

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гайдамашко Игорь Вячеславович
Должность: И.о. ректора
Дата подписания: 21.09.2022 14:18:44
Уникальный программный ключ:
с7b77973654876a9af403b180790b0a371557fdb

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

Декан факультета СПФ
Макиревская Ю.Э.
«03» 09 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:

- ознакомление основными понятиями информационной безопасности и методами защиты данных, необходимыми для применения в профессиональной работе, для продолжения образования;
- представление о различных студентах, формирование качества мышления, способности для профессиональной деятельности;
- формирование представлений об информационной безопасности как целостной части функциональных информационных систем и сетей, понимание значимости 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, составлении 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
		3	0
		0	0
			0

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 понятия 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. Моделирование систем защиты информации
6	Тема 6. Унифицированная классификация информационных ресурсов	Моделирование систем защиты информации. Классификация и общий анализ моделирования систем защиты информации. Системно-когнитивный подход к моделированию систем защиты информации
7	Тема 7. Угрозы, риски и классификация информации, их классификация	Наиболее распространенные угрозы доступности. Неотъемлемые атрибуты доступности. Классификация и общий анализ моделирования систем защиты информации
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 и общий анализ моделирования систем защиты информации
11	Тема 11. Определение, анализ и классификация средств защиты информации	Методология выбора функций защиты информации. Определение, назначение и анализ индикаторов функций защиты информации. Классификация и общий анализ моделирования систем защиты информации. Классификация и общий анализ моделирования систем защиты информации
12	Тема 12. Определение, анализ и классификация средств защиты информации	Определение, анализ индикаторов функций защиты информации. Классификация и общий анализ моделирования систем защиты информации. Классификация и общий анализ моделирования систем 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 понятия 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 классификация информационных ресурсов	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 классификация функций защиты информации	2	-	4
14	Тема 14. Методы проектирования систем защиты информации	2	-	4
15	Тема 15. Унифицированная классификация функций защиты информации	2	-	4
16	Тема 16. Особенности защиты в ИТ-ДМ	2	-	4
17	Тема 17. Особенности защиты информации в сетях ЭИИМ	2	-	4
18	Тема 18. Организация и обеспечение работ по безопасности информации	2	-	4
	Зачет с оценкой	-	-	-
	ИТОГО	36	-	72

4.1.1. Исключительные 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. Методы проектирования систем защиты информации	Система защиты информации и объектно-ориентированные принципы ее построения Особенности построения систем защиты информации
15	Тема 15. Управление процессами функционирования систем защиты информации	Классификация и анализ существующих средств защиты информации Полнота, своевременность и объем охвата Процедуры управления процессами функционирования систем защиты информации Средства 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 компьютерных сетей и телекоммуникационных сетей ЭВМ Цели, функции и задачи защиты информации в сетях ЭВМ
18	Тема 18. Организация и обеспечение работ по безопасности информации	Перечень и объем содержания 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. Первоначальные акты информационной безопасности в Российской Федерации	Изучение вопросов и задач практического занятия
2	Тема 2. Доверия информационной безопасности Российской Федерации	Изучение вопросов и задач практического занятия
3	Тема 3. Определение и оценка показателей информационной безопасности	Изучение вопросов и задач практического занятия
4	Тема 4. Методологический базис теории	Изучение вопросов и задач практического занятия

информационная безопасность	Изучение вопросов и задач практического занятия
Тема 3. Методы систем и процессов защиты информации	Изучение вопросов и задач практического занятия
Тема 6. Унифицированные системы информационной безопасности	Изучение вопросов и задач практического занятия
Тема 7. Угроз, каналы коммуникационного получения информации, их классификация	Изучение вопросов и задач практического занятия
Тема 8. Определение системной модели безопасности информации	Изучение вопросов и задач практического занятия
Тема 9. Методы и модели оценки уязвимости информации	Изучение вопросов и задач практического занятия
10. Тема 10. Определение, анализ и классификация функций защиты информации	Изучение вопросов и задач практического занятия
11. Тема 11. Определение, анализ и классификация видов защиты информации	Изучение вопросов и задач практического занятия
12. Тема 12. Определение, анализ и классификация средств защиты информации	Изучение вопросов и задач практического занятия
13. Тема 13. Определение и классификация аппаратно-программных средств систем 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.scribdirect.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.i-pdfbooks.ru» — Саратов, [2019]. — URL: <http://www.i-pdfbooks.ru/> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей. — Текст: электронный

5. lucylib.com — электронно-библиотечная система / ЗАО «Лидияшисаи, ООО «Лидияшисаи» — центр Идфин-М., Москва, [2011]. — URL: <http://lucylib.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. Вачагдас, ООО «ПКОИРРД Справочники» — 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» — электронная библиотека (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.

Основные средства по дисциплине охватывают:

- материалы для промежуточного 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.i-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. — Оренбург: Межрегиональный Академический институт информации (МАИИИ), 2014. — 256 с. — Текст: электронный // Цифровой образовательный ресурс ИР: SMART. [сайт]. — URL: <https://www.i-pdfbooks.ru/333430.html> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей

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

4. Майвела, Э. Безопасность сетей: учебное пособие / Э. Майвела. — 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.i-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, — Оренбург: Межрегиональный Академический институт информации (МАИИИ), 2019. — 48 с. — Текст: электронный // Цифровой образовательный ресурс ИР: SMART. [сайт]. — URL: <https://www.i-pdfbooks.ru/95409.html> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей

6. Бельюс, А. И. Основы информационной безопасности. 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.i-pdfbooks.ru/106023.html> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей

7. Костин, В. П. Методы и средства защиты компьютерной информации: информативность, безопасность, компьютерные сети: учебное пособие / В. П. Костин. — Москва: Издательский Дом МПС, 2018. — 71 с. — ISBN 978-5-906053-53-7. — Текст: электронный // Цифровой образовательный ресурс ИР: SMART. [сайт]. — URL: <https://www.i-pdfbooks.ru/98210.html> (дата обращения: 25.08.2021) — Режим доступа: для авторизованных пользователей

4.2.2 Современные 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 Комиссарио государственного университета база данных. — Сочка, [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 осмысления 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 консультационный кабинет или после занятия (или во время занятия при его заверше к студентам «Беседа по теме») за разъяснениями, четко формулируя вопросы/запросы в понимании учебного материала.

Практические задания следует выполнять четко и сознательно с помощью методических рекомендаций и алгоритмов, образуемых на предыдущих занятиях.

При подготовке к промежуточной аттестации необходимо получить у преподавателя перечень дополнительных единиц балла занятий и типовые содержание заданий по программе павильон и практические умения 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 молодых, 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 дисциплины

В целях максимального использования 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.
- Промежуточные аттестации ориентирует на определенный подход к обучению и ориентирует на решение и процесс обучения команды, обучающейся самостоятельно и развивая навыки жизни и деятельности, специфичной различных компетенций обучения и потребности личности, общества и государства в выработке у обучающихся социальных позитивных качеств, убеждений, черт и качества характера, ответственности и здравого смысла.

Присвоение всех видов занятий при прохождении дисциплины, присвоение курсовых, промежуточных и текущих аттестаций возможно с применением электронного обучения и дистанционных образовательных технологий.

5.4. Материально-технические обеспечения дисциплины

При обучении дисциплины используются следующие материально-технические обеспечения:

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. Управленческая безопасность в защищенных ОХ
15. Функции, задачи защиты информации
16. Аутентификация субъектов и объектов АСОД
17. Определение потенциально возможных нарушений защиты компьютерной информации.

18. Протокол аудита информации KERBEROS

19. Проектная система защиты информации в АСОД

20. Алгоритм аутентификации в АСОД

21. Структура и структура области знаний о защите информации в АСОД

22. Задачи защиты и информации в корпоративных сетях

23. Алгоритмы и алгоритмические средства информации

24. Брендмаурри и их характеристики

25. Организационные средства защиты информации

26. Механизмы защиты информации в трестах 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 сетевого управления

37. Планирование защиты информации

38. Суть, принципы и методы компьютерной стандартности в области

39. АСОД

40. Обеспечение информационной деятельности и службы защиты информации

41. Требования обязательных программ по защите информации

42. Роль стандартов информационной безопасности и их анализ

43. Организационно-правовые основы защиты информации в АСОД в России и за рубежом

44. Руководящие документы Голландии России

45. Анализ некоторых алгоритмов электронной подписи

46. Американизация, Китайские, Европейские и Египетские и Египетские критерии безопасности информационных технологий

47. Схема и общие содержание основных работ по защите информации

48. СХЕМА И ОБЩИЕ СОДЕРЖАНИЕ ОСНОВНЫХ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

49. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

50. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

51. Методические рекомендации обучающимся по изучению дисциплины

52. Промежуточная аттестация может быть выписана студенту по результатам текущей

53. аттестации и (или) по результатам федерального интернет тестирования (ФЭИО), интернет

54. Тренингов)

55. Чтобы освоить учебный материал любой дисциплины, необходимо регулярно посещать все

56. занятия, не откладывать и читать лекции и обязательно конспектировать учебно-методические

57. рекомендации по практическим занятиям. Практические занятия дают знания, которые подчас

58. невозможно найти даже в лучших учебниках. Положительное обучение заключается в том, что

59. теория преподавателя, поэтому следует стараться выдвигать, анализировать основные положения,

60. идеи, выводы, найти личную учебную литературу, еслиosome преподавателем. При

61. конспектировании обязательно использовать памятки для конспектирующего студента

62. содержания и усвоение знаний

63. На время практических занятий необходимо проводить продуктивную активность, отвечать

64. на вопросы преподавателя, показывать способность самостоятельного мышления.

Информация с применением используется электронная книга. Перечень литературы и свободно распространяемой приравненной литературы, в том числе отечественной разработки:

Таблица – Перечень программного обеспечения

№	Перечень ПК
1	Microsoft Windows
2	Арабиатур Т-2/Р
3	Справочно-справочная система Колесников Павел

При организации занятий, тестов и промежуточной аттестации с применением электронного обучения и дистанционных образовательных технологий используются различные электронные образовательные ресурсы и сайты интернета, входящие в состав МОС СУ.

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 равной дисциплины, адаптированной при необходимости для обучения указанных обучающихся.

Организация обучения, тестов 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, организуется совместная с другими обучающимися в общей группе, используя специальные и реабилитационные методы обучения создания комфортного психологического климата в студенческой группе или, при соответствующем состоянии обучающегося, по индивидуальной программе, которая является индивидуальной программой обучения 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 специальные индивидуальные технологии средств приема-передачи учебной информации в доступных формах для студентов с речевыми нарушениями, осуществляется выпуск адаптированных форматов печатных материалов (аудионый файл), 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 доступно, с индивидуальными ценами – аудиотекст (например, с использованием программ-синтезаторов речи).

Для обеспечения приема тестов контроля усвоения и промежуточной аттестации обучающихся инвалидов и лиц с ОВЗ фонд оценочных средств по дисциплине, позволяющий оценить достигаемые ими результаты 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, исключено на бумаге, письменно на компьютере, в форме тестирования и т.д.). При необходимости обучающимся предоставляется дополнительное время для подготовки ответа при промежуточной аттестации.

Профиль «Математика и информатика»

АННОТАЦИЯ

рабочей программы дисциплины
Информатики безопасности
двухлетняя часть учебного плана, формируемой участниками образовательных отношений
иных форм обучения

Общая трудность дисциплины (ЕЦТ/час.)	З/УОС
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. Определение 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 проектирования 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)	ПКУВ-2. Способен разрабатывать механизмы обучения в различных областях информатики и информатики с применением компьютерных технологий
Ключи и наименование индикатора компетенции	ПКУВ-2.1. Анализирует и разрабатывает адаптивные варианты методов обучения информатики с применением компьютерных технологий. ПКУВ-2.2. Использует компьютерные технологии для разработки информативных моделей реальных процессов окружающего мира
Дисциплины, участвующие в формировании компетенции	Компьютерное моделирование Программное обеспечение ЭИМ и практикум по решению задач на ЭИМ

<p>Образовательные учреждения Фирма предоставляющая услуги</p>	<p>Компьютерные сети Методический модуль Теория и методика обучения информатике Схемы работоспособности Сети для управления базой данных Проектирование информационных систем Педагогические (методические) проекты Практические задания, самостоятельная работа</p>
	<p>Вместе с оценкой</p>