) : Федеральная государственная информационная система / Министерство Культуры РФ. – Москва, [2004-]. – Режим доступа: https://rusneb.ru (дата обращения: 10.07.2019). – Режим доступа: для авториз. пользователей. – Текст : электронный.

7. Polpred.com Обзор СМИ : электронно-библиотечная система / Г. Вачнадзе, ООО «ПОЛПРЕД Справочники». – Москва, [1997-]. – URL https://polpred.com/ (дата обращения: 10.07.2019). – Режим доступа: для авториз. пользователей. – Текст : электронный.

8. КиберЛенинка : научная электронная библиотека открытого доступа / ООО «Итеос». – Электрон. дан. – Москва, [2014-]. – URL: https://cyberleninka.ru/ (дата обращения: 10.07.2019). – Текст : электронный.

9. eLIBRARY.RU : научная электронная библиотека / Компания «Научная электронная библиотека» (eLIBRARY.RU). – Москва, [2000-]. – URL: https://elibrary.ru/ (дата обращения: 10.07.2019). – Режим доступа: для авториз. пользователей. – Текст : электронный

Учебно-методическое и информационное обеспечение дисциплины соответствует библиотечному фонду СГУ

Зав.библиотекой  Мысина Е.С.

подпись

4.3 Формы и содержание текущей и промежуточной аттестации по дисциплине

Текущая аттестация по дисциплине осуществляется в форме устного опроса.

Содержание текущей аттестации по дисциплине раскрывается в фонде оценочных средств, предназначенном для проверки соответствия уровня подготовки по дисциплине.

Оценочные средства по дисциплине содержат:

- перечень вопросов устного опроса;
- перечень вопросов к зачету с оценкой.

Перечень вопросов устного опроса и подготовки к зачету с оценкой:

1. Системный подход к проблеме защиты компьютерной информации в современных АСОД.
2. Стандарт шифрования США DES.
3. Системная классификация средств защиты информации и их эффективности.
4. Шифрование с секретным ключом.
5. Объекты и элементы защиты в современных АСОД.
6. Шифрование с открытым ключом.
7. Определение канал несанкционированного получения информации (КНПИ). Их классификация и характеристики.
8. Симметричные и несимметричные алгоритмы шифрования.
9. Модели защиты информации.
10. Компьютерные вирусы.
11. Формы атак на информацию.
12. Общие принципы построения защищенных ОС.
13. Методы защиты компьютерной информации.
14. Управление безопасностью в защищенных ОС.
15. Функции, задачи защиты информации.

16. Аутентификация субъектов и объектов АСОД.
17. Определение потенциально возможных нарушителей защиты компьютерной информации.
18. Протокол аутентификации KERBEROS.
19. Проектирование систем защиты информации в АСОД.
20. Алгоритм аутентификации в АСОД.
21. Структура и содержание общей модели оценки уязвимости в АСОД.
22. Задача защиты и информации в корпоративных сетях.
23. Аппаратные и программные средства информации.
24. Брандмауэры и их характеристики.
25. Организационные средства защиты информации.
26. Механизмы защиты информации в трактах передачи данных и в канал связи.
27. Физические средства защиты информации.
28. Управление доступа к данным.
29. Криптографические средства защиты информации.
30. Защита электронной почты.
31. Законодательные средства защиты и морально-этические нормы.
32. Защита IP.
33. Оперативно-диспетчерское управление защитой информации.
34. Защита WEB.
35. Календарно-плановое руководство защитой информации.
36. Защита средств сетевого управления.
37. Планирование защиты информации.
38. Сущность, принципы и методы концептуальной стандартизации в области построения АСОД.
39. Обеспечение повседневной деятельности и службы защиты информации.
40. Требование общегосударственной программы по защите информации.
41. Роль стандартов информационной безопасности и их анализ.
42. Организационно-правовая основа защиты информации в АСОД в России и за рубежом.
43. Руководящие документы Гостехкомиссии России.
44. Анализ некоторых алгоритмов электронной подписи.
45. Американские, Канадские, Федеральные, Европейские и Единые критерии безопасности информационных технологий.
46. Схема и общее содержание основных работ по защите информации.

5 УСЛОВИЯ ОСВОЕНИЯ И РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

5.1 Методические рекомендации обучающимся по изучению дисциплины

Промежуточная аттестация может быть выставлена студенту по результатам текущей аттестации и (или) по результатам федерального интернет тестирования (ФЭПО, интернет тренажеры).

Чтобы освоить учебный материал любой дисциплины, необходимо регулярно посещать все занятия, не опаздывать к началу занятий и обязательно конспектировать учебно-методические рекомендации на практических занятиях. Практические занятия дают знания, которые подчас невозможно найти даже в лучших учебниках. Невозможно дословно законспектировать все, что говорит преподаватель, поэтому следует постараться выделить, записать основные положения, идеи, выводы, понять логику учебного материала, излагаемого преподавателем. При конспектировании желательно использовать понятные для конспектирующего студента сокращения и условные знаки.

Во время практических занятий необходимо проявлять продуктивную активность, отвечать на вопросы преподавателя, показывать способность самостоятельного мышления.

С целью более глубокого освоения темы дисциплины, конспекты следует дополнять и дорабатывать для систематизации и обобщения, используя информацию, полученную во время практического занятия, а также рекомендуемую учебно-методическую литературу и Интернет-

ресурсы. Аналогичную работу необходимо выполнять и при разработке тем дисциплины, предлагаемых для самостоятельного изучения.

Рекомендуется выработать в себе привычку просматривать, перечитывать перед новым практическим занятием текст предыдущего занятия.

Если возникают вопросы, обязательно обращайтесь за консультациями к преподавателю после занятия (или во время занятия при его вопросе к студентам: «Все понятно?») за разъяснениями, четко формулируя имеющийся «пробел» в понимании учебного материала.

Практические задания следует выполнять четко в соответствии с планом, методическими рекомендациями и алгоритмами, сформулированными преподавателем.

При подготовке к промежуточной аттестации необходимо получить у преподавателя перечень дидактических единиц базы знаний и типовое содержание заданий по проверке навыков и практических умений по дисциплине.

5.2 Организация самостоятельной работы студента по дисциплине

Самостоятельная работа студентов включает проработку практических занятий, чтение обязательной и дополнительной литературы, знакомство с содержанием электронных источников, анализ ситуаций, разработку моделей, выполнение практических заданий.

Для обеспечения выполнения самостоятельной работы по дисциплине «Информационная безопасность» студенты обеспечиваются:

- учебной, учебно-методической и справочной литературой;
- раздаточным справочно-методическим материалом, включающим алгоритмические схемы решения задач;
- доступом к средствам вычислительной техники и необходимому программному обеспечению.

5.3 Особенности преподавания дисциплины

Проведение всех видов занятий (лекционные, практические, лабораторные и т.д.) при преподавании дисциплины, проведение консультаций, промежуточная и текущая аттестация возможна с применения электронного обучения и дистанционных образовательных технологий.

Преподавание дисциплины ведется с применением элементов следующих видов образовательных технологий: информационные технологии: использование электронных образовательных ресурсов (электронный конспект, размещенный в локальной сети) при подготовке к практическим и самостоятельным занятиям.

Проблемное обучение: стимулирование студентов к самостоятельному приобретению знаний, необходимых для решения конкретных задач при выполнении домашних и практических работ.

Контекстное обучение: мотивация студентов к усвоению знаний путем выявления связей между конкретным знанием и его применением для решения профессиональных задач при выполнении домашних заданий.

Обучение на основе опыта: активизация познавательной деятельности студента за счет ассоциации и собственного опыта с предметом изучения при выполнении домашних заданий.

Междисциплинарное обучение: использование знаний из разных областей, их группировка и концентрация в контексте решаемой задачи на практических занятиях.

5.4 Материально-техническое обеспечение дисциплины

1. При организации занятий, текущей и промежуточной аттестации с применением электронного обучения и дистанционных образовательных технологий используются различные электронные образовательные ресурсы и онлайн сервисы, в том числе: Skype, Zoom, Big Blue Button, Moodle, WhatsApp.
2. Аудитории для проведения занятий лекционного типа
3. Презентационный комплект (ноутбук, проектор, экран)

4. Аудитории для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (Компьютеры 14шт. с возможностью подключения к сети «Интернет»)

5. Аудитории для самостоятельной работы (Компьютерный класс - 15 компьютеров. Локальная сеть. Подключение к сети Интернет. Электронные базы данных)

Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства*:*

1. Microsoft Windows 7 Professional, 8 Pro, 8.1 Pro, 10 Pro
Лицензионный договор №03181000468150000030-0003440-01 (06/16гпд) от 13.01.2016.
Срок действия – бессрочная лицензия.
Лицензионный договор №ВК01492/2892 (163/16д) от 05.04.2016.
Срок действия – 05.04.2020.
2. Microsoft Office Professional Plus 2007, 2010, 2013, 2016.
Состав продукта:
Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Outlook, Microsoft Publisher, Microsoft Access, Microsoft OneNote, Microsoft InfoPath.
Лицензионный договор №03181000468150000029-003440-01 (05/16-гпд) от 13.01.2016.
Срок действия – бессрочная лицензия.
3. Антивирусное программного обеспечение Kaspersky Security. Отечественное ПО.
Лицензионный договор №ВК (ИКЗ 181232005119923200100100070010000000) № 101/18д от 02.03.2018 г.
Срок действия обновлений – по 30.03.2019.
Лицензионный договор №04-S00310L (92/19д) от 01.03.2019 г.
Срок действия обновлений – по 28.03.2020 г.
4. Архиватор 7-zip. Свободно распространяемое ПО.
Бесплатное программное обеспечение. Срок действия – бессрочная лицензия.
5. Adobe Reader. Свободно распространяемое ПО.
Бесплатное программное обеспечение. Срок действия – бессрочная лицензия.

5.5. Методическое обеспечение образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья

Условия организации и содержание обучения и контроля знаний инвалидов и обучающихся с ОВЗ по дисциплине определяются программой дисциплины, адаптированной при необходимости для обучения указанных обучающихся.

Организация обучения, текущей и промежуточной аттестации студентов-инвалидов и студентов с ОВЗ осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Исходя из психофизического развития и состояния здоровья студентов-инвалидов и студентов с ОВЗ, организуются занятия совместно с другими обучающимися в общих группах, используя социально-активные и рефлексивные методы обучения создания комфортного психологического климата в студенческой группе или, при соответствующем заявлении такого обучающегося, по индивидуальной программе, которая является модифицированным вариантом основной рабочей программы дисциплины. При этом содержание программы дисциплины не изменяется. Изменяются, как правило, формы обучения и контроля знаний, образовательные технологии и дидактические материалы.

Обучение студентов-инвалидов и студентов с ОВЗ также может осуществляться индивидуально и/или с применением дистанционных технологий.

Дистанционное обучение обеспечивает возможность коммуникаций с преподавателем, а также с другими обучаемыми посредством вебинаров (например, с использованием программы

Skype), что способствует сплочению группы, направляет учебную группу на совместную работу, обсуждение, принятие группового решения.

В учебном процессе для повышения уровня восприятия и переработки учебной информации студентов-инвалидов и студентов с ОВЗ применяются мультимедийные и специализированные технические средства приема-передачи учебной информации в доступных формах для студентов с различными нарушениями, обеспечивается выпуск альтернативных форматов печатных материалов (крупный шрифт), электронных образовательных ресурсов в формах, адаптированных к ограничениям здоровья обучающихся, наличие необходимого материально-технического оснащения.

Подбор и разработка учебных материалов производятся преподавателем с учетом того, чтобы студенты с нарушениями слуха получали информацию визуально, с нарушениями зрения – аудиально (например, с использованием программ-синтезаторов речи).

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся инвалидов и лиц с ОВЗ фонд оценочных средств по дисциплине, позволяющий оценить достижение ими результатов обучения и уровень сформированности компетенций, предусмотренных учебным планом и рабочей программой дисциплины, адаптируется для обучающихся инвалидов и лиц с ограниченными возможностями здоровья с учетом индивидуальных психофизиологических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости обучающимся предоставляется дополнительное время для подготовки ответа при прохождении аттестации.

Приложение к рабочей программе дисциплины
44.03.05 Педагогическое образование с двумя профилями подготовки

Бакалавриат

Профиль «Математика и информатика»

АННОТАЦИЯ

рабочей программы дисциплины
Информационная безопасность
дисциплина Блока 1 в вариативной части
очная форма обучения

Составитель аннотации – Симаворян С.Ж., доцент каф. ПМиИ

Общая трудоемкость дисциплины (ЗЕТ / час.)	3/108
Цель изучения дисциплины	Освоение основ «Информационной информации» для студентов по направлению подготовки 44.04.05 «Педагогическое образование с двумя профилями подготовки»
Содержание дисциплины	Тема 1. Нормативно-правовые акты информационной безопасности в Российской Федерации Тема 2. Доктрина информационной безопасности Российской Федерации Тема 3. Определение и основные понятия теории информационной безопасности Тема 4. Методологический базис теории информационной безопасности Тема 5. Модели систем и процессов защиты информации Тема 6. Унифицированная концепция информационной безопасности Тема 7. Угрозы, каналы несанкционированного получения информации, их классификация Тема 8. Определение системы показателей уязвимости информации Тема 9. Методы и модели оценки уязвимости информации Тема10. Определение, анализ и классификация функций защиты информации Тема 11. Определение, анализ и классификация задач защиты информации Тема 12. Определение, анализ и классификация средств защиты информации Тема 13. Определение и общеметодологические принципов архитектурного построения систем защиты информации Тема 14. Методы проектирования систем защиты информации Тема 15. Управление процессами функционирования защиты информации Тема 16. Особенности защиты в ПЭВМ. Тема 17. Особенности защиты информации в сетях ЭВМ. Тема 18. Организация и обеспечение работ по безопасности информации
Формируемые компетенции (коды)	ПКУВ-2 Способен разрабатывать методику обучения отдельным разделам информатики и программирования с применением компьютерных технологий
Коды и наименование индикатора достижения компетенции	ПКУВ-2.1 Анализирует и разрабатывает альтернативные варианты методики обучения информатике с применением компьютерных технологий ПКУВ-2.2 Использует компьютерные технологии для разработки информационных моделей реальных процессов окружающего мира

Наименование дисциплин, необходимых для освоения данной дисциплины	Б1.В.02 Программирование Б1.В.06 Компьютерное моделирование Б1.В.07 Программное обеспечение ЭВМ и практикум по решению задач на ЭВМ Б1.В.08 Компьютерные сети Б1.В.ДВ.02.01 Основы кибербезопасности
Образовательные технологии	Практические занятия
Формы текущего контроля успеваемости	Текущая аттестация по дисциплине осуществляется в форме устного опроса
Форма промежуточной аттестации	ЗачётО

Зав. кафедрой Прикладной математики и информатики Макарова И.Л.