Министерство образования и науки 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

УТВЕРЖДАЮ
Зам. директора по УМР
_____ В.В. Дикова
«____»_____2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Уровень высшего образования	Бакалавриат
Направление подготовки	44.03.01 Педагогическое образование
Профили	«Безопасность жизнедеятельности»
Формы обучения	Заочная

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 направлению подготовки 44.03.01 Педагогическое образование.

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

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

Одобрена на заседании кафедры информационных технологий 14 марта 2019 г., протокол №8.

Заведующая кафедрой М. В. Мащенко

Рекомендована к печати методической комиссией факультета спорта и безопасности жизнедеятельности 31 августа 2020 г., протокол № 1.

Председатель методической комиссии ФСБЖ Л. А. Сорокина

Декан ФСБЖ А.В. Неймышев

Главный специалист отдела информационных ресурсов О. В. Левинских

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины 4
2. Место дисциплины в структуре образовательной программы 4
3. Результаты освоения дисциплины 4
4. Структура и содержание дисциплины 5
4.1. Объем дисциплины и виды контактной и самостоятельной работы 5
4.2. Содержание и тематическое планирование дисциплины 5
4.3. Содержание тем дисциплины 6
5. Образовательные технологии 7
6. Учебно-методические материалы 8
6.1. Планирование самостоятельной работы (очная форма обучения) 8
6.2. Задания и методические указания по организации самостоятельной работы 9
7. Учебно-методическое и информационное обеспечение 10
8. Материально-техническое обеспечение дисциплины 10
9. Текущий контроль качества усвоения знаний 11
10. Итоговая аттестация 11

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Задачи дисциплины:

- 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 для ориентирования в современном информационном пространстве;

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

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Курс «Информационная безопасность» предназначен для студентов, обучающихся по направлению «Педагогическое образование» и относится к факультативам. Курс имеет как теоретический, так и прикладной характер и призван сообщить будущим специалистам основные принципы и технические решения организации безопасного хранения, обработки и передачи информации, позволяющие предотвратить ее искажение, утрату и несанкционированное копирование.

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины направлен на формирование и развитие компетенций:

ОК-3 – способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве;

ПК-1 – готовностью реализовывать образовательные программы по учебному предмету в соответствии с требованиями образовательных стандартов.

В результате изучения курса студенты должны **знать:**

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

– организационно-правовое обеспечение защиты информации;

– угрозы информационной безопасности и средства защиты в современном информационном пространстве;

– основные методологические положения защиты информации., позволяющие обеспечивать охрану жизни и здоровья обучающихся;

– основные сервисы современных информационных систем обеспечения информационной безопасности;

– достоинства и недостатки, перспективы развития современных систем защиты информации.

уметь:

– ограничивать использование ресурсов компьютера и локальной сети на основе раздельного доступа пользователей в операционную систему;

– организовывать безопасную работу в Интернет и всем современном информационном пространстве;

– выполнять резервное копирование, восстановление данных в различных информационных системах;

– использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов;

– обеспечивать охрану жизни и здоровья обучающихся в современном информационном пространстве;

– реализовывать образовательные программы по учебному предмету.

владеть навыками:

– анализа деятельности организации на соответствие нормативно-правовым актам в области информационной безопасности.

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	Количество часов
Общая трудоемкость дисциплины по учебному плану	**72**
Контактная работа, в том числе:	**8**
Лекции	4
Лабораторные занятия	4
Самостоятельная работа, в том числе:	**64**
Самоподготовка к текущему контролю знаний	4
Подготовка к зачету	60

4.2. Содержание и тематическое планирование дисциплины

Наименование разделов и тем дисциплины (модуля)	Всего часов	Вид контактной работы, час			Самостоятельная работа, час	Формы текущего контроля успеваемости
		Лекции	Лаб. работы	Из них в интерактивной форме		
Введение в проблему информационной безопасности	4	0,5		0,5	3,5	тест
Угрозы информационной безопасности и методы их реализации	7	0,5		0,5	6,5	тест, отчет по лабораторной работе
Правовые и организационные аспекты защиты информации	8	0,5	1	1	6,5	тест, отчет по лабораторной работе

Наименование разделов и тем дисциплины (модуля)	Всего часов	Вид контактной работы, час			Самостоятельная работа, час	Формы текущего контроля успеваемости
		Лекции	Лаб. работы	Из них в интерактивной форме		
Административный уровень обеспечения информационной безопасности	6	0,5	1	1	4,5	тест, отчет по лабораторной работе
Процедурный уровень обеспечения информационной безопасности	7	0,5			6,5	тест, отчет по лабораторной работе
Программно-технический уровень обеспечения информационной безопасности	23	1	1	1	21	тест, отчет по лабораторной работе
Общие меры по созданию безопасной ИС в образовательном учреждении.	13	0,5	1	1	11,5	тест, отчет по лабораторной работе
Зачет	4				4	выполнение заданий на зачете
Итого	**72**	**4**	**4**	**5**	**64**	

4.3. 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.

Содержание лабораторных работ по курсу

Тема занятия	Количество часов
1. Анализ основных нормативных документов в области информационной безопасности.	1
2. Политика информационной безопасности организации. Частная модель угроз.	1
3. Обеспечение безопасности при работе с документами.	1
4. Обучение детей основам информационной безопасности, воспитание информационной культуры.	1

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-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

6.1. Планирование самостоятельной работы (заочная форма обучения)

Темы занятий	Количество часов			Содержание самостоятельной работы	Формы контроля СРС
	Всего	Аудиторных	Самос. работы		
Введение в проблему информационной безопасности	4	0,5	3,5	Самостоятельное изучение теоретических вопросов – п.1,2 (список прилагается) с помощью указанных источников информации, подготовка тезисов по изученному материалу. Подготовка к тесту	Обсуждение тезисов, тест
Угрозы информационной безопасности и методы их реализации	7	0,5	6,5	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	8	1,5	6,5	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	6	1,5	4,5	Подготовка к лабораторной работе, тесту	Отчет по лабораторной работе, тест

Темы занятий	Количество часов			Содержание самостоятельной работы	Формы контроля СРС
	Всего	Аудиторных	Самос. работы		
Процедурный уровень обеспечения информационной безопасности	7	0,5	6,5	Подготовка к лабораторной работе, тесту	Тест
Программно-технический уровень обеспечения информационной безопасности	23	2	21	Выполнение домашней работы №2, 3. Подготовка к лабораторной работе, тесту	Обсуждение домашней работы. Отчёт по лабораторной работе, тест
Общие меры по созданию безопасной ИС в образовательном учреждении.	13	1,5	11,5	Выполнение домашней работы №4. Подготовка к лабораторной работе, тесту	Обсуждение домашней работы. Отчёт по лабораторной работе, тест
Зачет	4		4	Подготовка к зачету	Выполнение заданий на зачете
Всего	**72**	**8**	**64**		

6.2. Задания и методические указания по организации самостоятельной работы

Список вопросов, выносимых на самостоятельное изучение

1. История развития систем защиты информации.
2. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах.
3. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
4. Компьютерные преступления.
5. Основные методы реализации угроз информационной безопасности.

Задания для самостоятельной работы (домашние задания)

В рамках самостоятельной работы студентов предусмотрено выполнение творческих домашних заданий. Их цель – закрепление знаний, полученных на практических занятиях.

Домашнее задание №1.

Найти и проанализировать статистических данные об атаках, которым подвергаются компьютерные системы и потерях банков.

Домашнее задание №2.

Проанализировать компьютерные средства реализации защиты в информационных системах вуза, выявить недостатки и предложить пути их решения.

Домашнее задание №3.

Выполнить анализ эффективности 2-3 антивирусных программ.

Домашнее задание №4.

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.

Домашнее задание №5.

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Основная литература

1. Курило, А.П. Основы управления информационной безопасностью.: учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов [и др.]. М. : Горячая линия-Телеком, 2012. 244 с. URL: http://e.lanbook.com/books/element.php?pl1_id=5178 (дата обращения 2017 г.).

2. Малюк, А.А. Введение в информационную безопасность : учебное пособие / А.А. Малюк, В.С. Горбатов, В.И. Королев. М. : Горячая линия-Телеком, 2012. 288 с. URL: http://e.lanbook.com/books/element.php?pl1_id=5171 (дата обращения 2017 г.).

3. Милославская, Н.Г. Управление рисками информационной безопасности: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. М.: Горячая линия-Телеком, 2012. 130 с. URL: http://e.lanbook.com/books/element.php?pl1_id=5179 (дата обращения 2017 г.).

4. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник / О.В. Прохорова. – Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. 113 с. URL: http://www.iprbookshop.ru/43183.html (дата обращения 2017 г.).

Дополнительная литература

1. Васильев, В.И. Интеллектуальные системы защиты информации [Электронный ресурс] : учебное пособие / В.И. Васильев. М.: Машиностроение, 2013. 172 с. URL: https://e.lanbook.com/book/5792 (дата обращения 2017 г.).

2. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. 266 с. URL: http://www.iprbookshop.ru/52209.html (дата обращения 2017 г.).

3. Фаронов, А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А.Е. Фаронов. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. 154 с. URL: http://www.iprbookshop.ru/52160.htm (дата обращения 2017 г.).

4. Зайцев, А.П. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников. М.: Горячая линия-Телеком, 2012. 616 с. URL: https://e.lanbook.com/book/5154 (дата обращения 2017 г.).

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебная аудитория 313А: 11 посадочных мест для студентов, рабочее место преподавателя, интерактивная доска, стационарный мультимедиакомплекс.

9. ТЕКУЩИЙ КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

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.

10. ИТОГОВАЯ АТТЕСТАЦИЯ

Итоговая аттестация выпускников представляет собой форму контроля (оценки) освоения выпускниками программы «Информационная безопасность» в соответствии с требованиями, установленными к содержанию, структуре и условиям реализации программы.

Перечень обязательных видов работы студента, необходимых для получения допуска:

- Посещение лекционных занятий.

- Ответы на теоретические вопросы на лабораторных занятиях.

- Решение практических задач на лабораторных занятиях, выполнение заданий для самостоятельной работы.

- Выполнение домашних работ.

Форма проведения итоговой аттестации: студент получает билет, в котором сформулированы один теоретический вопрос и одно практическое задания, и приступает к решению практической задач и подготовке ответа на теоретический вопрос. На подготовку ответа отводится не более 30 минут. При подготовке запрещается пользоваться конспектами и учебной литературой, получать информацию из сети Интернет.

Если выполнение практического задания на компьютере и его демонстрация признаны успешными, то студент приступает к устному ответу на теоретический вопрос. Оценку преподаватель выставляет сразу после ответа экзаменующегося.

Типовые теоретические вопросы

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.

Выполните поиск и анализ перечисленных документов в одной из справочно-информационных систем, заполните следующую таблицу:

№ п.п.	Название нормативно-правового документа	Дата принятия	Краткий обзор документа
	Об информации, информатизации и защите информации		

Задание 2.

Разработайте кроссворд по основным понятиям информационной безопасности. Установите пароль на изменение файла, пользователь, имеющий право на изменение может вносить записи только в ячейки кроссворда, не изменяя структура и формулировку вопросов. Установите пароль на открытие файла. Добавьте видимую цифровую подпись к документу.

Задание 3.

В программе Microsoft Excel создайте тест (4-5 вопросов) по безопасности дорожного движения. При вводе правильного ответа соответствующая ячейка должна загораться зеленым цветом. Организуйте защиту файла таким образом, чтобы отвечающему не были доступны сведения, необходимые для проверки ответов.

Задание 5.

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 6.

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 7.

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 8.

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 9.

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 10.

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

Критерии оценки:

«Зачтено» выставляется студентам, успешно сдавшим зачет и показавшим глубокое знание теоретической части курса, умение проиллюстрировать изложение практическими примерами, правильно или с незначительными ошибками выполнивших практическое задание.

«Не зачтено» выставляется, если студент показал существенные пробелы в знаниях основных положений теории, не умеет применять теоретические знания на практике, не выполнил практическое задание или выполнил, допустив грубые ошибки.