

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:
c7b77973654876a9af4d3b280790b7d371557fdb

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



Макаревская Ю.Э.

« 03 » 09 2021 г.



УТВЕРЖДАЮ
Проректор по УРиКОД

В.П. Ермакова

« 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	Трудоёмкость (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 «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  _____
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 «Основы кибербезопасности» является освоение основ информационной безопасности для студентов по направлению подготовки 44.03.05 «Магистратура и информатика».

Задачи дисциплины:

- овладение основными понятиями кибербезопасности и методами защиты данных, необходимыми для проведения в профессиональной работе; для продолжения образования;
- интеллектуальные развитие студентов, формирование качества мышления, необходимых для профессиональной деятельности;

- формирование представлений о целях и методах кибербезопасности;

- формирование представлений о кибербезопасности как сетевой части функционирования вычислительных систем и сетей, понимания значимости процессов кибербезопасности для будущей профессиональной деятельности.

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОИ НАПРАВЛЕНИЯ (СПЕЦИАЛЬНОСТИ)

Дисциплина «Основы кибербезопасности» является частью, формирующая участие в образовательных отношениях.

Таблица 1

Код и наименование компетенции	Дисциплины, участвующие в формировании компетенции
ПКУВ-2 Способен разрабатывать методику обучения отапливаемых помещений информатик и программирования с применением компьютерных технологий	Компьютерное моделирование Программное обеспечение ЭЕМ и периферии по решению задач по ЭЕМ Компьютерная сеть Медицинский модуль Теория и методики обучения информатике- Информационная безопасность. Системы управления базой данных Проектирование информационных систем Педагогическая (методическая) практика

Таблица 2

Код и наименование компетенции	Дисциплины, участвующие в освоении компетенции	И в результате изучения дисциплины обучающиеся должны:
ПКУВ-2 Способен разрабатывать методику обучения отапливаемых помещений информатик 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

Компетенция и индикаторы их достижения Код и наименование компетенции	Код и наименование индикатора достижения компетенции	В результате изучения дисциплины обучающиеся должны:
	ПКУВ-2.2 Использует компьютерные технологии для разработки информационных моделей реальных процессов окружающего мира	Знать методы анализа реальных данных для анализа проблем и принятия решений по кибербезопасности; Уметь анализировать и систематизировать разрозненные данные, Владеть навыками привнесения процедур анализа и принятия решений при решении задач по кибербезопасности

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Тематический план дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 108 часов.

№ парагра, темы	Наименование модуля (раздела, темы) дисциплины		ОБФО	
	Всего часов	Лекции	Практические занятия	Выполнение лабораторных работ и их трудоемкость, часы
1	Тема 1. Кибербезопасность в свете национальной безопасности современной России	6	2	4
2	Тема 2. Интуитивные и внешние угрозы кибербезопасности Российской Федерации	6	2	4
3	Тема 3. Правовые основы обеспечения кибербезопасности 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 работ, безопасный поиск, подавление вредной почты, спама, шантажа ИО	12	4	8
6	Тема 6. Безопасная работа в Интернете: зонирование сети, защита ИО	18	6	12
7	Тема 7. Защита ИО. Casperky Internet Security ESUT 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 на предусмотрено.

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, мысли при осуществлении 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 законодательства обеспечения кибернетической безопасности Российской Федерации
4	Тема 4. Основные информационные угрозы и общие рекомендации по организации безопасной работы в Интернете	Общий обзор угроз. Финансовая махинация. Кража данных учетных записей. Предоставление программы. Неполнота, возможность предоставления Рекомендаций по организации безопасной работы в Интернете
5	Тема 5. Безопасная работа в Интернете: анализ веб-сайтов, безопасный поиск, платжные порталы	Потенциально опасные веб-сайты, снижение риска безопасный поиск. Безопасная работа с веб-браузером. Настройка на веб-сайтах, порталы
6	Тема 6. Безопасная работа в Интернете: электронная почта, платжки, зашифрованные ПО	Безопасность при работе с электронной почтой и с приложениями обмена сообщениями. Безопасная работа с банковскими картами и платжными системами. Зашифрованные ПО, основные сведения
7	Тема 7. Защита от ПО. Кaspersky Internet Security, ESET NOD32 Smart Security, Dr Web Security Space	Загрузка, установка и подготовка в работе ПО антивирусных программ
8	Тема 8. Проверка компьютера и восстановление данных в экстренной ситуации	Удаление вирусов. Проверка данных. Финансовая безопасность компьютера. Дополнительные учебные задания.
9	Тема 9. Безопасность в социальных сетях	Правила безопасной работы. Настройка безопасности и конфиденциальности в социальных сетях. Ознакомление, ВКонтакте, Facebook, Мой Мир. Блоги-платформы. Автономные блоги (Standalone)

	Миробота Тематические социальные сети: Форумы Видеоконтент Безопасности
--	---

4.1.3. Лабораторные занятия

В учебном плане отсутствуют

4.1.4. Самостоятельная работа студентов

№ 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, платжные порталы	Изучение вопросов и задач практического занятия
6	Тема 6. Безопасная работа в Интернете: электронная почта, платжки, зашифрованные ПО	Изучение вопросов и задач практического занятия
7	Тема 7. Защита от ПО. Кaspersky 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-методические и информационные обеспеченные дисциплины

4.2.1. Литература

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

5. *Удаленный центр Информ-Мэ*. – Москва, [2011-]. – URL: <http://infomai.com/> (дата обращения: 25.08.2023). – Режим доступа: для авторов, пользователей. – Текст: электронный.

6. *Направления электронной библиотеки (ЕЛБ)*. – Федеральная государственная информационная система / Министерство культуры РФ. – Москва, [2004-]. – Режим доступа: <https://infobib.ru> (дата обращения: 25.08.2023). – Режим доступа: для авторов, пользователей. – Текст: электронный.

7. *Profread.com Обзор СМН*: электронно-библиотечная система / Г. Пачукадзе, ООО «ЛОДНЕРД(Сироничинан» – Москва, [1997-]. – URL: <http://profread.com/> (дата обращения: 25.08.2023). – Режим доступа: для авторов, пользователей. – Текст: электронный.

8. *Киберфлотилия*: научная электронная библиотека открытого доступа / ООО «Итрос» – Ленинград, [2014-]. – URL: <https://cyberflotilla.ru/> (дата обращения: 25.08.2023). – Текст: электронный.

9. *eLIBRARY.RU*: научная электронная библиотека / Компания «Научная электронная библиотека (eLIBRARY.RU)» – Москва, [2006-]. – URL: <https://elibrary.ru/> (дата обращения: 25.08.2023). – Режим доступа: для авторов, пользователей. – Текст: электронный.

4.3 Формы и содержание текстов и промежуточный аттестации по дисциплине
 Для оценки сформированности компетенций разрабатываются оценочные средства по дисциплине.

Формы и содержание текстов и промежуточный аттестации по дисциплине раскрыты в фонде оценочных средств, который является открытым документом.

Оценочные средства по дисциплине содержат:

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

Перечень вопросов учебного курса и подходов к занятию с оценкой:

1. Понятие "информационная безопасность" и ее задачи
2. Составляющие информационной безопасности
3. Понятие защиты информации и ее задачи
4. Методы защиты информации;
5. Методы защиты персональных данных;
6. Методы защиты механизмы шифрования;
7. Методы защиты противодействие атакам вредоносных программ;
8. Методы защиты регулятивные;
9. Методы защиты приуроживание;
10. Методы защиты избуждение;
11. Информационная безопасность
12. Понятие кибербезопасности
13. Компьютерная безопасность
14. Компьютерные преступления
15. Понятие информационных угроз
16. Предопределенные программные обеспечения
17. Понятие киберпреступности
18. Классификация киберпреступности
19. Мотивированность и стимулы атаки
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

электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/97562.html> (дата обращения: 25.08.2023). — Режим доступа: для авторизир. пользователей

2. Артемов, А. В. Информационная безопасность: курс лекций / А. В. Артемов. — Орел: Местнонациональная Академия безопасности и качества (МАБНБ), 2014. — 256 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/23430.html> (дата обращения: 25.08.2023). — Режим доступа: для авторизир. пользователей

3. Ермаков, Д. Г. Приспособление антивирусных программ для обеспечения информационной безопасности / Д. Г. Ермаков, А. В. Цирюков. — Екатеринбург: Уралский федеральный университет, 2021. — 61 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/96577.html> (дата обращения: 25.08.2023). — Режим доступа: для авторизир. пользователей

4. Мэйнолд, Э. Безопасность сетей: учебные пособия / Э. Мэйнолд. — 3-е изд. — Москва: Интернет-Университет Информационных Технологий (ИИТЭИТ), Ай Пи Ар Медиа, 2021. — 371 с. — ISBN 978-5-4497-0863-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/101992.html> (дата обращения: 25.08.2023). — Режим доступа: для авторизир. пользователей

5. Основные направления безопасности: учебно-методическое пособие / составители С. Ю. Мухом. — Орел: Местнонациональная Академия безопасности и качества (МАБНБ), 2019. — 88 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/95409.html> (дата обращения: 25.08.2023). — Режим доступа: для авторизир. пользователей

6. Белюс, А. В. Основы кибербезопасности: Стандрты, концепции, методы и средства обеспечения / А. В. Белюс, В. А. Соловуха. — Москва: Технофора, 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: 25.08.2023). — Режим доступа: для авторизир. пользователей

7. Костин, В. И. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей: учебное пособие / В. И. Костин. — Москва: Издательский дом МНЭ-ИС, 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: 25.08.2023). — 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 Современного государственного университета*: база данных. — Сочи, [2017-]. — URL: <http://lib.sgu.ru/> (дата обращения: 25.08.2023). — Текст: электронный.
2. *ScienceDirect*: полнотекстовая база данных / издательство Elsevier. — URL: <https://www.sciencedirect.com/> (дата обращения: 25.08.2023). — Режим доступа: для авториз. пользователей. — Текст: электронный.
3. *Springer Nature*: полнотекстовая база данных / Springer Nature Switzerland AG. Part of Springer Nature. — URL: <https://link.springer.com/> (дата обращения: 25.08.2023). — Режим доступа: для авториз. пользователей. — Текст: электронный.
4. *IPRbooks*: электронно-библиотечная система / ИБС IPRbooks; ООО «Ай Пи Эр Медиа», электронное переводческое издание «www.iprbookshop.ru». — Саратов, [2010-]. — URL: <http://www.iprbookshop.ru/> (дата обращения: 25.08.2023). — Режим доступа: для авториз. пользователей. — Текст: электронный.

В целях максимального усвоения дисциплины используются следующие технологии обучения:

- Практическая работа - совместная деятельность студентов в группе под руководством лектора, направлена на решение общей задачи путем творческого сопоставления результатов индивидуальной работы членами команды с акцентом на коммуникативный и ответственности.
- Самостоятельная работа студента, предусматривает выполнение работы - задания, которое требует от студента самостоятельного вникновения в изучаемый материал, анализ, определение первоисточников, и т.д. и т.п., как правило, творческого подхода и ориентированности на решение задачи на комплексный подход к обучению и развитию личности и деятельности, ориентированной на развитие личности обучающегося и потребности личности, общества и государства и в работе у обучающихся сложными политехническими задачами, черт и качеств характера, отношений и опыта поведения.
- Преподнесение дисциплины опирается на комплексный подход к обучению и ориентированности на решение задачи на комплексный подход к обучению и развитию личности и деятельности, ориентированной на развитие личности обучающегося и потребности личности, общества и государства и в работе у обучающихся сложными политехническими задачами, черт и качеств характера, отношений и опыта поведения.

Применение всех видов занятий при преподавании дисциплины, позволяет коммуникативной, коммуникативной и коммуникативной деятельности с применением электронного обучения и дистанционных образовательных технологий.

5.4 Материально-техническое обеспечение дисциплины

При обучении дисциплине необходимо использовать материально-техническое обеспечение: 1. Кабинет для проведения лекционных и практических занятий, оборудованный индивидуальными компьютерами, тестовым контролем и промежуточной аттестацией коммутационно-сетевыми средствами, обеспечивающие обучение и учебно-наглядные пособия. 2. Помещение для самостоятельной работы библиотекаря, читальный зал, помещение для самостоятельной работы, стола, стулья. Компьютерная техника с подключением к сети Интернет с обеспечением доступа в ЭИОС университета.

Дистанционная поддержка дисциплины.

Для передачи раздаточного материала в практическим занятием, доминирующей, 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	Средовой-правовая система Консультант Плюс

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

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

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

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

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

- 30. Справочное приложение
- 31. Административное приложение или приложение открытого ключа
- 32. ЭИОС
- 33. Защита документов MS Word
- 34. Защита документов MS Excel
- 35. Архивирование файлов Windows и их защита
- 36. Паруша и методы борьбы с ними.
- 37. Антивирусные программы и пакеты.

5.5 ОСОБЕННОСТИ И РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

5.3 Методические рекомендации обучающихся по изучению дисциплины
Промежуточная аттестация может быть выставлена студенту по результатам текущей аттестации и (или) по результатам факельного интернет-тестирования (ФЭИО), интернет-тестирования).

Чтобы освоить учебный материал любой дисциплины, необходимо регулярно посещать все занятия, не отпадать в начале занятий и обязательно комментировать учебно-методические рекомендации на практических занятиях. Практические занятия дают знания, которые подчас невозможно найти даже в лучших учебниках. Необходимо постоянно акцентировать все, что говорит преподаватель, поэтому следует постараться выписать основные положения, идеи, выводы, понять логику учебного материала, излагать его преподавателем. При необходимости желательно использовать памятки для заинтересованного студента общения и учебные листы.

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

С целью более глубокого освоения темы дисциплины, студенты советуют дополнять и дополнять для систематизации и обобщения, использовать информационно, полученную во время практического занятия, а также рекомендованную учебно-методическую литературу и Интернет-ресурсы. Анализировать работу необходимо выполнять и при разработке тем дисциплины, предлагаемых для самостоятельного изучения.

Рекомендуется работать в себе привычку просматривать, пересматривать через тематический практический занятием текст предыдущего занятия.

Если возникает вопрос, обязательно обращайтесь за консультацией к преподавателю после занятия (или во время занятия при его вопросе в студенте «Все понятно?») и разъяснении, четко формулируя конкретные вопросы в понимании учебного материала.

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

При выполнении промежуточной аттестации необходимо получить у преподавателя перечень дополнительных заданий базисной и типовой содержание заданий по программе анализа и практических условий по дисциплине.

5.3 Организация самостоятельной работы студента по дисциплине

Самостоятельная работа студента включает подготовку практических занятий, чтение обязательной и дополнительной литературы, взаимодействие с содержанием электронных источников, анализ ситуаций, разработку моделей, выполнение практических заданий.

Для обеспечения выполнения самостоятельной работы по дисциплине «Информационная безопасность» студентам 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

Бакалавриат

Профиль «Математика и информатика»

АННОТАЦИЯ

рабочей программы дисциплины
 Основы кибербезопасности
 дисциплины части учебного плана, формируемой участниками образовательных отношений
 очной формы обучения

Общая трудоемкость дисциплины (ЭЕТ / 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. Интуитивное и впадение угрозы кибернетической безопасности Российской Федерации. Тема 3. Правовые основы обеспечения кибернетической безопасности Российской Федерации Тема 4. Основные информативные 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, мессенджеры Тема 7. Защита ПО. Каренский 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 ИСУВ-2. Способен разрабатывать методику обучения отдаленным разделам информатики и программирования с применением компьютерных технологий ИСУВ-2.1. Анализирует и разрабатывает альтернативные варианты методики обучения информатике с применением компьютерных технологий ИСУВ-2.2. Использует компьютерные технологии для разработки информативных моделей реальных процессов окружающей среды Компьютерное моделирование Программное обеспечение ЭИМ и практикум по решению задач на ЭИМ Компьютерные сети Методический модуль Теория и методика обучения информатике Информационная безопасность Системы управления базами данных Проектирование информационных систем Педагогическая (методическая) практика Практическое занятие, самостоятельная работа
Формируемые компетенции (коды)	
Коды и наименование индикатора	
достижимости	
компетенции	
Дисциплина, участвующая в формировании компетенции	
Образовательные технологии	

знаний. Иными словами, как правило, формы обучения и контроля знаний, образовательные технологии и оценочные материалы.

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

Дистанционное обучение обеспечивает возможность коммуникации с преподавателем, а также с другими обучающимися посредством webinar (например, с использованием программы Skype), что способствует созданию группы, расширяет учебную группу на совместную работу, обучение, принятие группового решения.

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

Подбор и разработка учебных материалов производится преподавателем с учетом того, чтобы студенты с нарушениями слуха получили информативно визуально, с нарушениями зрения – аудиально (например, с использованием программы-синтезаторов речи).

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся инвалидам и лиц с ОВЗ фонд оценочных средств по дисциплине, позволяющий оценить достижение ими результатов обучения и уровень сформированности компетенций, предусмотренных учебным планом и лиц с 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 обучающийся предоставляется дополнительное время для подготовки ответа при прохождении аттестации.

Фирма промышленной ИНТЕЛЛЕКТУАЛ	Листы с рисунками
---------------------------------------	-------------------