

Ханты-Мансийский автономный округ – Югра

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



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

СЕРТИФИКАТ

00A149B935DEB390813D33F26DAD2317F1

ВЛАДЕЛЕЦ ДИРЕКТОР

АУ «ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ»

КЛЮСОВА ВИКТОРИЯ ВИКТОРОВНА

ДЕЙСТВИТЕЛЕН С 14.02.2022 ПО 10.05.2023

Дополнительная профессиональная программа (повышение квалификации)

Роль педагога в обеспечении информационной безопасности обучающихся в сети интернет

Разработчик(и) программы:

**Маковчик Д.Н., старший преподаватель кафедры естественнонаучных и математических
дисциплин, АУ «Институт развития образования»**

Ханты-Мансийск, 2022

Раздел 1. Характеристика программы

1.1. Цель реализации программы – совершенствование профессиональных компетенций слушателей по вопросам, связанным с информационной безопасностью школьников.

1.2. Планируемые результаты обучения:

Учитель

Трудовая функция	Трудовое действие	Знать	Уметь
Общепедагогическая функция. Обучение	Планирование и проведение учебных занятий. Формирование навыков, связанных с информационно-коммуникационными технологиями	1. Психологические основы здоровьесберегающих технологий; 2. нормативно-правовые и организационные основы деятельности образовательных организаций; 3. риски и угрозы при решении практических задач получения, хранения, обработки и передачи информации; классификации информационных угроз; программы для обеспечения информационной безопасности школьников в сети Интернет в условиях Открытого информационного пространства; 4. способы обеспечения информационной безопасности школьников в сети Интернет в условиях Открытого информационного пространства; 5. способы обеспечения информационной безопасности школьников в сети Интернет в условиях открытого информационного пространства;	1. регулировать поведение обучающихся при помощи здоровьесберегающих технологий; 2. свободно применять основополагающие понятия и категории образовательного права в практической деятельности; использовать нормативные правовые акты в обсуждении и решении теоретических и практических вопросов; 3. использовать программные продукты для эффективного обеспечения информационной безопасности школьников в сети Интернет в условиях открытого информационного пространства; 4. использовать информационно-коммуникационные технологии в процессе обучения; 5. работать с понятийным аппаратом в области информационной безопасности

1.3. Категория слушателей: учителя образовательных организаций.

1.4. Форма обучения - Очно-заочная

1.5. Срок освоения программы: 36 часов.

Раздел 2. Содержание программы

2.1. Учебный тематический план

№ 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		
	<u>Входная диагностика</u>	1			1	Тестирование
1.	Модуль 1. Информационная безопасность школьника.	17	3	8	6	
1.1	Общий анализ проблемы и необходимость защиты детей	2	1		1	
1.2	Нормативные документы. Закон о защите детей от информации, причиняющей вред их здоровью и развитию	2	1		1	
1.3	Теоретические основы информационной безопасности школьника в учебном процессе	2		1	1	
1.4	Система педагогических условий обеспечения информационной безопасности детей и подростков в школе	1		1	0	
1.5.	Практическая реализация программы информационной безопасности школьника	1		1	0	
1.6	Профилактика терроризма и экстремизма в образовательной среде	1		1	0	
1.7.	Основные аспекты информационной безопасности	7	1	4	2	
	Промежуточный контроль	1			1	Тестирование
2	Модуль 2. Защита детей от вредной информации.	17	3	4	10	
2.1	Вирусы и средства борьбы с ними. Использование антивирусных продуктов	3	2		1	

2.2	Безопасный поиск в Интернете	2		1	1	
2.3	Безопасность ребенка в социальных сетях	2		1	1	
2.4	Специальное программное обеспечение для обеспечения безопасности детей	2	1		1	
2.5	Повышение безопасности детей при использовании мобильных устройств	2		1	1	
2.6	Обеспечение информационной безопасности детей в Интернете. Роль школы.	2		1	1	
2.7	Профилактическая работа родителей с ребенком по защите от вредной информации. Рекомендации психологов Института онлайн-безопасности семьи	3			3	
	Промежуточный контроль	1			1	Тестирование
3	Итоговая аттестация	1			1	тестирование
	Итого	36	6	12	18	

2.2. Рабочая программа

Входное тестирование (самостоятельная работа – 1 ч.)

Самостоятельная работа. Определение стартовых условий запуска программы.

Модуль 1. Информационная безопасность школьника.

Тема 1.1. Общий анализ проблемы и необходимость защиты детей (лекция – [1] ч. , самостоятельная работа - [1] ч.).

Лекция. В теме рассматривается понятие информационного общества и проблемы, возникающих у детей при работе с информацией.

Самостоятельная работа. Модель состояния информационной безопасности личности учащегося.

Тема 1.2. Нормативные документы. Закон о защите детей от информации, причиняющей вред их здоровью и развитию. (лекция – [1] ч. , самостоятельная работа - [1] ч.)

Лекция. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (ред. от 01.05.2017).

Самостоятельная работа. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (в ред. от 29.07.2017 г.). Федеральный закон от 24.07.1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» (в ред. от 28.12.2016 г.). Федеральный список экстремистских материалов с возможностью поиска.

Тема 1.3. Теоретические основы информационной безопасности школьника в учебном процессе (практическое занятие – 1 ч, самостоятельная работа - 2 ч.)

Практическая работа: Информационная безопасность в школе. Социально-педагогический аспект информационной безопасности детей и подростков в условиях школы.

Самостоятельная работа: освоить электронные учебно-методические материалы, размещенные в системе дистанционного обучения АУ ДПО ХМАО-Югры «Институт развития образования» (тема 1.3)

Тема 1.4. Система педагогических условий обеспечения информационной безопасности детей и подростков в школе. (практическое занятие - 1 ч.)

Практическая работа: Анализ современной ситуации в области информатизации образования. Концепция информационной безопасности школьников и педагогические условия ее реализации.

Организация информационно-безопасного образовательного процесса в школе, взаимосвязь с родителями школьников в решении проблемы.

Тема 1.5. Практическая реализация программы информационной безопасности школьника (практическое занятие - 1 ч.)

Практическая работа: Задачи по обеспечению информационной безопасности школьников в непрерывном общем образовании. Практические советы по безопасности для детей разного возраста.

Тема 1.6. Профилактика терроризма и экстремизма в образовательной среде (практическое занятие - 1 ч.)

Практическая работа: Ксенофобия и молодежный экстремизм. Вопросы профилактики радикализма в молодежной среде. О профилактике проявлений экстремизма среди общественных объединений, в том числе молодежных.

Тема 1.7. Основные аспекты информационной безопасности (лекция – 1 ч., практическое занятие - 4 ч., самостоятельная работа – 2 ч.)

Лекция. В теме рассматриваются основные аспекты информационной безопасности.

Практическая работа: Анализ основных аспектов информационной безопасности:

- правовая охрана программ и данных,
- защита информации,
- проблема ложной информации,
- защита Интернет,
- свобода слова и цензура в Интернет,
- качество программного обеспечения,
- надежность работы компьютера и безопасность общества и т.п.

Самостоятельная работа: изучить электронные учебно-методические материалы, размещенные в системе дистанционного обучения АУ ДПО ХМАО-Югры «Институт развития образования» (тема 1.7)

Промежуточный контроль (самостоятельная работа – 1 час.).

Определение достаточных/недостаточных знаний в области содержания первого модуля программы.

Модуль 2. Защита детей от вредной информации.

Тема 2.1. Вирусы и средства борьбы с ними. Использование антивирусных продуктов (лекция – 2 ч., самостоятельная работа - 1 ч.)

Лекция. Что такое компьютерные вирусы, современные тенденции развития угроз, технологии, используемые для борьбы с вредоносными программами и другими сетевыми угрозами.

Самостоятельная работа. Виды вирусов. Обзор антивирусной защиты.

Тема 2.2 Безопасный поиск в Интернете (практическое занятие – 1 ч., самостоятельная работа - 1 ч.)

Практическая работа: Функции безопасного поиска, которые предлагают поисковые системы общего назначения. Поисковые системы, предназначенных специально для детей. Веб-браузер Яндекс, который предлагает расширенные возможности по обеспечению безопасного поиска

Самостоятельная работа: изучить электронные учебно-методические материалы, размещенные в системе дистанционного обучения АУ ДПО ХМАО-Югры «Институт развития образования» (тема 2.2).

Тема 2.3. Безопасность ребенка в социальных сетях (практическое занятие – 1 ч., самостоятельная работа - 1 ч.)

Практическая работа: Как повысить безопасность ребенка, который пользуется социальными сетями. В социальных сетях присутствуют не только порядочные пользователи, но и люди, которые способны принести ребенку вред.

Самостоятельная работа: изучить электронные учебно-методические материалы, размещенные в системе дистанционного обучения АУ ДПО ХМАО-Югры «Институт развития образования» (тема 2.3)

Тема 2.4. Специальное программное обеспечение для обеспечения безопасности детей (лекция – 1 ч., самостоятельная работа - 1 ч.)

Лекция. Специализированные программы, которые обладают расширенными возможностями по контролю использования ЭВМ и сети Интернет.

Самостоятельная работа. Специализированные программы, которые обладают расширенными возможностями по контролю использования ЭВМ и сети Интернет.

Тема 2.5. Повышение безопасности детей при использовании мобильных устройств (практическое занятие – 1 ч., самостоятельная работа - 1 ч.)

Практическая работа: Услуги операторов связи, которые позволяют повысить безопасность детей при использовании мобильных телефонов для целей обычной связи и для доступа в Интернет.

Самостоятельная работа: Средства мобильных операционных систем, направленные на защиту детей.

Тема 2.6. Обеспечение информационной безопасности детей в Интернете. Роль школы. (практическое занятие – 1 ч., самостоятельная работа - 1 ч.)

Практическая работа: Обеспечение информационной безопасности детей в Интернете: российский и зарубежный опыт; Видеолекция Академии АйТи

Самостоятельная работа: изучить электронные учебно-методические материалы, размещенные в системе дистанционного обучения АУ ДПО ХМАО-Югры «Институт развития образования» (тема 2.6)

Тема 2.7. Профилактическая работа родителей с ребенком по защите от вредной информации. Рекомендации психологов Института онлайн-безопасности семьи (самостоятельная работа - 3 ч.)

Самостоятельная работа: Учет возрастных особенностей детей. рекомендации для родителей, столкнувшихся с рисками виртуальной среды. Основные рекомендации для восстановления доверия в семье.

Промежуточный контроль (самостоятельная работа – 1 час.).

Определение достаточных/недостаточных знаний в области содержания второго модуля программы.

Итоговая аттестация (самостоятельная работа - 1 ч.) Тестирование

Раздел 3. Формы аттестации и оценочные материалы

Входной контроль

Форма: тестирование

Описание, требования к выполнению: 10 заданий. Время выполнения 1 час.

Критерии оценивания: 60% и более правильных ответов – достаточные исходные (базовые) знания в области направления программы, слушатель готов к обучению по дополнительной профессиональной программе повышения квалификации. Менее 60% – недостаточные исходные (базовые) знания в области направления программы.

Примеры заданий:

1. Какой из нижеперечисленных информационных ресурсов является наиболее опасным для детей с точки зрения информации, не прошедшей предварительной фильтрации?

- а) СМИ
- б) школьная литература
- в) газеты
- г) интернет

2. Какой государственный орган ведет реестр запрещенных сайтов?

- а) Роскомстат
- б) ФСБ
- в) МВД
- г) Роскомнадзор

Количество попыток: 3

Промежуточный контроль

Раздел программы: Информационная безопасность школьника.

Форма: тестирование

Описание, требования к выполнению: 10 заданий. Время выполнения 1 час.

Критерии оценивания: 60% и более правильных ответов – достаточные исходные (базовые) знания в области направления программы, слушатель готов к обучению по дополнительной профессиональной программе повышения квалификации. Менее 60% – недостаточные исходные (базовые) знания в области направления программы.

Примеры заданий:

1. Какой закон ввел обязанность владельцев интернет-сайтов удалить интернет-страницу, на которой размещается запрещенная к распространению информация, после получения соответствующего уведомления от хостинг-провайдера?

- А) ФЗ 139
- Б) ФЗ 458
- В) ФЗ «Об образовании в Российской Федерации»
- Г) ФЗ 64
- Д) ФЗ 436

2. Что является ведущим фактором социализации в информационном обществе?

- а) семья
- б) школа
- в) референтная группа
- г) информация

Количество попыток: 3

Итоговая аттестация

По совокупности промежуточного контроля.

Раздел 4. Организационно-педагогические условия реализации программы

4.1. Организационно-методическое и информационное обеспечение программы.

Нормативные документы

1. О национальных целях развития Российской Федерации на период до 2030 года: Указ Президента Российской Федерации № 474 от 21.07.2020.
2. Об утверждении методических рекомендаций по созданию и функционированию детских технопарков «Кванториум» на базе общеобразовательных организаций / Распоряжение Минпросвещения России 12.01.2021 г., № Р-4.
3. Об утверждении методических рекомендаций по созданию и функционированию в общеобразовательных организациях, расположенных в сельской местности и малых городах, центров образования естественно-научной и технологической направленностей / Распоряжение Минпросвещения России 12.01.2021 г., № Р-6.
4. Профессиональный стандарт «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель) / Приказ Минтруда России от 18.10.2013 № 544н (Зарегистрировано в Минюсте России 06.12.2013 № 30550).
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 г. № 273-ФЗ «Об образовании в Российской Федерации».
7. Федеральный государственный образовательный стандарт основного общего образования (утв. приказом Министерства образования и науки РФ от 17 декабря 2010 г. № 1897) (с изменениями и дополнениями от 29 декабря 2014 г., 31 декабря 2015 г., 11 декабря 2020 г.).
8. Федеральный государственный образовательный стандарт среднего общего образования (утв. приказом Министерства образования и науки РФ от 17 мая 2012 г. N 413) (с изменениями и дополнениями от: 29 декабря 2014 г., 31 декабря 2015 г., 29 июня 2017 г., 24 сентября, 11 декабря 2020 г.).
9. Концепция преподавания предметной области «Технология» в образовательных организациях Российской Федерации, реализующих основные общеобразовательные программы [Электронный ресурс]. – URL: <https://docs.edu.gov.ru/document/c4d7feb359d9563f114aea8106c9a2aa/download/737>

Литература

1. 16 правил интернет-безопасности для детей, 2020 год, URL: <https://zen.yandex.ru/media/luckychild/16-pravil-internetbezopasnosti-dlia-detei-5f2488dad1bb713ff1dfda5e>
2. Денисов, Д. В. Безопасность в Интернете: защита от внешних угроз / Д.В. Денисов. - М.: Синергия, 2016. - **213** с.
3. Информационная безопасность детей. Родительское Всероссийское Сопротивление, URL: <http://r-v-s.su>
4. Новикова Н.Н. Формирование информационно-коммуникационной среды технологического образования // Концепт. Спецвыпуск № 06. [Электронный ресурс] – URL: <http://ekoncept.ru/2014/14569.htm>. (дата обращения 15.03.2018).
5. Обухович, В. В. Интернет-безопасность школьников / В. В. Обухович. — Текст : непосредственный // Педагогика высшей школы. — 2016. — № 3.1 (6.1). — С. 149-151. — URL: <https://moluch.ru/th/3/archive/43/1468/> (дата обращения: 18.01.2021).
6. Федеральная программа безопасного детского интернета «Гоголь». URL: <http://www.gogul.tv>

Яныкина А.П., Какадий И.И. Особенности современных технологий управления образованием и применение их в практической деятельности // Экономика и предпринимательство. – 2017. – № 5-1 (82-1)..

7. Савушкин, Сергей Николаевич Безопасное общение. Информация для детей и родителей / Савушкин Сергей Николаевич. - М.: Сфера, 2017..

8. Чашин, Александр Николаевич Борьба с правонарушениями в сети Интернет. Выпуск 5/2016 / Чашин Александр Николаевич. - М.: Дело и сервис (ДиС), 2016..

Электронные обучающие материалы

1. Самоучитель Python [сайт]. – URL: <https://pythonworld.ru/samouchitel-python>
2. Теоретический материал по работе с датчиками компании «Амперка» [сайт] – URL: <http://wiki.amperka.ru>

Интернет-ресурсы

1. <http://www.avp.ru> –сервер антивирусной лаборатории Евгения Касперского
2. <http://www.viruslist.com/ru/viruslist.html> Лаборатория Касперского
3. <http://www.dials.ru> - сервер антивирусной лаборатории «Лаборатория Данилова» и «ДиалогНаука».
4. <http://www.adinf.ru> - WEB-сайт разработчиков антивируса ADInf
5. <http://www.symantcc.ru> - Российское Интернет-представительство компании Symantec
6. <http://www.scrf.gov.ru/Documents/Decree/2000/09-09/html> - доктрина информационной безопасности
7. <http://www.pps.ru/bib/index.html> – библиотека информационной безопасности
8. <http://www.compulink.ru/security/?go=public> - публикации по информационной безопасности
9. <http://beda.stup.ac.ru/psf/ziss/wmaster/books/other/avpve/1CLASSI/sub.htm> ФГОС на страницах Википедии <http://ru.wikipedia.org/wiki>
10. Федеральные государственные образовательные стандарты <http://fgos.isiorao.ru/index.php>
11. Федеральный _____ государственный образовательный стандарт. <http://standart.edu.ru>
12. Федеральный институт развития образования <http://www.firo.ru>
13. Юридические словари: <http://www.systema.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).

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и/или наушниками.

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)****Роль педагога в обеспечении информационной безопасности обучающихся в сети интернет**

Образовательная программа «РОЛЬ ПЕДАГОГА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ В СЕТИ ИНТЕРНЕТ» предназначена для подготовки руководителей и заместителей руководителей образовательных организаций, методистов, педагогических работников образовательных организаций Ханты-Мансийского автономного округа – Югры с целью изучения широкого спектра вопросов, связанных с информационной безопасностью школьников.

Как учить школьников оценке электронной информации, ее адекватному восприятию и критическому осмыслению на основе нравственных и культурных ценностей. На что обращать внимание учащихся в аспектах информационной безопасности, как мотивировать на корректное поведение в сети Интернет?

Эти и другие вопросы рассматриваются в программе повышения квалификации «Роль педагога в обеспечении информационной безопасности обучающихся в сети Интернет».

Данная программа повышения квалификации построена на основе модульного принципа. Первый и второй модули программы – инвариантные, предусматривают ознакомление с современными трендами развития программного обеспечения, методическими подходами к его использованию, нормативно-правовой базой, регулирующей применение дистанционных образовательных технологий в учебном процессе, и нацелены на совершенствование заявленных общекультурных и общепрофессиональных компетенций.

В целях обеспечения индивидуализации и контроля достижения планируемых результатов обучения в программе предусмотрена входная диагностика владения профессиональными компетенциями, на совершенствование которых нацелена программа повышения квалификации.

Итоговая самодиагностика, тестирование по курсу и Итоговая аттестация позволяют определить эффективность работы слушателя программы.

Программа одобрена на заседании Ученого совета АУ «Институт развития образования», протокол № 4 от «26» апреля 2022 г.

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

**РОЛЬ ПЕДАГОГА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОБУЧАЮЩИХСЯ В СЕТИ ИНТЕРНЕТ**

Календарный месяц, в котором проводится обучение по программе	Срок проведения обучения по программе
октябрь	Срок освоения программы: 36 часов в течении 6 дней

Примечание:

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