ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ
Государственное бюджетное образовательное учреждение города Москвы дополнительного профессионального образования (повышения квалификации) специалистов Городской методический центр Департамента образования и науки города Москвы

УТВЕРЖДАЮ

Директор ГБОУ ГМЦ ДОНМ

_____ А.С. Зинин

«23» октября 2020 г.

Дополнительная профессиональная программа
(повышение квалификации)

Формирование культуры информационной безопасности как фактор обеспечения безопасного поведения школьников в сети Интернет

(16 часов)

Автор (ы) курса:
И. В. Гусенко,
Г. Р. Царева

Москва – 2020

Раздел 1. «Характеристика программы»

1.1. Цель реализации программы

Совершенствование профессиональных компетенций обучающихся в области формирования культуры информационной безопасности как фактора обеспечения безопасного поведения школьников в сети Интернет.

Совершенствуемые компетенции[1]

№ п\п	Компетенция	Направление подготовки 44.03.01 Педагогическое образование
		Код компетенции
1.	Способен осуществлять профессиональную деятельность в соответствии с нормативными и правовыми актами в сфере образования и нормами профессиональной этики.	ОПК-1
2.	Способен осуществлять педагогическую деятельность на основе специальных научных знаний.	ОПК-8

1.2. Планируемые результаты обучения

№ п\п	Знать – уметь	Направление подготовки 44.03.01 Педагогическое образование
		Код компетенции
1.	Уметь: -разрабатывать воспитательные мероприятия, направленные на формирование культуры информационной безопасности школьников с учетом нормативных и правовых актов. Знать: -нормативные и правовые акты в сфере информационной безопасности детей; -основные виды угроз глобальной сети Интернет; -современные способы противодействия основным видам угроз и рисков глобальной сети Интернет; -правила безопасного поведения в сети Интернет;	ОПК-1, ОПК-8

[1] **Из ФГОС 3 ++**

	-алгоритм разработки воспитательных мероприятий, направленных на формирование культуры информационной безопасности школьников с учетом нормативных и правовых актов.	

1.3. Категория обучающихся: уровень образования – ВО, получающие высшее образование; область профессиональной деятельности – воспитание школьников в общеобразовательных организациях.

1.4. Программа реализуется с использованием дистанционных образовательных технологий.

1.5. Режим занятий: доступ к образовательной платформе организации круглосуточно при соблюдении установленных сроков обучения.

1.6. Трудоемкость программы: 16 часов.

Раздел 2. «Содержание программы»

2.1. Учебный (тематический) план

№ п/п	Наименование разделов (модулей) и тем	Внеаудиторная работа Практическое занятие			Формы контроля
		Трудоемкость	Лекции, презентации	Практические занятия	
1.	Нормативно-правовое обеспечение информационной безопасности школьников.	**2**	**1**	**1**	Тест №1
2.	Понятие информационной безопасности. Классификация угроз информационной безопасности и современные способы противодействия угрозам в сети Интернет.	**8**	**3**	**5**	Тест №2
3.	Правила безопасного поведения школьников в сети Интернет.	**6**	**2**	**4**	Проект
	Итоговая аттестация				Зачет на основании совокупности выполненных работ и результатов тестирования.
	Итого:	**16**	**6**	**10**	

2.2. Учебная программа

№ п/п	Виды учебных занятий, учебных работ	Содержание
Тема 1. Нормативно-правовое обеспечение информационной безопасности школьников.	*Лекция - презентация – 1 час*	Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Закон «Об образовании» № 273 ФЗ от 29.12.2012 года. Распоряжение Правительства РФ от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей». Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.
	Практическое занятие – 1 час	Тест №1
Тема 2. Понятие информационной безопасности. Классификация угроз информационной безопасности и современные способы противодействия угрозам в сети Интернет.	*Лекция - презентация – 1 час*	Понятие информационной безопасности. Актуальные угрозы информационной безопасности школьников в сети Интернет: *нежелательный контент; кибермошенничество; вредоносные программы.* Современные способы защиты от угроз сети Интернет.
	Практическое занятие – 1 час	Выполнение интерактивных заданий, направленных на закрепление теоретического материала.
	Лекция - презентация – 1 час	Интернет риски для пользователей социальных сетей: *кража личной информации, кибербуллинг, секстинг, пропаганда суицида, материалы экстремистского характера.* Проблема подлинности информации. Правила поведения в киберпространстве.
	Практическое занятие – 2 часа	Подготовка к выполнению проекта. Разработка памятки в виде инфографики «Основы безопасного использования социальных сетей».
	Лекция - презентация – 1 час	Интернет зависимость, способы её выявления у обучающихся. Современные методы профилактики интернет-зависимости.
	Практическое занятие –	Изучение статистики интернет-зависимости у российских подростков, выявление

	1 час	признаков, указывающих на наличие интернет-зависимости у школьника. http://security.mosmetod.ru/internet-zavisimosti/127-statistika-internet-zavisimosti-u-rossijskikh-podrostkov
	Практическое занятие – 1 час	Тест №2
Тема 3. Правила безопасного поведения школьников в сети Интернет.	*Лекция - презентация – 1 час*	Правила безопасного поведения в сети Интернет. Методы и функции родительского контроля. Полезные программы и приложения. Интернет-ресурсы, деятельность которых направлена на противодействие распространения опасного контента во всемирной сети.
	Практическое занятие – 1 час	Подготовка к выполнению проекта. Обзор предложенных интернет-ресурсов. Разработка интерактивного задания «Правила безопасного поведения в сети Интернет».
	Лекция - презентация – 1 час	Формы воспитательной работы и их классификация. Алгоритм разработки воспитательных мероприятий, направленных на формирование культуры информационной безопасности школьников с учетом нормативных и правовых актов.
	Практическое занятие – 3 часа	Проект. Разработка воспитательного мероприятия, направленного на формирование культуры информационной безопасности школьников с учетом нормативных и правовых актов.
Итоговая аттестация		Зачет на основании совокупности выполненных работ и результатов тестирования.

Раздел 3. «Формы аттестации и оценочные материалы»

3.1. Текущий контроль осуществляется в формате тестирования с автоматической проверкой.

Тест № 1 – Нормативно-правовое обеспечение информационной безопасности школьников.

Фрагмент теста № 1

1. Информационная безопасность детей – это:

a) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации, и поддерживающей инфраструктуре;

b) состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;

c) комплекс мероприятий, направленных на обеспечение информационной безопасности.

2. Что не относится к информации, причиняющей вред здоровью и (или) развитию детей?

a) информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с Федеральным законом № 436 от 29.12.2010;

b) информация, обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;

c) информация, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей.

Тест № 2 – Актуальные угрозы информационной безопасности и современные способы противодействия угрозам в сети Интернет.

Фрагмент теста № 2

1. Что такое фишинг?

a) незаконное копирование и распространение материалов (как для деловых, так и для личных целей);

b) любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ;

c) совокупность методов, позволяющих обмануть пользователя и заставить его раскрыть свой пароль, номер кредитной карты и другую конфиденциальную информацию.

2. Что из нижеперечисленных вариантов ответа является антивирусной программой?

a) WinRAR;

b) AVG;

c) Mac OS.

3.2. Промежуточная аттестация

Проект

Разработка воспитательного мероприятия, направленного на формирование культуры информационной безопасности школьников с учетом нормативных и правовых актов.

Требования к проекту:

1. Проектирование осуществляется на основании алгоритма разработки воспитательных мероприятий, направленных на формирование культуры информационной безопасности школьников с учетом нормативных и правовых актов.

2. Воспитательное мероприятие:

а) направлено на создание необходимых условий для развития у школьников способностей:

- распознавать негативную информацию в сети Интернет;
- противостоять угрозам сети Интернет путем применения современных способов защиты от вредной информации;

b) направлено на формирование устойчивых поведенческих навыков в сфере информационной безопасности;

c) разрабатывается с учетом возрастных особенностей обучающихся.

Технические требования:

1. Работа представляется в виде презентации в формате pdf.
2. Объем не более 15 слайдов.

Критерии оценивания проекта:

1. Все требования к проекту выполнены.
2. Проект логически последователен, все его пункты отражены и взаимосвязаны.

Оценивание: зачет/незачет.

3.3. Итоговая аттестация: зачет на основании совокупности результатов тестирования и проектной работы.

Раздел 4. «Организационно-педагогические условия реализации программы»

4.1. Учебно-методическое обеспечение и информационное обеспечение программы.

4.1.1. Нормативно-правовые документы

Электронные ресурсы:

1. Информационно-правовой портал ГАРАНТ.РУ, Федеральный закон от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию". [Электронный ресурс]// URL: http://ivo.garant.ru/#/document/12181695/paragraph/1:0

(дата обращения: 01.11.2020).

2. Информационно-правовой портал КонсультантПлюс, Распоряжение Правительства РФ от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей» [Электронный ресурс]// URL:

http://www.consultant.ru/document/cons_doc_LAW_190009/65c73cdecf9794a8f8f67bdb438d964c9336f436/ (дата обращения: 01.11.2020).

3. Информационно-правовой портал ГАРАНТ.РУ, Постановление Главного государственного санитарного врача РФ от 29 декабря 2010 г. N 189 "Об утверждении СанПиН 2.4.2.2821-10 "Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях". [Электронный ресурс]// URL: http://base.garant.ru/12183577/ (дата обращения: 01.11.2020).

4. Городской методический центр ДОНМ, Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования [Электронный ресурс]// URL: http://security.mosmetod.ru/stati/141-metodicheskie-rekomendatsii-po-ogranicheniyu-v-obrazovatelnykh-organizatsiyakh dostupa-obuchayushchikhsya-k-vidam-informatsii-rasprostranyaemoj-posredstvom-seti-internet-prichinyayushchej-vred-zdorovyu-i-ili-razvitiyu-detej-a-takzhe-ne-sootvetstvuyushchej. (дата обращения: 01.11.2020).

Список основной литературы:

1. Информационная безопасность детей. Российский и зарубежный опыт [Электронный ресурс]: монография / Л. Л. Ефимова, С. А. Кочерга. — М.: ЮНИТИ-ДАНА, 2017. — 239 с.

2. Стороженко Л.Д. Опасный интернет: что и как угрожает нашим детям. Кибербезопасность – предупреждение информационного терроризма// Материалы 56-й Международной научной студенческой конференции. Новосибирск: Новосибирский национальный исследовательский гос. ун-т, 2018.С 84-85.

3. Белякова, Е.Г., Загвязинская, Э.В., Березенцева, А.И. Информационная культура и информационная безопасность школьников // Образование и наука. - 2017. - Т. 19. № 8. -С. 147-162.

4. Соколова Д.В. Агрессия в интернете: распространение кибербуллинга среди российских подростков // Медиаскоп. 2017. № 2. С. 11.

5. Храмова М. В., Пицик Е. Н. Отношение родителей к потенциальным опасностям при увлечении школьников соцсетями// Образовательные технологии и общество. 2017. №3. С 386-396.

6. Будыкин С. В. Информационная безопасность детей и подростков в современном мире: психологические аспекты проблемы// Психология и право. 2017. Т. 7. № 1. С. 13-24.

7. Ищенко А.Н., Прокопенко А.Н., Страхов А.А. Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере // Проблемы правоохранительной деятельности. 2017. № 2. С. 55-62.

8. Банщикова, С.Л., Гольтяпина, И.Ю. Обязанности родителей по обеспечению информационной безопасности несовершеннолетних детей и административная ответственность за неисполнение обязанности // Вестник Сибирского института бизнеса и информационных технологий. - 2018. - № 1 (25). - С. 95-100.

9. Дадаева, М.С. Государственная система кибербезопасности и предупреждение экстремизма среди несовершеннолетних // Современные научные исследования и разработки. -2018. - Т. 1. № 5 (22). - С. 183-185.

10. Молодцова, Е. Ю. К вопросу организации мероприятий по информационной безопасности учащихся в образовательном учреждении / Е. Ю. Молодцова, М. Ю. Склямина. — Текст : непосредственный // Молодой ученый. — 2014. — № 18.1 (77.1). — С. 65-68. — URL: https://moluch.ru/archive/77/13215/ (дата обращения: 01.11.2020).

Электронные ресурсы:

1. Министерство внутренних дел, Безопасный Интернет детям. [Электронный ресурс]// URL: www.мвд.рф/безопасный-интернет-детям (дата обращения: 01.11.2020).

2. Портал детской безопасности МЧС России, Интернет-безопасность. [Электронный ресурс]// URL: https://www.spas-extreme.ru/themes/internet_bezopasnost (дата обращения: 01.11.2020).

3. Роскомнадзор, Персональные данные. [Электронный ресурс]// URL: http://xn--80aalcbc2bocdadlpp9nfk.xn--d1acj3b/personalnye_dannye/ (дата обращения: 01.11.2020).

4. Министерство просвещения Российской Федерации, Изучи интернет – управляй им. [Электронный ресурс]// URL: https://xn----7sbikand4bbyfwe.xn--p1ai/ (дата обращения: 01.11.2020).

5. Фонд развития Интернет, Дети России онлайн. [Электронный ресурс]// URL: http://detionline.com/ (дата обращения: 01.11.2020).

6. Городской методический центр ДОНМ, Безопасность в Интернете. [Электронный ресурс]// URL: http://security.mosmetod.ru/ (дата обращения: 01.11.2020).

4.2. Материально-технические условия реализации программы

Для реализации программы необходимо следующее материально-техническое обеспечение:

1. Компьютерное и мультимедийное оборудование для использования видео- и аудиовизуальных средств обучения с подключением к сети Интернет, пакет слайдовых презентаций.

2. Образовательный цифровой ресурс для дистанционной реализации обучения: http://learn.mosmetod.ru/.