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

СОГЛАСОВАНО
Декан факультета СПФ
_____ Макаревская Ю.Э.
«01» 09 2021 г.

УТВЕРЖДАЮ
Проректор по УРиКОД
_____ В.П. Ердакова
«03» 09 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы кибербезопасности

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	Трудоем-кость (час./зет.)	Лекцион. занятий, (час.)	Практич. занятий, (час.)	Лаборат. занятий, (час.)	СРС, (час.)	КР/КП	Форма промежуточного контроля (экз./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 «Основы кибербезопасности»

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 _____ Макарова И.Л.
подпись Ф.И.О.

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

Директор НОБ _____ Мысина Е.С.
подпись Ф.И.О.

Структура рабочей программы соответствует предъявляемым требованиям:

Отдел качества образования и методического обеспечения _____ Васильченко В.В.
подпись 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 «Основы кибербезопасности» является освоение основ кибернетической безопасности для студентов по направлению подготовки 44.03.05 «Математика и информатика»

Задачи дисциплины:

- овладение основными понятиями кибербезопасности 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 о целях и методах кибербезопасности;
- формирование представлений о кибербезопасности как неотъемлемой части функционирования вычислительных систем и сетей, понимания значимости вопросов кибербезопасности для будущей профессиональной деятельности.

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП НАПРАВЛЕНИЯ (СПЕЦИАЛЬНОСТИ)

Дисциплина «Основы кибербезопасности» является частью, формируемая участниками образовательных отношений.

Таблица 1

Код и наименование компетенции	Дисциплины, участвующие в формировании компетенции
ПКУВ-2 Способен разрабатывать методику обучения отдельным разделам информатики и программирования с применением компьютерных технологий	Компьютерное моделирование Программное обеспечение ЭВМ и практикум по решению задач на ЭВМ Компьютерные сети Методический модуль Теория и методика обучения информатике Информационная безопасность Системы управления базами данных Проектирование информационных систем Педагогическая (методическая) практика

3 ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Таблица 2

Компетенции и индикаторы их достижения		В результате изучения дисциплины обучающиеся должны:
Код и наименование компетенции	Код и наименование индикатора достижения компетенции	
ПКУВ-2 Способен разрабатывать методику обучения отдельным разделам информатики и программирования с применением компьютерных технологий	ПКУВ-2.1. Анализирует и разрабатывает альтернативные варианты методики обучения информатике с применением компьютерных технологий	Знать основные принципы сбора информации по кибербезопасности; Уметь решать задачи по отбору актуальной информации по кибербезопасности; Владеть методами системного обобщения информации для решения задач по кибербезопасности
	ПКУВ-2.2. Использует компьютерные технологии для разработки информационных моделей реальных процессов окружающего мира	Знать методы анализа разнородных данных для анализа проблем и принятия решений по кибербезопасности; Уметь анализировать и систематизировать разнородные данные; Владеть навыками применения процедур анализа и принятия решений при решении задач по кибербезопасности

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Тематический план дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единиц, 108 часов.

№ раздела, темы	Наименование модуля (раздела, темы) дисциплины	ОФО				
		Всего часов	Виды учебной нагрузки и их трудоемкость, часы			
			Лекции	Практические занятия	Лабораторные работы	СРС
1	Тема 1. Кибернетическая безопасность в системе национальной безопасности современной России	6	-	2	-	4
2	Тема 2. Внутренние и внешние угрозы кибернетической безопасности Российской Федерации	6	-	2	-	4
3	Тема 3. Правовые основы обеспечения кибернетической безопасности Российской Федерации	6	-	2	-	4
4	Тема 4. Основные информационные угрозы и общие рекомендации по организации безопасной работы в Интернете	6	-	2	-	4
5	Тема 5. Безопасная работа в Интернете: анализ веб-сайтов, безопасный поиск, надежные пароли	12	-	4	-	8
6	Тема 6. Безопасная работа в Интернете: электронная почта, платежи, защитное ПО	18	-	6	-	12
7	Тема 7. Защитное ПО. Kaspersky Internet Security ESET NOD32 Smart Security, Dr.Web Security Space	18	-	6	-	12

8	Тема 8. Проверка компьютера и восстановление данных в экстренной ситуации	18	-	6	-	12
9	Тема 9. Безопасность в социальных сетях	18	-	6	-	12
	Зачет с оценкой	-	-	-	-	-
	ИТОГО	108	-	36	-	72

4.1.1 Лекционные занятия

Учебным планом не предусмотрены.

4.1.2 Практические занятия

№ п/п	Наименование модуля, раздела дисциплины	Краткое содержание
1	Тема 1. Кибернетическая безопасность в системе национальной безопасности современной России	Анализ сущности и содержание Доктрины информационной безопасности Российской Федерации, модели его совершенствования в рамках кибернетической безопасности
2	Тема 2. Внутренние и внешние угрозы кибернетической безопасности Российской Федерации	Анализ внутренних и внешних утроз кибернетической безопасности Российской Федерации
3	Тема 3. Правовые основы обеспечения кибернетической безопасности Российской Федерации	Анализ законодательного обеспечения кибернетической безопасности Российской Федерации
4	Тема 4. Основные информационные угрозы и общие рекомендации по организации безопасной работы в Интернете	Общий обзор утроз Финансовые махинации Кража данных учетных записей Вредоносные программы Неосторожность пользователя Рекомендации по организации безопасной работы в Интернете
5	Тема 5. Безопасная работа в Интернете: анализ веб-сайтов, безопасный поиск, надежные пароли	Потенциально опасные веб-сайты: снижение риска Безопасный поиск Безопасная работа с веб-браузером Регистрация на веб-сайтах, пароли
6	Тема 6. Безопасная работа в Интернете: электронная почта, платежи, защитное ПО	Безопасность при работе с электронной почтой и с системами обмена сообщениями Безопасная работа с банковскими картами и платежными системами Защитное ПО, основные сведения
7	Тема 7. Защитное ПО. Kaspersky Internet Security, ESET NOD32 Smart Security, Dr.Web Security Space	Загрузка, установка и подготовка к работе ПО антивирусных программ
8	Тема 8. Проверка компьютера и восстановление данных в экстренной ситуации	Резервное копирование Шифрование данных Физическая безопасность компьютера Дополнительные учетные записи.
9	Тема 9. Безопасность в социальных сетях	Правила безопасной работы Настройки безопасности и конфиденциальности в социальных сетях Одноклассники, ВКонтакте, Facebook, Мой Мир Блог-платформы Автономные блоги (Standalone)
		Микроблоги Тематические социальные сети Форумы Видеохостинги Фотохостинги

4.1.3 Лабораторные занятия

В учебном плане отсутствуют

4.1.4 Самостоятельная работа студента

№ п/п	Наименование модуля, раздела дисциплины	Вид СРС
1	Тема 1. Кибернетическая безопасность в системе национальной безопасности современной России	Изучение вопросов и задач практического занятия
2	Тема 2. Внутренние и внешние угрозы кибернетической безопасности Российской Федерации	Изучение вопросов и задач практического занятия
3	Тема 3. Правовые основы обеспечения кибернетической безопасности Российской Федерации	Изучение вопросов и задач практического занятия
4	Тема 4. Основные информационные угрозы и общие рекомендации по организации безопасной работы в Интернете	Изучение вопросов и задач практического занятия
5	Тема 5. Безопасная работа в Интернете: анализ веб-сайтов, безопасный поиск, надежные пароли	Изучение вопросов и задач практического занятия
6	Тема 6. Безопасная работа в Интернете: электронная почта, платежи, защитное ПО	Изучение вопросов и задач практического занятия
7	Тема 7. Защитное ПО. Kaspersky Internet Security, ESET NOD32 Smart Security, Dr.Web Security Space	Изучение вопросов и задач практического занятия
8	Тема 8. Проверка компьютера и восстановление данных в экстренной ситуации	Изучение вопросов и задач практического занятия
9	Тема 9. Безопасность в социальных сетях	Изучение вопросов и задач практического занятия

4.1.5 Интерактивные формы занятий

В учебном плане отсутствуют

4.2 Учебно-методическое и информационное обеспечение дисциплины

4.2.1 Литература

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст :

электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97562.html (дата обращения: 25.08.2021). — Режим доступа: для авторизир. пользователей
2. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/33430.html (дата обращения: 25.08.2021). — Режим доступа: для авторизир. пользователей
3. Ермаков, Д. Г. Применение антивирусных программ для обеспечения информационной безопасности / Д. Г. Ермаков, А. В. Прохоцкий. — Екатеринбург : Уральский федеральный университет, ЭБС АСВ, 2013. — 64 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/66577.html (дата обращения: 25.08.2021). — Режим доступа: для авторизир. пользователей
4. Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/101992.html (дата обращения: 25.08.2021). — Режим доступа: для авторизир. пользователей
5. Основы национальной безопасности : учебно-методическое пособие / составители С. Ю. Махов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2019. — 88 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/95409.html (дата обращения: 25.08.2021). — Режим доступа: для авторизир. пользователей
6. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/108023.html (дата обращения: 25.08.2021). — Режим доступа: для авторизир. пользователей
7. Костин, В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 31 с. — ISBN 978-5-906953-53-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/98200.html (дата обращения: 25.08.2021). — Режим доступа: для авторизир.пользователей.

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: 25.08.2021). – Текст : электронный.
2. ScienceDirect: полнотекстовая база данных / издательство Elsevier. – URL: https://www.sciencedirect.com/ (дата обращения: 25.08.2021). – 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: 25.08.2021). – 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: 25.08.2021). – 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: 25.08.2021). – 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: 25.08.2021). – 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: 25.08.2021). – Режим доступа: для авторизир. пользователей. – Текст : электронный.
8. КиберЛенинка : научная электронная библиотека открытого доступа / ООО «Инос». – Электрон. дан. – Москва, [2014-]. – URL: https://cyberleninka.ru/ (дата обращения: 25.08.2021). – Текст : электронный.
9. eLIBRARY.RU : научная электронная библиотека / Компания «Научная электронная библиотека» (eLIBRARY.RU). – Москва, [2000-]. – URL: https://elibrary.ru/ (дата обращения: 25.08.2021). – Режим доступа: для авториз. пользователей. – Текст : электронный.

4.3 Формы и содержание текущей и промежуточной аттестации по дисциплине

Для оценки сформированности компетенций разрабатываются оценочные средства по дисциплине.

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

Оценочные средства по дисциплине содержат:

- материалы для текущего контроля оценки знаний по дисциплине;
- материалы для промежуточного контроля оценки знаний по дисциплине.

Перечень вопросов устного опроса и подготовки к зачету с оценкой:

1. Понятие "информационная безопасность" и ее задачи
2. Составляющие информационной безопасности
3. Понятие защиты информации и ее задачи
4. Методы защиты противостояние;
5. Методы защиты управление доступом;
6. Методы защиты механизмы шифрования;
7. Методы защиты противодействие атакам вредоносных программ;
8. Методы защиты регламентация;
9. Методы защиты принуждение;
10. Методы защиты побуждение
11. Информационная безопасность
12. Понятие кибербезопасности
13. Компьютерная безопасность
14. Компьютерные преступления
15. Понятие информационных угроз
16. Вредоносное программное обеспечение
17. Понятие киберпреступности
18. Классификация киберпреступности
19. Мошенничество и отмывание денег
20. Киберпреступность и терроризм
21. Хакеры
22. Спам
23. Киберпреступность и Интернет
24. Кибератаки
25. Кибератаки и их типы
26. Похищение паролей
27. Стадии Кибератаки
28. Защита от киберпреступности
29. Шифрование данных

30. Симметричное шифрование
31. Асимметричное шифрование или шифрование открытым ключом
32. ЭЦП
33. Защита документов MS Word
34. Защита документов MS Excel
35. Архивирование файлов Windows и их защита
36. Вирусы и методы борьбы с ними.
37. Антивирусные программы и пакеты.

5 УСЛОВИЯ ОСВОЕНИЯ И РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

5.1 Методические рекомендации обучающимся по изучению дисциплины

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

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

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

С целью более глубокого освоения темы дисциплины, конспекты следует дополнять и дорабатывать для систематизации и обобщения, используя информацию, полученную во время практического занятия, а также рекомендуемую учебно-методическую литературу и Интернет-ресурсы. Аналогичную работу необходимо выполнять и при разработке тем дисциплины, предлагаемых для самостоятельного изучения.

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

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

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

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

5.2 Организация самостоятельной работы студента по дисциплине

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

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

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

5.3 Особенности преподавания дисциплины

В целях максимального усвоения дисциплины используются следующие технологии обучения:

- Практическая 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

При обучении дисциплине необходимо следующее материально-техническое обеспечение:

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: столы, стулья. Компьютерная техника с подключением к сети «Интернет» с обеспечением доступа в ЭИОС университета.

Дистанционная поддержка дисциплины.

Для передачи раздаточного материала к практическим занятиям, домашних заданий, обмена информацией с преподавателем используется электронная почта.

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

Таблица - Перечень программного обеспечения

№	Перечень ПО
1	Microsoft Windows
2	Архиватор 7-zip
3	Справочно-правовая система КонсультантПлюс

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

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

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

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

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

изменяется. Изменяются, как правило, формы обучения и контроля знаний, образовательные технологии и дидактические материалы.

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

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

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

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

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

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

Бакалавриат

Профиль «Математика и информатика»

АННОТАЦИЯ

рабочей программы дисциплины

Основы кибербезопасности

дисциплины части учебного плана, формируемой участниками образовательных отношений

очная форма обучения

Общая трудоемкость дисциплины (ЗЕТ / час.)	3/108
Цель изучения дисциплины	Освоение основ кибернетической безопасности для студентов по направлению подготовки 44.04.05 «Педагогическое образование с двумя профилями подготовки»
Содержание дисциплины	Тема 1. Кибернетическая безопасность в системе национальной безопасности современной России Тема 2. Внутренние и внешние угрозы кибернетической безопасности Российской Федерации. Тема 3. Правовые основы обеспечения кибернетической безопасности Российской Федерации Тема 4. Основные информационные угрозы и общие рекомендации по организации безопасной работы в Интернете Тема 5. Безопасная работа в Интернете: анализ веб-сайтов, безопасный поиск, надежные пароли Тема 6. Безопасная работа в Интернете: электронная почта, вложения, защитное ПО Тема 7. Защитное ПО. Kaspersky Internet Security. ESET NOD32 Smart Security, Dr.Web Security Space Тема 8. Проверка компьютера и восстановление данных в экстренной ситуации Тема 9. Безопасность в социальных сетях
Формируемые компетенции (коды)	ПКУВ-2 Способен разрабатывать методику обучения отдельным разделам информатики и программирования с применением компьютерных технологий
Коды и наименование индикатора достижения компетенции	ПКУВ-2.1 Анализирует и разрабатывает альтернативные варианты методики обучения информатике с применением компьютерных технологий ПКУВ-2.2 Использует компьютерные технологии для разработки информационных моделей реальных процессов окружающего мира
Дисциплины, участвующие в формировании компетенции	Компьютерное моделирование Программное обеспечение ЭВМ и практикум по решению задач на ЭВМ Компьютерные сети Методический модуль Теория и методика обучения информатике Информационная безопасность Системы управления базами данных Проектирование информационных систем Педагогическая (методическая) практика
Образовательные технологии	Практические занятия, самостоятельная работа

Форма промежуточной аттестации	Зачёт с оценкой