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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.08.06 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Уровень высшего образования	Бакалавриат
Направление подготовки	44.03.05 Педагогическое образование (с двумя профилями подготовки)
Профили	Все профили
Форма обучения	Очная

Нижний Тагил
2022

Рабочая программа дисциплины «Информационная безопасность и защита информации». Нижнетагильский государственный социально-педагогический институт (филиал) федерального государственного автономного образовательного учреждения высшего образования «Российский государственный профессионально-педагогический университет», Нижний Тагил, 2022. 12 с.

Настоящая программа составлена в соответствии с требованиями ФГОС ВО по направлению 44.03.05 Педагогическое образование (с двумя профилями подготовки) (№125 от 22.02.2018).

Автор: канд. пед. наук, доцент, доцент кафедры ИТ _____ Е. С. Васева

Одобрен на заседании кафедры ИТ 17 июня 2022 г., протокол № 14

Заведующий кафедрой ИТ _____М.В. Мащенко

Рекомендован к печати методической комиссией ФЕМИ 21 июня 2022 г., протокол № 9.

Председатель методической комиссии ФЕМИ _____В.А. Гордеева

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Задачи дисциплины:

– познакомить студентов с правовыми основами и нормами профессиональной этики в сфере обеспечения информационной безопасности;

– сформировать навыки взаимодействия с участниками образовательных отношений при соблюдении норм профессиональной этики и требований соблюдения конфиденциальности информации;

– 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;

– 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 и защита информации» 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». Реализуется кафедрой информационных технологий.

Дисциплина «Информационная безопасность и защита информации» базируется на компетенциях, полученных при изучении дисциплин «Технологии цифрового образования», «Информационные системы и управление данными», «Сети и телекоммуникации», «Теория и методика обучения информатике».

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины направлен на формирование и развитие следующих компетенций:

Наименование категории (группы) универсальных компетенций	**Код и наименование универсальной компетенции**	**Код и наименование индикатора достижения универсальной компетенции**
Правовые и этические основы профессиональной деятельности	ОПК-1. Способен осуществлять профессиональную деятельность в соответствии с нормативно-правовыми актами в сфере образования и нормами	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 вопросам

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
	профессиональной этики	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.
		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.
Взаимодействие с участниками образовательных отношений	ОПК-7. Способен взаимодействовать с участниками образовательных отношений в рамках реализации образовательных программ	ОПК-7.1. Взаимодействует с родителями (законными представителями) обучающихся с учетом требований нормативно-правовых актов в сфере образования и индивидуальной ситуации обучения, воспитания, развития обучающегося.
		ОПК-7.2. Взаимодействует со специалистами в рамках психолого-медико-педагогического консилиума.
		ОПК-7.3. Взаимодействует с представителями организаций образования, социальной и духовной сферы, СМИ, бизнес-сообществ и др.
Информационно-коммуникационные технологии для профессиональной деятельности	ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-9.1. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности.
		ОПК-9.2. Демонстрирует способность использовать цифровые ресурсы для решения задач профессиональной деятельности.
Педагогическая деятельность по проектированию и реализации	ПК-1. Способен осваивать и использовать теоретические знания и	ПК-1.1. Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета).

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
образовательного процесса в образовательных организациях дошкольного, начального общего, основного общего, среднего общего образования. Воспитательная деятельность	практические умения и навыки в предметной области при решении профессиональных задач	ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.
		ПК-1.3. Демонстрирует умение разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные.
Педагогическая деятельность по проектированию и реализации образовательного процесса в образовательных организациях дошкольного, начального общего, основного общего, среднего общего образования. Развивающая деятельность	ПК-3. Способен формировать развивающую образовательную среду для достижения личностных, предметных и метапредметных результатов обучения средствами преподаваемых учебных предметов	ПК-3.1. Владеет способами интеграции учебных предметов для организации развивающей учебной деятельности (исследовательской, проектной, групповой и др.).
		ПК-3.2. Использует образовательный потенциал социокультурной среды региона в преподавании (предмета по профилю) в учебной и во внеурочной деятельности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Объем дисциплины и виды контактной и самостоятельной работы

Вид работы	Кол-во часов
Общая трудоемкость дисциплины по учебному плану	**108**
Контактная работа, в том числе:	**46**
Лекции	18
Лабораторные занятия	28
Самостоятельная работа, в том числе:	**62**
Самоподготовка к текущему контролю знаний	35
Подготовка к экзамену, экзамен	27

4.2. Учебно-тематический план

Наименование разделов и тем дисциплины (модуля)	Всего часов	Вид контактной работы, час		Сам. работа	Формы текущего контроля успеваемости
		Лекции	Лаб. работы		
Тема 1. Введение в проблему информационной безопасности	5	2		3	тест
Тема 2. Угрозы информационной безопасности и методы их реализации	8	2	2	4	тест, отчет по лабораторной работе
Тема 3. Правовые и организационные аспекты защиты информации	10	2	4	4	тест, отчет по лабораторной работе
Тема 4. Административный уровень обеспечения информационной безопасности	10	2	4	4	тест, отчет по лабораторной работе
Тема 5. Процедурный уровень обеспечения информационной безопасности	8	2	2	4	тест, отчет по лабораторной работе
Тема 6. Программно-технический уровень обеспечения информационной безопасности	22	4	10	8	тест, отчет по лабораторной работе
Тема 7. Общие меры по созданию безопасной ИС в образовательном учреждении.	18	4	6	8	тест, отчет по лабораторной работе
Экзамен	27			27	выполнение заданий на экзамене
Итого	**108**	**18**	**28**	**62**	

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.

Тематика лабораторных занятий

№ 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	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	4

№ п.п.	Тема занятия	Количество часов
	образования	
10.	Обучение детей основам информационной безопасности, воспитание информационной культуры.	4
	Итого	28

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Обучение по дисциплине «Информационная безопасность и защита информации» целесообразно построить с использованием компетентностного подхода, в рамках которого образовательный процесс строится с учетом специфики будущей профессиональной деятельности студентов. Лекционные занятия должны стимулировать познавательную ативность студентов, поэтому в ходе лекций необходимо обращение к примерам, взятым из практики, включение проблемных вопросов и ситуаций.

Основными методами, используемыми на практических занятиях, будут: практикум с использованием практико-ориентированных задач, метод проектов, метод проблемных ситуаций.

6. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

6.1. Организация самостоятельной работы студентов

Самостоятельная работа студентов включает изучение вопросов, вынесенных за рамки аудиторных занятий, расширение и углубление знаний по темам, рассмотренным на лекционных занятиях. При подготовке к практическим занятиям студенты изучают учебные тексты, выполняют тренировочные задания, решают задачи, разрабатывают проекты, готовят доклады, рассматривают способы реализации технологий обеспечения информационной безопасности, обеспечение информационной безопасности учащихся при организации образовательного процесса. Лабораторные работы преподавателям проверяются по отчетам, устные выступления оцениваются в ходе практического занятия.

6.2. Организация текущего контроля и промежуточной аттестации

Текущий контроль усвоения знаний ведется по итогам представления выполненных самостоятельных заданий и защиты отчетов по лабораторным работам; участия в дискуссиях на лекционных занятиях, проверки результатов тестирования.

Текущий контроль учебных достижений студентов может быть проведен с использованием накопительной балльно-рейтинговой системы оценки (НБРС). В этом случае оценке в баллах подлежат как результаты текущих опросов, так и результаты выполнения практических заданий. Для оценки используется шкала баллов, разработанная в соответствии с Положением о НБРС.

Промежуточная аттестация по данной дисциплине проводится в форме экзамена в 10 семестре.

Примеры вопросов к экзамену

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 экзамен и показавшим глубокое знание теоретической части курса, умение проиллюстрировать изложение практическими примерами, правильно и без ошибок выполнивших практическое задание.

«Хорошо» выставляется студентам, сдавшим экзамен 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 экзамен 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: *указывается до 5 наименований не старше 5 лет*

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: 2022 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: 2022 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: 2022 г.).

Дополнительная литература: *указывается до 5 наименований не старше 5 лет*

1. 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: 2022 г.).

2. 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: 2022 г.).

3. 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: 2022 г.).

4. 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: 2022 г.).

5. 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: 2022 г.).

Программное обеспечение общего и профессионального назначения: LibreOffice, LibreOffice Base, LibreOffice Impress, Kaspersky Endpoint Security – 300, Adobe Reader, браузер Google chrome/Mozilla Firefox, Oracle VM VirtualBox.

Информационные системы и платформы:

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. Электронная информационно-образовательная среда РГППУ (https://eios.rsvpu.ru/).
4. Платформа для организации и проведения вебинаров «Mirapolis Virtual Room».

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Учебная аудитория для проведения занятий лекционного типа.
2. Учебная аудитория для проведения занятий лабораторного типа, проведения групповых и индивидуальных консультаций, проведения текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами с доступом в интернет, доступом в электронную информационно-образовательною среду, программное обеспечение общего и профессионального назначения.