

Ханты-Мансийский автономный округ – Югра

**Автономное учреждение дополнительного профессионального
образования Ханты-Мансийского автономного округа - Югры
«Институт развития образования»**

Дополнительная профессиональная программа (повышение квалификации)

**Обеспечение информационной безопасности обучающихся: технологические и
социальные особенности**

Разработчик(и) программы:

Зайцева О.С., канд. пед. наук, доцент, АУ «Институт развития образования»



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

СЕРТИФИКАТ

20813F7E714B1AD0C8D511ABFAD0CBE5

ВЛАДЕЛЕЦ ДИРЕКТОР

АУ «ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ»

КЛЮСОВА ВИКТОРИЯ ВИКТОРОВНА

ДЕЙСТВИТЕЛЕН С 03.05.2023 ПО 26.07.2024

Ханты-Мансийск, 2024

Раздел 1. Характеристика программы

1.1. Цель реализации программы – совершенствование профессиональной компетенции слушателей в области обеспечения информационной безопасности обучающихся.

1.2. Планируемые результаты обучения:

Учитель

Трудовая функция	Трудовое действие	Знать	Уметь
Воспитательная деятельность (Профстандарт: 01.001 Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель))	Регулирование поведения обучающихся для обеспечения безопасной образовательной среды	1. Действующие нормативные документы в области информационной безопасности детей. 2. Основные информационные угрозы. 3. Основные механизмы защиты детей от информационных угроз.	1. Применять механизмы выявления и защиты детей от основных социальных угроз. 2. Применять механизмы выявления и защиты детей от возникающих угроз при работе с персональными устройствами. 3. Применять механизмы выявления и защиты детей от фишинга; угроз, связанных с кибербуллингом. 4. Применять механизмы выявления и защиты детей от угроз, связанных с экстремизмом, группами смерти и группами, запрещёнными на территории РФ.

1.3. Категория слушателей: учителя, реализующие программы начального общего, основного общего и среднего общего образования.

1.4. Форма обучения - Очно-заочная

1.5. Срок освоения программы: 36 часов.

Раздел 2. Содержание программы

Инвариантный модуль

№ п/п	Наименование разделов(модулей) и тем	Всего часов	Виды учебных занятий, учебных работ		Самостоятельная работа, час	Формы контроля
			Лекция, час	Интерактивное (практическое) занятие, час		
	Входное тестирование	1	0	0	1	Тест
1	Модуль 1. Нормативно- правовые основы и технологические особенности информационной безопасности детей	12	3	3	6	
1.1	Нормативно- правовое обеспечение информационной безопасности детей	2	0	0	2	
1.2	Информационная безопасность детей	3	2	0	1	
1.3	Технологические аспекты информационной безопасности детей	6	1	3	2	
1.4	Промежуточная аттестация	1	0	0	1	Тест
2	Модуль 2. Социальные особенности информационной безопасности обучающихся	21	4	8	9	
2.1	Техно- психологические угрозы сети Интернет	7	1	3	3	
2.2	Социально- технологические угрозы сети Интернет	7	2	2	3	
2.3	Социально- психологические угрозы сети Интернет	6	1	3	2	

2.4	Промежуточная аттестация	1	0	0	1	Тест
3	Итоговая аттестация	2	0	0	2	Тест
	Итого	36	7	11	18	

2.2. Рабочая программа

Инвариантный модуль

Входное тестирование (самостоятельная работа – 1 ч.)

Самостоятельная работа. Определение стартовых условий запуска программы.

Модуль 1. Нормативно-правовые основы и технологические особенности информационной безопасности детей

1.1. Нормативно-правовое обеспечение информационной безопасности детей

(самостоятельная работа – 2 ч.)

Самостоятельная работа. Проанализировать законодательные и нормативные акты Российской Федерации в области информационной безопасности. Изучить нормативно-правовые документы, регламентирующие деятельность по обеспечению информационной безопасности детей в Интернет.

1.2. Информационная безопасность детей (лекция – 2 ч., самостоятельная работа – 1 ч.)

Лекция. Методы защиты информации при проведении учебных занятий. Анализ сайтов с целью безопасного использования в учебной и воспитательной деятельности. Подходы создания безопасной учетной записи ребенка в системе. Организация безопасного поиска в сети Интернет. Специальное программное обеспечение для обеспечения безопасности детей: «Интернет Цензор», «Time Boss», «KinderGate» др. Сетевая гигиена.

Самостоятельная работа. Проанализировать формы, методы и содержание профилактической работы с ребенком по защите от вредной информации.

1.3. Технологические особенности информационной безопасности детей (лекция – 1 ч., практическое занятие – 3 ч., самостоятельная работа – 2 ч.)

Лекция. Вредоносное программное обеспечение (ПО): виды, механизмы работы, назначение. Спам и навязчивая реклама как разновидность вредоносного ПО. Квалифицированные хакерские атаки. Безопасность детей при использовании мобильных устройств.

Практическое занятие. Определение мер противодействия распространённым ошибкам, создающим уязвимости для кибератак.

Самостоятельная работа. Изучить нормативные документы, определяющие ответственность за нарушение правил сбора, хранения, использования и удаления охраняемой законом информации.

Промежуточный контроль (самостоятельная работа – 1 ч.)

Самостоятельная работа. Тестирование.

Модуль 2. Социальные особенности информационной безопасности обучающихся

2.1. Техно-психологические угрозы сети Интернет (лекция – 1 ч., практическое занятие – 3 ч., самостоятельная работа – 3 ч.)

Лекция. Анализ принципов и механизмов вовлечения несовершеннолетних в компьютерные игры и азартные онлайн-игры. Игровая зависимость и зависимость от азартных онлайн-игр. Виды и типы фишинга.

Практическое занятие. Определение безопасного ресурса среди представленных фишинговых электронных писем и сайтов.

Самостоятельная работа. Проанализировать методы психологического манипулирования и технологическое обеспечение мошенничества.

2.2. Социально-технологические угрозы сети Интернет (лекция – 2 ч., практическое занятие – 2 ч., самостоятельная работа – 3 ч.)

Лекция. Принципы функционирования и угрозы криптосетей. Методы и инструменты вовлечения детей в опасные сообщества. Криптовалюта как феномен теневого рынка. Анализ предложенных ситуаций и выявление признаков Интернет-угроз. Кибербуллинг.

Практическое занятие. Формирование собственных сценариев противодействия возникшему кибербуллингу с позиций ключевых социальных ролей участников.

Самостоятельная работа. Проанализировать технологии, методики и инструментов предотвращения информационных угроз.

2.3. Социально-психологические угрозы сети Интернет (лекция – 1 ч., практическое занятие – 3 ч., самостоятельная работа – 2 ч.)

Лекция. Экстремизм и хулиганство. Наличие идеологической или религиозной подоплеки. Признаки вовлечения школьника в экстремистское сообщество. Ответственность. Религиозные и политические радикальные группы

Практическое занятие. Разработка алгоритма корректного и эффективного реагирования на угрозу, сопровождение ситуации педагогическим коллективом, взаимодействие с правоохранительными структурами. Выявление признаков вовлечения ребенка в экстремистские группы по комплексу признаков на его странице в социальной сети.

Самостоятельная работа. На основе анализа специальной литературы выделить признаки и особенности деструктивных группы.

Промежуточный контроль (самостоятельная работа – 1 ч.)

Самостоятельная работа. Тестирование.

Итоговая аттестация (самостоятельная работа – 2 ч.)

Самостоятельная работа. Тестирование.

Раздел 3. Формы аттестации и оценочные материалы

Входной контроль

Форма: тестирование

Описание, требования к выполнению:

Входная диагностика проводится в форме тестирования с автоматической проверкой. Входное тестирование состоит из 8 заданий. Каждый верный ответ оценивается в 1 балл. Максимальное количество баллов – 8. Время на выполнения 1 час.

Критерии оценивания:

80 – 100% выполненных заданий – высокий уровень готовности слушателей.

60 – 70% – средний уровень готовности слушателей.

0 – 50% – недостаточные исходные (базовые) знания в области направления программы.

Примеры заданий:

Задание 1.

Инструкция. Выберите правильные ответы.

Какие приоритетные задачи устанавливает Концепция информационной безопасности детей для семьи, государства и организаций, заинтересованных в обеспечении информационной безопасности детей?

- а) Повышение уровня медиаграмотности детей.
- б) Усвоение детьми системы семейных ценностей.

- в) Формирование у детей навыков по выбору правильного образовательного профиля.
- г) Сохранение конфиденциальности документированной информации.

Задание 2.

Инструкция. Выберите правильные ответы.

Как ребенку не открыть фишинговый сайт?

- а) Не переходить по ссылкам от незнакомцев.
- б) Настроить многофакторную систему авторизации в платёжных и почтовых системах.
- в) Сохранить в избранное адреса сайтов, где часто совершаются платежи.
- г) Установить антивирусную программу и обновления операционной системы.
- д) Включить защищённый режим в браузере.

Количество попыток: 3

Промежуточный контроль

Раздел программы. Модуль 1. Нормативно-правовые основы и технологические особенности информационной безопасности детей

Форма: Тестирование.

Описание, требования к выполнению:

10 заданий. Время выполнения 1 час.

Критерии оценивания:

60% выполненных заданий и выше – оценка «зачтено» (слушатель освоил содержание темы программы). Менее 60% выполненных заданий – оценка «не зачтено» (результат недостаточен, рекомендовано повторное прохождение темы).

Примеры заданий:

Задание 1.

Инструкция. Выберите один правильный ответ.

Что нужно сделать для обеспечения защиты школьников от всех технологических угроз сети Интернет?

- а) Установить на все устройства комплексные системы защиты с антивирусом, спам-фильтром, сканером трафика, брандмауэром и выставить все установки в режим максимально возможной защиты.
- б) Достаточно поставить антивирус и соблюдать правила цифровой гигиены.
- в) Единственный способ защититься от всех угроз сети Интернет – никогда не подключаться к сети Интернет. Других гарантированных способов не существует.
- г) Выходить в Интернет только из внутренней корпоративной сети.

Задание 2.

Инструкция. Выберите один правильный ответ.

Произошла утечка персональных данных: в Интернет попала база с фамилиями и номерами телефонов учащихся. В течение дня ученики получают оскорбительные сообщения и ссылку на «архив с твоими грязными фотографиями». Каковы правильные действия учителя в этой ситуации?

- а) Самостоятельно проверить архив с фотографиями на предмет опасного для детей и \ или запрещенного контента, обратиться в полицию.
- б) Издать приказ по учебному заведению с запретом переходить по ссылке из сообщения.

- в) Написать в Роскомнадзор с требованием провести проверку информации, размещенной по ссылке и заблокировать ресурс в случае выявления нарушений.
- г) Провести классный час на тему «Азбука защиты от фишинга в сети Интернет», рассказать, что чрезвычайно опасно переходить по ссылкам из непрошенных писем.

Количество попыток: 3

Раздел программы. Модуль 2. Социальные особенности информационной безопасности обучающихся

Форма: Тестирование.

Описание, требования к выполнению:

10 заданий. Время выполнения 1 час.

Критерии оценивания:

60% выполненных заданий и выше – оценка «зачтено» (слушатель освоил содержание темы программы). Менее 60% выполненных заданий – оценка «не зачтено» (результат недостаточен, рекомендовано повторное прохождение темы).

Примеры заданий:

Задание 1.

Инструкция. Выберите один правильный ответ.

Какие рекомендации по информационной безопасности руководитель может дать родителям (законным представителям) детей 9-12 лет?

- а) Регулярно разговаривать с ребенком о том, что происходит в его «онлайн-жизни».
- б) Установить систему «Родительского контроля» на устройствах, с которых ребенок будет выходить в Интернет.
- в) Установить программу-шпион на устройствах ребенка для скрытого наблюдения за его действиями в Интернет.
- г) Запретите ребенку иметь аккаунты в социальных сетях.

Задание 2.

Инструкция. Выберите один правильный ответ.

В ответ на какое увлечение учеников в классе педагогу следует отреагировать настороженно и провести мониторинг социальных сетей с целью выяснить, нет ли среди учащихся класса тех, кто увлечен сообществами по теме «Колумбайн»?

- а) Предпочтение в одежде длинных темных плащей.
- б) Предпочтение одежды с символикой акул и касаток.
- в) Появление значков Columbian.
- г) Предпочтение играть в онлайн-игре PUBG на стороне террористов.

Количество попыток: 3

Итоговая аттестация

Форма: Тестирование.

Описание, требования к выполнению:

10 заданий. Время выполнения 2 час.

Критерии оценивания:

60% выполненных заданий и выше – оценка «зачтено» (слушатель освоил содержание темы программы). Менее 60% выполненных заданий – оценка «не зачтено» (результат недостаточен, рекомендовано повторное прохождение темы).

Примеры заданий:

Задание 1.

Инструкция. Выберите один правильный ответ.

Родители одного из учеников сообщают, что готовы написать заявление в полицию на другого ученика, который вымогает у их сына деньги «на общак» и совершает мелкие кражи. Какое действие педагога будет наиболее эффективным?

- а) Воспитательная беседа с учеником в присутствии его родителей.
- б) Организация контакта социального педагога с семьей учащегося в связи с вероятностью вовлечения ребенка в криминальное сообщество, а также информирование директора школы о необходимости обратиться в полицию в связи с субкультурно-обусловленным преступлением.
- в) Классный час на тему «Блатная жизнь: мифы и реальность» с участием представителя ФСИН.
- г) Самостоятельное обращение в полицию для постановки ученика на учет.

Задание 2.

Инструкция. Выберите один правильный ответ.

Какой признак с огромной вероятностью свидетельствует о том, что ребенок покупает наркотики в сети Darknet?

- а) Использует символику растафарианства, выступает за легализацию марихуаны, слушает раста-рэпы с текстами про марихуану.
- б) У него в пенале были найдены неизвестные таблетки, которые оказались сильными антидепрессантами.
- в) Из его кармана выпал маленький предмет, похожий на комок изоленты, который он очень быстро поднял и спрятал обратно.
- г) На его руке браслет из большого количества маленьких разноразмерных магнитов.

Количество попыток: 3

Раздел 4. Организационно-педагогические условия реализации программы

4.1. Организационно-методическое и информационное обеспечение программы.

Нормативные документы

1. Концепция информационной безопасности детей, утвержденной распоряжением Правительства РФ от 02.12.2015 N 2471. (дата обращения 21.09.2021).
2. Постановление Главного государственного санитарного врача Российской Федерации от 28.09.2020 № 28 «Об утверждении санитарных правил СП 2.4. 3648-20 «Санитарноэпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи».
3. Профессиональный стандарт «Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель)», приложение к приказу Минтруда РФ № 544н от 18.10.2013г.
4. Указ Президента Российской Федерации от 21 июля 2020 года г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года» //
5. Распоряжение Правительства РФ от 29.05.2015 г. № 996 – р «Стратегия развития воспитания в Российской Федерации до 2025 года».
6. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 01.01.2024)

7. Федеральный закон от 29.12.2010 N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
8. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Федеральный государственный образовательный стандарт начального общего образования (утв. приказом Министерства образования и науки РФ от 31 мая 2021 г. № 286).
10. Федеральный государственный образовательный стандарт основного общего образования (утв. приказом Министерства образования и науки РФ от 31 мая 2021 г. № 287).

Литература

1. Информационная безопасность : учебное пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. Н. Лаптев. – Краснодар : КубГАУ, 2020. – 332 с.
2. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. – Москва : РТУ МИРЭА, 2021. – 79 с.
3. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие для СПО / С. Н. Никифоров. – Санкт-Петербург : Лань, 2021. – 96 с.
4. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие для СПО / С. Н. Никифоров. – Санкт-Петербург : Лань, 2021. – 124 с.
5. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. – Санкт-Петербург : Лань, 2024. – 124 с.

Электронные обучающие материалы

Электронные учебные материалы на платформе Moodle: <https://do.iro86.ru/>

Интернет-ресурсы

6. Единое содержание общего образования [сайт]. – <https://edsoo.ru>
7. КонсультантПлюс [сайт]. – <http://consultant.ru>
8. Министерство Просвещения РФ [сайт]. – <https://edu.gov.ru/>
9. Российская электронная школа [сайт]. – <https://resh.edu.ru/>
10. Яндекс учебник [сайт]. – <https://education.yandex.ru/>

4.2. Материально-технические условия реализации программы

Технические средства обучения

Для реализации программы необходимо компьютерное и мультимедийное оборудование для использования аудиовизуальных средств обучения с подключением к сети Интернет, пакет слайдовых презентаций (по темам учебной программы).

Функционирующий сайт с разработанным специализированным разделом, на базе которого реализуется обучение с использованием дистанционных образовательных технологий. В специализированном разделе Интернет-портала размещаются лекционные материалы, материалы самостоятельных и практических работ, макеты, алгоритмы, оценочные материалы согласно разработанной программе повышения квалификации.

Аннотация
к дополнительной профессиональной программе
(повышение квалификации)

Обеспечение информационной безопасности обучающихся: технологические и социальные особенности

Образовательная программа повышения квалификации «Обеспечение информационной безопасности обучающихся: технологические и социальные особенности» (далее – Программа) разработана для учителей, реализующих программы начального общего, основного общего и среднего общего образования; педагогов дополнительного образования, осуществляющих обучение по дополнительным общеобразовательным программам. Программа направлена на совершенствование профессиональных компетенций слушателей по вопросам совершенствование профессиональной компетенции слушателей в области обеспечения информационной безопасности обучающихся.

Данная программа повышения квалификации построена на основе модульного принципа. Программа состоит из 2-х модулей. Все модули программы предусматривают совершенствование профессиональных, общепрофессиональных, общекультурных компетенций учителя, способствующих активизации образовательной деятельности обучающихся.

Первый модуль программы «Нормативно-правовые основы и технологические особенности информационной безопасности детей» предусматривает изучение следующих вопросов: нормативно-правовое обеспечение информационной безопасности детей; информационная безопасность детей; технологические аспекты информационной безопасности детей.

Второй модуль программы «Социальные особенности информационной безопасности обучающихся» предусматривает изучение следующих вопросов: техно-психологические угрозы сети Интернет; Социально-технологические угрозы сети Интернет; Социально-психологические угрозы сети Интернет.

В целях обеспечения персонализации обучения и контроля достижения планируемых результатов обучения в программе предусмотрен входной контроль владения профессиональными компетенциями, на совершенствование которых нацелена дополнительная профессиональная программа. После каждого модуля предусмотрен промежуточный контроль. Итоговая аттестация в форме тестирования позволяет определить эффективность работы слушателя программы.

Программа курса повышения квалификации педагогов, ориентированная на механизмы выявления и защиты детей от информационных угроз, является ***своевременной и актуальной***.

Программа утверждена на заседании Ученого совета АУ «Институт развития образования», протокол № 02 от «21» марта 2024 г.

**Календарный учебный график
к дополнительной профессиональной программе
(повышение квалификации)**

**Обеспечение информационной безопасности обучающихся: технологические и
социальные особенности**

Календарный месяц, в котором проводится обучение по программе	Срок проведения обучения по программе
март – ноябрь (по мере комплектования групп)	Срок освоения программы: 36 часа в течение 9 дней

Примечание:

Календарным учебным графиком является расписание учебных занятий, которое составляется и утверждается для каждой учебной группы