

Документ подписан посредством электронной подписи

Информация о владельце:

ФИО: Кислова Наталья Николаевна

Должность: Проректор по УМР и качеству образования

Дата подписания: 14.12.2023

Уникальный программный ключ:

52802513f5b14a975b7e9b13008093d5726b159bf6064f865ae65b96a966c035

**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

**«Самарский государственный социально-педагогический университет»**

**Кафедра информатики, прикладной математики и методики их преподавания**

УТВЕРЖДАЮ

Проректор по УМР и КО,  
председатель УМС СГСПУ

 Н.Н. Кислова

# МОДУЛЬ "ПРЕДМЕТНОЕ ОБУЧЕНИЕ. ИНФОРМАТИКА"

## Методы и технологии защиты информации рабочая программа дисциплины (модуля)

Закреплена за кафедрой	<b>Информатики, прикладной математики и методики их преподавания</b>		
Учебный план	ФМФИ-621ИДо(5г).plx Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки) Направленность (профиль) «Информатика» и «Дополнительное образование (в области информатики и ИКТ)»		
Квалификация	<b>бакалавр</b>		
Форма обучения	<b>очная</b>		
Общая трудоемкость	<b>3 ЗЕТ</b>		
Часов по учебному плану	108	Виды контроля в семестрах:	
в том числе:		зачеты с оценкой 9	
аудиторные занятия	42		
самостоятельная работа	66		

### Распределение часов дисциплины по семестрам

Семестр(Курс.Номер семестра на курсе)	9(5.1)		Итого	
	УП	РПД	УП	РПД
Вид занятий				
Лекции	16	16	16	16
Лабораторные	26	26	26	26
В том числе инт.	4	4	4	4
Итого ауд.	42	42	42	42
Контактная работа	42	42	42	42
Сам. работа	66	66	66	66
Итого	108	108	108	108

Программу составил(и):

**Добудько А.В.**

При наличии обучающихся из числа лиц с ограниченными возможностями здоровья, которым необходим особый порядок освоения дисциплины (модуля), по их желанию разрабатывается адаптированная к ограничениям их здоровья рабочая программа дисциплины (модуля).

Рабочая программа дисциплины

**Методы и технологии защиты информации**

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) (приказ Минобрнауки России от 22.02.2018 г. № 125)

составлена на основании учебного плана:

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль) «Информатика» и «Дополнительное образование (в области информатики и ИКТ)»

утвержденного учёным советом вуза от 31.08.2020 протокол № 1.

Рабочая программа одобрена на заседании кафедры

**Информатики, прикладной математики и методики их преподавания**

Протокол от 25.08.2020 г. №1

Зав. кафедрой Т.В. Добудько

Начальник УОП



Н.А. Доманина

### 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

**Цель изучения дисциплины:** формирование готовности бакалавров к использованию методов и технологий защиты информации в профессиональной деятельности

**Задачи изучения дисциплины:**

формирование у бакалавров систематизированных знаний, умений и навыков в области методов и технологий защиты информации.

**Область профессиональной деятельности:**

**01 Образование и наука (в сфере начального общего, основного общего, среднего общего образования, профессионального обучения, профессионального образования, дополнительного образования; в сфере научных исследований)**

### 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ОП: Б1.О.03

#### 2.1 Требования к предварительной подготовке обучающегося:

Содержание дисциплины базируется на материале:

«Программное обеспечение электронно-вычислительной машины»

«Теоретические основы информатики»

«Вычислительные системы, сети и телекоммуникации»

«Основы цифровой микроэлектроники»

#### 2.2 Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

«Технология разработки электронных образовательных ресурсов в школе и методика их оценки»

Производственная практика (преддипломная практика)

### 3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

**ОПК-1. Способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики**

**ОПК-1.1. Знает приоритетные направления развития системы образования Российской Федерации, законы и иные нормативные правовые акты, регламентирующие деятельность в сфере образования в Российской Федерации, нормативные документы по вопросам обучения и воспитания детей и молодежи, федеральные государственные образовательные стандарты, законодательные документы о правах ребенка, актуальные вопросы трудового законодательства; конвенцию о правах ребенка**

Знает: положения основных нормативных документов, регламентирующих деятельность в области защиты информации образовательных учреждений.

**ОПК-1.2. Умеет применять основные нормативно-правовые акты в сфере образования и нормы профессиональной этики**

Умеет: оценивать возможные последствия существующих угроз информационного общества, выбирать способы защиты от угроз, анализировать и обобщать информацию о состоянии информационной среды образовательной организации.

**ОПК-1.3. Владеет действиями по соблюдению правовых, нравственных и этических норм, требований профессиональной этики в условиях реальных педагогических ситуаций; действиями по осуществлению профессиональной деятельности в соответствии с требованиями федеральных государственных образовательных стандартов в части анализа содержания современных подходов к организации и функционированию системы образования**

Владеет: приемами защиты информации обучающихся в образовательном процессе при работе со средствами информационно-коммуникационных технологий.

### 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Интеракт.
	<b>Раздел 1. Методы и технологии защиты информации</b>			
1.1	Информация как объект защиты /Лек/	9	2	
	Информация как объект защиты /Лаб/	9	2	
	Информация как объект защиты /Ср/	9	8	
1.2	Информационная безопасность /Лек/	9	2	
	Информационная безопасность /Лаб/	9	2	
	Информационная безопасность /Ср/	9	8	
1.3	Критерии оценки безопасности компьютерных систем /Лек/	9	2	
	Критерии оценки безопасности компьютерных систем /Лаб/	9	2	
	Критерии оценки безопасности компьютерных систем /Ср/	9	8	
1.4	Криптографические средства защиты информации /Лек/	9	2	
	Криптографические средства защиты информации /Лаб/	9	2	

	Криптографические средства защиты информации /Ср/	9	8	
1.5	Электронная цифровая подпись /Лек/	9	2	
	Электронная цифровая подпись /Лаб/	9	4	
	Электронная цифровая подпись /Ср/	9	8	
1.6	Защита от копирования /Лек/	9	2	
	Защита от копирования /Лаб/	9	4	
	Защита от копирования /Ср/	9	8	
1.7	Программы с потенциально опасными последствиями /Лек/	9	2	
	Программы с потенциально опасными последствиями /Лаб/	9	4	2
	Программы с потенциально опасными последствиями /Ср/	9	8	
1.8	Защита в интернет /Лек/	9	2	
	Защита в интернет /Лаб/	9	4	2
	Защита в интернет /Ср/	9	10	

## 5. Оценочные и методические материалы по дисциплине (модулю)

### 5.1. Содержание аудиторной работы по дисциплине (модулю)

<p>Лекция №1. Информация как объект защиты. Вопросы Введение в защиту информации и информационную безопасность. Нормативные документы, регламентирующие деятельность в области защиты информации образовательных учреждений.</p> <p>Лекция №2. Информационная безопасность Вопросы Информационная безопасность. Основные угрозы информационной безопасности. Обеспечение информационной безопасности. Аппаратно-программные средства защиты информации</p> <p>Лекция №3. Критерии оценки безопасности компьютерных систем Вопросы Критерии оценки безопасности компьютерных систем. Оранжевая книга. Основные элементы политики безопасности. Классы безопасности.</p> <p>Лекция №4. Криптографические средства защиты информации Вопросы Простые криптосистемы. Шифрование методом замены (подстановки). Шифрование методом перестановки. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Организационные проблемы криптозащиты.</p> <p>Лекция №5. Электронная цифровая подпись Вопросы Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Алгоритм безопасного хэширования SHA. Отечественный стандарт хэш-функции. Алгоритмы электронной цифровой подписи. Алгоритм цифровой подписи Эль Гамала (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.</p> <p>Лекция №6. Защита от копирования Вопросы Защита от копирования. Защита CD от копирования. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя. Протоколы идентификации с нулевой передачей знаний.</p> <p>Лекция №7. Программы с потенциально опасными последствиями Вопросы Программы с потенциально опасными последствиями. Вирус. Люк. Троянский конь. Логическая бомба. Программные закладки. Атака салями.</p> <p>Лекция №8. Защита в интернет Вопросы Межсетевые экраны. Компьютерные атаки и технологии их обнаружения. Безопасность электронной коммерции. Безопасность электронных платежных систем. Идеальная служба информационной безопасности.</p> <p>Лабораторная работа №1. Информация как объект защиты Задания: ознакомится с положения основных нормативных документов, регламентирующих деятельность в области защиты информации образовательных учреждений</p> <p>Лабораторная работа №2. Средства защиты компьютера от вирусов Задания: Ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидностями вирусов, способами заражения и методами борьбы. Ознакомиться с различными видами программных средств защиты от вирусов. Получить навыки работы с антивирусным пакетом.</p> <p>Лабораторная работа №3. Построение кода постоянной длины Вопросы 1. Изучить метод построения кода постоянной длины и оценить эффективность полученного кода.</p> <p>Лабораторная работа №4. Построение кода переменной длины Задания 1. Изучить метод построения кода переменной длины, оценить эффективность полученного кода и сравнить ее с эффективностью кода постоянной длины.</p>
---

Лабораторная работа №5. Методы защиты информации. Шифр простой перестановки  
Задания  
1. Выполнить шифрование заданного сообщения простейшим шифром перестановки и выполнить проверку правильности шифрования.

Лабораторная работа №6. Методы защиты информации. Шифр Цезаря  
Задания  
1. Освоить технологию шифрования и дешифрования информации с использованием шифра Цезаря.

Лабораторная работа №7. Модифицированный шифр Цезаря со сдвигом по кодовому слову  
Задания  
1. Освоить технологию шифрования и дешифрования информации с использованием Модифицированного шифра Цезаря.

Лабораторная работа №8. Архивация информации. Сравнение методов сжатия данных. Сравнение архиваторов и типов файлов  
Задания  
1. Получить практические навыки по архивированию данных при помощи архиватора.  
2. Сравнить степень сжатия файлов различных типов с различным содержанием разными архиваторами.

### 5.2. Содержание самостоятельной работы по дисциплине (модулю)

#### Содержание обязательной самостоятельной работы по дисциплине

№ п/п	Темы дисциплины	Содержание самостоятельной работы студентов	Продукты деятельности
1	Информация как объект защиты.	Оформление отчета по лабораторной работе	Отчет по по лабораторной работе
2	Информационная безопасность	Оформление отчета по лабораторной работе	Отчет по по лабораторной работе
3	Критерии оценки безопасности компьютерных систем	Оформление отчета по лабораторной работе	Отчет по по лабораторной работе
4	Криптографические средства защиты информации	Оформление отчета по лабораторной работе	Отчет по по лабораторной работе
5	Электронная цифровая подпись	Оформление отчета по лабораторной работе	Отчет по по лабораторной работе
6	Защита от копирования	Оформление отчета по лабораторной работе	Отчет по по лабораторной работе
7	Программы с потенциально опасными последствиями	Оформление отчета по лабораторной работе	Отчет по по лабораторной работе
8	Защита в интернет	Оформление отчета по лабораторной работе	Отчет по по лабораторной работе

#### Содержание самостоятельной работы по дисциплине на выбор студента

№ п/п	Темы дисциплины	Содержание самостоятельной работы студентов	Продукты деятельности
1	Информация как объект защиты.	Подготовка презентации	Презентация
2	Информационная безопасность	Подготовка презентации	Презентация
3	Критерии оценки безопасности компьютерных систем	Подготовка презентации	Презентация
4	Криптографические средства защиты информации	Подготовка презентации	Презентация
5	Электронная цифровая подпись	Подготовка презентации	Презентация
6	Защита от копирования	Подготовка презентации	Презентация
7	Программы с потенциально опасными последствиями	Подготовка презентации	Презентация
8	Защита в интернет	Подготовка презентации	Презентация

### 5.3. Образовательные технологии

При организации изучения дисциплины будут использованы следующие образовательные технологии: информационно-коммуникационные технологии, технология организации самостоятельной работы, технология рефлексивного обучения, технология модульного обучения, технология игрового обучения, технологии групповой дискуссии, интерактивные технологии, технология проблемного обучения, технология организации учебно-исследовательской деятельности, технология проектного обучения, технология развития критического мышления.

#### 5.4. Текущий контроль, промежуточный контроль и промежуточная аттестация

Балльно-рейтинговая карта дисциплины оформлена как приложение к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине оформлен отдельным документом.

### 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

#### 6.1. Рекомендуемая литература

##### 6.1.1. Основная литература

	Авторы, составители	Заглавие, ссылка на электронную библиотечную систему	Издательство, год
Л1.1	Ю.Н. Загинайлов	Теория информационной безопасности и методология защиты информации: учебное пособие <a href="http://biblioclub.ru/index.php?page=book&amp;id=276557">http://biblioclub.ru/index.php?page=book&amp;id=276557</a>	М.; Берлин: Директ-Медиа, 2015
Л1.2	С.А. Нестеров	Основы информационной безопасности: учебное пособие <a href="http://biblioclub.ru/index.php?page=book&amp;id=363040">http://biblioclub.ru/index.php?page=book&amp;id=363040</a>	СПб.: Издательство Политехнического университета, 2014

##### 6.1.2. Дополнительная литература

	Авторы, составители	Заглавие, ссылка на электронную библиотечную систему	Издательство, год
Л2.1	Ю.Н. Загинайлов	Основы информационной безопасности: курс визуальных лекций <a href="http://biblioclub.ru/index.php?page=book&amp;id=362895">http://biblioclub.ru/index.php?page=book&amp;id=362895</a>	М.; Берлин: Директ-Медиа, 2015
Л2.2	В.Г. Спицын	Информационная безопасность вычислительной техники: учебное пособие <a href="http://biblioclub.ru/index.php?page=book&amp;id=208694">http://biblioclub.ru/index.php?page=book&amp;id=208694</a>	Томск: Эль Контент, 2011
Л2.3	В.Ф. Шаньгин	Защита компьютерной информации. Эффективные методы и средства <a href="http://biblioclub.ru/index.php?page=book&amp;id=86475">http://biblioclub.ru/index.php?page=book&amp;id=86475</a>	М.: ДМК Пресс, 2010

#### 6.2 Перечень программного обеспечения

- Acrobat Reader DC
- Dr.Web Desktop Security Suite, Dr.Web Server Security Suite
- GIMP
- Microsoft Office 365 Pro Plus - subscription license (12 month) (Пакет программ Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher, Teams, OneDrive, Yammer, Stream, SharePoint Online).
- Microsoft Windows 10 Education
- XnView
- Архиватор 7-Zip
- 1С:ИТС ПРОФ ВУЗ
- Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ»

#### 6.3 Перечень информационных справочных систем

- Информационно-образовательная программа «Росметод»
- СПС «ГАРАНТ-Аналитик»
- СПС «Консультант-Плюс»
- Elsevier (база данных «Freedom Collection» и коллекции электронных книг «Freedom Collection eBook collection»)
- SCOPUS издательства Elsevier
- SpringerNature (национальная подписка на полнотекстовые ресурсы)
- БД «Polpred.com. Обзор СМИ»
- УИС РОССИЯ
- ЭБС «E-LIBRARY.RU»
- ЭБС «РУКОНТ» (Контекстум)
- ЭБС «Университетская библиотека онлайн»
- ЭБС «ЮРАЙТ» (Коллекция Легендарные книги)
- ЭБС «IPR BOOKS»

### 7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Наименование специального помещения: помещение для самостоятельной работы, Читальный зал. Оснащенность: ПК-4шт., Принтер-1шт., Телефон-1шт., Письменный стол-4 шт., Парта-2 шт.
7.2	Наименование специального помещения: учебная аудитория для проведения лекционных занятий, практических занятий, групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации, Учебная аудитория. Оснащенность: Меловая доска-1шт., Комплект учебной мебели, ноутбук, проекционное оборудование (мультимедийный проектор и экран).

### **8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Работа над теоретическим материалом происходит кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометить важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю.

Проработка рабочей программы дисциплины, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Конспектирование источников, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с информационными источниками в разных форматах.

Также в процессе изучения дисциплины методические рекомендации могут быть изданы отдельным документом.

Балльно-рейтинговая карта дисциплины «Методы и технологии защиты информации»

Курс 5 Семестр 9

Вид контроля		Минимальное количество баллов	Максимальное количество баллов
<b>Наименование раздела</b>			
Текущий контроль по разделу:			
1	Аудиторная работа	8	16
2	Самостоятельная работа (специальные обязательные формы)	10	20
3	Самостоятельная работа (специальные формы на выбор студента)	2	4
Контрольное мероприятие по разделу		-	-
Промежуточный контроль		20	40
Промежуточная аттестация		36	60
Итого:		<b>56</b>	<b>100</b>

Виды контроля	Перечень или примеры заданий, критерии оценки и количество баллов	Темы для изучения и образовательные результаты
<b>Текущий контроль по разделу «Методы и технологии защиты информации»</b>		
1	Аудиторная работа Лабораторная работа №1. Информация как объект защиты Лабораторная работа №2. Средства защиты компьютера от вирусов Лабораторная работа №3. Построение кода постоянной длины Лабораторная работа №4. Построение кода переменной длины Лабораторная работа №5. Методы защиты информации. Шифр простой перестановки Лабораторная работа №6. Методы защиты информации. Шифр Цезаря Лабораторная работа №7. Модифицированный шифр Цезаря со сдвигом по кодовому слову Лабораторная работа №8. Архивация информации. Сравнение методов сжатия данных Сравнение архиваторов и типов файлов Критерий оценивания: 1 балл – выполнена базовая часть лабораторной работы, 2 балла – выполнена базовая и дополнительная(индивидуальная) часть лабораторной работы. Итого – 8x2=16 баллов	Темы Информация как объект защиты Информационная безопасность Критерии оценки безопасности компьютерных систем Криптографические средства защиты информации Электронная цифровая подпись Защита от копирования Программы с потенциально опасными последствиями Защита в интернет Образовательные результаты Знает: положения основных нормативных документов, регламентирующих деятельность в области защиты информации образовательных учреждений Умеет: оценивать возможные последствия существующих угроз информационного общества, выбирать способы защиты от угроз, анализировать и обобщать информацию о состоянии информационной среды образовательной организации.



			Владеет: приемами защиты информации обучающихся в образовательном процессе при работе со средствами информационно-коммуникационных технологий.
2	Самостоятельная работа (обязательные формы)	<p>Подготовка письменного отчета по лабораторной работе</p> <p>Критерии оценки</p> <p>Отчеты содержат результаты выполнения всех заданий лабораторных работ (0-0,5 балла)</p> <p>В документе приведены снимки экрана ключевых моментов работ (0-0,5 балла)</p> <p>Отчеты содержат оформленный по ГОСТ библиографический список (0-0,5 балла)</p> <p>Текст работы и иллюстрации оформлены согласно требованиям ГОСТ (0-0,5 балла)</p> <p>Итого: 2x5=10</p>	<p>Темы</p> <p>Информация как объект защиты</p> <p>Информационная безопасность</p> <p>Критерии оценки безопасности компьютерных систем</p> <p>Криптографические средства защиты информации</p> <p>Электронная цифровая подпись</p> <p>Защита от копирования</p> <p>Программы с потенциально опасными последствиями</p> <p>Защита в интернет</p> <p>Образовательные результаты</p> <p>Знает: положения основных нормативных документов, регламентирующих деятельность в области защиты информации образовательных учреждений</p> <p>Умеет: оценивать возможные последствия существующих угроз информационного общества, выбирать способы защиты от угроз, анализировать и обобщать информацию о состоянии информационной среды образовательной организации.</p> <p>Владеет: приемами защиты информации обучающихся в образовательном процессе при работе со средствами информационно-коммуникационных технологий.</p>
3	Самостоятельная работа (на выбор студента)	<p>Подготовлена презентация по отдельным темам модуля.</p> <ul style="list-style-type: none"> <li>• Презентация раскрывает ключевые аспекты выбранной темы.</li> <li>• Презентация оформлена согласно требованиям к деловым презентациям.</li> <li>• Презентация снабжена необходимыми иллюстрациями.</li> <li>• Студент продемонстрировал презентацию перед аудиторией и ответил на все полученные вопросы.</li> </ul> <p>Каждый критерий оценивается в 1 балл.</p> <p>Итого – 4x1=4 балла</p>	<p>Темы</p> <p>Информация как объект защиты</p> <p>Информационная безопасность</p> <p>Критерии оценки безопасности компьютерных систем</p> <p>Криптографические средства защиты информации</p> <p>Электронная цифровая подпись</p> <p>Защита от копирования</p> <p>Программы с потенциально опасными последствиями</p> <p>Защита в интернет</p> <p>Образовательные результаты</p>

		<p>Знает: положения основных нормативных документов, регламентирующих деятельность в области защиты информации образовательных учреждений</p> <p>Умеет: оценивать возможные последствия существующих угроз информационного общества, выбирать способы защиты от угроз, анализировать и обобщать информацию о состоянии информационной среды образовательной организации.</p> <p>Владеет: приемами защиты информации обучающихся в образовательном процессе при работе со средствами информационно-коммуникационных технологий.</p>
Контрольное мероприятие по разделу		
Промежуточный контроль (количество баллов)	Минимальное количество баллов – 20, максимальное – 40	
Промежуточная аттестация	Представлены в фонде оценочных средств для промежуточной аттестации по дисциплине	