

СОГЛАСОВАНО

Декан факультета СПФ

Макиревская Ю.Э.

« 03 » 05 2021 г.

УТВЕРЖДАЮ

Проректор по УРиКОД

В.П. Ерлакова

« 03 » 09 2021 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

Год набора - 2021

Семестр	Трудоемкость (час./лет.)	Лекцион. занятий, (час.)	Практич. занятий, (час.)	Лаборат. занятий, (час.)	СРС, (час.)	КР/КП	Форма промежуточного контроля (экс./зачет)
8	108/3	-	36	-	72	-	Зачет с оценкой
ИТОГО	108/3	-	36	-	72	-	Зачет с оценкой

Сочи 2021 г.

Лист согласования рабочей программы дисциплины «Информационная безопасность»

Рабочую программу составил:

 \_\_\_\_\_  
Доцент кафедры ПМИИ Симаворян С.Ж.

**РАБОЧАЯ ПРОГРАММА РАССМОТРЕНА И ОДОБРЕНА**  
на заседании кафедры Прикладной математики и информатики.  
Протокол № 1 от «31» августа 2021г.

Заведующий кафедрой  \_\_\_\_\_  
подпись Макарова И.Л. ф.и.о.

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

Директор НОБ  \_\_\_\_\_  
подпись Мысина Е.С. ф.и.о.

Структура рабочей программы соответствует предъявляемым требованиям:

Отдел качества образования и  
методического обеспечения  \_\_\_\_\_  
подпись Васильченко В.В. ф.и.о.

## 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

## 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:

- освоение основных понятий информационной безопасности и методов защиты данных, необходимых для применения в профессиональной работе, для продолжения образования;
- изучать актуальные проблемы студентов, формировать качества мышления, необходимые для профессиональной деятельности;
- формировать представления об информационной безопасности как целостной части функциональных информационных систем и сетей, дополнив знаниями качества контроля информационной безопасности для будущей профессиональной деятельности.

## 2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБОЕЙ НАПРАВЛЕНИЯ (СПЕЦИАЛЬНОСТИ)

Дисциплина «Информационная безопасность» является частью, формирующей умениями обязательных отношений.

Таблица 1

Код и наименование дисциплины	Дисциплины, участвующие в формировании компетенции
ПКУВ-2 Способен разрабатывать методику обучения отдельным разделам информативной и программной техники с применением компьютерных технологий	Компьютерное моделирование Прогнозное обеспечение ЭВМ и сетей по решению задач на ЭВМ Компьютерные сети Методический модуль Теория и методика обучения информатике Основы кибербезопасности Системы управления базами данных Проектирование информационных систем Педагогическая (методическая) практика

Таблица 2

Компетенции и индикаторы их достижения	И результат изучения дисциплины обучающиеся должны:
Код и наименование дисциплины	дисциплины обучающиеся должны:

Компетенции и индикаторы их достижения	Код и наименование дисциплины	И результат изучения дисциплины обучающиеся должны:
ПКУВ-2.1 Анализирует и разрабатывает альтернативные варианты методов обучения информатике с применением компьютерных технологий	ПКУВ-2.1	Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информативной безопасности Уметь решать стандартные задачи профессиональной деятельности на основе информативной безопасности Владеть навыками подготовки отчетов, презентаций, сообщений, рефератов, научных докладов, публикаций, и библиографии по научно-педагогической работе с учетом требований информативной безопасности
ПКУВ-2.2 Использует компьютерные технологии для разработки информативных моделей реальных процессов окружающего мира	ПКУВ-2.2	Знать основные стандарты оформления технической документации на различных стадиях жизненного цикла информативной безопасности Уметь применять стандарты оформления технической документации на различных стадиях жизненного цикла информативной безопасности Владеть навыками составления технической документации по завершению информации на различных этапах жизненного цикла информативной безопасности

## 4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Тематический план дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

№	Наименование модуля (раздела, темы) дисциплины	ОФО	
		Э	З
		Э	З

Виды учебных нагрузок в их трудоемкости, часы

4.1.2 Практические задания

№ п/п	Наименование модуля, раздела дисциплины	Краткое описание
1	Тема 1. Нормативно-правовые акты информационной безопасности в Российской Федерации	Это 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 элементы теории информационной безопасности	Понятие информационной безопасности. Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности
4	Тема 4. Методология базис теории информационной безопасности	Цели и особенности моделирования систем защиты информации. Классификация и общий анализ моделирования систем защиты информации. Классификация и общий анализ моделирования систем защиты информации
5	Тема 5. Модели систем и процессов защиты информации	Классификация и общий анализ моделирования систем защиты информации. Классификация и общий анализ моделирования систем защиты информации
6	Тема 6. Унифицированная концепция информационной безопасности	Модели общей оценки угроз информации. Системно-концептуальный подход к моделированию систем защиты информации
7	Тема 7. Угрозы, риски и классификация информации, их классификация	Наиболее распространяемые угрозы доступности. Неотъемлемые угрозы доступности
8	Тема 8. Определение системы индикаторов уязвимости информации	Система показателей уязвимости информации
9	Тема 9. Методы и модели оценки уязвимости информации	Аналитическая модель оценки уязвимости информации. Статистическая модель оценки уязвимости информации
10	Тема 10. Определение, анализ и классификация функций защиты информации	Определение, назначение и анализ индикаторов функций защиты информации. Классификация функций защиты информации. Классификация функций защиты информации
11	Тема 11. Определение, анализ и классификация средств защиты информации	Методология выбора функций защиты информации. Определение, назначение и анализ индикаторов средств защиты информации. Обобщение полного множества функций защиты информации. Классификация средств защиты информации. Методология выбора средств защиты информации
12	Тема 12. Определение, анализ и классификация средств защиты информации	Определение, анализ индикаторов средств защиты информации. Обобщение полного множества средств защиты информации

№ п/п	Тема	Практические задания	Информационные ресурсы	СРС
1	Тема 1. Нормативно-правовые акты информационной безопасности в Российской Федерации	2	-	4
2	Тема 2. Доктрина информационной безопасности Российской Федерации	2	-	4
3	Тема 3. Определение и основные элементы теории информационной безопасности	2	-	4
4	Тема 4. Методология базис теории информационной безопасности	2	-	4
5	Тема 5. Модели систем и процессов защиты информации	2	-	4
6	Тема 6. Унифицированная концепция информационной безопасности	2	-	4
7	Тема 7. Угрозы, риски и классификация информации, их классификация	2	-	4
8	Тема 8. Определение системы индикаторов уязвимости информации	2	-	4
9	Тема 9. Методы и модели оценки уязвимости информации	2	-	4
10	Тема 10. Определение, анализ и классификация функций защиты информации	2	-	4
11	Тема 11. Определение, анализ и классификация средств защиты информации	2	-	4
12	Тема 12. Определение, анализ и классификация средств защиты информации	2	-	4
13	Тема 13. Определение и обобщение полного множества функций защиты информации	2	-	4
14	Тема 14. Методы проектирования систем защиты информации	2	-	4
15	Тема 15. Унифицированная концепция функций защиты информации	2	-	4
16	Тема 16. Обобщение функций защиты информации	2	-	4
17	Тема 17. Обобщение средств защиты информации и средств защиты информации	2	-	4
18	Тема 18. Организация и обеспечение работ по безопасности информации	2	-	4
	Зачет с оценкой	-	-	-
	<b>ИТОГО</b>	<b>26</b>	<b>-</b>	<b>72</b>

4.1.1 Учебные задания

Учебная работа по предмету.

13	Тема 13. Определение и классификация систем защиты информации. Методы выбора средств защиты информации	информации Классификация средств защиты информации Методы выбора средств защиты информации
14	Тема 14. Определение и классификация систем защиты информации. Методы выбора средств защиты информации	Система защиты информации и объектно-ориентированные принципы ее построения Особенности построения систем защиты информации
15	Тема 15. Методы проектирования систем защиты информации	Классификация и анализ существующих средств защиты информации Постепенность и общие принципы проектирования систем защиты информации Сущность организации управления защитой информации
16	Тема 16. Особенности защиты в ЭВМ	Особенности защиты информации в персональных ЭВМ Угрозы информации в персональных ЭВМ Обеспечение безопасности информации в ПЭВМ
17	Тема 17. Особенности защиты информации в сетях ЭВМ.	Основные технологии компьютерной безопасности и безопасности сетей ЭВМ Цели, функции и задачи защиты информации в сетях ЭВМ
18	Тема 18. Организация и обеспечение работ по безопасности информации	Перечень и общие содержание основных вопросов организации и обеспечения работ по защите информации Структура и функции органов защиты информации Стандарты и спецификации в области информационной безопасности

#### 4.1.3 Лабораторные занятия

В учебном плане отсутствуют.

#### 4.1.4 Самостоятельная работа студента

№ п/п	Наименование модуля, раздела дисциплины	Выд. СРС
1	Тема 1. Понятия и термины, связанные с информационной безопасностью в Российской Федерации	Изучение вопросов и задач практического занятия
2	Тема 2. Доверия информационно-коммуникационной безопасности Российской Федерации	Изучение вопросов и задач практического занятия
3	Тема 3. Определение и классификация систем защиты информации	Изучение вопросов и задач практического занятия
4	Тема 4. Методология систем безопасности	Изучение вопросов и задач практического занятия

№ п/п	Наименование модуля, раздела дисциплины	Выд. СРС
5	Тема 5. Методы систем и средств защиты информации	Изучение вопросов и задач практического занятия
6	Тема 6. Унифицированные системы защиты информации	Изучение вопросов и задач практического занятия
7	Тема 7. Угроз, методы их классификации, принципы построения систем защиты информации, их особенности	Изучение вопросов и задач практического занятия
8	Тема 8. Определение системности защиты информации	Изучение вопросов и задач практического занятия
9	Тема 9. Методы и модели защиты информации	Изучение вопросов и задач практического занятия
10	Тема 10. Определение, цели и классификация функций защиты информации	Изучение вопросов и задач практического занятия
11	Тема 11. Определение, цели и классификация задач защиты информации	Изучение вопросов и задач практического занятия
12	Тема 12. Определение, цели и классификация средств защиты информации	Изучение вопросов и задач практического занятия
13	Тема 13. Определение и классификация средств защиты информации	Изучение вопросов и задач практического занятия
14	Тема 14. Методы проектирования систем защиты информации	Изучение вопросов и задач практического занятия
15	Тема 15. Управление процессами функционирования систем защиты информации	Изучение вопросов и задач практического занятия
16	Тема 16. Особенности защиты в ПЭВМ	Изучение вопросов и задач практического занятия
17	Тема 17. Особенности защиты информации в сетях ЭВМ	Изучение вопросов и задач практического занятия
18	Тема 18. Организация и обеспечение работ по безопасности информации	Изучение вопросов и задач практического занятия

#### 4.1.5 Интерактивные формы занятий

В учебном плане отсутствуют.

<https://www.scribd.com/> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей. — Текст: электронный

3. Springer Nature — полнотекстовая база данных / Springer Nature Switzerland AG. Part of Springer Nature. — URL: <https://link.springer.com/> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей. — Текст: электронный

4. iPDFbooks — электронно-библиотечная система / iPDFbooks; ООО «АВ Ин-Эр Медиа», электронное периодическое издание «www.pdfbooks.ru» — Саратов, [2019]. — URL: <http://www.pdfbooks.ru/> (дата обращения: 24.08.2021) — Режим доступа: для авторизованных пользователей. — Текст: электронный

5. [Luminat.com](http://luminat.com) — электронно-библиотечная система / ЗАО «Луминат», ООО «Луминат-издательский центр». — Москва, [2011]. — URL: <http://luminat.com/> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей. — Текст: электронный

6. Национальная электронная библиотека (НЭБ) — федеральная государственная информационная система / Министерство Культуры РФ — Москва, [2004]. — Режим доступа: <http://nebib.ru/> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей. — Текст: электронный

7. [Rpdroid.com](http://rpdroid.com) Обзор СММ — электронно-библиотечная система / Г. Вачагуле, ООО «ПКОИРРД.Справочник» — Москва, [1997]. — URL: <http://rpdroid.com/> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей. — Текст: электронный

8. CyberLibrary — научная электронная библиотечная открытого доступа / ООО «ITres». — Электронный файл — Москва, [2014]. — URL: <https://cyberlibrary.ru/> (дата обращения: 25.08.2021) — Текст: электронный

9. eLIBRARY.RU — научная электронная библиотечная система / Компания «Наука» — Электронный файл (eLIBRARY.RU) — Москва, [2000]. — URL: <https://elibrary.ru/> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей. — Текст: электронный

#### 4.3 Формы и содержание текстов и промежуточной аттестации по дисциплине

Для оценки информированности компетенций разрабатываются типовые средства по дисциплине.

Формы и содержание текстов и промежуточной аттестации по дисциплине расширяется и фонд оценочных средств, который является составным документом.

- Оценочные средства по дисциплине содержат:
  - материалы для текущего контроля оценки знаний по дисциплине;
  - материалы для промежуточного контроля оценки знаний по дисциплине.

Перечень вопросов учебного курса и подготовка к занятию с оценкой:

1. Системный подход и архитектура защиты компьютерной информации в современных АСОД.

2. Становление шифрования США DES.

3. Системная классификация средств защиты информации и их эффективность.

4. Шифрование с открытым ключом.

5. Объемы и элементы защиты в современных АСОД.

6. Шифрование с открытым ключом.

7. Определенные каналы передачи информации по числам информации (КНИИ). Их классификация и характеристики.

8. Симметричные и несимметричные алгоритмы шифрования.

9. Механизм защиты информации.

10. Компьютерные вирусы.

11. Формы атак на информизацию.

12. Области прикладной построения защищенных ОС.

#### 4.2 Учебно-методические и информационные обеспеченные 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 (ИИТУИТ), АВ Ин-Эр Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст: электронный // Цифровой образовательный ресурс ИР: SMART. [сайт]. — URL: <https://www.pdfbooks.ru/97562.html> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей

2. Артемов, А. В. Информационная безопасность: курс лекций / А. В. Артемов. — Орел: Межрегиональный Академический институт информации (МАИИИ), 2014. — 256 с. — Текст: электронный // Цифровой образовательный ресурс ИР: SMART. [сайт]. — URL: <https://www.pdfbooks.ru/333430.html> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей

3. Ермаков, Д. Г. Принципы антивирусных программ для обеспечения информационной безопасности / Д. Г. Ермаков, А. В. Прыжковский. — Екатеринбург: Уральский федеральный университет, ЭБС АС/В, 2013. — 64 с. — Текст: электронный // Цифровой образовательный ресурс ИР: SMART. [сайт]. — URL: <https://www.pdfbooks.ru/66577.html> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей

4. Мейвельд, Э. Безопасность сетей: учебное пособие / Э. Мейвельд. — 3-е изд. — Москва: Интернет-Университет Информационных Технологий (ИИТУИТ), АВ Ин-Эр Медиа, 2021. — 571 с. — ISBN: 978-5-4497-0863-2. — Текст: электронный // Цифровой образовательный ресурс ИР: SMART. [сайт]. — URL: <https://www.pdfbooks.ru/101992.html> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей

5. Основы информационной безопасности: учебно-методическое пособие / составители С. Ю. Милоз, — Орел: Межрегиональный Академический институт информации (МАИИИ), 2019. — 48 с. — Текст: электронный // Цифровой образовательный ресурс ИР: SMART. [сайт]. — URL: <https://www.pdfbooks.ru/95409.html> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей

6. Бельюс, А. И. Основы кибербезопасности. Статистика, политика, методы и средства обеспечения / А. И. Бельюс, В. А. Солодуха. — Москва: Технофор, 2021. — 482 с. — ISBN 978-5-94836-612-9. — Текст: электронный // Цифровой образовательный ресурс ИР: SMART. [сайт]. — URL: <https://www.pdfbooks.ru/106623.html> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей

7. Костин, В. И. Методы и средства защиты компьютерной информации: информационный базис. — Орел: Методы и средства защиты компьютерной информации: информационный базис. — Москва: Издательский Дом ИРИС, 2018. — 71 с. — ISBN 978-5-906053-53-7. — Текст: электронный // Цифровой образовательный ресурс ИР: SMART. [сайт]. — URL: <https://www.pdfbooks.ru/98210.html> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей

##### 4.2.2 Современное профессиональные базы данных и информационные справочные системы

##### 4.2.3 Информационные ресурсы

##### 4.2.4 Интернет-ресурсы и другие электронные информационные источники

##### Общие Интернет-ресурсы, электронные библиотечные системы

1. Электронная библиотека Copyrighted Contentsof the university database. — Сайт, [2017-]. — URL: <http://lib.aut.ru/> (дата обращения: 25.08.2021) — Текст: электронный

2. ScienceDirect — полнотекстовая база данных / издательство Elsevier. — URL:

С целью более глубокого изучения темы лекциями, конспекты следует дополнять и дорабатывать для систематизации и обобщения, используя информацию, полученную на время практического занятия, в том же формате учебно-методическую литературу и Интернет-ресурсы. Анализировать работу необходимо полностью в при работе тем дисциплины, представляя для самостоятельного изучения.

Руководствуясь выработкой в себе привычку просматривать, перерабатывать перед началом практического занятия текст предыдущего занятия.

Если возникает вопрос, обязательно обращайтесь в консультативный кабинет или после занятия (или во время занятия при его заверше к студентам «беседа попутно») за разъяснениями, четко формулируя вопросы/запросы в понимании учебного материала.

Практические задания следует выполнять четко и сознательно с помощью методических рекомендаций и алгоритмов, формулируя четкие вопросы преподавателю.

При подготовке к промежуточной аттестации необходимо получить у преподавателя перечень практических единиц темы и типовые содержание заданий по программе наглядно и практически усвоить по дисциплине.

### 5.2. Организация самостоятельной работы студента по дисциплине

Самостоятельная работа студента включает приобретение практических знаний, чтение обязательной и дополнительной литературы, знакомство с содержанием электронных источников, анализ текущих разработок молодежи, исполнение практических заданий

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

- учебной, учебно-методической и справочной литературой,
- разделенным справочно-методическим материалом, включенным алгоритмические схемы решения задач,
- доступом в средства вычислительной техники и информационному программному обеспечению

### 5.3. Особенности применения инноваций

В целях максимального усвоения дисциплины используются следующие технологии обучения:

- Проектная работа - совместная деятельность студентов в группе под руководством лектора, направленной на решение одной задачи путем творческого сплочения результатов индивидуальной работы членов команды с активным взаимодействием и ответственностью.
- Самостоятельная работа студента, предусматривает выполнение работы - заданий, которое требует от студента самостоятельного игнал обработки полученных ранее информации в форме, определенной преподавателем, и требующей, как правило, творческого подхода.

Применение дисциплины опирается на определенный подход к обучению и ориентирован на решение и процесс обучения команды, образованной обучающихся различными методами жизни и деятельности, специфичной различных компетенций обучения и потребности личности, общества и государства в подготовке к выполнению социальных ролей, знаний, убеждений, черт и качества характера, отечественной и заграничной.

Применение всех видов занятий при преподавании дисциплины, проведение консультаций, промежуточных и текущих аттестаций возможно с применением электронного обучения и дистанционных образовательных технологий.

### 5.4. Материально-техническое обеспечение дисциплины

При обучении дисциплины используются следующие материально-технические ресурсы:

1. Кабинет для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: комплект специализированной мебели, демонстрационное оборудование и учебно-наглядные пособия.

2. Помещение для самостоятельной работы: библиотека, читальный зал, помещение для самостоятельной работы: столов, стульев. Компьютерная техника с подключением к сети «Интернет» с обеспечением доступа в ЭИОС университета.

Для передачи раздаточного материала и практическим занятиям, домашних заданий, обмена

13. Методы защиты компьютерной информации
14. Управление безопасностью в защищенных ОС.
15. Функции, задачи защиты информации
16. Авторитарная субъектив и объектов АСОД.
17. Определенные потенциально возможных нарушений защиты компьютерной информации.

информации.

18. Протокол аудита информации KERBEROS
19. Проектные системы защиты информации в АСОД
20. Алгоритм аутентификации в АСОД
21. Структура и структура областей знаний о безопасности в АСОД
22. Задачи защиты и информации в компьютерных сетях.
23. Аппаратные и программные средства защиты информации.
24. Брендмаурри и их характеристики.
25. Организационные средства защиты информации
26. Механизмы защиты информации в сетях передачи данных и в канал связи.
27. Базисные средства защиты информации.
28. Управление доступом к данным
29. Криптографические средства защиты информации
30. Защита электронной почты
31. Законодательные средства защиты, и морально-этические нормы.
32. Защита IP
33. Оперативно-аналитические управление защитой информации.
34. Защита WEB
35. Классификационные руководство защитой информации.
36. Защита средств сетевой управления.
37. Планирование защиты информации.
38. Суть, принципы и методы компьютерной стандартными в области системы АСОД.
39. Обеспечение конфиденциальности, доступности и службы защиты информации.
40. Требования обязательных программ по защите информации.
41. Роль стандартов информационной безопасности и их анализ.
42. Организационно-технические основы защиты информации в АСОД в России и за рубежом

43. Руководящие документы Голландии России.
44. Анализ некоторых алгоритмов электронной подписи.
45. Американизация, Китайские, Европейские и Египетские и Египетские критерии безопасности информационных технологий.
46. Схема и общие содержание основных работ по защите информации.

### 5.5. УСЛОВИЯ ОСВОЕНИЯ И РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

5.1. Методические рекомендации обучаемым по изучению дисциплины  
Промежуточная аттестация может быть вынесена студенту по результатам текущего аттестации и (или) по результатам федерального интернет тестирования (ФЭИО), интернет тренингов).

Чтобы освоить учебный материал любой дисциплины, необходимо регулярно посещать все занятия, не откладывать и читать лекции и обязательно конспектировать учебно-методические рекомендации по практическим занятиям. Практические занятия дают знания, которые подчас невозможно найти даже в лучших учебниках. Положительное обучение заключается в том, что теория преподавателя, поэтому следует стараться выдвигать, задавать основные вопросы, идеи, вопросы, читать учебный материал, если можно преподавателем. При конспектировании обязательно использовать памятки для конспектирующего студента содержания и усвоение задач.

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

Базовый пакет

Профиль «Математика и информатика»

АННОТАЦИЯ

рабочей программы дисциплины

Информатики безопасности

дисциплины части учебного плана, формирующей участникам образовательных отношений отличную форму обучения

Общая трудность дисциплины (ЕЦТ/час.)	3/108
Цель, изучаемые дисциплины	Ознакомление с основами «Информационной информатики» для студентов по направлению подготовки 44.04.05 «Педагогическое образование с двумя профилями подготовки»
Содержание дисциплины	Тема 1. Информационно-правовые акты информативной безопасности в Российской Федерации Тема 2. Документ информативной безопасности Российской Федерации Тема 3. Определенные и основные понятия теории информативной безопасности Тема 4. Методологическая база теории информативной безопасности Тема 5. Методы системы и процессы защиты информации Тема 6. Унифицированные концепции информативной безопасности Тема 7. Угрозы, каналы несанкционированного получения информации, их классификация Тема 8. Определенные системы показателей уязвимости информации Тема 9. Методы и модели оценки уязвимости информации Тема 10. Определенные, анализ и классификация функций защиты информации Тема 11. Определенные, анализ и классификация задач защиты информации Тема 12. Определенные, анализ и классификация средств защиты информации Тема 13. Определенные и общетеоретические принципы архитектурного построения систем защиты информации Тема 14. Методы построения систем защиты информации Тема 15. Управление процессами функционирования защиты информации Тема 16. Особенности защиты в ИТБМ. Тема 17. Особенности защиты информации в сетях ЭИМ. Тема 18. Организация и обеспечение работ по безопасности информации
Формируемые компетенции (годы)	ПКУИ-2. Способен разрабатывать методику обучения в области информативной информатики и программной защиты с применением компьютерных технологий
Коды и наименование индикатора достижений компетенции	ПКУИ-2.1. Анализирует и разрабатывает алгоритмические варианты методики обучения информатики с применением компьютерных технологий ПКУИ-2.2. Использует компьютерные технологии для разработки информативных моделей реальных процессов окружающего мира
Дисциплины, участвующие в формировании компетенции	Компьютерное моделирование Программное обеспечение ЭИМ и прикладное по решению задач на ЭИМ

информации с применением используется электронная почта. Перенос, дублирование и свободное распространение информации осуществляется, в том числе, посредством средств массовой информации.

Таблица – Перечень программного обеспечения

№	Перечень ПК
1	Microsoft Windows
2	Антивирус Т-DR
3	Справочно-справочная система Консультант Плюс

При организации занятий, теорий и практических занятий с применением электронного обучения и дистанционных образовательных технологий используются различные электронные образовательные ресурсы и сайты интернета, входящие в состав МБОУ СОУ.

5.5. Методические 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 при работе инвалидов, адаптированной при необходимости для обучения указанных обучающихся.

Организация обучения, текущий и промежуточный 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, организуется защита совместно с другими обучающимися в общей группе, используя слайды-вопросы и реферативные методы обучения с созданием комфортного психологического климата в студенческой группе или, при соответствующем состоянии обучающегося, по индивидуальной программе, которая является индивидуальной программой основной рабочей программы дисциплины. При этом содержание программы дисциплины не изменяется. Изменяется, как правило, формы обучения и контроля знаний, образовательные технологии и методические материалы.

Обучение студентов-инвалидов и студентов с ОВЗ также может осуществляться индивидуальными курсами с применением адаптированных технологий.

Дистанционное обучение обеспечивает возможность коммуникаций с преподавателем, и также с другими обучающимися посредством вебинаров (например, с использованием программ Skype), что способствует сплочению группы, направляет учебную группу на совместную работу, обсуждение, принятие группового решения.

В учебном процессе для повышения уровня усвоения и переработки учебной информации студентами-инвалидами и студентами с ОВЗ проводятся методические и специализированные технологии средств приема-передачи учебной информации в доступных формах для студентов с речевыми нарушениями, обеспечивается доступ к интерактивным формам печатных материалов (аудионый файл), электронных образовательных ресурсов в формах, адаптированных к ограничениям здоровья обучающихся, наличие необходимого методического обеспечения.

Подбор и разработка учебных материалов производится преподавателем с учетом того, чтобы студенты с нарушениями слуха получали информацию доступно, с индивидуальными заданиями – аудиторными (например, с использованием программ-синтезаторов речи).

Для обеспечения приема курсового контроля успеваемости и промежуточной аттестации обучающихся инвалиды и лица с ОВЗ фонд оценочных средств по дисциплине, позволяющий оценить достижения учащихся 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 (устны, индивидуально на бумаге, письменно на компьютере, в форме тестирования и т.д.). При необходимости обучающиеся представляются дополнительные время для подготовки ответа при промежуточной аттестации.

<p>Образовательные учреждения Фирма предоставляющая услуги</p>	<p>Компьютерные сети Методический модуль Теория и методика обучения информатике Схемы конкурентности Сетины управления базой данных Проектирование информационных систем Педагогическая (педагогическая) практика Практические занятия, самостоятельная работа  Занят с оценкой</p>
--	---