

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

СОГЛАСОВАНО
Декан факультета
Волков А.Н.
« 30 » августа 2021 г.

УТВЕРЖДАЮ
Проректор по УРиКОД
В.П. Ермакова
« 30 » августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность

Шифр и направление подготовки 09.03.03 Прикладная информатика

Квалификация (степень) выпускника бакалавр

Профиль подготовки бакалавра Прикладная информатика в экономике

Форма обучения Очная

Выпускающая кафедра кафедра информационных технологий

Кафедра-разработчик рабочей программы кафедра прикладной математики и информатики

Год набора 2021

Семестр	Трудоем- кость (час./зет.)	Лекцион. занятий, (час.)	Практич. занятий, (час.)	Лаборат. занятий, (час.)	СРС, (час.)	КР/КП	Форма промежуточного контроля (экз./зачет)
4	108/3	36	0	18	27	-	Экзамен(27)
ИТОГО	108/3	36	0	18	27		Экзамен(27)

Сочи 2021 г.

Лист согласования рабочей программы дисциплины Информационная безопасность

Рабочую программу составили:


_____ Симаворян С.Ж.

РАБОЧАЯ ПРОГРАММА РАССМОТРЕНА И ОДОБРЕНА

Заведующий кафедрой



подпись

Макарова И.Л.

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

Директор НОБ



подпись

Мысина Е.С.

Структура рабочей программы соответствует предъявляемым требованиям

Отдел качества образования и
методического обеспечения



подпись

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ РПД

Рабочая программа переутверждена на 2022/2023 учебный год, протокол № 1 заседания кафедры от «30» августа 2022 года.

В программу внесены дополнения и(или) изменения.

Внесены изменения в пункт 4.2.1, актуализирована литература

Заведующий кафедрой


Подпись

Копырин А.С.

ФИО

Рабочая программа переутверждена на 20__/20__ учебный год, протокол №__ заседания кафедры от «__» _____ 20__ года.

В программу внесены дополнения и(или) изменения.

Заведующий кафедрой

Подпись

ФИО

Рабочая программа переутверждена на 20__/20__ учебный год, протокол №__ заседания кафедры от «__» _____ 20__ года.

В программу внесены дополнения и(или) изменения.

Заведующий кафедрой

Подпись

ФИО

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 в экономике»

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 относится к обязательной части учебного плана

Таблица 1 - Дисциплины, участвующие в формировании компетенции

Код и наименование компетенции	Дисциплины, участвующие в формировании компетенции
Общепрофессиональные компетенции	
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;	Алгоритмизация и программирование Вычислительные системы, сети и телекоммуникации Теория вероятностей и математическая статистика Ознакомительная практика Технологическая (проектно-технологическая) практика Экономика фирмы (предприятия) Информационные системы и технологии
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;	Технологическая (проектно-технологическая) практика Алгоритмизация и программирование Вычислительные системы, сети и телекоммуникации Проектирование информационных систем Ознакомительная практика Информационные системы и технологии Менеджмент

3 ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК – универсальные компетенции;

ОПК – общепрофессиональные компетенции;

ПКУВ – профессиональные компетенции установленные вузом.

Таблица 2 - Компетенции и индикаторы их достижения

Компетенции и индикаторы их достижения		В результате изучения дисциплины обучающиеся должны:
Код и наименование компетенции	Код и наименование индикатора достижения компетенции	
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-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.	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 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-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.	Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
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-3.3 Применяет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	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.	Знать основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.

Компетенции и индикаторы их достижения		В результате изучения дисциплины обучающиеся должны:
Код и наименование компетенции	Код и наименование индикатора достижения компетенции	
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;	ОПК-4.2 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Уметь применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;	ОПК-4.3 Применяет навыки составления технической документации на различных этапах жизненного цикла информационной системы.	Владеть навыками составления технической документации на различных этапах жизненного цикла информационной системы.

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Тематический план дисциплины

№ раздела, темы	Наименование модуля (раздела, темы) дисциплины	Всего часов	Виды учебной нагрузки и их трудоемкость, часы			СРС
			Контактная работа			
			Лекции	Практические занятия	Лабораторные работы	
1	Тема 1. Нормативно-правовые акты информационной безопасности в Российской Федерации	5	2	0	1	2
2	Тема 2. Доктрина информационной безопасности Российской Федерации	4	2	0	1	1
3	Тема 3. Определение и основные понятия теории информационной безопасности	5	2	0	1	2
4	Тема 4. Методологический базис теории информационной безопасности	4	2	0	1	1
5	Тема 5. Модели систем и процессов защиты информации	5	2	0	1	2
6	Тема 6. Унифицированная концепция информационной безопасности	4	2	0	1	1
7	Тема 7. Угрозы, каналы несанкционированного получения информации, их классификация	5	2	0	1	2
8	Тема 8. Определение системы показателей уязвимости информации	4	2	0	1	1
9	Тема 9. Методы и модели оценки уязвимости информации	5	2	0	1	2
10	Тема 10. Определение, анализ и классификация функций защиты информации	4	2	0	1	1
11	Тема 11. Определение, анализ и классификация задач защиты информации	5	2	0	1	2

12	Тема 12. Определение, анализ и классификация средств защиты информации	4	2	0	1	1
13	Тема 13. Определение и общеметодологические принципы архитектурного построения систем защиты информации	5	2	0	1	2
14	Тема 14. Методы проектирования систем защиты информации	4	2	0	1	1
15	Тема 15. Управление процессами функционирования систем защиты информации	5	2	0	1	2
16	Тема 16. Особенности защиты в ПЭВМ.	4	2	0	1	1
17	Тема 17. Особенности защиты информации в сетях ЭВМ.	5	2	0	1	2
18	Тема 18. Организация и обеспечение работ по безопасности информации	4	2	0	1	1
	Экзамен	27	0	0	0	0
	ИТОГО	108	36	0	18	27

4.1.1 Лекционные занятия

№ п/п	Наименование темы 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 распространенные 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	Тема 10. Определение, анализ и классификация функций защиты информации	<p>Определение, назначение и анализ понятия функций защиты информации</p> <p>Обоснование полного множества функций защиты информации</p> <p>Методология выбора функций защиты информации</p>
11	Тема 11. Определение, анализ и классификация задач защиты информации	<p>Определение, назначение и анализ и понятия задач защиты информации</p> <p>Обоснование полного множества задач защиты информации</p> <p>Классификация задач защиты информации</p> <p>Методология выбора задач защиты информации</p>
12	Тема 12. Определение, анализ и классификация средств защиты информации	<p>Определение, анализ понятия средств защиты информации</p> <p>Обоснование полного множества средств защиты информации</p> <p>Классификация средств защиты информации</p> <p>Методология выбора средств защиты информации</p>
13	Тема 13. Определение и общеметодологические принципы архитектурного построения систем защиты информации	<p>Система защиты информации и общеметодологические принципы ее построения</p> <p>Основы архитектурного построения систем защиты информации</p>
14	Тема 14. Методы проектирования систем защиты информации	<p>Классификация и анализ постановок задач проектирования систем защиты информации</p> <p>Последовательность и общее содержание проектирования систем защиты информации</p>
15	Тема 15. Управление процессами функционирования защиты информации	<p>Общая организация управления защитой информации</p> <p>Технология планирования защиты информации, основные макропроцессы управления защитой информации</p>
16	Тема 16. Особенности защиты в ПЭВМ.	<p>Особенности защиты информации в персональных ЭВМ</p> <p>Угрозы информации в персональных ЭВМ</p> <p>Обеспечение целостности информации в ПЭВМ</p>
17	Тема 17. Особенности защиты информации в сетях ЭВМ.	<p>Основные положения концепции построения и использования сетей ЭВМ</p> <p>Цели, функции и задачи защиты информации в сетях ЭВМ</p>
18	Тема 18. Организация и обеспечение работ по безопасности информации	<p>Перечень и общее содержание основных вопросов организации и обеспечения работ по защите информации</p> <p>Структура и функции органов защиты информации</p> <p>Стандарты и спецификации в области информационной безопасности</p>

4.1.2 Практические занятия

В учебном плане отсутствуют

4.1.3 Лабораторные задания

№ п/п	Наименование темы дисциплины	Краткое содержание
1	Тема 1. Нормативно-правовые акты информационной безопасности в Российской Федерации	Анализ и составление полного перечня литературы по информационно й без-опасности
2	Тема 2. Доктрина информационной безопасности Российской Федерации	Анализ сущности и содержание Док-трины информационной безопасности Российской Федерации, модели его со-вершенствования
3	Тема 3. Определение и основные понятия теории информационной безопасности	Формулирование и решение проблем информационной безопасности
4	Тема 4. Методологический базис теории информационной безопасности	Анализ задач моделирования систем защиты информации
5	Тема 5. Модели систем и процессов защиты информации	Анализ моделей оценки угроз защиты информации
6	Тема 6. Унифицированная концепция информационной безопасности	Анализ сущности системного подход к моделированию систем защиты инфор-мации и его развития
7	Тема 7. Угрозы, каналы несанкционированного получения информации, их классификация	Анализ угроз и каналов несанкциони-рованного получения информации в АСОД, примеры
8	Тема 8. Определение системы показателей уязвимости информации	Анализ системы показателей уязвимо-сти информации
9	Тема 9. Методы и модели оценки уязвимости информации	Расчеты по аналитической модели оценки защищенности информации Расчеты по статистической модели оценки защищенности информации
10	Тема10. Определение, анализ и классификация функций защиты информации	Анализ понятия функций защиты ин-формации Анализ функций защиты информации
11	Тема 11. Определение, анализ и классификация задач защиты информации	Анализ задач защиты информации и оценка их эффективности
12	Тема 12. Определение, анализ и классификация средств защиты информации	Анализ средств защиты информации и оценка их эффективности
13	Тема 13. Определение и общеметодологические принципов архитектурного построения систем защиты информации	Анализ архитектурного построения си-стем защиты информации, примеры
14	Тема 14. Методы проектирования систем защиты информации	Анализ задач проектирования систем защиты информации
15	Тема 15. Управление процессами функционирования защиты информации	Моделирование процессов управления защитой информации
16	Тема 16. Особенности защиты в ПЭВМ.	Анализ задач защиты информации в ПЭВМ
17	Тема 17. Особенности защиты	Анализ целей, функций и задач защиты информации в

	информации в сетях ЭВМ.	сетях ЭВМ
18	Тема 18. Организация и обеспечение работ по безопасности информации	Анализ стандартов и спецификаций в области информационной безопасности

4.1.4 Самостоятельная работа студента

№ п/п	Наименование темы дисциплины	Краткое содержание
1	Тема 1. Нормативно-правовые акты информационной безопасности в Российской Федерации	Изучение вопросов лекции, лабораторного занятия
2	Тема 2. Доктрина информационной безопасности Российской Федерации	Изучение вопросов лекции, лабораторного занятия
3	Тема 3. Определение и основные понятия теории информационной безопасности	Изучение вопросов лекции, лабораторного занятия
4	Тема 4. Методологический базис теории информационной безопасности	Изучение вопросов лекции, лабораторного занятия
5	Тема 5. Модели систем и процессов защиты информации	Изучение вопросов лекции, лабораторного занятия
6	Тема 6. Унифицированная концепция информационной безопасности	Изучение вопросов лекции, лабораторного занятия
7	Тема 7. Угрозы, каналы несанкционированного получения информации, их классификация	Изучение вопросов лекции, лабораторного занятия
8	Тема 8. Определение системы показателей уязвимости информации	Изучение вопросов лекции, лабораторного занятия
9	Тема 9. Методы и модели оценки уязвимости информации	Изучение вопросов лекции, лабораторного занятия
10	Тема 10. Определение, анализ и классификация функций защиты информации	Изучение вопросов лекции, лабораторного занятия
11	Тема 11. Определение, анализ и классификация задач защиты информации	Изучение вопросов лекции, лабораторного занятия
12	Тема 12. Определение, анализ и классификация средств защиты информации	Изучение вопросов лекции, лабораторного занятия
13	Тема 13. Определение и общеметодологические принципы архитектурного построения систем защиты информации	Изучение вопросов лекции, лабораторного занятия
14	Тема 14. Методы проектирования систем защиты информации	Изучение вопросов лекции, лабораторного занятия
15	Тема 15. Управление процессами функционирования защиты информации	Изучение вопросов лекции, лабораторного занятия
16	Тема 16. Особенности защиты в ПЭВМ.	Изучение вопросов лекции, лабораторного занятия
17	Тема 17. Особенности защиты информации в сетях ЭВМ.	Изучение вопросов лекции, лабораторного занятия
18	Тема 18. Организация и обеспечение работ по безопасности информации	Изучение вопросов лекции, лабораторного занятия

4.2.1 Литература

1. Информационная безопасность. Учебник Фомин Д.В. Информационная безопасность : учебник / Фомин Д.В.. — Москва : Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст : электронный // IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/118876.html> (дата обращения: 21.06.2022). — Режим доступа: для авторизир. пользователей. - DOI: <https://doi.org/10.23682/118876>
2. Информационная безопасность в организациях. Учебное пособие Ревнивых А.В. Информационная безопасность в организациях : учебное пособие / Ревнивых А.В.. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/108227.html> (дата обращения: 21.06.2022). — Режим доступа: для авторизир. пользователей
3. Информационная безопасность. Учебно-методическое пособие Моргунов А.В. Информационная безопасность : учебно-методическое пособие / Моргунов А.В.. — Новосибирск : Новосибирский государственный технический университет, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/98708.html> (дата обращения: 21.06.2022). — Режим доступа: для авторизир. пользователей

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. — URL: <https://www.iprbookshop.ru/97562.html> (дата обращения: 04.09.2021). — Режим доступа: для авторизованных пользователей. - Текст : электронный.
2. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. — Ставрополь : Северо-Кавказский федеральный университет, 2016. — 242 с. — URL: <https://www.iprbookshop.ru/62945.html> (дата обращения: 04.09.2021). — Режим доступа: для авторизованных пользователей. - Текст : электронный.
3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — URL: <https://www.iprbookshop.ru/87995.html> (дата обращения: 04.09.2021). — Режим доступа: для авторизованных пользователей. - Текст : электронный.
4. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — DOI: <https://doi.org/10.23682/86938> . - URL: <https://www.iprbookshop.ru/86938.html> (дата обращения: 04.09.2021). — Режим доступа: для авторизованных пользователей . - Текст : электронный.
5. Бекетнова, Ю. М. Международные основы и стандарты информационной безопасности финансово-экономических систем : учебное пособие / Ю. М. Бекетнова, Г. О. Крылов, С. Л. Ларионова. — Москва : Прометей, 2018. — 174 с. — ISBN 978-5-907003-27-9. — URL: <https://www.iprbookshop.ru/94454.html> (дата обращения: 04.09.2021). — Режим доступа: для авторизованных пользователей. - Текст : электронный.
6. Гульятеева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гульятеева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — URL: <https://www.iprbookshop.ru/91640.html> (дата обращения: 04.09.2021). — Режим доступа: для авторизованных пользователей. - Текст : электронный.
7. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: <https://doi.org/10.29039/1761-6>. - ISBN 978-5-369-01761-6. - URL: <https://znanium.com/catalog/product/1189326> (дата обращения: 07.09.2021). — Режим доступа: по подписке. - Текст : электронный.
8. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное

пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - URL: <https://znanium.com/catalog/product/1013711> (дата обращения: 07.09.2021). — Режим доступа: по подписке. - Текст : электронный.

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: 10.07.2021). — Текст : электронный.
2. ScienceDirect : полнотекстовая база данных / издательство Elsevier. — URL: <https://www.sciencedirect.com/> (дата обращения: 10.07.2021). — 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: 10.07.2021). — 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: 10.07.2021). — 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: 10.07.2021). — 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: 10.07.2021). — 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: 10.07.2021). — Текст : электронный.
9. eLIBRARY.RU : научная электронная библиотека / Компания «Научная электронная библиотека» (eLIBRARY.RU). — Москва, [2000-]. — URL: <https://elibrary.ru/> (дата обращения: 10.07.2021). — Режим доступа: для авториз. пользователей. — Текст : электронный

4.3 Текущая и промежуточная 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.

Примерные вопросы для подготовки к промежуточной аттестации:

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

В течение семестра студенты осуществляют учебные действия на лекционных и практических занятиях, усваивают и повторяют основные понятия. Контроль эффективности самостоятельной работы студентов осуществляется путем проверки освоения ими учебных заданий, предусмотренных для самостоятельной отработки.

Преподавание и изучение учебной дисциплины осуществляется в виде лекционных и практических/лабораторных занятий, групповых и индивидуальных форм работы, самостоятельной работы студентов

Методические рекомендации

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 новой лекцией и предстоящим практическим занятием текст предыдущей лекции.

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 студента является ключевой составляющей учебного процесса, которая определяет формирование навыков, умений и знаний, приемов познавательной деятельности и обеспечивает интерес к творческой работе.

Организация самостоятельной работы студентов осуществляется по трем направлениям:

- определение цели, программы, плана задания или работы;
- со стороны преподавателя студенту оказывается помощь в технике изучения материала, подборе литературы для ознакомления и написания курсовой работы, проекта, реферата;
- контроль усвоения знаний, приобретения навыков по дисциплине, оценка выполненной контрольной и курсовой работы, проекта.

Мерами по обеспечению выполнения обучающимися всех видов самостоятельной работы являются (указать при наличии ниже перечисленных пунктов):

- наличие помещений для курсового проектирования, СРС;
- обеспечение средствами вычислительной техники, программное обеспечение;
- наличие раздаточного материала, комплектов индивидуальных заданий, учебно-методических материалов, тем рефератов со списком рекомендуемой литературы, рекомендаций по решению типовых задач, образцов отчетов о выполнении СРС и т.п.;

обеспечение учебно-методической и справочной литературой всех видов самостоятельной работы (например методические указания по выполнению курсовых проектов, работ, РГР, контрольных работ, сборники тестовых заданий, сборники задач по дисциплине).

Каждый обучающийся по дисциплине обеспечен учебно-методической литературой.

5.3 Особенности преподавания дисциплины

Преподавание дисциплины ведется с применением элементов следующих видов образовательных технологий: В целях максимального усвоения дисциплины используются следующие технологии обучения

- Лекция - учебное занятие, составляющее основу теоретического обучения и дающее систематизированные основы научных знаний по дисциплине, раскрывающее состояние и перспективы развития соответствующей области науки и техники, концентрирующее внимание обучающихся на наиболее сложных, узловых вопросах, стимулирующее их познавательную деятельность и способствующее формированию творческого мышления.

- Лабораторная работа - совместная деятельность студентов в группе под руководством лидера, направленная на решение общей задачи путем творческого сложения результатов индивидуальной работы членов команды с делением полномочий и ответственности

- Самостоятельная работа студента, предусматривает выполнение работы - задание, которое требует от студента воспроизведения и/или обработки полученной ранее информации в форме, определяемой преподавателем, и требующей, как правило, творческого подхода

Преподавание дисциплины опирается на современный подход к обучению и ориентируется на внесение в процесс обучения новизны, обусловленной особенностями динамики развития жизни и деятельности, спецификой различных технологий обучения и потребностями личности, общества и государства в выработке у обучаемых социально полезных знаний, убеждений, черт и качеств характера, отношений и опыта поведения

Проведение всех видов занятий при преподавании дисциплины, проведение консультаций, промежуточная и текущая аттестация возможна с применения электронного обучения и дистанционных образовательных технологий

5.4 Материально-техническое обеспечение дисциплины

1. Аудитории для проведения занятий лекционного типа
2. Презентационный комплект (ноутбук, проектор, экран)
3. Аудитории для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (Компьютеры с возможностью подключения к сети «Интернет»)
4. Аудитории для самостоятельной работы (Компьютерный класс. Локальная сеть. Подключение к сети Интернет. Электронные базы данных)

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

1. *Microsoft Windows*
2. *Microsoft Office Professional Plus*
3. *Антивирусное программного обеспечение Kaspersky Security.*
4. *Архиватор 7-zip.*
5. *Adobe Reader.*

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 так же 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 производится 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.

АННОТАЦИЯ

рабочей программы дисциплины

Информационная безопасность

дисциплина обязательной части учебного плана

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 в экономике»
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; Тема 10. 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 принципы 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; ОПК-4
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.
Дисциплины, участвующие в формировании компетенции	Алгоритмизация и программирование Вычислительные системы, сети и телекоммуникации Теория вероятностей и математическая статистика Ознакомительная практика Экономика фирмы (предприятия) Информационные системы и технологии Технологическая (проектно-технологическая) практика Проектирование информационных систем Ознакомительная практика Информационные системы и технологии Менеджмент
Образовательные технологии	Лекция; Лабораторная работа; Самостоятельная работа студента
Форма промежуточной аттестации	Экзамен