Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Кислова Наталья Николаевна
Должность: Проректор по УМР и качеству образования
Дата подписания: 03.04.2024 21:16:49
Уникальный программный ключ:
52802513f5b14a975b3e9b13008093d5726b159bf6064f865ae65b96a966c035

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

ПРЕДМЕТНО-МЕТОДИЧЕСКИЙ МОДУЛЬ ПО ПРОФИЛЮ "ИНФОРМАТИКА"

Информационная безопасность и защита информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информатики, прикладной математики и методики их преподавания**

Учебный план ФМФИ-624ИДо(5г)
Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профиль): «Информатика» и «Дополнительное образование (в области информатики и ИКТ)»

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **2 ЗЕТ**

Часов по учебному плану 72
в том числе:
аудиторные занятия 24
самостоятельная работа 48

Виды контроля в семестрах:
зачеты 7

Распределение часов дисциплины по семестрам

Семестр(Курс.Номер семестра на курсе)	**7(4.1)**		Итого	
Вид занятий	УП	РПД	УП	РПД
Лекции	8	8	8	8
Лабораторные	16	16	16	16
В том числе инт.	6	6	6	6
Итого ауд.	24	24	24	24
Контактная работа	24	24	24	24
Сам. работа	48	48	48	48
Итого	72	72	72	72

Программу составил(и):

Добудько Александр Валерьянович

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

Информационная безопасность и защита 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 СГСПУ от 26.04.2024 г. протокол №10

Рабочая программа одобрена на заседании кафедры

Информатики, прикладной математики и методики их преподавания

Протокол от 25.06.2024 №11
Зав. кафедрой Т.В. Добудько

Начальник УОП


_____ Н.А. Доманина

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

Задачи изучения дисциплины: формирование у обучающихся систематизированных знаний, умений и навыков в области информационной безопасности и методов защиты информации

Область профессиональной деятельности: 01 Образование и наука

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ОП: Б1.О.07

2.1 Требования к предварительной подготовке обучающегося:

Содержание дисциплины базируется на материале:

Программное обеспечение систем и сетей

Теоретические основы информатики, Системное администрирование

Разработка приложений для мобильных устройств

Основы цифровой микроэлектроники

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

Производственная практика (педагогическая практика) (по профилю "Информатика"), Методика обучения информатике

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

ПК-1. Способен осуществлять педагогическую деятельность по реализации образовательного процесса по предмету

ПК-1.1. Умеет реализовывать образовательную программу по предмету с учетом специфики содержания, методов и инструментов соответствующей области научного знания

Знает: основные понятия «информационной безопасности»; правовые основы информационной безопасности и защиты персональных данных; программные и технические средства защиты информации; основы криптографических методы защиты информации.

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

ПК-1.2. Реализует образовательную программу по предмету с использованием технологий профессиональной деятельности

Умеет: использовать знания по информационной безопасности и защите информации при реализации образовательной программы по информатике.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часов	Интеракт.
	Раздел 1. Методы и технологии защиты информации			
1.1	Информация как объект защиты. Информационная безопасность /Лек/	7	2	0
1.2	Информация как объект защиты /Лаб/	7	2	0
1.3	Информация как объект защиты /Ср/	7	6	0
1.4	Информационная безопасность /Лаб/	7	2	0
1.5	Информационная безопасность /Ср/	7	6	0
1.6	Критерии оценки безопасности компьютерных систем. Криптографические средства защиты информации /Лек/	7	2	0
1.7	Критерии оценки безопасности компьютерных систем /Лаб/	7	2	0
1.8	Критерии оценки безопасности компьютерных систем /Ср/	7	6	0
1.9	Криптографические средства защиты информации /Лаб/	7	2	0
1.10	Криптографические средства защиты информации /Ср/	7	6	0
1.11	Электронная цифровая подпись. Защита от копирования /Лек/	7	2	0
1.12	Электронная цифровая подпись /Лаб/	7	2	2
1.13	Электронная цифровая подпись /Ср/	7	6	0
1.14	Защита от копирования /Лаб/	7	2	2
1.15	Защита от копирования /Ср/	7	6	0
1.16	Программы с потенциально опасными последствиями. Защита в интернет /Лек/	7	2	0
1.17	Программы с потенциально опасными последствиями /Лаб/	7	2	2
1.18	Программы с потенциально опасными последствиями /Ср/	7	6	0
1.19	Защита в интернет /Лаб/	7	2	0
1.20	Защита в интернет /Ср/	7	6	0

5. Оценочные и методические материалы по дисциплине (модулю)

5.1. Содержание аудиторной работы по дисциплине (модулю)

7 семестр, 4 лекции, 8 лабораторных занятий

Раздел 1. Методы и технологии защиты информации

Лекция №1 (2 часа)

Информация как объект защиты. Информационная безопасность

Информация как объект защиты

Вопросы и задания

1. Введение в защиту информации и информационную безопасность.
2. Нормативные документы, регламентирующие деятельность в области информационной безопасности и защиты информации образовательных учреждений.

Информационная безопасность

Вопросы и задания

1. Информационная безопасность.
2. Основные угрозы информационной безопасности.
3. Обеспечение информационной безопасности.
4. Аппаратно-программные средства защиты информации

Лабораторное занятие №1 (2 часа)

Информация как объект защиты

Вопросы и задания:

1. Ознакомление с положениями основных нормативных документов, регламентирующих деятельность в области защиты информации образовательных учреждений

Лабораторное занятие №2 (2 часа)

Информационная безопасность

Вопросы и задания:

1. Ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидностями вирусов, способами заражения и методами борьбы.
2. Ознакомиться с различными видами программных средств защиты от вирусов. Получить навыки работы с антивирусным пакетом.

Лекция №2 (2 часа)

Критерии оценки безопасности компьютерных систем. Криптографические средства защиты информации

Критерии оценки безопасности компьютерных систем

Вопросы и задания

1. Критерии оценки безопасности компьютерных систем.
2. Оранжевая книга.
3. Основные элементы политики безопасности.
4. Классы безопасности.

Криптографические средства защиты информации

Вопросы и задания

1. Простые криптосистемы.
2. Шифрование методом замены (подстановки).
3. Шифрование методом перестановки.
4. Шифрование методом гаммирования.
5. Шифрование с помощью аналитических преобразований.
6. Комбинированные методы шифрования.
7. Организационные проблемы криптозащиты.

Лабораторное занятие №3 (2 часа)

Критерии оценки безопасности компьютерных систем

Вопросы и задания

1. Изучить метод построения кода постоянной длины и оценить эффективность полученного кода.

Лабораторное занятие №4 (2 часа)

Криптографические средства защиты информации

Вопросы и задания

1. Изучить метод построения кода переменной длины, оценить эффективность полученного кода и сравнить ее с эффективностью кода постоянной длины.

Лекция №3 (2 часа)

Электронная цифровая подпись. Защита от копирования

Электронная цифровая подпись

Вопросы и задания

1. Проблема аутентификации данных и электронная цифровая подпись.
2. Однонаправленные хэш-функции. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов
3. Алгоритм безопасного хэширования SHA.
4. Отечественный стандарт хэш-функции.
5. Алгоритмы электронной цифровой подписи. Алгоритм цифровой подписи Эль Гамаля (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.

Защита от копирования

Вопросы и задания

1. Защита от копирования. Защита CD от копирования.
2. Защиты от несанкционированного доступа.
3. Идентификация и аутентификация пользователя. Протоколы идентификации с нулевой передачей знаний.

Лабораторное занятие №5 (2 часа)

Электронная цифровая подпись

Вопросы и задания

1. Выполнить шифрование заданного сообщения простейшим шифром перестановок и выполнить проверку правильности шифрования.

Лабораторное занятие №6 (2 часа)

Защита от копирования

Вопросы и задания

1. Освоить технологию шифрования и дешифрования информации с использованием шифра Цезаря.

Лекция №4 (2 часа)

Программы с потенциально опасными последствиями. Защита в интернет

Программы с потенциально опасными последствиями

Вопросы и задания

1. Программы с потенциально опасными последствиями.
2. Вирус. Люк. Троянский конь. Логическая бомба. Программные закладки. Атака салями.

Защита в интернет

Вопросы и задания

1. Межсетевые экраны.
2. Компьютерные атаки и технологии их обнаружения.
3. Безопасность электронной коммерции. Безопасность электронных платежных систем.
4. Идеальная служба информационной безопасности.

Лабораторное занятие №7 (2 часа)

Программы с потенциально опасными последствиями

Вопросы и задания

1. Освоить технологию шифрования и дешифрования информации с использованием модифицированного шифра Цезаря.

Лабораторное занятие №8 (2 часа)

Защита в интернет

Вопросы и 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	Продукты деятельности
1	Информация как объект защиты.	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
2	Информационная безопасность	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
3	Критерии оценки безопасности компьютерных систем	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
4	Криптографические средства защиты информации	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
5	Электронная цифровая подпись	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
6	Защита от копирования	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
7	Программы с потенциально опасными последствиями	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
8	Защита в интернет	Оформление отчета по лабораторной работе	Отчет по лабораторной работе

Содержание самостоятельной работы по дисциплине на выбор

№ п/п	Темы дисциплины	Содержание самостоятельной работы	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	В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской	Введение в информационную безопасность и защиту информации: учебное пособие URL: https://biblioclub.ru/index.php?page=book&id=575113	Новосибирск: Новосибирский государственный технический университет, 2017

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие, ссылка на электронную библиотечную систему	Издательство, год
Л2.1	Загинайлов, Ю. Н.	Основы информационной безопасности: курс визуальных лекций: учебное пособие URL: https://biblioclub.ru/index.php?page=book&id=362895	Москва; Берлин: Директ-Медиа, 2015
Л2.1	Загинайлов, Ю. Н.	Теория информационной безопасности и методология защиты информации: учебное пособие URL: https://biblioclub.ru/index.php?page=book&id=276557	Москва; Берлин: Директ-Медиа, 2015

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

6.3 Перечень информационных справочных систем, профессиональных баз данных

- ЭБС «Университетская библиотека онлайн»
- Базы данных Springer eBooks

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Наименование специального помещения: помещение для самостоятельной работы, Читальный зал. Оснащенность: ПК-4шт. с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СГСПУ, 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 с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СГСПУ, 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; помечать 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 удается 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.

Приложение

Балльно-рейтинговая карта дисциплины «Информационная безопасность и защита информации»

Курс 4 Семестр 7

Вид контроля		Минимальное количество баллов	Максимальное количество баллов
Наименование раздела «Методы и технологии защиты информации»			
Текущий контроль по разделу:			
1	Аудиторная работа	8	16
2	Самостоятельная работа (специальные обязательные формы)	10	20
3	Самостоятельная работа (специальные формы на выбор)	2	4
Контрольное мероприятие по разделу		-	-
Промежуточный контроль		20	40
Промежуточная аттестация		36	60
	Итого:	**56**	**100**

Виды контроля		Перечень или примеры заданий, критерии оценки и количество баллов	Темы для изучения и образовательные результаты
Текущий контроль по разделу «Методы и технологии защиты информации»			
1	Аудиторная работа	Лабораторная работа №1. Информация как объект защиты Лабораторная работа №2. Информационная безопасность Лабораторная работа №3. Критерии оценки безопасности компьютерных систем Лабораторная работа №4. Криптографические средства защиты информации Лабораторная работа №5. Электронная цифровая подпись Лабораторная работа №6. Защита от копирования Лабораторная работа №7. Программы с потенциально опасными последствиями Лабораторная работа №8. Защита в интернет Критерий оценивания: 1 балл – выполнена базовая часть лабораторной работы, 2 балла – выполнена базовая и дополнительная(индивидуальная) часть лабораторной работы. Итого – 8х2=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 Результаты обучения: Знает: основные понятия «информационной безопасности»; правовые основы информационной безопасности и защиты персональных данных; программные и технические средства защиты информации; основы криптографических методы защиты информации. Умеет: оценивать возможные последствия существующих угроз информационного общества, выбирать способы защиты от угроз, анализировать и обобщать информацию о состоянии информационной среды образовательной организации; использовать знания по информационной безопасности и защите информации при реализации образовательной программы по информатике.
2	Самостоятельная работа (обязательные формы)	Подготовка письменного отчета по лабораторной работе Критерии оценки Отчеты содержат результаты выполнения всех заданий лабораторных работ (0-0,5 балла)	Темы: Информация как объект защиты Информационная безопасность Критерии оценки безопасности компьютерных систем Криптографические средства защиты информации

		В документе приведены снимки экрана ключевых моментов работ (0-0,5 балла) Отчеты содержат оформленный по ГОСТ библиографический список (0-0,5 балла) Текст работы и иллюстрации оформлены согласно требованиям ГОСТ (0-0,5 балла) Итого: 2х5=10	Электронная цифровая подпись Защита от копирования Программы с потенциально опасными последствиями Защита в интернет Результаты обучения: Знает: основные понятия «информационной безопасности»; правовые основы информационной безопасности и защиты персональных данных; программные и технические средства защиты информации; основы криптографических методы защиты информации. Умеет: оценивать возможные последствия существующих угроз информационного общества, выбирать способы защиты от угроз, анализировать и обобщать информацию о состоянии информационной среды образовательной организации; использовать знания по информационной безопасности и защите информации при реализации образовательной программы по информатике.
3	Самостоятельная работа (на выбор)	Подготовлена презентация по отдельным темам модуля. • Презентация раскрывает ключевые аспекты выбранной темы. • Презентация оформлена согласно требованиям к деловым презентациям. • Презентация снабжена необходимыми иллюстрациями. • Обучающийся продемонстрировал презентацию перед аудиторией и ответил на все полученные вопросы. Каждый критерий оценивается в 1 балл. Итого – 4х1=4 балла	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 Результаты обучения: Знает: основные понятия «информационной безопасности»; правовые основы информационной безопасности и защиты персональных данных; программные и технические средства защиты информации; основы криптографических методы защиты информации. Умеет: оценивать возможные последствия существующих угроз информационного общества, выбирать способы защиты от угроз, анализировать и обобщать информацию о состоянии информационной среды образовательной организации; использовать знания по информационной безопасности и защите информации при реализации образовательной программы по информатике.
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	