

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Родин Олег Федорович
Должность: И.о. директора
Дата подписания: 2025.02.06
Уникальный программный ключ:
2246bb4b5eca53e35a45d6a91259e790782354e7

Министерство просвещения Российской Федерации
Нижнетагильский государственный социально-педагогический институт (филиал)
Федерального государственного автономного образовательного учреждения
высшего образования

«Российский государственный профессионально-педагогический университет»

Факультет спорта и безопасности жизнедеятельности
Кафедра информационных технологий и физико-математического образования

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.07.09 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

Направление подготовки	44.03.01 Педагогическое образование
Профили подготовки	Безопасность жизнедеятельности и Физическая культура
Автор(ы)	Е. С. Васева, к. пед. н., доцент

Одобрена на заседании кафедры информационных технологий и физико-математического образования. Протокол от 6 февраля 2025 г. № 6.

Рекомендована к использованию в образовательной деятельности методической комиссией факультета спорта и безопасности жизнедеятельности. Протокол от 16 февраля 2025 г. № 6.

Нижний Тагил
2025

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель: формирование компетенций будущих учителей в области обеспечения информационной безопасности участников образовательных отношений и защиты информации в условиях современной информационной образовательной среды.

Задачи дисциплины:

1. Познакомить студентов с правовыми основами и нормами профессиональной этики в сфере обеспечения информационной безопасности.
2. Сформировать навыки взаимодействия с участниками образовательных отношений при соблюдении норм профессиональной этики и требований соблюдения конфиденциальности информации.
3. Сформировать умения обоснованного выбора и использования современных информационных технологий и программных средств, в том числе отечественного производства, для решения задач обеспечения информационной безопасности участников образовательных отношений.
4. Сформировать способности использовать теоретические знания и практические умения в области информационной безопасности и защиты информации при разработке учебных программ, отборе содержания учебных предметов, разработке различных форм учебных занятий, формировании развивающей образовательной среды.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность» является частью учебного плана по направлению подготовки 44.03.01 Педагогическое образование, профиль «Безопасность жизнедеятельности». Дисциплина реализуется на факультете спорта и безопасности жизнедеятельности. Дисциплина входит в предметно-методический модуль по профилю Безопасность жизнедеятельности и относится к обязательной части.

Дисциплина «Информационная безопасность» базируется на компетенциях, полученных при изучении дисциплин «Технологии цифрового образования», «Концептуальные основы безопасности жизнедеятельности», «Безопасность жизнедеятельности», «Нормативно-правовые основы профессиональной деятельности».

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина направлена на формирование следующих компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Дескрипторы
ОПК-1. Способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной	ОПК-1.1. Понимает и объясняет сущность приоритетных направлений развития образовательной системы Российской Федерации, законов и иных нормативно-правовых актов, регламентирующих образовательную деятельность в Российской Федерации, нормативных документов по	Знает основные нормативно-правовые документы, регламентирующие отношения в сфере информационной безопасности. Умеет формулировать требования к обеспечению информационной безопасности информационной образовательной среды.

этики	вопросам обучения и воспитания детей и молодежи, федеральных государственных образовательных стандартов дошкольного, начального общего, основного общего, среднего общего, среднего профессионального образования, профессионального обучения, законодательства о правах ребенка, трудового законодательства.	Владеет навыками обеспечения информационной безопасности информационной образовательной среды.
	ОПК-1.2. Применяет в своей деятельности основные нормативно-правовые акты в сфере образования и нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности.	Знает основные нормативно-правовые документы, регламентирующие отношения в сфере обеспечения информационной безопасности персональных данных субъектов образовательных отношений. Умеет формулировать требования к обеспечению информационной безопасности персональных данных субъектов образовательных отношений. Владеет навыками обеспечения информационной безопасности персональных данных субъектов образовательных отношений.
ПК-1 – Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач	ПК-1.1. Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета).	Знает основные понятия информационной безопасности. Умеет применять предметные знания в области информационной безопасности при реализации образовательного процесса.
	ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.	Знает требования ФГОС ОО, в том числе в части формирования компетенций обучающихся в области обеспечения личной информационной безопасности. Умеет определять структуру и содержание образовательных программ по учебному предмету в соответствии с образовательными стандартами с учетом требований информационной безопасности. Владеет приемами отбора содержания обучения.
	ПК-1.3. Демонстрирует умение разрабатывать различные формы учебных занятий, применять	Знает методы, приемы и технологии обучения, в том числе информационные.

	методы, приемы и технологии обучения, в том числе информационные.	Умеет создавать условия для формирования у обучающихся конкретных знаний, умений и навыков в области информационной безопасности. Владеет приемами и технологиями обучения, в том числе информационными
--	---	--

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Объем дисциплины и виды контактной и самостоятельной работы

Общая трудоемкость дисциплины составляет 3 зач. е (108 ч.), семестр изучения – 1, распределение по видам нагрузки представлено в таблице.

Вид работы	Форма обучения
	заочная
Общая трудоемкость дисциплины по учебному плану	108
Контактная работа , в том числе:	10
Лекции	4
Лабораторные занятия	6
Самостоятельная работа	98
Подготовка к зачету	4

4.2.1. Учебно-тематический план дисциплины (заочная форма обучения)

Наименование разделов и тем дисциплины (модуля)	Всего часов	Вид контактной работы, час		Самостоятельная работа, час	Формы текущего контроля успеваемости	Форма промежуточной аттестации
		Лекции	Практические занятия			
Тема 1. Введение в проблему информационной безопасности	4	1		3	тест	Итоговый тест, отчеты по лабораторным работам
Тема 2. Угрозы информационной безопасности и методы их реализации	13		1	12	тест, отчет по лабораторной работе	
Тема 3. Правовые и организационные аспекты защиты информации	14	1	1	12	тест, отчет по лабораторной работе	
Тема 4. Административный уровень обеспечения информационной безопасности	15	1	1	13	тест, отчет по лабораторной работе	
Тема 5. Процедурный уровень обеспечения информационной безопасности	16		1	15	тест, отчет по лабораторной	

Наименование разделов и тем дисциплины (модуля)	Всего часов	Вид контактной работы, час		Самостоятельная работа, час	Формы текущего контроля успеваемости	Форма промежуточной аттестации
		Лекции	Практические занятия			
					работе	
Тема 6. Программно-технический уровень обеспечения информационной безопасности	19		1	18	тест, отчет по лабораторной работе	
Тема 7. Общие меры по созданию безопасной ИС в образовательном учреждении.	23	1	1	21	тест, отчет по лабораторной работе	
Зачет	4			4	выполнение заданий на зачете	
Итого	108	4	6	98		

Типовые задания для текущего контроля и промежуточной аттестации по дисциплине, критерии и шкалы оценивания, а также методические рекомендации для обучающихся представлены в приложении к рабочей программе дисциплины.

4.3. Содержание дисциплины

Тема 1. Введение в проблему информационной безопасности.

Программа информационной безопасности России и пути ее реализации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности.

Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. Международные стандарты информационного обмена.

Основные принципы защиты информации в компьютерных системах. Основные понятия и определения защиты информации.

Тема 2. Угрозы информационной безопасности и методы их реализации.

Виды возможных нарушений информационной системы. Понятие угрозы. Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации. Информационная безопасность в условиях функционирования в России глобальных сетей.

Тема 3. Правовые и организационные аспекты защиты информации.

Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Компьютерные преступления.

Тема 4. Административный уровень обеспечения информационной безопасности.

Основные понятия. Концепция безопасности. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем. Анализ рисков информационной системы предприятия. Стратегии управления рисками.

Тема 5. Процедурный уровень обеспечения информационной безопасности.

Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Тема 6. Программно-технический уровень обеспечения информационной безопасности.

Основные сервисы программно-технического уровня обеспечения информационной безопасности. Идентификация и аутентификация. Парольная аутентификация. Логическое управление доступом. Компьютерные вирусы, классификация. Признаки заражения компьютера вредоносным программным обеспечением. Средства защиты от компьютерных вирусов. Протоколирование и аудит. Криптографические средства защиты. Экранирование.

Тема 7. Общие меры по созданию безопасной ИС в образовательном учреждении.

Реализация основных направлений законодательства РФ по вопросам информационной безопасности образовательного учреждения. ФЗ «О персональных данных». ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Разработка методических рекомендаций. Использование контентной фильтрации Интернета, для фильтрации сайтов с одержимым, далёким от задач образования. Обучение детей основам информационной безопасности, воспитание информационной культуры.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной литературы

Основная литература

1. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 400 с. — ISBN 978-5-507-49250-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/414947> (дата обращения: 19.01.2025).

2. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/560516> (дата обращения: 19.01.2025).

3. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449350> (дата обращения: 19.01.2025).

Дополнительная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567915> (дата обращения: 19.01.2025).

2. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебник для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2025. — 170 с.

— (Высшее образование). — ISBN 978-5-534-17153-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/568566> (дата обращения: 19.01.2025).

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2024. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/543351> (дата обращения: 19.01.2025).

5.2. Электронные образовательные ресурсы, в т.ч. профессиональные базы данных и информационные справочные системы

https://www.ntspi.ru/library/directories_and_files/web_res/systems/	Электронно-библиотечные системы НТГСПИ
https://www.ntspi.ru/library/directories_and_files/web_res/systems/libraris/	Электронные базы данных НТГСПИ
https://www.ntspi.ru/library/periodika/	Периодика НТГСПИ
https://iprmedia.ru	ЭБС «Ай Пи Эр Медиа»
https://ibooks.ru	ЭБС «Айбукс»
https://urait.ru	ЭБС Юрайт
http://e.lanbook.com	ЭБС издательства «ЛАНЬ»
http://elibrary.ru	Научная электронная библиотека eLIBRARY.RU
http://www.consultant.ru	«КонсультантПлюс»
http://cyberleninka.ru	НЭБ «КиберЛенинка»
https://polpred.ru	ООО «Полпред-Справочники» (база данных)
https://eivis.ru	ООО «ИВИС»
www.delpress.ru	«Деловая пресса»

5.3. Комплект программного обеспечения

1. Среда электронного обучения «Русский Moodle» (<https://do.ntspi.ru>).
2. Интернет-платформа онлайн-курсов со свободным кодом «Open edX» (<https://www.edx.org/>).
3. Интернет-платформа онлайн-курсов «Открытое образование» (<https://openedu.ru/>).
4. Электронная информационно-образовательная среда РГППУ (<https://eios.rsvpu.ru/>).
5. Платформа для организации и проведения вебинаров «Mirapolis Virtual Room».
6. Microsoft Office.
7. Kaspersky Endpoint Security.
8. Adobe Reader.
9. Free PDF Creator.
10. 7-zip (<http://www.7-zip.org/>).
11. LibreOffice.
12. Браузеры Firefox, Яндекс.Браузер.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Помещения

Помещения для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационно-образовательную среду университета.

6.2. Оборудование и технические средства обучения

6.2.1. Оборудование, в т.ч. специализированное

Стационарный компьютер или ноутбук, проектор для показа слайдов и видео, акустические колонки.

6.2.2. Технические средства обучения

Презентации лекций, видео-презентации, видео-лекции, учебные кинофильмы, аудиозаписи, онлайн-платформы.

6.2.3. Учебные и наглядные пособия

Печатные и электронные учебные пособия и наглядный материал: графические изображения, схемы, таблицы, раздаточный материал.