Министерство просвещения Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования

«Ярославский государственный педагогический университет им. К.Д. Ушинского»

УТВЕРЖДАЮ
Директор института развития кадрового потенциала
_____ О.А. Коряковцева

«12» 09 2022 г.

Дополнительная профессиональная программа повышения квалификации

«Информационная безопасность»

согласно лицензии № 2284 от 22.07.2016 г.,
выданной Федеральной службой по надзору в сфере образования и науки

Ярославль, 2022.

Программа повышения квалификации «Информационная безопасность» обсуждена и принята на заседании кафедры теории и методики профессионального образования Института развития кадрового потенциала «12» сентября 2022 г., протокол №1.

Разработчики программы:

Ст. преподаватель _____ Рицкова Т.И.

СОГЛАСОВАНО.

_____

Зав. кафедрой теории и методики
профессионального образования
д.и.н., профессор _____ М.В. Новиков

_____

Эксперты:

Зам.директора ИРКП, к.псих.н., доцент А.Ю. Куликов

_____

ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Программа повышения квалификации «Информационная безопасность для педагогов» разработана на основании

Количество учебных часов: 24 часа

Развитие процесса информатизации всех сфер человеческой деятельности (в том числе и образовательной сферы) становится причиной возникновения новой проблемы - информационной безопасности человека и общества. Очевидно, что различные виды использования информационно-коммуникативных технологий влияют на поведение, процесс формирования моральных норм, на психику и жизнь будущих поколений. В условиях современного общества одним из важнейших аспектов деятельности педагога становится обеспечение информационной безопасности всех участников образовательного процесса и необходимой защиты информации.

Данная образовательная программа позволит педагогам повысить компетенции в области информационной безопасности, а также повысить уровень информационной культуры.

В процессе обучения по программе педагоги познакомятся с основными методами и средствами защиты информации при работе с ИКТ, а также со средствами и методами обеспечения информационной безопасности личности.

Актуальность программы определяется востребованностью преподавателей, которые имеют не только высокий уровень знаний и умений в области информационных технологий, но и владеют программно-техническими мерами защиты информации, хорошо осведомлены о проблемах информационной безопасности личности школьника в ИКТ- насыщенной среде.

Реализация программы направлена на совершенствование информационной культуры педагогов, необходимой для профессиональной деятельности.

Цель программы: повышение компетенций педагогических работников в области информационной безопасности.

Основные задачи программы:

- познакомить слушателей с основами информационной безопасности;
- развить умения в области защиты информации;
- дать представление об информационной безопасности личности и способах защиты от информационного воздействия;
- сформировать навыки безопасной работы с Интернет-ресурсами;
- познакомить слушателей с Федеральным законом №152-ФЗ «О персональных данных».

Образовательные ценности: практические умения и навыки в области защиты информации; теоретические знания в области информационной безопасности.

Основные принципы построения и структура программы: в основе программы лежит установка на формирование у слушателей понимания основ информационной безопасности и овладение практическими навыками защиты информации и личности.

Категория слушателей, особенности группы: образовательная программа предназначена для сотрудников системы образования, имеющих высшее или среднее профессиональное образование, владеющих навыками работы на персональном компьютере.

Ожидаемые результаты освоения программы:

- усвоение теоретических знаний по вопросам защиты информации, информационной безопасности личности, правилах размещения информации на школьных сайтах;
- развитие умений по защите информации в Интернете, при работе с ПК и мобильными устройствами.
- развитие навыков противодействия негативным информационным воздействиям.

Категория обучающихся, требование к образованию: преподаватели высших и средних учебных заведений и сузов, имеющие среднее профессиональное и (или) высшее образование; студенты, получающие высшее образование.

- **Форма обучения:** очная.
- **Трудоемкость обучения, срок освоения программы:** 24 часа.

Формы итогового контроля:

Защита итоговой работы. Зачет.

Лицам, успешно освоившим дополнительную профессиональную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: **удостоверение о повышении квалификации** установленного образца.

СОДЕРЖАНИЕ ПРОГРАММЫ

Учебный план

программы повышения квалификации
«Информационная безопасность для педагогов»

Программа может быть реализована в очном, очно-заочном, при необходимости-дистанционном формате.

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе:		Формы контроля
			лекции	практические занятия	
Понятие информационного общества. Основные понятия защиты информации и вредоносное ПО.		**4**	**2**	**2**	Тестовое задание, практическое задание
1	**Понятие информационного общества:** 1. Информационное общество 2. Глобальные проблемы, обусловленные информатизацией общества	2	1	1	Тестовое задание, практическое задание
	Основные понятия защиты информации и вредоносное ПО: 1. Информационная безопасность 2. Вредоносное программное обеспечение	2	1	1	
Антивирусная защита компьютера и мобильных устройств. Защита компьютера.		**4**	**2**	**2**	Тестовое задание, практическое задание
2	**Антивирусная защита компьютера и мобильных устройств:** 1. Антивирусная защита компьютера и мобильных устройств 2. Основные антивирусные программы	2	1	1	Тестовое задание, Практическое задание
	Защита компьютера: 1. Настройка прав доступа в операционной системе Windows 2. Защита информации в текстовом редакторе 3. Восстановление данных с помощью средств ОС	2	1	1	Практическая работа

Защита информации в интернете		**2**	**1**	**1**	Тестовое задание, Практическая работа
3	**Защита информации в интернете:** 1. Защищенная работа с браузером 2. Защита информации в социальных сетях	2	1	1	Тестовое задание Практическая работа
Информационно-психологическая безопасность личности		**2**	**1**	**1**	Тестовое задание
4	**Информационно-психологическая безопасность личности:**	2	1	1	Тестовое задание
	1. Информационно-психологическая безопасность личности 2. Источники и средства информационно-психологического воздействия				
Информационное манипулирование, нейролингвистическое программирование		**2**	**1**	**1**	Тестовое задание, Практическое задание
5	**Информационное манипулирование, нейролингвистическое программирование:** 1. Виды информационного манипулирования 2. Нейролингвистическое программирование	2	1	1	Тестовое задание, Практическое задание
Способы защиты личности от негативных факторов информации		**2**	**1**	**1**	Практическое задание
6	**Способы защиты личности от негативных факторов информации:** 1. Способы защиты личности от негативных факторов информации	2	1	1	Практическое задание
Особенности Интернет-общения. Девиантное поведение в сфере ИКТ.		**4**	**2**	**2**	Тестовое задание, Практическое задание
7	**Особенности Интренет-общения:** 1. Формы и особенности Интернет-общения 2. Информационная культура и сетевой этикет	2	1	1	Тестовое задание, Практическое задание

	Девиантное поведение в сфере ИКТ: 1. Девиантное поведение в сфере ИКТ 2. Методики выявления девиантного поведения в сфере ИКТ	2	1	1	Тестовое задание
Защита персональных данных. Размещение информации на официальном сайте образовательной организации		**1**	**-**	**1**	Тестовое задание
8	**Защита персональных данных. Размещение информации на официальном сайте образовательной организации:** 1. Персональные данные 2. Размещение информации на официальном сайте образовательной организации	1	-	1	Тестовое задание
Итоговая аттестация		**3**	**-**	**3**	Тестовое задание, Практическая работа
9	**Итоговая аттестация:** 1. Защита итогового проекта. Зачет.	3	-	3	Практическая работа. Зачет.
	Итого:	**24**	**10**	**14**	

Календарный учебный график
программы повышения квалификации
«Информационная безопасность для педагогов»

Теоретическое обучение и практические занятия: 3 дня.

Практические занятия проводятся в те же дни, что и теоретическое обучение, по темам, обозначенным в учебном плане, как закрепление знаний и совершенствование необходимых профессиональных компетенций.

Итоговая аттестация: проводится в последний день обучения.

Рабочая программа

РАЗДЕЛ 1. Защита информации.

Понятие информационного общества

Информационное общество. Характерные черты информационного общества. Критерии информационного общества. Процесс информатизации общества. Глобальные проблемы, обусловленные информатизацией общества.

Слушатели должны знать:

- содержание понятий «информационное общество», «информация» и «информатизация общества»;
- характерные черты и критерии информационного общества;
- глобальные проблемы, обусловленные информатизацией общества;

Слушатели должны уметь:

- ориентироваться в понятиях «информационное общество», «информация» и «информатизация общества»;

- выделять тенденции информатизации общества, которые находят отражение в педагогической деятельности;
- определять проблемы, связанные с информатизацией общества (в том числе в образовательной сфере).

Основные понятия защиты информации и вредоносное ПО

Информационная безопасность. Защита информации. Базовые принципы защиты информации: конфиденциальность, целостность и доступность. Средства защиты информации.
Вредоносное программное обеспечение. Виды вредоносного ПО. Проявление заражения устройства вредоносными программами.

Слушатели должны знать:
- содержание понятий «информационная безопасность», «защита информации», «вредоносное программное обеспечение»
- базовые принципы защиты информации и основные виды средств защиты информации
- основные виды вредоносного программного обеспечения и основные признаки заражения устройства данным ПО.

Слушатели должны уметь:
- ориентироваться в базовых принципах защиты информации;
- различать между собой различные виды вредоносного ПО;
- определять заражен ли ПК вредоносным ПО.

Антивирусная защита компьютера и мобильных устройств

Антивирусная программа. Достоинства и недостатки антивирусных программ. Вредоносное программное обеспечение для мобильных устройств. Антивирусная защита мобильных устройств. Основные антивирусные программы.

Слушатели должны знать:
- правила защиты компьютера от вредоносного ПО;
- достоинства и недостатки антивирусных программ;
- основные антивирусные программы;
- признаки заражения вредоносным ПО устройства.

Слушатели должны уметь:
- выбирать среди большого количества антивирусную программу соответственно целям использования и возможностям определенного компьютера/мобильного устройства;
- устанавливать антивирусную программу на ПК и мобильное устройство

Защита компьютера

Учетная запись пользователя Windows. Установления пароля учетной записи. Восстановление забытого пароля. Закрытие доступа к личным папкам пользователя. Настройка брандмауэра Windows. Архивация данных. Восстановление данных. Безвозвратное удаление информации. Защита информации в текстовом редакторе.

Слушатели должны знать:
- параметры учетной записи пользователя операционной системы;
- инструменты для установления и восстановления пароля;
- инструменты и программы для восстановления данных на компьютере, съемном носителе.

Слушатели должны уметь:

- настраивать учетную запись пользователя операционной системы;
- устанавливать и восстанавливать пароли учетных записей;
- защищать информацию с помощью архивации данных;
- безвозвратно удалять информацию с компьютера.

Защита информации в Интернете

Настройка браузера. Блокировка рекламы и нежелательных сайтов. Кэш браузера. Файлысооые. Режим инкогнито. Хранение паролей в браузере. Защита информации в социальных сетях. Правила безопасной работы в социальной сети.

Слушатели должны знать:

- основные параметры настройки браузера для безопасной работы;
- правила безопасной работы в социальных сетях;

Слушатели должны уметь:

- настраивать работу браузера в безопасном режиме для пользователя;
- устанавливать надежные пароли.

РАЗДЕЛ 2. Защита личности от негативных факторов информации

Информационно-психологическая безопасность личности

Информационно-психологическая безопасность. Дезинформация, виды дезинформации. Информационный прессинг, информационное зомбирование, информационная агрессия. Источники и средства информационно-психологического воздействия.

Слушатели должны знать:

- понятия «дезинформация», «информационный прессинг», «информационное зомбирование», «информационная агрессия»;
- основные источники информационно-психологического воздействия;
- основные средства информационно-психологического воздействия.

Слушатели должны уметь:

- различать виды информационного-психологического воздействия.

Информационное манипулирование, нейролингвистическое программирование

Информационное манипулирование. Психологическая атака, давление, манипулирование. Приемы психологического давления. Приёмы «Азбуки пропаганды».Техники нейролингвистического программирования.

Слушатели должны знать:

- понятия «информационное манипулирование», «нейролингвистическое программирование»
- основные приемы психологического давления и нейролингвистического программирования.

Слушатели должны уметь:

- распознавать в практических ситуациях информационное манипулирование.

Способы защиты личности от негативных факторов информации

Основные способы защиты личности: уход, вытеснение, блокировка, управление, затаивание, игнорирование.

Слушатели должны знать:
- основные способы защиты личности от информационного воздействия;
- приёмы защиты от информационного манипулирования.

Слушатели должны уметь:
- определять тип защиты в конфликтной ситуации.

РАЗДЕЛ 3. Взаимодействие в Интернет-среде Особенности Интернет-общения

Формы общения в Интернет-среде. Особенности Интернет-общения. Информационная культура. Сетевой этикет.

Слушатели должны знать:
- основные формы и виды Интернет-общения;
- правила информационной культуры;
- правила сетевого этикета.

Слушатели должны уметь:
- применять правила сетевого этикета;
- составлять электронные письма в соответствии с правилами информационной культуры.

Девиантное поведение в сфере ИКТ

Девиантное поведение в сфере ИКТ. Виды девиантного поведения в сфере ИКТ: скрипт - кидди, киберхулиганство, диффамация в киберпространстве, кибертерроризм, компьютерное преступление, кибербуллинг, интернет-зависимость, геймерство, хакерство. Способы диагностики девиантного поведения у подростков. Рекомендации по профилактике девиантного поведения у подростков.

Слушатели должны знать:
- основные виды девиантного поведения в сфере ИКТ;
- способы диагностики девиантного поведения.

Слушатели должны уметь:
- распознавать признаки интернет-зависимости, геймерства и т.п. у подростков;

Защита персональных данных. Размещение информации на сайте организации

Федеральный закон №152-ФЗ «О персональных данных». Защита персональных данных обучающихся. Информация, запрещенная к размещению на официальном сайте ОУ. Публикация персональных данных педагогов на сайте ОУ. Размещение фотографий с мероприятий на официальном сайте ОУ.

Слушатели должны знать:
- основные положения Федерального закона №152-ФЗ «О персональных данных»
- требования к информации, размещаемой на официальном сайте ОУ согласно ФЗ «О персональных данных».

Слушатели должны уметь:

- отбирать информацию для размещения на официальном сайте ОУ.

Материально-техническое оснащение: мультимедийные аудитории, тренинговая аудитория, компьютерный класс, бумага, флипчарт; техническое оборудование, способствующее лучшему теоретическому и практическому усвоению программного материала: подъёмник для перемещения кресел-колясок инвалидов, кресло-коляска для инвалидов; знаки доступности, предупреждающие знаки, тактильные пиктограммы в соответствии с СП 59.13330.2012; трость для инвалидов по зрению, затемняющая маска.

Образовательные технологии, активные формы и методы ведения занятий:
методы проблемного обучения, групповые дискуссии, IT-методы, обучение на основе опыта, решение ситуационных задач, кейсы.

Кадровое обеспечение: реализация программы обеспечивается профессорскопреподавательским составом кафедры «Теории и методики профессионального образования», а также ведущих специалистов и практиков в сфере ИКТ.

Список литературы

а) основная литература

1. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. Москва, 2018.
2. Гафнер В.В. Информационная безопасность: Учебное пособие. Ростов-на-Дону, 2010.
3. Громо, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. Старый. Оскол, 2010.
4. Партык, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. Москва, 2018.
5. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. Москва, 2018.

б) дополнительная литература

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. Москва, 2019.
2. Ефимов, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография. / Л.Л. Ефимова, С.А. Кочерга. Москва, 2015.
3. Конотопов М.В. Информационная безопасность. Лабораторный практикум. Москва, 2013.
4. Кузнецов А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. Москва, 2017.
5. Мельников Д.А. Информационная безопасность открытых систем: учебник. Москва, 2013.
6. Петров С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. Москва, 2012.
7. Семененко В.А. Информационная безопасность / В.А. Семененко. Москва, 2011.

8. Чернопятов А. Наука, образование и практика: профессионально-общественная аккредитация, тьюторство, информационные технологии, информационная безопасность. Москва, 2013.
9. Ярочкин В.И. Информационная безопасность: Учебник для вузов. Москва, 2008.

ФОРМЫ АТТЕСТАЦИИ

К итоговой аттестации допускаются слушатели, освоившие дополнительную профессиональную программу в полном объеме.

Форма итоговой аттестации - зачет (тестирование).

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Перечень вопросов к итоговой аттестации

Итоговая аттестация предполагает зачет в форме тестирования.

Оценка "зачет" - выставляется слушателям, верно ответившим более 60% вопросов.

Список примерных тем итогового теста:

1. Безопасность в Интернете;
2. Защита персональных данных;
3. Информационная безопасность человека;
4. Безопасная работа с ПК;
5. Как предотвратить кибербуллинг?
6. Интернет-зависимость - реальность нашего времени;
7. Что такое сетевой этикет?
8. Как не стать жертвой компьютерного преступника;
9. Личная безопасность в социальных сетях;
10. Вредоносное ПО. Как предотвратить заражение компьютера?
11. Синий кит. Что это и как от него защититься?
12. Информационная безопасность в школе. Как организовать?
13. Профилактика интернет-зависимости у детей.
14. Профилактика компьютерной зависимости у детей.
15. Формирование сетевой культуры в коллективе.