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

**СОГЛАСОВАНО**
Декан СПФ _____ Иванов И.А.
«3» августа 2019 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.) | КРЗ | Форма промежуточного контроля (экз./зачет) |
|---|---|---|---|---|---|---|---|---|
| **ОФО** | | | | | | | | |
| **8** | **108/3** | **-** | **36** | **-** | **72** | **-** | **-** | **ЗачетО** |
| **ИТОГО** | **108/3** | **-** | **36** | **-** | **72** | **-** | **-** | **ЗачетО** |

**Сочи 2019 г.**

Рабочая программа по дисциплине Основы кибербезопасности составлена в соответствии с требованиями ФГОС ВО 3++ по направлению подготовки 44.03.05 Педагогическое образование с двумя профилями подготовки (утвержден Приказом Минобрнауки № 125 от 22.02.2018)

Рабочую программу составил: подпись Симаворян С.Ж.

**РАБОЧАЯ ПРОГРАММА РАССМОТРЕНА И ОДОБРЕНА**

на заседании кафедры Прикладной математики и информатики

Протокол № 1 от «29» 08 2019 г.

Заведующий кафедрой Макарова И.Л.

Руководитель ОПОП Иванов И.А.

Рабочая программа одобрена на заседании Учебно-методического совета направления 44.03.05 Педагогическое образование (с двумя профилями подготовки)

Протокол № 01 от «30» 08 2019 г.

Председатель УМСН Иванов И.А.

Структура рабочей программы соответствует предъявляемым требованиям

Отдел качества образования и методического обеспечения Васильченко В.В.

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ РПД**

Рабочая программа переутверждена на 2020/2021 учебный год, протокол № 1 заседания кафедры от «29» августа 2020 г. В программу внесены дополнения и (или) изменения:

5.3 Особенности преподавания дисциплины

5.4 Материально-техническое обеспечение дисциплины

Обновлен список литературы.

Заведующий кафедрой  Макарова И.Л.

подпись ФИО

Рабочая программа переутверждена на 2022/2023 учебный год, протокол №1 заседания кафедры от «30» августа 2022 г. В программу внесены дополнения и(или) изменения.

На основании распоряжения ректора № 243-р, от 06.07.22 г. в рабочую программу дисциплины внесены изменения – Профессиональные компетенции установленные вузом (ПКУВ) на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников считать Профессиональными компетенциями определенными организацией самостоятельно на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников (ПК).

ПКУВ-2 считать ПК-2.

Заведующий кафедрой  Макарова И.Л

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

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 «Основы кибербезопасности» является относится к Блоку 1 «Дисциплины (модули)», и является вариативной дисциплиной.

Таблица 1

| **Наименование категории (группы) компетенций** | **Код и наименование компетенции** | **Предшествующие дисциплины** | **Последующие дисциплины** |
|---|---|---|---|
| **Универсальные компетенции** | | | |
| | ПКУВ-2 | Б1.В.02 Программирование<br>Б1.В.06 Компьютерное моделирование<br>Б1.В.07 Программное обеспечение ЭВМ и практикум по решению задач на ЭВМ<br>Б1.В.08 Компьютерные сети<br>Б1.В.ДВ.02.02 Информационная безопасность<br>Б1.В.ДВ.03.01 Системы управления базами данных | Б1.В.09 Методический модуль<br>Б1.В.09.02 Теория и методика обучения информатике<br>Б1.В.ДВ.03.02 Проектирование информационных систем |

## 3 ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**УК** – универсальные компетенции;
**ОПК** – общепрофессиональные компетенции;
**ПК** – профессиональные компетенции;
**ПКО** – профессиональные компетенции обязательные;
**ПКР** – профессиональные компетенции рекомендуемые;
**ПКУВ** – профессиональные компетенции, установленные вузом.

Таблица 2

| **Компетенции и индикаторы их достижения** | | | В результате изучения дисциплины обучающиеся должны: |
|---|---|---|---|
| Категория компетенций | 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 | З.1-ПКУВ-2.1 Знать основные принципы сбора информации по кибербезопасности;<br>У.1-ПКУВ-2.1 Уметь решать задачи по отбору актуальной информации по кибербезопасности;<br>Н.1-ПКУВ-2.3 Владеть методами системного обобщения информации для решения задач по кибербезопасности |
| | | ПКУВ-2.2 Использует компьютерные технологии для разработки информационных моделей реальных процессов окружающего мира | З.1-ПКУВ-2.2 Знать методы анализа разнородных данных для анализа проблем и принятия решений по кибербезопасности;<br>У.1-ПКУВ-2.2 Уметь анализировать и систематизировать разнородные данные,<br>Н.1-ПКУВ-2.2 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 модуля (раздела, темы) дисциплины | ОФО | | | | | |
|---|---|---|---|---|---|---|---|
| | | Всего часов | Виды учебной нагрузки и их трудоемкость, часы | | | | |
| | | | Лекции | Практические занятия | Лабораторные работы | СРС | Контроль |
| 1 | Тема 1. Кибернетическая безопасность в системе национальной безопасности современной России | 6 | - | 2 | - | 4 | 0 |
| 2 | Тема 2. Внутренние и внешние угрозы кибернетической безопасности Российской Федерации. | 6 | - | 2 | - | 4 | 0 |
| 3 | Тема 3. Правовые основы обеспечения кибернетической безопасности Российской Федерации | 6 | - | 2 | - | 4 | 0 |
| 4 | Тема 4. Основные информационные угрозы и общие рекомендации по организации безопасной работы в Интернете | 6 | - | 2 | - | 4 | 0 |
| 5 | Тема 5. Безопасная работа в Интернете: анализ веб-сайтов, безопасный поиск, надежные пароли | 12 | - | 4 | - | 8 | 0 |
| 6 | Тема 6. Безопасная работа в Интернете: электронная почта, платежи, защитное ПО | 18 | - | 6 | - | 12 | 0 |
| 7 | Тема 7. Защитное ПО. Kaspersky Internet Security. ESET NOD32 Smart Security, Dr.Web Security Space | 18 | - | 6 | - | 12 | 0 |
| 8 | Тема 8. Проверка компьютера и восстановление данных в экстренной ситуации | 18 | - | 6 | - | 12 | 0 |
| 9 | Тема 9. Безопасность в социальных сетях | 18 | - | 6 | - | 12 | 0 |
| | ЗачетО | - | - | - | - | - | - |
| | ИТОГО | 72 | - | 36 | - | 72 | 0 |

#### 4.1.1 Лекционные занятия

Учебным планом не предусмотрены.

#### 4.1.2 Практические занятия

| № п/п | Наименование модуля, раздела дисциплины | Объем, часов | Краткое содержание | Формируемые ЗУН | Ссылки на литературу |
|---|---|---|---|---|---|
| 1 | Тема 1. Кибернетическая безопасность в системе национальной безопасности современной России | 2 | Анализ сущности и содержание Доктрины информационной безопасности Российской Федерации, модели его совершенствования в рамках кибернетической безопасности | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 2 | Тема 2. Внутренние и внешние угрозы кибернетической безопасности Российской Федерации. | 2 | Анализ внутренних и внешних угроз кибернетической безопасности Российской Федерации | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 3 | Тема 3. Правовые основы обеспечения кибернетической безопасности Российской Федерации | 2 | Анализ законодательного обеспечения кибернетической безопасности Российской Федерации | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 4 | Тема 4. Основные информационные угрозы и общие рекомендации по организации безопасной работы в Интернете | 2 | Общий обзор угроз Финансовые махинации Кража данных учетных записей Вредоносные программы Неосторожность пользователя Рекомендации по организации безопасной работы в Интернете | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 5 | Тема 5. Безопасная работа в Интернете: анализ веб-сайтов, безопасный поиск, надежные пароли | 4 | Потенциально опасные веб-сайты: снижение риска Безопасный поиск Безопасная работа с веб-браузером Регистрация на веб-сайтах, пароли | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 6 | Тема 6. Безопасная работа в Интернете: электронная почта, платежи, защитное ПО | 6 | Безопасность при работе с электронной почтой и с системами обмена сообщениями Безопасная работа с банковскими картами и платежными системами Защитное ПО, основные сведения | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 7 | Тема 7. Защитное ПО. Kaspersky Internet Security. ESET NOD32 Smart Security, Dr.Web Security Space | 6 | Загрузка, установка и подготовка к работе ПО антивирусных программ | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 8 | Тема 8. Проверка компьютера и восстановление данных в экстренной | 6 | Резервное копирование Шифрование данных Физическая безопасность компьютера | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, | [1-7] |

| | | | | | |
|---|---|---|---|---|---|
| | ситуации | | Дополнительные учетные записи. | У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | |
| 9 | Тема 9. Безопасность в социальных сетях | 6 | 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 | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| | ИТОГО | 36 | | | |

**4.1.3 Лабораторные занятия**

В учебном плане отсутствуют

**4.1.4 Самостоятельная работа студента**

| № п/п | Наименование модуля, раздела дисциплины | Объем, часов | Вид СРС | Формируемые ЗУН | Ссылки на литературу |
|---|---|---|---|---|---|
| 1 | Тема 1. Кибернетическая безопасность в системе национальной безопасности современной России | 4 | Изучение вопросов и задач практического занятия | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 2 | Тема 2. Внутренние и внешние угрозы кибернетической безопасности Российской Федерации. | 4 | Изучение вопросов и задач практического занятия | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 3 | Тема 3. Правовые основы обеспечения кибернетической безопасности Российской Федерации | 4 | Изучение вопросов и задач практического занятия | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 4 | Тема 4. Основные информационные угрозы и общие рекомендации по организации безопасной работы в Интернете | 4 | Изучение вопросов и задач практического занятия | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 5 | Тема 5. Безопасная работа в Интернете: анализ веб-сайтов, безопасный поиск, надежные пароли | 8 | Изучение вопросов и задач практического занятия | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 6 | Тема 6. Безопасная работа в Интернете: электронная почта, | 12 | Изучение вопросов и задач практического занятия | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, | [1-7] |

| | | | | | |
|---|---|---|---|---|---|
| | платежи, защитное ПО | | | З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | |
| 7 | Тема 7. Защитное ПО. Kaspersky Internet Security. ESET NOD32 Smart Security, Dr.Web Security Space | 12 | Изучение вопросов и задач практического занятия | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 8 | Тема 8. Проверка компьютера и восстановление данных в экстренной ситуации | 12 | Изучение вопросов и задач практического занятия | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| 9 | Тема 9. Безопасность в социальных сетях | 12 | Изучение вопросов и задач практического занятия | З.1-ПКУВ-2.1, У.1-ПКУВ-2.1, Н.1-ПКУВ-2.3, З.1-ПКУВ-2.2, У.1-ПКУВ-2.2, Н.1-ПКУВ-2.2. | [1-7] |
| | ИТОГО | 72 | | | |

#### 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 [Электронный ресурс] / В. А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — 978-5-94774-821-5. — Режим доступа: http://www.iprbookshop.ru/52209.html

2. Артемов, А. В. Информационная безопасность [Электронный ресурс] : курс лекций / А. В. Артемов. — Электрон. текстовые данные. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/33430.html

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

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

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

6. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Москва, Вологда : Инфра-Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/98349.html

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

**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: 10.07.2019). – Текст : электронный.

2. ScienceDirect: полнотекстовая база данных / издательство Elsevier. – URL: https://www.sciencedirect.com/ (дата обращения: 10.07.2019). – 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: 10.07.2019). – 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: 10.07.2019). – 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: 10.07.2019). – 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: 10.07.2019). – 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: 10.07.2019). – Режим доступа: для авториз. пользователей. – Текст : электронный.

8. КиберЛенинка : научная электронная библиотека открытого доступа / ООО «Итеос». – Электрон. дан. – Москва, [2014-]. – URL: https://cyberleninka.ru/ (дата обращения: 10.07.2019). – Текст : электронный.

9. eLIBRARY.RU : научная электронная библиотека / Компания «Научная электронная библиотека» (eLIBRARY.RU). – Москва, [2000-]. – URL: https://elibrary.ru/ (дата обращения: 10.07.2019). – Режим доступа: для авториз. пользователей. – Текст : электронный

Учебно-методическое и информационное обеспечение дисциплины соответствует библиотечному фонду СГУ

Зав.библиотекой  Мысина Е.С.

подпись

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

Текущая аттестация по дисциплине осуществляется в форме устного опроса.

Содержание текущей аттестации по дисциплине раскрывается в фонде оценочных средств, предназначенном для проверки соответствия уровня подготовки по дисциплине.

Оценочные средства по дисциплине содержат:

- перечень вопросов устного опроса;
- перечень вопросов к зачету.

Перечень вопросов устного опроса и подготовки к зачету:

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.

## 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

Проведение всех видов занятий (лекционные, практические, лабораторные и т.д.) 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. При организации занятий, текущей и промежуточной аттестации с применением электронного обучения и дистанционных образовательных технологий используются различные электронные образовательные ресурсы и онлайн сервисы, в том числе: Skype, Zoom, Big Blue Button, Moodle, WhatsApp.
2. Аудитории для проведения занятий лекционного типа
3. Презентационный комплект (ноутбук, проектор, экран)
4. Аудитории для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (Компьютеры 14шт. с возможностью подключения к сети «Интернет»)
5. Аудитории для самостоятельной работы (Компьютерный класс - 15 компьютеров. Локальная сеть. Подключение к сети Интернет. Электронные базы данных)

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

*1. Microsoft Windows 7 Professional, 8 Pro, 8.1 Pro, 10 Pro*
*Лицензионный договор №03181000468150000030-0003440-01 (06/16гпд) от 13.01.2016.*
*Срок действия – бессрочная лицензия.*
*Лицензионный договор №ВК01492/2892 (163/16д) от 05.04.2016.*
*Срок действия – 05.04.2020.*
*2. Microsoft Office Professional Plus 2007, 2010, 2013, 2016.*
*Состав продукта:*
*Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Outlook, Microsoft Publisher, Microsoft Access, Microsoft OneNote, Microsoft InfoPath.*
*Лицензионный договор №03181000468150000029-003440-01 (05/16-гпд) от 13.01.2016.*
*Срок действия – бессрочная лицензия.*
*3. Антивирусное программного обеспечение Kaspersky Security. Отечественное ПО.*
*Лицензионный договор №ВК (ИКЗ 181232005119923200100100070010000000) № 101/18д от 02.03.2018 г.*
*Срок действия обновлений – по 30.03.2019.*
*Лицензионный договор №04-S00310L (92/19д) от 01.03.2019 г.*
*Срок действия обновлений – по 28.03.2020 г.*
*4. Архиватор 7-zip. Свободно распространяемое ПО.*
*Бесплатное программное обеспечение. Срок действия – бессрочная лицензия.*
*5. Adobe Reader. Свободно распространяемое ПО.*
*Бесплатное программное обеспечение. Срок действия – бессрочная лицензия.*

### 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**
дисциплина Блока 1 в вариативной части
очная форма обучения

Составитель аннотации – Симаворян С.Ж., доцент каф. ПМиИ

| | |
|---|---|
| **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<br>Тема 2. Внутренние и внешние угрозы кибернетической безопасности Российской Федерации.<br>Тема 3. Правовые основы обеспечения кибернетической безопасности Российской Федерации<br>Тема 4. Основные информационные угрозы и общие рекомендации по организации безопасной работы в Интернете<br>Тема 5. Безопасная работа в Интернете: анализ веб-сайтов, безопасный поиск, надежные пароли<br>Тема 6. Безопасная работа в Интернете: электронная почта, платежи, защитное ПО<br>Тема 7. Защитное ПО. Kaspersky Internet Security. ESET NOD32 Smart Security, Dr.Web Security Space<br>Тема 8. Проверка компьютера и восстановление данных в экстренной ситуации<br>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<br>ПКУВ-2.2 Использует компьютерные технологии для разработки информационных моделей реальных процессов окружающего мира |
| **Наименование дисциплин, необходимых для освоения данной дисциплины** | Б1.В.02 Программирование<br>Б1.В.06 Компьютерное моделирование<br>Б1.В.07 Программное обеспечение ЭВМ и практикум по решению задач на ЭВМ<br>Б1.В.08 Компьютерные сети<br>Б1.В.ДВ.02.02 Информационная безопасность<br>Б1.В.ДВ.03.01 Системы управления базами данных |
| **Образовательные технологии** | Практические занятия |
| **Формы текущего** | Текущая аттестация по дисциплине осуществляется в форме устного |

| | |
|---|---|
| **контроля успеваемости** | опроса |
| **Форма промежуточной аттестации** | ЗачётО |

Зав. кафедрой Прикладной математики и информатики Макарова И.Л.