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

СОГЛАСОВАНО
Декан ФИИЦТ
_____ А.Н. Волков
«10» 04 2023 г.

УТВЕРЖДАЮ
Проректор по УРиКОД
_____ А.В. Иваненко
«10» 04 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Шифр и направление подготовки 09.03.03 Прикладная информатика

Квалификация (степень) выпускника бакалавр

Профиль подготовки бакалавра «Цифровые технологии в аналитической деятельности»

Форма обучения Очная

Выпускающая кафедра Информационных технологий и математики

Кафедра-разработчик рабочей программы Информационных технологий и математики

Семестр	Трудоем-кость (час./зет.)	Лекцион. занятий, (час.)	Практич. занятий, (час.)	Лаборат. занятий, (час.)	СРС, (час.)	КР/КП (час.)	Форма промежуточного контроля (экз./зачет)
4	**108/3**	**36**	**-**	**18**	**27**	**-**	**Экзамен (27)**
ИТОГО	**108/3**	**36**	**-**	**18**	**27**	**-**	**Экзамен (27)**

Сочи 2023 г.

Лист согласования рабочей программы дисциплины «Информационная безопасность»

Рабочую программу составил:
Симаворян С.Ж., к.т.н., доцент кафедры Информационных технологий и математики

РАБОЧАЯ ПРОГРАММА РАССМОТРЕНА И ОДОБРЕНА

Заведующий кафедрой _____ Копырин А.С.

Учебно-методическое и информационное обеспечение дисциплины соответствует библиотечному фонду СГУ:

Директор НОБ _____ Онищенко Е.В.

Структура рабочей программы соответствует предъявляемым требованиям.

Отдел качества образования и методического обеспечения _____

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ РПД

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

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

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 09.03.03 «Прикладная информатика»

Задачи дисциплины:

- овладение основными понятиями информационной безопасности и методами защиты данных, необходимыми для применения в профессиональной работе, для продолжения образования;
- 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» относится к Блоку 1. Дисциплины (модули). Обязательная часть

Таблица 1 - Дисциплины, участвующие в формировании компетенции

№ п/п	Наименование компетенции	**Дисциплины, участвующие в формировании компетенции** (перечисляются дисциплины, практики, кроме ГЭ, ВКР)
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Теория вероятностей и математическая статистика Экономика фирмы (предприятия) Информационные системы и технологии Алгоритмизация и программирование Вычислительные системы, сети и телекоммуникации Ознакомительная практика Технологическая (проектно-технологическая) практика
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	Менеджмент Информационные системы и технологии Алгоритмизация и программирование Вычислительные системы, сети и телекоммуникации Проектирование информационных систем Ознакомительная практика Технологическая (проектно-технологическая) практика

3 ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Таблица 2 Компетенции и индикаторы их достижения

Компетенции и индикаторы их достижения		Результат обучения по дисциплине(показатели освоения компетенций)
Код и наименование компетенции	Код и наименование индикатора достижения компетенции	
Общепрофессиональные компетенции		
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-	ОПК-3.1 Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	З.1-ОПК-3.1 Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности.
	ОПК-3.2 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической	У.1-ОПК-3.2 Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры

коммуникационных технологий и с учетом основных требований информационной безопасности;	культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	ОПК-3.3 Применяет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Н.1-ОПК-3.3 Владеть навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно- исследовательской работе с учетом требований информационной безопасности.
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1 Демонстрирует знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы	З.1-ОПК-4.1 Знать основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
	ОПК-4.2 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	У.1-ОПК-4.2 Уметь применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
	ОПК-4.3 Применяет навыки составления технической документации на различных этапах жизненного цикла информационной системы	Н.1-ОПК-4.3 Владеть навыками составления технической документации на различных этапах жизненного цикла информационной системы.

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Тематический план дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов

Таблица 3 – Распределение фонда времени по темам

№ раздела, темы	Наименование темы дисциплины	ОФО				
		Всего часов	Виды учебной нагрузки и их трудоемкость, часы			
			Лекции	Практические занятия	Лабораторные работы	СРС
1	Тема 1. Нормативно-правовые акты информационной безопасности в Российской Федерации	3	2	-	-	1
2	Тема 2. Доктрина информационной безопасности Российской Федерации	6	2	-	2*	2
3	Тема 3. Определение и основные понятия теории информационной безопасности	3	2	-	-	1
4	Тема 4. Методологический базис теории информационной безопасности	6	2	-	2*	2
5	Тема 5. Модели систем и процессов защиты информации	3	2	-	-	1
6	Тема 6. Унифицированная концепция информационной безопасности	6	2	-	2*	2
7	Тема 7. Угрозы, каналы несанкционированного получения информации, их классификация	3	2	-	-	1
8	Тема 8. Определение системы показателей уязвимости информации	6	2	-	2*	2
9	Тема 9. Методы и модели оценки уязвимости информации	5	2	-	2*	1

10	Тема10. Определение, анализ и классификация функций защиты информации	4	2	-	-	2
11	Тема 11. Определение, анализ и классификация задач защиты информации	3	2	-	-	1
12	Тема 12. Определение, анализ и классификация средств защиты информации	6	2	-	2*	2
13	Тема 13. Определение и общеметодологические принципов архитектурного построения систем защиты информации	3	2	-	-	1
14	Тема 14. Методы проектирования систем защиты информации	6	2	-	2*	2
15	Тема 15. Управление процессами функционирования защиты информации	3	2	-	-	1
16	Тема 16. Особенности защиты в ПЭВМ.	6	2	-	2*	2
17	Тема 17. Особенности защиты информации в сетях ЭВМ.	3	2	-	-	1
18	Тема 18. Организация и обеспечение работ по безопасности информации	6	2	-	2*	2
	Экзамен	27	-	-	-	-
	ИТОГО	108	36	-	18	27

* ***Лабораторное занятие проводиться в форме практической подготовки.***

4.1.1 Лекционные занятия

№ п/п	Наименование дисциплины	Краткое содержание
1	Тема 1. Нормативно-правовые акты информационной безопасности в Российской Федерации	Что такое законодательный уровень информационной безопасности и почему он важен? Обзор российского законодательства в области информационной безопасности
2	Тема 2. Доктрина информационной безопасности Российской Федерации	Сущность и содержание Доктрины информационной безопасности Российской Федерации
3	Тема 3. Определение и основные понятия теории информационной безопасности	Понятие информационной безопасности Основные составляющие информационной безопасности Важность и сложность проблемы информационной безопасности
4	Тема 4. Методологический базис теории информационной безопасности	Цели и особенности моделирования систем защиты информации Классификация и общий анализ моделирования систем защиты информации
5	Тема 5. Модели систем и процессов защиты информации	Общая модель процесса защиты Модели общей оценки угроз информации
6	Тема 6. Унифицированная концепция информационной безопасности	Системно-концептуальный подход к моделированию систем защиты информации
7	Тема 7. Угрозы, каналы несанкционированного получения информации, их классификация	Наиболее распространённые угрозы доступности Некоторые примеры угроз доступности
8	Тема 8. Определение системы показателей уязвимости информации	Система показателей уязвимости информации
9	Тема 9. Методы и модели оценки уязвимости информации	Аналитическая модель оценки защищенности информации Статистическая модель оценки защищенности информации
10	Тема10. Определение, анализ и классификация функций защиты информации	Определение, назначение и анализ понятия функций защиты информации Обоснование полного множества функций защиты информации Методология выбора функций защиты информации
11	Тема 11. Определение, анализ и	Определение, назначение и анализ и понятия задач защиты

	классификация задач защиты информации	информации Обоснование полного множества задач защиты информации Классификация задач защиты информации Методология выбора задач защиты информации
12	Тема 12. Определение, анализ и классификация средств защиты информации	Определение, анализ понятия средств защиты информации Обоснование полного множества средств защиты информации Классификация средств защиты информации Методология выбора средств защиты информации
13	Тема 13. Определение и общеметодологические принципов архитектурного построения систем защиты информации	Система защиты информации и общеметодологические принципы ее построения Основы архитектурного построения систем защиты информации
14	Тема 14. Методы проектирования систем защиты информации	Классификация и анализ постановок задач проектирования систем защиты информации Последовательность и общее содержание проектирования систем защиты информации
15	Тема 15. Управление процессами функционирования защиты информации	Общая организация управления защитой информации Технология планирования защиты информации, основные макропроцессы управления защитой информации
16	Тема 16. Особенности защиты в ПЭВМ.	Особенности защиты информации в персональных ЭВМ Угрозы информации в персональных ЭВМ Обеспечение целостности информации в ПЭВМ
17	Тема 17. Особенности защиты информации в сетях ЭВМ.	Основные положения концепции построения и использования сетей ЭВМ Цели, функции и задачи защиты информации в сетях ЭВМ
18	Тема 18. Организация и обеспечение работ по безопасности информации	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

4.1.2 Практические занятия

Учебным планом не предусмотрены

4.1.3 Лабораторные занятия

№ п/п	Наименование дисциплины	Краткое содержание
1	Тема 2. Доктрина информационной безопасности Российской Федерации	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №1.*** Проводится обзор российского законодательства в области информационной безопасности. Проводится анализ сущности и содержания Доктрины информационной безопасности Российской Федерации
2	Тема 4. Методологический базис теории информационной безопасности	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №2.*** Изучаются основные понятия информационной безопасности, выделяются основные составляющие информационной безопасности.Определяются основные цели и особенности моделирования систем защиты информации. Проводится классификация и общий анализ моделирования систем защиты информации для конкретного объекта по заданию преподавателя.
3	Тема 6. Унифицированная концепция информационной безопасности	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №3.*** По заданию преподавателя на разных конкретных объектах строятся возможные общие модели

		процесса защиты информации. Строятся модели общей оценки угроз информации, проводится анализ и их сравнение с точки зрения системно-концептуального подхода к моделированию систем защиты информации.
4	Тема 8. Определение системы показателей уязвимости информации	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №4.*** По заданию преподавателя для конкретных объектов определяются угрозы и каналы несанкционированного получения информации. Проводится системный анализ показателей уязвимости информации.
5	Тема 9. Методы и модели оценки уязвимости информации	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №5.*** Проводятся рассчеты по аналитической модели оценки защищённости информации, по статистической модели оценки защищенности информации.
6	Тема 12. Определение, анализ и классификация средств защиты информации	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №6.*** Определяются задачи защиты информации, проводится обоснование полного множества задач защиты информации. Определяются средства защиты информации, проводится обоснование полного множества средств защиты информации.
7	Тема 14. Методы проектирования систем защиты информации	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №7.*** Для конкретного примера разрабатывается архитектура системы защиты информации на основе последовательности и общего содержания алгоритма проектирования систем защиты информации
8	Тема 16. Особенности защиты в ПЭВМ.	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №8.*** На конкретном примере для сети персональных ЭВМ разрабатываются: общая организация управления защитой информации, технология планирования защиты информации, определяются основные макропроцессы управления защитой информации, фиксируются особенности защиты информации в персональных ЭВМ, определяются угрозы, каналы утечки информации, функции, задачи и средства защиты информации.
9	Тема 18. Организация и обеспечение работ по безопасности информации	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №9.*** Формулируются цели, функции и задачи защиты информации в сетях ЭВМ, перечень и общее содержание основных вопросов организации и обеспечения работ по защите информации. Разрабатывается структура и функции органов защиты информации.. Сравниваются стандарты и спецификации в области информационной безопасности.

4.1.4 Самостоятельная работа студента

№ п/п	Наименование дисциплины	Вид СРС
1	Тема 1. Нормативно-правовые акты информационной безопасности в Российской Федерации	Изучение вопросов устного опроса, домашнего задания
2	Тема 2. Доктрина информационной безопасности Российской Федерации	Изучение вопросов устного опроса, домашнего задания и задач лабораторного занятия

3	Тема 3. Определение и основные понятия теории информационной безопасности	Изучение вопросов устного опроса, домашнего задания
4	Тема 4. Методологический базис теории информационной безопасности	Изучение вопросов устного опроса, домашнего задания и задач лабораторного занятия
5	Тема 5. Модели систем и процессов защиты информации	Изучение вопросов устного опроса, домашнего задания
6	Тема 6. Унифицированная концепция информационной безопасности	Изучение вопросов устного опроса, домашнего задания и задач лабораторного занятия
7	Тема 7. Угрозы, каналы несанкционированного получения информации, их классификация	Изучение вопросов устного опроса, домашнего задания
8	Тема 8. Определение системы показателей уязвимости информации	Изучение вопросов устного опроса, домашнего задания и задач лабораторного занятия
9	Тема 9. Методы и модели оценки уязвимости информации	Изучение вопросов устного опроса, домашнего задания и задач лабораторного занятия
10	Тема10. Определение, анализ и классификация функций защиты информации	Изучение вопросов устного опроса, домашнего задания
11	Тема 11. Определение, анализ и классификация задач защиты информации	Изучение вопросов устного опроса, домашнего задания
12	Тема 12. Определение, анализ и классификация средств защиты информации	Изучение вопросов лекции и задач лабораторного занятия
13	Тема 13. Определение и общеметодологические принципов архитектурного построения систем защиты информации	Изучение вопросов устного опроса, домашнего задания
14	Тема 14. Методы проектирования систем защиты информации	Изучение вопросов лекции и задач лабораторного занятия
15	Тема 15. Управление процессами функционирования защиты информации	Изучение вопросов устного опроса, домашнего задания
16	Тема 16. Особенности защиты в ПЭВМ.	Изучение вопросов лекции и задач лабораторного занятия
17	Тема 17. Особенности защиты информации в сетях ЭВМ.	Изучение вопросов устного опроса, домашнего задания
18	Тема 18. Организация и обеспечение работ по безопасности информации	Изучение вопросов лекции и задач лабораторного занятия

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 : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-

1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97562.html (дата обращения: 06.04.2023). — Режим доступа: для авторизир. пользователей.
2. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/33430.html (дата обращения: 06.04.2023). — Режим доступа: для авторизир. пользователей.
3. Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/10677.html (дата обращения: 06.04.2023). — Режим доступа: для авторизир. пользователей.
4. Голиков, А. М. Основы информационной безопасности : учебное пособие / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2007. — 288 с. — ISBN 978-5-868889-467-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/13957.html (дата обращения: 06.04.2023). — Режим доступа: для авторизир. пользователей.
5. Горюхина, Е. Ю. Информационная безопасность : учебное пособие / Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева. — Воронеж : Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015. — 221 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/72672.html (дата обращения: 06.04.2023). — Режим доступа: для авторизир. пользователей.
6. Федин, Ф. О. Информационная безопасность : учебное пособие / Ф. О. Федин, В. П. Офицеров, Ф. Ф. Федин. — Москва : Московский городской педагогический университет, 2011. — 260 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/26486.html (дата обращения: 06.04.2023). — Режим доступа: для авторизир. пользователей.
7. Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/101992.html (дата обращения: 06.04.2023). — Режим доступа: для авторизир. пользователей.
8. Основы национальной безопасности : учебно-методическое пособие / составители С. Ю. Махов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2019. — 88 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/95409.html (дата обращения: 06.04.2023). — Режим доступа: для авторизир. пользователей.
9. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Москва, Вологда : Инфра-Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/98349.html (дата обращения: 06.04.2023). — Режим доступа: для авторизир. пользователей.
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 с. — ISBN 978-5-906953-53-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/98200.html (дата обращения: 06.04.2023). — Режим доступа: для авторизир. пользователей.

4.2.2 Современные профессиональные базы данных (СПБД) и информационные справочные системы (ИСС)

Таблица 4 – Перечень современных профессиональных баз данных (СПБД) и информационные справочные системы (ИСС)

№	Наименование СПБД
1.	ScienceDirect : полнотекстовая база данных : сайт / издательство Elsevier. – URL: https://www.sciencedirect.com/ (дата обращения: 06.04.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
2.	SpringerNature : полнотекстовая база данных: сайт / Springer Nature Switzerland AG. Part of Springer Nature. – URL: https://link.springer.com/ (дата обращения: 06.04.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
3.	Электронная библиотека Сочинского государственного университета : база данных. – Сочи, 2017 – . – URL: http://lib.sutr.ru/ (дата обращения: 06.04.2023). – Текст : электронный.
	Наименование ИИС
1.	КонсультантПлюс : справочно-правовая система: сайт / Компания «КонсультантПлюс». – Москва, 1997 – . – Режим доступа: локальная сеть СГУ (дата обращения: 06.04.2023) – Текст : электронный.

4.2.3. Интернет-ресурсы и другие электронные информационные источники

Общие Интернет-ресурсы, электронные библиотечные системы

Таблица 5 – Интернет-ресурсы и электронные информационные источники

№	Наименование Интернет-ресурсов и электронных информационных источников
1.	Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Эр Медиа». – Саратов, 2010 – . – URL: http://www.iprbookshop.ru/ (дата обращения: 06.04.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
2.	Университетская библиотека онлайн : электронно-библиотечная система : сайт / ООО «Нексмедиа». – Москва : Директ-Медиа, 2001 – . – URL: https://biblioclub.ru/index.php?page=book_blocks&view=main_ub (дата обращения: 06.04.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
3.	Образовательная платформа Юрайт : электронно-библиотечная система : сайт / ООО «Электронное издательство Юрайт». – – Москва, 2020 – . – URL: https://urait.ru/catalog/organization/DE41FE6D-0B08-4394-B225-3DD636CCCE1F (дата обращения: 06.04.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
4.	Сервис и туризм : тематическая коллекция / ЭБС Book.ru. – Москва, 2010 –. – URL: https://www.book.ru/cat/578/1 (дата обращения: 06.04.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
5.	Комплект Сочинского государственного университета / Консультант студента : электронно-библиотечная система : сайт / ООО «Политехресурс» – Электронная библиотека технического вуза. – Москва : Политехресурс, 2013 – . – URL: http://www.studentlibrary.ru/catalogue/switch_kit/x2019-138.html (дата обращения: 06.04.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
6.	Сетевая электронная библиотека классических университетов «Лань» : сайт / ООО ЭБС «Лань. – Санкт-Петербург, 2009 – . – URL: https://e.lanbook.com/ (дата обращения: 06.04.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
7.	Национальная электронная библиотека (НЭБ) : Федеральная государственная информационная система : сайт / Министерство культуры РФ. – Москва, 2004 – . – Режим доступа: https://rusneb.ru (дата обращения: 06.04.2023). – Режим доступа: локальная сеть СГУ. – Текст : электронный.

8.	Polpred.com Обзор СМИ : электронно-библиотечная система : сайт / Г. Вачнадзе, ООО «ПОЛПРЕД Справочники». – Москва, 1997 – . – URL https://polpred.com/ (дата обращения: 06.04.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
9.	eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru/ (дата обращения: 06.04.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
10.	КиберЛенинка : научная электронная библиотека открытого доступа : сайт. – Москва, 2014 –. – URL: https://cyberleninka.ru// (дата обращения: 06.04.2023). – Текст : электронный.

4.3 Формы и содержание текущей и промежуточной аттестации по дисциплине

Для оценки сформированности компетенций разрабатываются оценочные средства по дисциплине.

Форма и содержание текущей и промежуточной аттестации по дисциплине раскрывается в фонде оценочных средств, который является отдельным документом.

Оценочные средства по дисциплине содержат:

материалы для текущего контроля оценки знаний по дисциплине;

материалы для промежуточного контроля оценки знаний по дисциплине;

критерии оценивания;

шкалы оценивания.

Перечень вопросов подготовки к экзамену:

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. Задачи 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.

Примерная шкала оценивания ответов обучающегося при проведении промежуточной аттестации по дисциплине (Экзамен):

Оценка **«отлично»** выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, чётко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приёмами выполнения практических задач, правильно и точно подтверждает сделанные при решении практических заданий выводы соответствующими нормативными документами, точно и правильно производит расчет показателей, демонстрирует полноту и правильность раскрытых процедур и действий в предложенном практическом задании.

Оценка **«хорошо»** выставляется обучающемуся, если он твёрдо 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 приёмами их выполнения.

Оценка **«удовлетворительно»** выставляется обучающемуся, если он 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, затрудняется подтвердить сделанные при решении практических заданий выводы хотя бы одним нормативным документом, допускает ошибки при проведении расчетов показателей, неточно использует основные процедуры и действия в предложенном практическом заданий.

Оценка **«неудовлетворительно»** выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

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 лабораторного 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 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. Комплект электронных презентаций/ слайдов, аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук).
2. Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет, рабочие места обучающихся, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.
3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

- Microsoft Windows.
- Microsoft Office.
- Бесплатное ПО, свободно распространяемое: LibreOffice.

При организации занятий, текущей и промежуточной аттестации с применением электронного обучения и дистанционных образовательных технологий используются различные электронные образовательные ресурсы и онлайн сервисы, входящие в состав ЭИОС СГУ.

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
09.03.03 Прикладная информатика

Бакалавриат

Профиль: «Цифровые технологии в аналитической деятельности»

АННОТАЦИЯ
рабочей программы дисциплины
«Информационная безопасность»
очная форма обучения

Общая трудоемкость дисциплины (ЗЕТ / час.)	3/108
Цель изучения дисциплины	Освоение основ информационной безопасности для студентов по направлению подготовки 09.03.03 «Прикладная информатика»
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)	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью.

Коды и наименование индикатора достижения компетенции	ОПК-3.1 Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3.2 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3.3 Применяет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно- исследовательской работе с учетом требований информационной безопасности ОПК-4.1 Демонстрирует знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы ОПК-4.2 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы ОПК-4.3 Применяет навыки составления технической документации на различных этапах жизненного цикла информационной системы
Наименование дисциплин, необходимых для освоения данной дисциплины	Теория вероятностей и математическая статистика Экономика фирмы (предприятия) Информационные системы и технологии Алгоритмизация и программирование Вычислительные системы, сети и телекоммуникации Менеджмент Проектирование информационных систем Ознакомительная практика Технологическая (проектно-технологическая) практика
Образовательные технологии	Лекции, лабораторные работы, самостоятельная работа студентов
Форма промежуточной аттестации	Экзамен