

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Алексеева Инна Сергеевна

Должность: И.о. ректора, и.о. проректора по стратегическому развитию и

цифровизации образовательного процесса

Дата подписания: 15.07.2024 10:57:51

Уникальный программный ключ:

623a014e46114d90ca02a8a3a09eaf63845228af

МИНИСТЕРСТВО ОБРАЗОВАНИЯ СТАВРОПОЛЬСКОГО КРАЯ

Государственное бюджетное образовательное учреждение высшего образования

«СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ»

Кафедра математики, информатики и цифровых образовательных технологий

УТВЕРЖДАЮ

Заведующий кафедрой



К.А. Киричек

протокол № 8

от 28.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

Кибербезопасность

(наименование учебной дисциплины)

Уровень основной образовательной программы

бакалавриат

Направление(я) подготовки (специальность)

44.03.05 Педагогическое образование (с двумя профилями подготовки)

Форма обучения

очная

Срок освоения

5 лет 0 месяцев

Кафедра

математики, информатики и цифровых образовательных технологий

Год начала

подготовки

2022

Ставрополь, 2024 г.

Программу составил(-и): к. пед. н., доцент, Жук Е.П.

Рабочая программа дисциплины "Кибербезопасность" разработана в соответствии с ФГОС: 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).

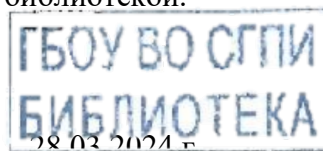
Рабочая программа дисциплины составлена на основании учебного плана: 44.03.05 Педагогическое образование (с двумя профилями подготовки), утвержденного учёным советом вуза от 25.04.2024, протокол № 4.

Рабочая программа одобрена на заседании кафедры математики, информатики и цифровых образовательных технологий от 28.03.2024 г., протокол № 8 для исполнения в 2024-2025 учебном году.

Зав. кафедрой  К.А. Киричек

Рабочая программа дисциплины согласована с заведующим библиотекой.

Зав. библиотекой  Фролова Т.А.



Срок действия рабочей программы дисциплины: 2024-2025 учебный год.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

получение базовых знаний и навыков в области формирования условий, при которых все составляющие персонального киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями, а также обеспечения культуры безопасного поведения в киберпространстве.

2. ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- ознакомление с миром кибербезопасности и мотивацией киберпреступников и специалистов по кибербезопасности;
- изучение этических требований и законов в области информационной безопасности и методов разработки политик безопасности;
- изучение функций специалистов по кибербезопасности и карьерных возможностей;
- получение фундаментальных знаний в различных областях безопасности;
- развитие умений, навыков и способностей определения кибератак и их признаки, процессы и контрмеры информационной безопасности;
- приобретение навыков по управлению информационной безопасностью, использованию средств контроля, защиты и технологий минимизации последствий.

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ООП: Б1.В.ДВ.01

3.1. Требования к предварительной подготовке обучающегося:

Алгебра
Архитектура компьютера
Безопасность жизнедеятельности
Геометрия
Дискретная математика
Дифференциальные уравнения
Математическая логика
Математический анализ
Методы исследовательской и проектной деятельности
Методы математической обработки данных
Основы медицинских знаний
Практикум по решению предметных задач
Программирование
Программное обеспечение систем и сетей
Теория алгоритмов
Теория вероятностей и математическая статистика
Теория чисел
Технологии цифрового образования
Учебная (ознакомительная) практика
Учебная практика (научно-исследовательская работа (получение первичных навыков научно-
Философия
Числовые системы

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

Большие данные
Веб-технологии
Глубокое обучение
Информационная безопасность и защита информации
История математики и информатики
Математическое и компьютерное моделирование
Математическое программное обеспечение

Основы военной подготовки	
Основы искусственного интеллекта	
Производственная практика (научно-исследовательская работа)	
Современные модели и средства оценивания в обучении	
Теория и методика организации дистанционного обучения в образовательных организациях	
Теория игр и исследование операций	
Теория функций действительного переменного	
Этика. Эстетика	
4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ	
Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации,	УК-1.1 Демонстрирует знание особенностей системного и критического мышления,
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной	УК-8.1 Оценивает факторы риска, умеет обеспечивать личную безопасность и

В результате освоения дисциплины обучающийся должен:

знать: – место информационной безопасности в системе национальной безопасности страны; – классификации основных угроз безопасности информации; – знать, как участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.	уметь: – формировать собственное суждение и оценку информации; – применять особенности системного и критического мышления; – осуществлять поиск информации, соответствующей решаемой задаче; – применять логические формы и процедуры; – осуществлять поиск информации, соответствующей решаемой задаче; – формировать собственные мнения и суждения, аргументирует свои выводы и точку зрения. – организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	владеть: – демонстрирует навыки поиска релевантной информации; – демонстрирует способность к рефлексии по поводу собственной и чужой мыслительной деятельности. – поиска информации для решения поставленной задачи по различным типам запросов;
--	---	--

5. ОБЪЕМ УЧЕБНОЙ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины составляет 2 зачетные (-ых) единицы (-ы) (72), включая промежуточную аттестацию.

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Се местр на курсе>)	7 (4.1)		Итого	
Неделя	16 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	20	20	20	20
Контактная работа (Эк, Зч, ЗчО)	0,3	0,3	0,3	0,3
Итого ауд.	36	36	36	36
Контактная работа	36,3	36,3	36,3	36,3
Сам. работа	35,7	35,7	35,7	35,7
Итого	72	72	72	72

6. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ ПО РАЗДЕЛАМ (ТЕМАМ) И ВИДАМ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Примечание
	Раздел 1.					
1.1	Кибербезопасность: мир и преступников /Тема/	7	0			
1.2	/Лек/	7	2	УК-1.1 УК-1.3 УК-8.1		
1.3	/Пр/	7	2	УК-1.1 УК-1.3 УК-8.1		
1.4	/Ср/	7	4	УК-1.1 УК-1.3 УК-8.1		
1.5	Куб кибербезопасности /Тема/	7	0			
1.6	/Лек/	7	2	УК-1.3 УК-8.1		
1.7	/Пр/	7	2	УК-1.3 УК-8.1		
1.8	/Ср/	7	4	УК-1.3 УК-8.1		
1.9	Свойства противодействия угрозам кибербезопасности /Тема/	7	0			
1.10	/Лек/	7	2	УК-1.2 УК-8.2		
1.11	/Пр/	7	2	УК-1.2 УК-8.2		
1.12	/Ср/	7	5	УК-1.2 УК-8.2		
1.13	Угрозы кибербезопасности, уязвимости и атаки /Тема/	7	0			

1.14	/Лек/	7	2	УК-1.1 УК-8.2		
1.15	/Пр/	7	4	УК-1.1 УК-8.2		
1.16	/Ср/	7	4,7	УК-1.1 УК-8.2		
1.17	Способы защиты информации ограниченного доступа /Тема/	7	0			
1.18	/Лек/	7	2	УК-1.2 УК-8.1		
1.19	/Пр/	7	4	УК-1.2 УК-8.1		
1.20	/Ср/	7	8	УК-1.2 УК-8.1		
1.21	Способы обеспечения целостности данных /Тема/	7	0			
1.22	/Лек/	7	2	УК-1.3 УК-8.1		
1.23	/Пр/	7	4	УК-1.3 УК-8.1		
1.24	/Ср/	7	6	УК-1.3 УК-8.1		
1.25	Защита уровней обеспечения кибербезопасности /Тема/	7	0			
1.26	/Лек/	7	4	УК-1.3 УК-8.1		
1.27	/Пр/	7	2	УК-1.3 УК-8.1		
1.28	/Ср/	7	4	УК-1.3 УК-8.1		
1.29	Промежуточная аттестация /Тема/	7	0			
1.30	/КПА/	7	0,3	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2		

Планы проведения учебных занятий отражены в оценочных материалах (Приложение 2.).

7. КОНТРОЛЬ КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль качества освоения учебного материала по дисциплине проводится в форме текущего контроля успеваемости и промежуточной аттестации в соответствии с «Положением о формах, периодичности и порядке текущего контроля успеваемости и промежуточной аттестации обучающихся в ГБОУ ВО СГПИ и его филиалах».

Для аттестации обучающихся на соответствие их персональных достижений требованиям образовательной программы используются оценочные материалы текущего контроля успеваемости и промежуточной аттестаций (Приложение 2).

Уровень сформированности компетенции			
не сформирована	сформирована частично	сформирована в целом	сформирована полностью

«Не зачтено»		«Зачтено»	
«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
Описание критериев оценивания			
Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания.	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала. - способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; Возможны незначительные неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - наличие собственной обоснованной позиции по обсуждаемым вопросам; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ			

Учебно-методическое обеспечение дисциплины включает рабочую программу дисциплины, методические материалы, оценочные материалы.

Учебно-методическое обеспечение самостоятельной работы обучающихся включает: учебники, учебные пособия, электронные образовательные ресурсы, методические материалы.

Самостоятельная работа обучающихся является формой организации образовательного процесса по дисциплине и включает следующие виды деятельности: поиск (подбор) и обзор

научной и учебной литературы, электронных источников информации по изучаемой теме; работа с конспектом лекций, электронным учебником, со словарями и справочниками и др. источниками информации (конспектирование); составление плана и тезисов ответа; подготовка реферата; выполнение творческих заданий и проблемных ситуаций; подготовка к коллоквиуму, собеседованию, практическим занятиям; подготовка к зачету и экзамену.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

9.1. Рекомендуемая литература

9.1.1. Основная литература

Л.1.1	Гультяева Т. А. Основы информационной безопасности [Электронный ресурс]: учеб. пособие. - Новосибирск: НГТУ, 2018. - 79 с. – Режим доступа: https://e.lanbook.com/book/118233
Л.1.2	Киреева Н. В., Крыжановский А. В., Поздняк И. С., Чупахина Л. ..., Караулова О. А. Правовые нормы защиты информации в автоматизированных системах [Электронный ресурс]: учебное пособие. - Самара: ПГУТИ, 2020. - 60 с. – Режим доступа: https://e.lanbook.com/book/255446
Л.1.3	Лойко В. И., Лаптев В. Н., Аршинов Г. А., Лаптев С. Н. Информационная безопасность [Электронный ресурс]: учебное пособие. - Краснодар: КубГАУ, 2020. - 332 с. – Режим доступа: https://e.lanbook.com/book/254168

9.1.2. Дополнительная литература

Л.2.1	Крыжановский А. В., Поздняк И. С. Информационная безопасность [Электронный ресурс]: методические указания к практическим занятиям. - Самара: ПГУТИ, 2018. - 38 с. – Режим доступа: https://e.lanbook.com/book/182282
Л.2.2	Попова Н. П., Дмитриева А. П. Защита интеллектуальной собственности [Электронный ресурс]: тексты лекций. - Санкт-Петербург: БГТУ "Военмех" им. Д.Ф. Устинова, 2018. - 219 с. – Режим доступа: https://e.lanbook.com/book/122086
Л.2.3	Корнилова А. А., Юнусова Д. С., Исмагилова А. С. Защита персональных данных [Электронный ресурс]: учебное пособие. - Уфа: БашГУ, 2020. - 120 с. – Режим доступа: https://e.lanbook.com/book/179914

10.1 Интернет-ресурсы (базы данных, информационно-справочные системы и др.)

ЭБС «Лань»	https://e.lanbook.com
Национальная электронная библиотека (НЭБ)	https://rusneb.ru
ЭБС «Юрайт»	https://urait.ru
ЭБС «Журнальный зал»: русский толстый журнал как эстетический феномен	https://magazines.gorky.media
«Электронная библиотека ИМЛИ РАН»	http://biblio.imli.ru
«Электронная библиотека ИРЛИ РАН» (Пушкинский Дом)	http://lib.pushkinskijdom.ru
Научный архив	https://научныйархив.рф
ЭБС «Педагогическая библиотека»	http://pedlib.ru
ЭБС «Айбукс.ру»	https://www.ibooks.ru
Научная электронная библиотека eLibrary.ru	https://elibrary.ru
ЭБС Буконлайн	https://bookonline.ru
Научная электронная библиотека «Киберленинка»	https://cyberleninka.ru/
Государственная публичная научно-техническая библиотека России. Ресурсы открытого доступа	http://www.gpntb.ru/elektronnye-resursy-udalennogo-dostupa/1874-1024.html
Библиотека академии наук (БАН). Ресурсы открытого доступа	http://www.rasl.ru/e_resours/resursy_otkrytogo_dostupa.php

10.2. Профессиональные базы данных и информационные справочные системы

Университетская информационная система РОССИЯ	https://uisrussia.msu.ru
Единое окно доступа к образовательным ресурсам	http://window.edu.ru/catalog
Словари и энциклопедии	https://dic.academic.ru
Педагогическая мастерская «Первое сентября»	https://fond.1sept.ru
Сайт Единой коллекции цифровых образовательных ресурсов	http://school-collection.edu.ru
Национальная платформа «Открытое образование»	https://openedu.ru
Портал «Единая коллекция цифровых образовательных ресурсов»	http://school-collection.edu.ru
Российское образование. Федеральный портал	http://edu.ru
Портал Федеральных государственных образовательных стандартов высшего образования	http://fgosvo.ru
Единая цифровая коллекция первоисточников научных работ удостоверенного качества «Научный архив»	https://научныйархив.рф
Портал проекта «Современная цифровая образовательная среда в РФ»	https://online.edu.ru

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Занятия, текущий контроль успеваемости и промежуточная аттестация по дисциплине проводятся в учебных аудиториях, укомплектованных типовой мебелью для обучающихся и преподавателя, техническими и мультимедийными средствами обучения, включенными в локальную сеть вуза и с доступом к информационным ресурсам сети Интернет.

Рабочие места для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети Интернет и обеспечены доступом в электронную информационно-образовательную среду вуза.

Компьютерное оборудование имеет соответствующее лицензионное программное обеспечение:

1. Пакет программного обеспечения общего назначения Microsoft Office (MS Word, MS Microsoft Excel, MS PowerPoint).
2. Adobe Acrobat Reader.
3. Браузер (Internet Explorer, Mozilla Firefox, Google Chrome, Opera и др.).
4. Программа тестирования Айрен.