МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное научное учреждение
«Институт стратегии развития образования»

«УТВЕРЖДАЮ»
Заместитель директора
_____ /И.В. Ускова/
«_4_» _мая_ 2024 г.

Дополнительная профессиональная программа

(повышение квалификации)

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ: ПРАВИЛА ЦИФРОВОГО ПОВЕДЕНИЯ В ПОВСЕДНЕВНОЙ ЖИЗНИ

Авторы:
Федорова Ю.В., к.п.н., доцент
Рудаков Д.П., к. воен. н., доцент
Тохтуева С.Ю.

Москва – 2024

Раздел 1. Характеристика программы

1.1. Цель реализации программы: совершенствование профессиональных компетенций слушателей в области обеспечения безопасности в информационном пространстве при изучении учебного предмета «Основы безопасности и защиты Родины».

1.2. Планируемые результаты обучения:

Трудовая функция (Профессиональный стандарт «Педагог»)	**Трудовое действие**	**Знать**	**Уметь**
Общепедагогическая функция. Обучение (Профстандарт: 01.001 Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель))	Осуществление профессиональной деятельности в соответствии с требованиями федеральных государственных образовательных стандартов основного общего, среднего общего образования	Область обновления содержания по тематике «Безопасность в информационном пространстве» учебного предмета «Основы безопасности и защиты Родины»	Применять знания в области обеспечения безопасности в информационном пространстве для организации работы обучающихся на уроках с учетом обновленного содержания учебного предмета «Основы безопасности и защиты Родины»

1.3. Категория слушателей: учителя учебного предмета «Основы безопасности и защиты Родины»

1.4. Форма обучения: очно-заочная, с применением электронного обучения, дистанционных образовательных технологий.

1.5. Срок освоения программы: 16 ч.

Раздел 2. Содержание программы

2.1. Учебный (тематический) план

№ п/п	Наименование разделов (модулей) и тем	Всего часов	Виды учебных занятий, учебных работ		Формы контроля
			Лекции, час	Самостоятельная работа	
1	Общие принципы безопасности в цифровой среде	4	2	2	Тест № 1 Кейс № 1
2	Защита от вредоносного программного обеспечения	4	2	2	Тест № 2 Кейс № 2
3	Защита от опасного контента	4	2	2	Тест № 3 Кейс № 3
4	Деструктивные течения в Интернете и защита от них Защита прав в цифровом пространстве	4	2	2	Тест № 4 Кейс № 4
	Итоговая аттестация				Зачет
	Всего:	**16**	**8**	**8**	

2.2. Рабочая программа (содержание)

Теоретические основы и практические аспекты безопасности на уровне личности, общества и государства

2.2.1. Общие принципы безопасности в цифровой среде (лекция – 2 ч., самостоятельная работа – 2 ч.)

Лекция. Содержание и особенности преподавания Модуля 10 «Безопасность в информационном пространстве» Федеральной рабочей программы основного общего образования «Основы безопасности и защиты Родины» и Федеральной рабочей программы среднего общего образования «Основы безопасности и защиты Родины» в 5-9 классах и 10-11 классах.

Человек и цифровая среда, их взаимосвязь и новые возможности. Опасности и риски цифровой среды, ее положительные возможности. «Цифровая зависимость», ее признаки и последствия. Общие принципы безопасного поведения, необходимые для предупреждения возникновения опасных ситуаций в личном цифровом пространстве.

Самостоятельная работа. Изучение образовательных материалов по теме. Выполнение заданий текущего контроля (Тест № 1, Кейс № 1).

2.2.2. Защита от вредоносного программного обеспечения (лекция – 2 ч., самостоятельная работа – 2 ч.)

Лекция: Опасные явления цифровой среды: виды вредоносного программного обеспечения, его цели, принципы работы. Правила кибергигиены, необходимые для предупреждения возникновения опасных ситуаций в цифровой среде. Причины кражи персональных данных, паролей. Мошенничество и фишинг, приемы защиты от мошенников.

Самостоятельная работа. Изучение образовательных материалов по теме. Выполнение заданий текущего контроля (Тест № 2, Кейс № 2).

2.2.3. Защита от опасного контента (лекция – 2 ч., самостоятельная работа – 2 ч.).

Лекция: Основные виды опасного и запрещённого контента в Интернете и его признаки, приёмы распознавания опасностей при использовании Интернета. Поведенческие опасности в цифровой среде и их причины. Неосмотрительное поведение и коммуникация в Интернете как угроза для будущей жизни и карьеры. Достоверность информации в цифровой среде, проверка ее на достоверность. «Информационный пузырь», манипуляция сознанием, пропаганда. Понятие «фейк», цели и виды, распространение фейков. Правила и инструменты для распознавания фейковых текстов и изображений.

Самостоятельная работа: Изучение образовательных материалов по теме. Выполнение заданий текущего контроля (Тест № 3, Кейс № 3).

2.2.4. Деструктивные течения в Интернете и защита от них. Защита прав в цифровом пространстве (лекция – 2 ч., самостоятельная работа – 2 ч.).

Лекция: Противоправные действия в Интернете: кибербуллинг, вовлечение в деструктивные сообщества. Правила коммуникации и цифрового поведения, необходимых для защиты от кибербуллинга. Деструктивные сообщества и деструктивный контент в цифровой среде, их признаки. Механизмы вовлечения в деструктивные сообщества. Правила безопасного использования Интернета по предотвращению рисков и угроз вовлечения в различную деструктивную деятельность. Права человека в цифровой среде, их защита. Ответственность за действия в Интернете.

Самостоятельная работа: Изучение образовательных материалов по теме. Выполнение заданий текущего контроля (Тест № 4, Кейс № 4).

Раздел 3. Формы аттестации и оценочные материалы

3.1. Промежуточная аттестация

3.1.1. Тест с автоматической проверкой по теме: «Общие принципы безопасности в цифровой среде»

Описание и требования к выполнению: тест состоит из 5 заданий с выбором одного или нескольких правильных ответов.

Критерии оценивания: тест считается пройденным, если правильно выполнено не менее 60% заданий (3 вопроса).

Количество попыток: не ограничено.

Примеры заданий:

Вопрос. Укажите принципы безопасного поведения в цифровой среде.

Варианты ответов:

1. Использование однофакторной аутентификации.

2. Регулярное выполнение резервного копирования.

3. Запрет на частое обновление операционной системы.

4. Использование в пароле не менее 12 символов.

5. Удаление неиспользуемых учетных данных.

3.1.2. Тест с автоматической проверкой по теме: «Защита от вредоносного программного обеспечения».

Описание и требования к выполнению: тест состоит из 5 заданий с выбором одного или нескольких правильных ответов.

Критерии оценивания: тест считается пройденным, если правильно выполнено не менее 60% заданий (3 вопроса).

Количество попыток: не ограничено.

Примеры заданий:

Вопрос. Укажите приемы защиты от вредоносного программного обеспечения.

Варианты ответов:

1. Проверить права установленных приложений.

2. Избегать подписки на пуш-уведомления сайтов в браузерах.

3. Установка ручного запуска антивирусной программы.

4. Как можно чаще использовать аккаунт с правами администратора.

5. Использовать приложение для определения подозрительных сайтов.

3.1.3. Тест с автоматической проверкой по теме: «Защита от опасного контента».

Описание и требования к выполнению: тест состоит из 5 заданий с выбором одного или нескольких правильных ответов.

Критерии оценивания: тест считается пройденным, если правильно выполнено не менее 60% заданий (3 вопроса).

Количество попыток: не ограничено.

Примеры заданий:

Вопрос. Оцените верность утверждений.

А. «Информационный пузырь» представляет собой область цифрового пространства, где пользователю доступна та информация, которая соответствует его запросам.

Б. Один из приемов выхода из «информационного пузыря» - удаление неудобных оппонентов.

В. «Информационный пузырь» ограничивает цифровые возможности пользователя по поиску и анализу информации.

Варианты ответов:

1. Верно А и Б.

2. Верно А и В.

3. Верно Б и В.

4. Верно А, Б и В.

3.1.4 Тест с автоматической проверкой по теме: «Деструктивные течения в Интернете и защита от них Защита прав в цифровом пространстве».

Описание и требования к выполнению: тест состоит из 5 заданий с выбором одного или нескольких правильных ответов.

Критерии оценивания: тест считается пройденным, если правильно выполнено не менее 60% заданий (3 вопроса).

Количество попыток: не ограничено.

Примеры заданий:

Вопрос. К правовым методам, обеспечивающим информационную безопасность, относятся:

Варианты ответов:

1. Разработка аппаратных средств обеспечения правовых данных.

2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий.

3. Разработка и конкретизация нормативных правовых актов по обеспечению безопасности.

4. Размещение в сети Интернет нормативной правовой базы в области информационной безопасности.

Кейсы № 1 - 4 направлены на формирование практических навыков решения проблемных ситуаций по изучаемым вопросам.

Критерии оценивания выполнения кейсов:

1. Полнота решения кейса;

2. Доказательность и убедительность;

3. Наличие собственных взглядов на проблему.

Оценка: зачтено/не зачтено. Оценка «зачтено» выставляется, если решение кейса соответствует критериям оценивания.

3.2. Итоговая аттестация

По совокупности выполненных на положительную оценку тестов № 1 – 4 и кейсов № 1 - 4

Оценка: зачтено/ не зачтено

Раздел 4. Организационно-педагогические условия реализации программы

4.1. Организационно-методическое и информационное обеспечение программы

Нормативные документы

1. Конституция Российской Федерации, URL: http://pravo.gov.ru/proxy/ips/?searchres=&bpas=cd00000&intelsearch=%EA%EE%ED%F1%F2%E8%F2%F3%F6%E8%FF&sort=-1 (дата обращения: 03. июня 2024 г.).

2. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», URL: http://www.kremlin.ru/acts/bank/36698 (дата обращения: 03 июня 2024 г.).

3. Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 02 июля 2021 г. № 400, URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 03. июня 2024 г.).

4. Указ Президента Российской Федерации от 09 ноября 2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей», URL: http://www.kremlin.ru/acts/bank/48502 (дата обращения: 03. июня 2024 г.).

5. Профессиональный стандарт «Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель)», приложение к приказу Минтруда Российской Федерации от 18.10.2013 № 544н, URL: https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/index.php?ELEMENT_ID=56367 (дата обращения: 03 июня 2024 г.).

6. Паспорт национального проекта «Образование». Утверждён президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам (протокол от 24 декабря 2018 г. № 16) // Правительство России: офиц.сайт. — URL: http://government.ru/info/35566/ (дата обращения: 03 июня 2024 г.).

7. Приказ Министерства просвещения Российской Федерации от 01 февраля 2024г. № 67 «О внесении изменений в некоторые приказы Министерства просвещения Российской Федерации, касающиеся федеральных адаптированных образовательных программ». URL: http://publication.pravo.gov.ru/document/0001202402290002?index=2 (дата обращения: 03 июня 2024 г.).

Литература

1. Федеральная рабочая программа основного общего образования «Основы безопасности и защиты Родины» (для 5-9 классов образовательных организаций), 2024 г. URL: https://edsoo.ru/wp-content/uploads/2024/03/frp-obzr_10-11_22032024.pdf (дата обращения 03 июня 2024 г.).

2. Федеральная рабочая программа среднего общего образования «Основы безопасности и защиты Родины» (для 10-11 классов образовательных организаций), 2024 г. URL: https://edsoo.ru/wp-content/uploads/2024/03/frp-obzr_5-9_26032024.pdf (дата обращения 03 июня 2024 г.).

3. Основы безопасности жизнедеятельности. 8 – 9 классы В 2-х частях. Под редакцией Ю.С. Шойгу, URL: https://prosv.ru/product/osnovi-bezopasnosti-zhiznedeyatel-nosti-8-9-klassi-v-2-ch-chast-1-uchebnik01/ (дата обращения 03 июня 2024 г.).

4. Рудаков Д.П. Основы безопасности жизнедеятельности. Методическое пособие для учителя к учебнику под научной редакцией Ю.С. Шойгу «Основы безопасности жизнедеятельности. 8-9 классы. В двух частях» / Д.П. Рудаков. — 2-е изд., перераб. — Москва: Просвещение, 2023 — 144 с.

5. Основы безопасности жизнедеятельности. 10-11 классы. Базовый уровень: учебник / С.В. Ким, В.А. Горский. — 5-е изд. стер., — Москва: Просвещение, 2022 — 396 с.

6. Основы безопасности жизнедеятельности. 8-9 классы: учебник / Н.Ф. Виноградова, Д.В. Смирнов, Л.В. Сидоренко и др. — 4-е изд. стер., — Москва: Просвещение, 2022 — 271 с.

Электронные учебные материалы

Информационно-образовательная среда:

4.2. Материально-технические условия реализации программы

Технические средства обучения

1. Компьютер у каждого обучающегося.

2. Доступ обучающихся к информационно-телекоммуникационной сети Интернет.

5. Учебные материалы, размещенные в цифровой среде образовательной организации.

Видеозаписи занятий и все учебные материалы размещаются в информационной среде курса.