Министерство просвещения Российской Федерации
Нижнетагильский государственный социально-педагогический институт (филиал)
федерального государственного автономного образовательного учреждения
высшего образования
«Российский государственный профессионально-педагогический университет»

Факультет естествознания, математики и информатики
Кафедра информационных технологий

УТВЕРЖДАЮ
Зам. директора по УМР
_____ В. В. Дикова
«___» _____ 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.06.10 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень высшего образования	Бакалавриат
Направление подготовки	44.03.05 Педагогическое образование (с двумя профилями подготовки)
Профили	«Физика и информатика» «Математика и информатика»
Форма обучения	Очная

Нижний Тагил
2020

Рабочая программа дисциплины «Информационная безопасность». Нижний Тагил: Нижнетагильский государственный социально-педагогический институт (филиал) ФГАОУ ВО «Российский государственный профессионально-педагогический университет», 2020. – 13 с.

Настоящая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по программе 44.03.05 Педагогическое образование.

.

Автор: кандидат педагогических наук, доцент кафедры информационных технологий — Е. С. Васева

Рецензент: к.п.н., зам директора по ИТ НТ МУП «Нижнетагильские тепловые сети» — Д. В. Виноградов

Программа рассмотрена и одобрена на заседании кафедры информационных технологий 9 апреля 2020 г., протокол № 9.

Заведующая кафедрой — М. В. Мащенко

Программа рекомендована к печати методической комиссией факультета естествознания, математики и информатики 30 апреля 2020 г., протокол №8.

Председатель МК ФЕМИ — Н. З. Касимова

Программа рассмотрена и утверждена на заседании Ученого совета факультета естествознания, математики и информатики 30 апреля 2020 г., протокол №8.

Декан ФЕМИ — Т. В. Жуйкова

Главный специалист ОИР — О. В. Левинских

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины – формирование компетенций будущих учителей в области обеспечения информационной безопасности в условиях современного информационного пространства.

Задачи:

− познакомить студентов с правовыми основами обеспечения информационной безопасности;

− раскрыть понятийный аппарат фундаментального и прикладного аспектов курса;

− сформировать целостную систему знаний о современных моделях обеспечения безопасности управления информационными ресурсами;

− познакомить студентов с технологиями обеспечения информационной безопасности средствами систем обеспечения безопасности информации;

− сформировать умения использования соответствующих инструментальных программных средств обеспечения информационной безопасности обучающихся.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность» является частью учебного плана по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки). Дисциплина включена в Блок Б.1 «Дисциплины (модули)» и является составной частью раздела Б1.О «Обязательная часть», подраздела Б1.О.06 «Предметно-содержательный модуль». Реализуется кафедрой информационных технологий.

Дисциплина «Информационная безопасность» базируется на компетенциях, полученные при изучении дисциплин «Информационно-коммуникационные технологии», «Информационные системы и управление данными», «Сети и телекоммуникации». Теоретические знания и практические навыки, полученные при изучении дисциплины, могут быть использованы студентами при подготовке выпускной квалификационной работы.

3. Результаты освоения дисциплины

Дисциплина направлена на формирование компетенций УК-2, ПК-3, ПК-7.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ИУК 2.1. Знает основные положения нормативных правовых документов, относящихся к сфере профессиональной деятельности
	ИУК 2.2. Умеет определять конкретные задачи в рамках поставленной цели и выбирает оптимальные способы их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений
	ИУК 2.3. Выбирает способы решения задач с учетом этических норм, принятых в обществе
ПК-3 – способен применять предметные знания при реализации образовательного процесса	3.1. Знает закономерности, принципы и уровни формирования и реализации содержания образования; структуру, состав и дидактические единицы содержания школьных предметов: …
	3.2. Умеет осуществлять отбор учебного содержания для реализации в различных формах обучения в соответствии с дидактическими целями и возрастными особенностями обучающихся
	3.3. Владеет предметным содержанием; умениями

	отбора вариативного содержания с учетом взаимосвязи урочной и внеурочной форм обучения
ПК-7. Способен формировать у обучающихся конкретные знания, умения и навыки в области математики и информатики	7.1. Знает основные математические понятия и основы теоретической информатики, связи между ними и возможности использования при решении математических задач.
	7.2. Умеет решать типовые математические задачи и обучать методам их решения. 7.3. Умеет решать типовые задачи по информатике и программированию и обучать методам их решения.
	7.4. Подготовлен решать задачи разного уровня сложности по математике и информатике, определяя их место в школьном курсе.

В результате освоения дисциплины обучающийся должен **знать:**

− нормативно-правовую базу, регламентирующую отношения в сфере информационной безопасности, позволяющую организовать защиту жизни и здоровья обучающихся;

− основные понятия курса (информационная безопасность, угроза, защита информации, персональные данные, интеллектуальная собственность, конфиденциальность, авторские права и др.);

− административные и процедурные принципы обеспечения защиты информации при организации информационно-образовательной среды;

− основные сервисы современных информационных систем обеспечения информационной безопасности;

уметь:

− определять структуру и содержание образовательных программ по учебному предмету в соответствии с образовательными стандартами с учетом требований информационной безопасности;

− применять предметные знания в области информационной безопасности при реализации образовательного процесса;

− создавать условия для формирования у обучающихся конкретных знаний, умений и навыков в области информационной безопасности;

− организовывать ограничение доступа к контенту, далекого от дидактических задач,

− использовать программно-технические сервисы защиты информации;

владеть навыками:

− анализа деятельности организации на соответствие нормативно-правовым документам в области информационной безопасности;

− планирования образовательных программ по учебному предмету согласно требованиям образовательных стандартов и информационной безопасности;

− установки и настройки программно-технических сервисов защиты информации при проектировании, разработке и сопровождении информационно-образовательной среды.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Объем дисциплины и виды контактной и самостоятельной работы

Общая трудоемкость дисциплины составляет 3 зач. ед. (108 часов), их распределение по видам работ представлено в таблице.

Распределение трудоемкости дисциплины по видам работ

Вид работы	Кол-во часов
Общая трудоемкость дисциплины по учебному плану	**108**
Контактная работа, в том числе:	**38**
Лекции	12
Лабораторные занятия	26
Самостоятельная работа, в том числе:	**70**
Самоподготовка к текущему контролю знаний	61
Подготовка к зачету	9

4.2. Тематический план

Наименование разделов и тем дисциплины (модуля)	Всего часов	Вид контактной работы, час		Самостоятельная работа, час	Формы текущего контроля успеваемости
		Лекции	Лаб. работы		
Введение в проблему информационной безопасности	4	1		3	тест
Угрозы информационной безопасности и методы их реализации	8	2	2	4	тест, отчет по лабораторной работе
Правовые и организационные аспекты защиты информации	14	2	2	10	тест, отчет по лабораторной работе
Административный уровень обеспечения информационной безопасности	15	1	4	10	тест, отчет по лабораторной работе
Процедурный уровень обеспечения информационной безопасности	8	1	2	5	тест, отчет по лабораторной работе
Программно-технический уровень обеспечения информационной безопасности	27	3	10	14	тест, отчет по лабораторной работе
Общие меры по созданию безопасной ИС в образовательном учреждении.	23	2	6	15	тест, отчет по лабораторной работе
Зачет	9			9	выполнение заданий на зачете
Итого	**108**	**12**	**26**	**70**	

4.3. Практические занятия

№ п.п.	Тема занятия	Количество часов
1.	Анализ угроз информационной безопасности.	2
2.	Анализ основных нормативных документов в области информационной безопасности.	2
3.	Политика информационной безопасности организации. Частная модель угроз.	6
4.	Обеспечение безопасности при работе с документами.	2
5.	Возможности защиты информации в операционной системе Windows.	2
6.	Работа с командной строкой. Сетевая активность.	2
7.	Защита от несанкционированного доступа и сетевых хакерских атак.	2
8.	Основные признаки присутствия на компьютере вредоносных программ. Установка и предварительная настройка антивирусной программы.	2
9.	Использование контентной фильтрации Интернета, для фильтрации сайтов с одержимым, далёким от задач образования	2
10.	Обучение детей основам информационной безопасности, воспитание информационной культуры.	4
	Итого	26

4.4. Содержание тем 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.

Изучение и 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. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Представленный курс предусматривает наличие теоретических лекционных занятий, на которых студенты знакомятся с фундаментальными основами и принципами защиты информации на современном этапе развития информационных технологий студенты формируют навыки безопасной работы с различными видами информации.

Основными методами, используемыми при объяснении теоретического материала, являются:

– активные лекции;

– лекции с использованием презентаций;

– лекции с использованием демонстрационных материалов.

Основными методами, используемыми для практических занятий, являются:

– практикум с использованием демонстрационных примеров.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

6.1. Планирование самостоятельной работы

Темы занятий	Количество часов			Содержание самостоятельной работы	Формы контроля СРС
	Всего	Аудиторных	Самостоят. работы		
Введение в проблему информационной безопасности	4	1	3	Самостоятельное изучение теоретических	Обсуждение тезисов, тест

Темы занятий	Количество часов			Содержание самостоятельной работы	Формы контроля СРС
	Всего	Аудитор-ных	Самост оят. работы		
				вопросов – п.1,2 (список прилагается) с помощью указанных источников информации, подготовка тезисов по изученному материалу. Подготовка к тесту	
Угрозы информационной безопасности и методы их реализации	8	4	4	Самостоятельное изучение теоретического вопроса – п.5 (список прилагается) с помощью указанных источников информации. Подготовка таблицы по видам угроз информационной безопасности. Подготовка к тесту.	Проверка таблицы по видам угроз информационной безопасности. Обсуждение на занятии. Тест
Правовые и организационные аспекты защиты информации	14	4	10	Самостоятельное изучение теоретических вопросов – п.3,4 (список прилагается) с помощью указанных источников информации, подготовка тезисов по изученному материалу. Подготовка к лабораторному занятию. Выполнение домашней работы №1 Подготовка к тесту	Обсуждение тезисов, отчет по лабораторной работе, тест
Административный уровень обеспечения информационной безопасности	15	5	10	Подготовка к лабораторной работе, тесту	Отчет по лабораторной работе,

Темы занятий	Количество часов			Содержание самостоятельной работы	Формы контроля СРС
	Всего	Аудитор-ных	Самост оят. работы		
					тест
Процедурный уровень обеспечения информационной безопасности	8	3	5	Подготовка к лабораторной работе, тесту	Отчёт по лаборатор ной работе, тест
Программно-технический уровень обеспечения информационной безопасности	27	13	14	Выполнение домашней работы №2, 3. Подготовка к лабораторной работе, тесту	Обсужден ие домашней работы. Отчёт по лаборатор ной работе, тест
Общие меры по созданию безопасной ИС в образовательном учреждении.	23	8	15	Выполнение домашней работы №4. Подготовка к лабораторной работе, тесту	Обсужден ие домашней работы. Отчёт по лаборатор ной работе, тест
Экзамен	9		9	Подготовка к зачету	Выполнен ие заданий на зачете
Всего	**108**	**38**	**70**		

6.2. Организация текущего контроля и промежуточной аттестации

Качество усвоения учебного материала осуществляется по результатам выполнения заданий для самостоятельной работы на занятии, домашних работ. Особое место в контроле качества занимают отчеты по вопросам, выносимым на самостоятельное изучение. Целесообразно использование следующих форм текущего контроля:

- промежуточный контроль на практических занятиях для оценки самостоятельной работы студента при подготовке к ним;
- обсуждение результатов работы на занятиях и дома.

По результатам текущего контроля принимается решение на допуск студента к итоговому контролю (зачету).

Промежуточная аттестация по дисциплине в 9 семестре проводится в форме зачета с оценкой. Зачет выставляется по результатам ответа на устный вопрос и выполнения задания.

Примеры вопросов к зачету

1. Проблема информационной безопасности. Основные понятия.
2. Угрозы информационной безопасности.
3. Уровни обеспечения информационной безопасности.
4. Правовое обеспечение информационной безопасности. Основные нормативные документы.

5. ФЗ «О персональных данных».

6. ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

7. Концепция информационной безопасности предприятия.

8. Политика информационной безопасности предприятия.

9. Анализ рисков информационной системе предприятия. Стратегии управления рисками.

10. Процедурные меры обеспечения информационной безопасности.

11. Основные сервисы программно-технического уровня обеспечения информационной безопасности.

12. Идентификация и аутентификация.

13. Парольная аутентификация.

14. Логическое управление доступом.

15. Компьютерные вирусы, классификация.

16. Признаки заражения компьютера вредоносным программным обеспечением.

17. Средства защиты от компьютерных вирусов.

18. Протоколирование и аудит.

19. Криптографические средства защиты.

20. Экранирование.

Типовые практические задания

Задание 1.

С официального сайта GoogleChrome скачайте и установите плагин, позволяющий настроить белый список сайтов, настройте его для работы школьников по теме «Безопасное поведение на воде», при анализе информационных ресурсов используйте федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию».

Задание 2.

Создайте нового пользователя «Ученик» в операционной системе, назначьте ему группу пользователя, выбор обоснуйте. Для пользователя «Ученик» настройте главное меню и рабочий стол так, чтобы доступ открывался только к учебным файлам, настройки осуществляйте с учетной записи администратора.

Задание 3.

Выберите и установите на компьютер утилиту, позволяющую осуществить чистку реестра компьютера. Отключите автозапуск программ, обоснуйте выбор отключаемых программ. Найдите на компьютере все файлы дубликаты.

Задание 4.

Выберите и установите на компьютер антивирусное программное обеспечение. Выполните следующие настройки:

- Установить пароль, сделать общедоступными «Общий доступ к программе» и «Контроль обновлений», все остальные варианты включить в защиту.
- Добавить в исключения сайт https://www.ntspi.ru/ , а в усиленный режим сканирования добавить одну из программ, установленных на компьютере.
- Настроить выгрузку отчетов для веб-экранов в формате HML , в отчет включить: зараженные файлы, серьезные ошибки и файлы, не прошедшие проверку.
- Ограничить доступ с компьютера к трем сайтам. Попробовать перейти на эти сайты.
- Просканировать одну из папок, находящуюся на компьютере.

Задание 5.

Разработать план проведения родительского собрания по вопросам информационной безопасности детей в сети Интернет, подобрать или оформить демонстрационные материалы. Выбор возрастной категории учащихся можно осуществить самостоятельно.

Задание 6.

Разработать и оформить рекомендации родителям по обеспечению информационной безопасности детей в сети Интернет (в виде раздаточного материала).

Критерии оценки:

«Отлично» выставляется студентам, успешно сдавшим зачет с оценкой и показавшим глубокое знание теоретической части курса, умение проиллюстрировать изложение практическими примерами, правильно и без ошибок выполнивших практическое задание.

«Хорошо» выставляется студентам, сдавшим зачет с незначительными замечаниями, показавшим глубокое знание теоретического вопроса, умение проиллюстрировать изложение практическими примерами, выполнившим практическое задание в целом верно, допустившим незначительные ошибки, указывающие на наличие несистематичности и пробелов в знаниях.

«Удовлетворительно» выставляется студентам, сдавшим зачет со значительными замечаниями, показавшим знание основных положений теории при наличии существенных пробелов, испытывающим затруднения при выполнении практической работы.

«Неудовлетворительно» выставляется, если студент показал существенные пробелы в знаниях основных положений теории, не умеет применять теоретические знания на практике, не выполнил практическое задание.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Основная литература

1. Кисляков, П. А. Безопасность образовательной среды. Социальная безопасность : учебное пособие для вузов / П. А. Кисляков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 156 с. — (Высшее образование). — ISBN 978-5-534-11818-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456941 (дата обращения: 2020 г.).

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450371 (дата обращения: 2020 г.).

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: 2020 г.).

Дополнительная литература

4. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2020. — 318 с. — (Высшее образование). — ISBN 978-5-534-00475-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451108 (дата обращения: 2020 г.).

5. Информационное право : учебник для вузов / Н. Н. Ковалева [и др.] ; под редакцией Н. Н. Ковалевой. — Москва : Издательство Юрайт, 2020. — 353 с. — (Высшее

образование). — ISBN 978-5-534-13786-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/466887 (дата обращения: 2020 г.).

6. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454453 (дата обращения: 2020 г.).

7. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2020. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/448295 (дата обращения: 2020 г.).

8. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451486 (дата обращения: 2020 г.).

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебная аудитория 213А: 11 посадочных мест для студентов, рабочее место преподавателя, компьютеры – 12 шт., маркерная доска, проекционное оборудование.