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

СОГЛАСОВАНО
Декан СПФ
_____ Ю.Э. Макаревская
«10» 04 2023 г.

УТВЕРЖДАЮ
Проректор по УРиКОД
_____ А.В. Иваненко
_____ 2023 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

Семестр	Трудоем-кость (час./зет.)	Лекцион. занятий, (час.)	Практич. занятий, (час.)	Лаборат. занятий, (час.)	СРС, (час.)	КР/КП (час.)	Форма промежуточного контроля (экз./зачет)
8	**108/3**	**-**	**36**	**-**	**72**	**-**	**Зачет с оценкой**
ИТОГО	**108/3**	**-**	**36**	**-**	**72**	**-**	**Зачет с оценкой**

Сочи 2023 г.

Лист согласования рабочей программы дисциплины «Основы кибербезопасности»

Рабочую программу составил:
Симаворян С.Ж., к.т.н., доцент кафедры Информационных технологий и математики
Зубарев Е.В., старший преподаватель кафедры ПиППО

РАБОЧАЯ ПРОГРАММА РАССМОТРЕНА И ОДОБРЕНА

Заведующий кафедрой _____ Мушкина И.А.

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

Директор НОБ _____ Онищенко В.В.

Структура рабочей программы соответствует предъявляемым требованиям.

Отдел качества образования и методического обеспечения _____

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ РПД

Рабочая программа переутверждена на 20___/20___ учебный год, протокол №___ заседания кафедры от «__» ___________ 20_____г. В программу внесены дополнения и(или) изменения.

____

____

Заведующий кафедрой ___________________ ________________________

подпись ФИО

Рабочая программа переутверждена на 20___/20___ учебный год, протокол №___ заседания кафедры от «__» ___________ 20_____г. В программу внесены дополнения и(или) изменения.

____

____

Заведующий кафедрой _________________ ___________________

подпись ФИО

Рабочая программа переутверждена на 20___/20___ учебный год, протокол №___ заседания кафедры от «__» ___________ 20_____г. В программу внесены дополнения и(или) изменения.

____

____

Заведующий кафедрой _________________ ___________________

подпись ФИО

СОДЕРЖАНИЕ

1 ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....5
2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП НАПРАВЛЕНИЯ (СПЕЦИАЛЬНОСТИ).....5
3 ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....5
4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ.....6
5 УСЛОВИЯ ОСВОЕНИЯ И РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ.....12
Приложение к рабочей программе дисциплины АННОТАЦИЯ..... 16

1 ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Основы кибербезопасности» является освоение основ кибербезопасности 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 ОПОП НАПРАВЛЕНИЯ (СПЕЦИАЛЬНОСТИ)

Дисциплина относится к части, формируемой участниками образовательных отношений.

.

Таблица 1 – Междисциплинарные связи

№ п/п	Наименование компетенции	**Дисциплины, участвующие в формировании компетенции** (перечисляются дисциплины, практики, кроме ГЭ, ВКР)
ПК-2	Способен разрабатывать методику обучения отдельным разделам информатики и программирования с применением компьютерных технологий	Программирование Компьютерное моделирование Компьютерные сети Методический модуль Теория и методика обучения информатике Основы кибербезопасности Информационная безопасность Системы управления базами данных Проектирование информационных систем Педагогическая (методическая) практика Педагогическая практика (часть 2)

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	
ПК-2 Способен разрабатывать методику обучения отдельным разделам информатики и программирования с применением	ПК-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

Компетенции и индикаторы их достижения		В результате изучения дисциплины обучающиеся должны:
Код и наименование компетенции	Код и наименование индикатора достижения компетенции	
компьютерных технологий	ПК-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 3 зачетных единиц, 108 часов,

№ раздела, темы	Наименование (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	12	-	4	-	8
2	Тема 2. Внутренние и внешние угрозы кибернетической безопасности Российской Федерации.	12	-	4	-	8
3	Тема 3. Правовые основы обеспечения кибернетической безопасности Российской Федерации	12	-	4	-	8
4	Тема 4. Основные информационные угрозы и общие рекомендации по организации безопасной работы в Интернете	12	-	4	-	8
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	12	-	4	-	8
7	Тема 7. Защитное ПО. Kaspersky Internet Security. ESET NOD32 Smart Security, Dr.Web Security Space	12	-	4	-	8
8	Тема 8. Проверка компьютера и восстановление данных в экстренной ситуации	12	-	4	-	8
9	Тема 9. Безопасность в социальных сетях	12	-	4	-	8

	Зачет с оценкой	-	-	-	-	-
	ИТОГО	108	-	36	-	72

4.1.1 **Лекционные занятия**

Учебным планом не предусмотрены.

4.1.2 **Практические занятия**

№ п/п	Наименование темы 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 угроз 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 угроз 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) и микроблоги. Тематические социальные сети: Форумы. Видео и фото хостинги

4.1.3 **Лабораторные занятия**

В учебном плане отсутствуют

4.1.4 **Самостоятельная работа студента**

№ п/п	Наименование темы 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	Изучение вопросов и задач практического занятия

	кибернетической безопасности Российской Федерации.	
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: 05.06.2023). — Режим доступа: для авторизир. пользователей.
2. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/33430.html (дата обращения: 05.06.2023). — Режим доступа: для авторизир. пользователей.
3. Ермаков, Д. Г. Применение антивирусных программ для обеспечения информационной безопасности / Д. Г. Ермаков, А. В. Присяжный. — Екатеринбург : Уральский федеральный университет, ЭБС АСВ, 2013. — 64 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/66577.html (дата обращения: 05.06.2023). — 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 // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/101992.html (дата обращения: 05.06.2023). — 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. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/95409.html (дата обращения: 05.06.2023). — Режим доступа: для авторизир. Пользователей
6. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами /

А. И. Белоус, В. А. Солодуха. — Москва, Вологда : Инфра-Инженерия, 2020. — 692 c. — ISBN 978-5-9729-0486-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/98349.html (дата обращения: 05.06.2023). — 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 // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/98200.html (дата обращения: 05.06.2023). — Режим доступа: для авторизир. Пользователей

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

Таблица 3 – Перечень современных профессиональных баз данных (СПБД) и информационные справочные системы (ИСС)

№	Наименование СПБД
1.	ScienceDirect : полнотекстовая база данных : сайт / издательство Elsevier. – URL: https://www.sciencedirect.com/ (дата обращения: 05.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
2.	SpringerNature : полнотекстовая база данных: сайт / Springer Nature Switzerland AG. Part of Springer Nature. – URL: https://link.springer.com/ (дата обращения: 05.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
3.	Электронная библиотека Сочинского государственного университета : база данных. – Сочи, 2017 – . – URL: http://lib.sutr.ru/ (дата обращения: 05.06.2023). – Текст : электронный.
	Наименование ИИС
1.	КонсультантПлюс : справочно-правовая система: сайт / Компания «КонсультантПлюс». – Москва, 1997 – . – Режим доступа: локальная сеть СГУ (дата обращения: 05.06.2023) – Текст : электронный.

4.2.3 Нормативные документы

Нормативные документы

Примеры правильного описания:

1. Российская Федерация. Законы. Об образовании в Российской Федерации : Федеральный закон № 273-ФЗ : текст с изменениями и дополнениями на 2 декабря 2019 года : принят Государственной Думой 21 декабря 2012 года : одобрен Советом Федерации 26 декабря 2012 года. – Москва : Эксмо, 2018 – 144 с. – ISBN 978-5-392-26365-3. – URL: http://xn--273--84d1f.xn--p1ai/zakonodatelstvo/federalnyyzakon-ot-29-dekabrya-2012-g-no-273-fz-ob-obrazovanii-v-rf/ (дата обращения: 05.06.2023). – Текст : электронный.

2. Российская Федерация. Законы. О несостоятельности (банкротстве) : Федеральный закон № 127-ФЗ : текст с изменениями и дополнениями на 2 декабря 2019 года : принят Государственной Думой 27 сентября 2002 года : одобрен Советом Федерации 16 октября 2002 года. – Москва : Эксмо, 2019 – 510 с. – ISBN 978-5-04105596-7. – Текст : непосредственный.

3. Федеральный государственный образовательный стандарт высшего профессионального образования (ФГОС ВО 3++) магистратура по направлению подготовки 44.04.02 Психолого-педагогическое образование : утвержден приказом Министерства образования и науки Российской Федерации от «22» февраля 2018 г. № 127. – URL: https://fgosvo.ru/uploadfiles/FGOS%20VO%203++/Mag/440402_M_3_14032108.pdf (дата обращения: 05.06.2023). – Текст : электронный.

4.2.4. Интернет-ресурсы и другие электронные информационные источники
Общие Интернет-ресурсы, электронные библиотечные системы

№	Наименование Интернет-ресурсов и электронных информационных источников
1.	Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Эр Медиа». – Саратов, 2010 – . – URL: http://www.iprbookshop.ru/ (дата обращения: 05.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
2.	Университетская библиотека онлайн : электронно-библиотечная система : сайт / ООО «Нексмедиа». – Москва : Директ-Медиа, 2001 – . – URL: https://biblioclub.ru/index.php?page=book_blocks&view=main_ub (дата обращения: 05.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
3.	Образовательная платформа Юрайт : электронно-библиотечная система : сайт / ООО «Электронное издательство Юрайт». – – Москва, 2020 – . – URL: https://urait.ru/catalog/organization/DE41FE6D-0B08-4394-B225-3DD636CCCE1F (дата обращения: 05.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
4.	Сервис и туризм : тематическая коллекция / ЭБС Book.ru. – Москва, 2010 –. – URL: https://www.book.ru/cat/578/1 (дата обращения: 05.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
5.	Комплект Сочинского государственного университета / Консультант студента : электронно-библиотечная система : сайт / ООО «Политехресурс» – Электронная библиотека технического вуза. – Москва : Политехресурс, 2013 – . – URL: http://www.studentlibrary.ru/catalogue/switch_kit/x2019-138.html (дата обращения: 05.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
6.	Сетевая электронная библиотека классических университетов «Лань» : сайт / ООО ЭБС «Лань. – Санкт-Петербург, 2009 – . – URL: https://e.lanbook.com/ (дата обращения: 05.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
7.	Национальная электронная библиотека (НЭБ) : Федеральная государственная информационная система : сайт / Министерство культуры РФ. – Москва, 2004 – . – Режим доступа: https://rusneb.ru (дата обращения: 05.06.2023). – Режим доступа: локальная сеть СГУ. – Текст : электронный.
8.	Polpred.com Обзор СМИ : электронно-библиотечная система : сайт / Г. Вачнадзе, ООО «ПОЛПРЕД Справочники». – Москва, 1997 – . – URL https://polpred.com/ (дата обращения: 05.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
9.	eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru/ (дата обращения: 05.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
10.	КиберЛенинка : научная электронная библиотека открытого доступа : сайт. – Москва, 2014 –. – URL: https://cyberleninka.ru// (дата обращения: 05.06.2023). – Текст : электронный.

4.3 Формы и содержание текущей и промежуточной аттестации по дисциплине

Для оценки сформированности компетенций разрабатываются оценочные средства по дисциплине.

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

Оценочные средства по дисциплине содержат:

- материалы для текущего контроля оценки знаний по дисциплине;

- материалы для промежуточного контроля оценки знаний по дисциплине;
- критерии оценивания;
- шкалы оценивания.

Перечень вопросов подготовки к зачету с оценкой:

1. Понятие "информационная безопасность" и ее задачи
2. Составляющие информационной безопасности
3. Понятие защиты информации и ее задачи
4. Методы защиты препятствие;
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.

Примерные критерии оценивания результатов освоения дисциплины при проведении промежуточной аттестации:

Нормы оценки знаний предполагают учёт индивидуальных особенностей обучающихся, дифференцированный подход к обучению, проверке знаний, умений, уровня формирования компетенций.

В устных и письменных ответах обучающихся при выполнении практических заданий и расчетов учитываются: глубина знаний, владение необходимыми умениями (в объеме программы), логичность изложения материла, включая обобщения, выводы, соблюдение норм литературной речи, владение навыками и приемами выполнения практических заданий, подтверждение сделанных при решении практических заданий выводов соответствующими нормативными документами, правильность расчета показателей, полнота и правильность раскрытых процедур и действий в предложенном практическом задании.

Примерная шкала оценивания ответов обучающегося при проведении промежуточной аттестации по дисциплине (зачёт с оценкой):

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

Оценка **«хорошо»** выставляется обучающемуся, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приёмами их выполнения.

Оценка **«удовлетворительно»** выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, затрудняется подтвердить сделанные при решении практических заданий выводы хотя бы одним нормативным документом, допускает ошибки при проведении расчетов показателей, неточно использует основные процедуры и действия в предложенном практическом заданий.

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

5 УСЛОВИЯ ОСВОЕНИЯ И РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

5.1 Методические рекомендации обучающимся по изучению дисциплины

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

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

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

С целью более глубокого освоения темы дисциплины, конспекты следует дополнять и дорабатывать для систематизации и обобщения, используя информацию, полученную во время 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 литературы, знакомство с содержанием электронных источников, анализ ситуаций, разработку моделей, выполнение практических заданий.

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

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

5.3 Особенности преподавания дисциплины

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

Преподавание дисциплины ведется с применением элементов следующих видов образовательных технологий: информационные технологии: использование электронных образовательных ресурсов (электронный конспект, размещенный в локальной сети) при подготовке к практическим и самостоятельным занятиям.

Проблемное обучение: стимулирование студентов к самостоятельному приобретению знаний, необходимых для решения конкретных задач при выполнении домашних и практических работ.

Контекстное обучение: мотивация студентов к усвоению знаний путем выявления связей между конкретным знанием и его применением для решения профессиональных задач при выполнении домашних заданий.

Обучение на основе опыта: активизация познавательной деятельности студента за счет ассоциации и собственного опыта с предметом изучения при выполнении домашних заданий.

Междисциплинарное обучение: использование знаний из разных областей, их группировка и концентрация в контексте решаемой задачи на практических занятиях.

5.4 Материально-техническое обеспечение дисциплины

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

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

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

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

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

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

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

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

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

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

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

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

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

Бакалавриат

Профиль «Математика и информатика»

АННОТАЦИЯ

рабочей программы дисциплины
«Основы кибербезопасности»
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, платежи, 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)	ПК-2 Способен разрабатывать методику обучения отдельным разделам информатики и программирования с применением компьютерных технологий
Коды и наименование индикатора достижения компетенции	ПК-2.1 Анализирует и разрабатывает альтернативные варианты методики обучения информатике с применением компьютерных технологий ПК-2.2 Использует компьютерные технологии для разработки информационных моделей реальных процессов окружающего мира
Наименование дисциплин, необходимых для освоения данной дисциплины	Программирование Компьютерное моделирование Программное обеспечение ЭВМ и практикум по решению задач на ЭВМ Компьютерные сети Информационная безопасность Системы управления базами данных
Образовательные технологии	Практические занятия, самостоятельная работа
Форма промежуточной аттестации	Зачёт с оценкой