Управление образования и науки Тамбовской области

Тамбовское областное государственное образовательное автономное учреждение дополнительного профессионального образования "Институт повышения квалификации работников образования"

Дополнительная профессиональная программа (повышение квалификации)

Формирование кибербезопасного поведения обучающихся в социальных сетях

Разработчик(и) программы:
Жданова М.А., ТОГОАУ ДПО ИПКРО
Нехорошева О.Н., ТОГОАУ ДПО ИПКРО
Солопова Н.К., к.п.н., доцент

Тамбов, 2022

Раздел 1. Характеристика программы

1.1. Цель реализации программы – совершенствование профессиональных компетенций слушателей в области формирования кибербезопасного поведения обучающихся в социальных сетях..

1.2. Планируемые результаты обучения:

Трудовая функция	Трудовое действие	Знать	Уметь
Общепедагогическая функция. Обучение	Формирование навыков, связанных с информационно - коммуникативными технологиями	Социальные, психологические и технологические угрозы безопасности несовершеннолетних в социальных сетях. Основы организации и проектированияобразовательной деятельности по формированию кибербезопасного поведения обучающихся в социальных сетях.	Анализировать Интернет-контент с точки зрения кибаругроз. Выявлять социальные, психологические и технологические угрозы кибербезопасности несовершеннолетних в социальных сетях. Проектировать образовательную деятельность по профилактике киберугроз в социальных сетях с помощью цифровых ресурсов.
Воспитательная деятельность	Регулирование поведения обучающихся для обеспечения безопасной образовательной среды Формирование толерантности и навыков поведения в изменяющейся поликультурной среде	Нормативное регулирование в вопросах обеспечения кибербезопасности обучающихся. Основные приемы, способы, механизмы выявления и защиты несовершеннолетних от возникающих киберугроз. Понятие сетевого этикета. Общие правила сетевого этикета.	Использовать в образовательной деятельности нормативное регулирование в вопросах обеспечения кибербезопасности обучающихся. Применять приемы, способы, механизмы выявления и защиты несовершеннолетних от возникающих киберугроз. Применять правила сетевого этикета и поведения в виртуальной среде. Применять приемы и эффективные формы организации сетевых мероприятий.

1.3. Категория слушателей:
учителя-предметники

1.4. Форма обучения – Очно-заочная

1.5. Срок освоения программы: 36 ч.

Раздел 2. Содержание программы

№ 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**					
1	Модуль 1. Государственная политика в сфере образования	0	0	0	0	
1.1	Входной контроль	1	0	0	1	тест
1.2	Государственная политика в сфере общего образования Российской Федерации	1	1	0	0	
1.3	Цифровая трансформация образования	1	1	0	0	
1.4	Нормативное регулирование в вопросах обеспечения кибербезопасности обучающихся	2	0	0	2	практическая работа
2	Модуль 2. Социальные, психологические и технологические угрозы безопасности несовершеннолетних в социальных сетях	0	0	0	0	
2.1	Социальная сеть. Сетевой этикет	3	1	0	2	
2.2	Кибербезопасность и кибергигиена школьников	4	2	1	1	практическая работа
2.3	Виды киберугроз в социальных сетях	3	1	2	0	практическая работа
2.4	Психологические киберугрозынесовершеннолетних в социальных сетях	3	1	2	0	практическая работа
2.5	Социальные киберугрозы несовершеннолетних в социальных сетях	3	1	2	0	практическая работа
2.6	Технологические киберугрозы несовершеннолетних в социальных сетях	3	1	2	0	практическая работа
3	Модуль 3. Проектирование образовательной деятельности по формированию кибербезопасного поведения несовершеннолетних в социальных сетях	0	0	0	0	
3.1	Методические приемы, механизмы, формы профилактики кибербезопасности несовершеннолетних в соцсетях	2	0	2	0	практическая работа
3.2	Меры защиты несовершеннолетних от киберугроз в соцсетях	2	0	2	0	практическая работа

3.3	Планирование и организация деятельности обучающихся по защите от киберугроз	2	0	2	0	практическая работа
3.4	Проектирование образовательного мероприятия по кибербезопасности с использованием цифровых инструментов и сервисов	6	0	2	4	практическая работа
4	Итоговая аттестация (по совокупности выполненных работ)	0	0	0	0	
	Итого	36	9	17	10	

2.2. Рабочая программа

1 Модуль 1. Государственная политика в сфере образования

1.1 Входной контроль (самостоятельная работа - 1 ч.)

Самостоятельная работа·Самостоятельная работа. Выполнение теста.

1.2 Государственная политика в сфере общего образования Российской Федерации (лекция - 1 ч.)

Лекция·Образовательное законодательство Российской Федерации. Цели и ключевые задачи Российской Федерации в сфере образования. Национальный проект «Образование». Механизмы достижения поставленных целей. Законодательные и нормативные акты Российской Федерации в области кибербезопасности.

1.3 Цифровая трансформация образования (лекция - 1 ч.)

Лекция·«Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы». Программа «Цифровая экономика Российской Федерации». Национальная цель развития Российской Федерации «Цифровая трансформация». Суть цифровой трансформации образования. Технологическое обновление и новая дидактика образования, персонализация образовательной деятельности на основе использования растущего потенциала цифровых технологий. Актуальные навыки и практики преподавания в цифровую эпоху.

1.4 Нормативное регулирование в вопросах обеспечения кибербезопасности обучающихся (самостоятельная работа - 2 ч.)

Самостоятельная работа·Анализ образовательного кейса, размещенного на странице курса виртуальной обучающей среды http://68cdo.ru/moodle. Нормативно-правовое обеспечение информационной безопасности детей в цифровой образовательной среде: Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Федеральный закон от 8 июня 2020 г. № 177-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»; Указ Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года». Основные аспекты информационной безопасности в цифровой среде. Ключевые навыки управления информацией и данными. Концепция информационной безопасности детей, утвержденная Правительством РФ. Задание. На основе анализа материалов образовательного кейса «Нормативное регулирование в вопросах обеспечения кибербезопасности обучающихся» выберите не менее двух качественных и количественных критериев по актуальному направлению обеспечения кибербезопасности несовершеннолетних. Выполненную работу, разместить в личном кабинете слушателя на платформе дистанционного обучения.

2 Модуль 2. Социальные, психологические и технологические угрозы безопасности несовершеннолетних в социальных сетях

2.1 Социальная сеть. Сетевой этикет (лекция - 1 ч. самостоятельная работа - 2 ч.)

Лекция·Социальная сеть. Основные понятия. Виды социальных сетей. Сетевой этикет. Понятие сетевого этикета. Виды этикета. Общие правила сетевого этикета. Взаимное

уважение при сетевой коммуникации. Сетевой этикет и кибербезопасность.

Самостоятельная работа·На основе анализа ситуационных заданий, разработать памятку для обучающихся по правилам сетевого этикета в социальных сетях. Выполненную работу, разместить в личном кабинете слушателя на платформе дистанционного обучения.

2.2 Кибербезопасность и кибергигиена школьников (лекция - 2 ч. практическое занятие - 1 ч. самостоятельная работа - 1 ч.)

Лекция·Актуальность, проблемы кибербезопасности. Кибербезопасность, как составная часть информационной безопасности. Основные понятия и определения в области кибербезопасности. Понятие кибергигиены. Правила кибергигиены: обеспечение безопасности учетных записей, базовые приемы цифровой кибербезопасности школьников.

Практическая работа·Работа в микрогруппах. На основе предоставленных информационных ресурсов сети Интернет по профилактике кибербезопасности и кибергигиены несовершеннолетних составить краткую аннотацию информационного ресурса и рекомендации по его использованию. Обсудить полученные рекомендации в группе.

Самостоятельная работа·На основе анализа учебных материалов кейса «Кибербезопасность и кибергигиена школьников» составить Чек-лист правил кибергигиены для обучающихся. Выполненную работу разместить в личном кабинете слушателя на платформе дистанционного обучения.

2.3 Виды киберугроз в социальных сетях (лекция - 1 ч. практическое занятие - 2 ч.)

Лекция·Понятие «угроза кибербезопасности». Классификация угроз. Виды рисков в социальных сетях для обучающихся. Наиболее распространенные угрозы. Методика определения актуальных угроз кибербезопасности в социальных сетях.

Практическая работа·Работа в микрогруппах. На основе анализа предложенных видеороликов определить видыкиберугроз. Обсудить полученные результаты в группе.

2.4 Психологические киберугрозы несовершеннолетних в социальных сетях (лекция - 1 ч. практическое занятие - 2 ч.)

Лекция·Кибербезопасность в социальных сетях. Интернет-зависимость. Деструктивные агротехники («Синий кит, «Мимо», «Красная сова» и др.). Кибербуллинг: определение, причины возникновения. Виды и типы фитинга. Фитинг-атаки. Методы психологического манипулирования и технологическое обеспечение мошенничества. Анонимная сеть Darknet. Методы, инструменты вовлечения детей в сеть Darknet. Способы выявления. Особенности реагирования, возможности и инструменты противодействия.

Практическая работа·На основе предоставленного кейса Интернет ресурсов, определить тип психологических киберугроз несовершеннолетних в социальных сетях. Обсудить полученные результаты в группе.

2.5 Социальные киберугрозы несовершеннолетних в социальных сетях (лекция - 1 ч. практическое занятие - 2 ч.)

Лекция·Социальныекиберугрозы: экстремизм и хулиханство. Признаки вовлечения школьников в экстремистские сообщества. Религиозные и политические радикальные группы. Христианские ордоксальные секты. Форматы мониторинга социальных киберугроз несовершеннолетних в социальных сетях.

Практическая работа·Провести анализ предложенных ситуаций и выявить признаки социальных киберугроз несовершеннолетних в социальных сетях. Обсудить полученные результаты в группе.

2.6 Технологические киберугрозы несовершеннолетних в социальных сетях (лекция - 1 ч. практическое занятие - 2 ч.)

Лекция·Типы технологических киберугроз несовершеннолетних в социальных сетях. Организация защиты от вредоносного программного обеспечения - вирусы, черви, трояны, руткиты, макровирусы. Принципы, назначение, векторы работы технологических кибератак. Спам и навязчивая реклама как разновидность вредоносного программного обеспечения.

Практическая работа·Провести анализ предложенных ситуаций и выявить признаки технологических киберугроз несовершеннолетних в социальных сетях. Обсудить полученные

результаты в группе.

3 Модуль 3. Проектирование образовательной деятельности по формированию кибербезопасного поведения несовершеннолетних социальных сетях

3.1 Методические приемы, механизмы, формы профилактики кибербезопасности несовершеннолетних в соцсетях (практическое занятие - 2 ч.)

Практическая работа·Работа в микрогруппах. На основе рассмотренных ранее киберугроз (психологических, социальных, технологических) для несовершеннолетних: выбрать один из видов киберугроз; осуществить отбор приемов, механизмов, форм профилактики для выбранного вида киберугроз; подготовить методические или дидактические материалы для проектируемого занятия/мероприятия по профилактикекибербезопасностиобучающихся в соцсетях; обсудить полученные результаты в группе.

3.2 Меры защиты несовершеннолетних от киберугроз в соцсетях (практическое занятие - 2 ч.)

Практическая работа·Работа проводится в микрогруппах: осуществить выбор мер защиты обеспечения кибербезопасности, способов организации кибербезопасной работы обучающихся в социальных сетях; аргументировать свой выбор.

3.3 Планирование и организация деятельности обучающихся по защите от киберугроз (практическое занятие - 2 ч.)

Практическая работа·Работа в микрогруппах. Разработать дорожную карту мероприятий по защите от киберугроз с позиции социальных ролей участников образовательных отношений. Обсудить полученные результаты в группе.

3.4 Проектирование образовательного мероприятия по кибербезопасности с использованием цифровых инструментов и сервисов (практическое занятие - 2 ч. самостоятельная работа - 4 ч.)

Практическая работа·Работа в микрогруппах. Выбрать из разработанной дорожной карты одно из мероприятий. Осуществить выбор цифровых инструментов и сервисов, необходимых для проектирования занятия/ сценария мероприятия по киберпрофилактике в социальных сетях. Обсудить полученные результаты в группе.

Самостоятельная работа·Разработать технологическую карту занятия/сценария мероприятия по киберпрофилактике в социальных сетях. Выполненную работу, разместить в личном кабинете слушателя на платформе дистанционного обучения.

4 Итоговая аттестация осуществляется по совокупности результатов всех видов контроля, предусмотренных программой.

Раздел 3. Формы аттестации и оценочные материалы

Входной контроль

Форма: тестирование

Описание, требования к выполнению:

Входное тестирование состоит из 15 вопросов, максимальное количество баллов – 15. Время тестирования - 1 час.

Критерии оценивания:

Более 50% правильных ответов – достаточные исходные (базовые) знания в области направления программы, слушатель готов к обучению по данной программе повышения квалификации. Менее 50% правильных ответов – недостаточные исходные (базовые) знания в области направления программы. Слушателям, набравшим менее 50% правильных ответов, будет предложен индивидуальный план по устранению выявленных дефицитов.

Примеры заданий:

1. Какие проблемы решаются с помощью кибергигиены?

а) Нарушение безопасности, потеря данных.

б) Устаревшее программное обеспечение.

в) Устаревший антивирус.

г) Все выше перечисленное. (Верно)

2.Соотнесите виды сетевого кибербуллинга с его краткой характеристикой.

Виды сетевого кибербуллинга		Характеристика
1.Фишинг	А	Заманивание пользователя на поддельный сайт, с целью перехватить данные пользователя (данные карты, логин, пароль сайта-оригинала и т.п.).
2.Вишинг	Б	Мошенничество с помощью телефона. Цель – выманить платежные данные, с помощью которых можно украсть деньги с карты или кошелька. Часто дополнительно присылается СМС со ссылкой, которая ведет на фишинговый сайт.
3. "Липовые акции"	В	Пользователь может получить сообщение (по телефону, почте или SMS), что выиграл некий приз, а для его получения необходимо «уплатить налог», «оплатить доставку» или просто пополнить какой-то счет.
4.Фишинг-атаки	Г	Пользователю на электронную почту поступают всплывающие сообщения и ссылки на фишинговые веб-сайты, с целью обманным путем выявить у получателя личную информацию, часто финансового характера.
5.Ложная блокировка	Д	При попытке зайти в социальную сеть появляется баннер/экран/картинка, где подробно расписан вариант «спасения» от блокирования страницы, который включает отправку SMS на «короткий» номер или введение кода подтверждения. В первом случае происходит разовое списание денег, а во втором оформляется ежедневная подписка на какую-либо платную услугу.

Количество попыток: 2

Текущий контроль

Раздел программы: Модуль 1. Государственная политика в сфере общего образования Российской Федерации Тема 1.4 Нормативное регулирование в вопросах обеспечения кибербезопасности обучающихся

Форма: самостоятельная работа

Описание, требования к выполнению:

Условия организации самостоятельной работы: каждому слушателю предлагается провести анализ материалов образовательного кейса «Нормативное регулирование в вопросах обеспечения кибербезопасности обучающихся», указать не менее двух качественных и количественных критериев по актуальному направлению обеспечения кибербезопасности несовершеннолетних. Выполненную работу слушатели размещают в личном кабинете на платформе дистанционного обучения.

Критерии оценивания:

соответствие теме задания, логичность и аргументированность представленных критериев. Задание считается выполненным, если представлено не менее двух качественных и количественных критериев по актуальному направлению обеспечения кибербезопасности несовершеннолетних.

Примеры заданий:

Проанализировать материалы образовательного кейса «Нормативное регулирование в вопросах обеспечения кибербезопасности обучающихся», размещенного на странице курса виртуальной обучающей среды http://68cdo.ru/moodle
. Указать не менее двух качественных и количественных
критериев по актуальному направлению
обеспечения кибербезопасности несовершеннолетних.
Выполненную работу разместить в личном кабинете слушателя на платформе дистанционного обучения.

Количество попыток: не ограничено

Раздел программы: Модуль 2. Социальные, психологические и технологические угрозы безопасности несовершеннолетних в социальных сетях. Тема 2.1 Социальная сеть. Сетевой этикет

Форма: самостоятельная работа

Описание, требования к выполнению:

Условия организации самостоятельной работы: слушателям предлагается банк ситуационных заданий «Сетевой этикет и кибербезопасность», размещенный на странице курса виртуальной обучающей среды http://68cdo.ru/moodle; слушателю предлагается провести анализ ситуационных заданий, разработать памятку для обучающихся по правилам сетевого этикета в социальных сетях. Выполненную работу слушатели размещают в личном кабинете на платформе дистанционного обучения.

Критерии оценивания:

соответствие теме задания, логичность, педагогическая целесообразность содержания памятки.

Примеры заданий:

Проанализировать ситуационные задания «Сетевой этикет и кибербезопасность», размещенные на странице курса виртуальной обучающей среды http://68cdo.ru/moodle ; разработать памятку для обучающихся по правилам сетевого этикета в социальных сетях. Выполненную работу, разместить в личном кабинете слушателя на платформе дистанционного обучения.

Количество попыток: не ограничено

Раздел программы: Тема 2.2 Кибербезопасность и кибергигиена школьников
Форма: практическая работа
Описание, требования к выполнению:
Условия организации практической работы: работа проводится в микрогруппах 5-6 человек. На основе информационных ресурсов сети Интернет по профилактике кибербезопасности и кибергигиене несовершеннолетних, размещенных на странице курса виртуальной обучающей среды http://68cdo.ru/moodle, слушатели составляют краткую аннотацию информационных ресурсов и разрабатывают рекомендации по их использованию. Результаты выполненной работы представляют в виде таблицы 1. Слушатели обсуждают полученные результаты в группе.
Критерии оценивания:
соответствие теме задания, логичность, педагогическая целесообразность по использованию рекомендаций с точки зрения обеспечения кибербезопасности и кибергигиены несовершеннолетних.
Примеры заданий:

Проанализировать предоставленные информационные ресурсы сети Интернет по профилактике кибербезопасности и кибергигиене несовершеннолетних, размещенные на странице курса виртуальной обучающей среды http://68cdo.ru/moodle. Составить краткую аннотацию информационного ресурса и разработать рекомендации по его использованию, результаты работы представить в виде таблицы 1. Обсудить полученные рекомендации в группе.

Таблица 1. Ресурсы сети Интернет для использования в работе

по обеспечению кибербезопасности и кибергигиены несовершеннолетних

Название ресурса	Адрес в сети Интернет	Краткая аннотация	Рекомендации по использованию
Единый урок безопасности в сети Интернет	Единый урок РФ		
Центр безопасного Интернета в России	http://www.saferunet.ru/		

Безопасный Интернет для детей: законодательство, советы, международный опыт	http://i-deti.org/		
Официальный сайт «Лига безопасного Интернета»	http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/		

Количество попыток: не ограничено

Раздел программы: Тема 2.2 Кибербезопасность и кибергигиена школьников
Форма: самостоятельная работа
Описание, требования к выполнению:
Условия организации самостоятельной работы: слушателям по теме «Кибербезопасность и кибергигиена школьников» предлагается кейс учебных материалов, размещенный на странице курса виртуальной обучающей среды http://68cdo.ru/moodle; слушателю на основе анализа учебных материалов, предлагается составить Чек-лист правил кибергигиены для обучающихся. Выполненную работу слушатель размещает в личном кабинете на платформе дистанционного обучения.
Критерии оценивания:
полнота, логичность, соответствие правил кибергигиены видам киберугроз.
Примеры заданий:

Провести анализ учебных материалов кейса по теме «Кибербезопасность и кибергигиена школьников», размещенных на странице курса виртуальной обучающей среды http://68cdo.ru/moodle;

составить Чек-лист правил кибергигиены для обучающихся. Выполненную работу разместить в личном кабинете слушателя на платформе дистанционного обучения.

Количество попыток: не ограничено

Раздел программы: Тема 2.3 Виды киберугроз в социальных сетях
Форма: практическая работа
Описание, требования к выполнению:
Условия организации практической работы: работа проводится в микрогруппах 5-6 человек. Слушателям предлагается банк видеороликов, размещенный на странице курса виртуальной обучающей среды http://68cdo.ru/moodle. На основе анализа предложенных видеороликов слушатели определяют вид киберугроз. Слушатели обсуждают полученные результаты в группе.
Критерии оценивания:
правильность определения вида киберугроз в социальных сетях по выявленным опасным признакам (визуальные образы, текстовая информация, сообщества, подписки, друзья).
Примеры заданий:

Проанализировать предложенный банк видеороликов, размещенный на странице курса виртуальной обучающей среды http://68cdo.ru/moodle

; определить виды киберугроз. Обсудить полученные результаты в группе.

Количество попыток: не ограничено

Раздел программы: Тема 2.4 Психологические киберугрозы несовершеннолетних в социальных сетях
Форма: практическая работа
Описание, требования к выполнению:
Условия организации практической работы: работа проводится в микрогруппах 5-6 человек. На основе предложенного кейса Интернет ресурсов по теме «Психологические киберугрозы несовершеннолетних в социальных сетях», размещенного на странице курса виртуальной обучающей среды http://68cdo.ru/moodle слушатели определяют тип психологических киберугроз несовершеннолетних в социальных сетях. Слушатели обсуждают полученные результаты в группе.
Критерии оценивания:
выявление опасных признаков и соотнесение с типом психологических киберугроз несовершеннолетних в социальных сетях.
Примеры заданий:

На основе предоставленного кейса Интернет ресурсов по теме «Психологические киберугрозы несовершеннолетних в социальных сетях», размещенного на странице курса виртуальной обучающей среды http://68cdo.ru/moodle, определить тип психологических киберугроз несовершеннолетних в социальных сетях. Обсудить полученные результаты в группе.

Количество попыток: не ограничено

Раздел программы: Тема 2.5 Социальные киберугрозы несовершеннолетних в социальных сетях
Форма: практическая работа
Описание, требования к выполнению:
Условия организации практической работы: работа проводится в микрогруппах 5-6 человек. Слушателям предлагается банк ситуационных заданий «Социальные киберугрозы несовершеннолетних в социальных сетях», размещенный на странице курса виртуальной обучающей среды http://68cdo.ru/moodle. На основе предложенных ситуаций, слушатели проводят анализ и выявляют признаки социальных видов киберугроз несовершеннолетних. Слушатели обсуждают полученные результаты в группе.
Критерии оценивания:
правильность выявленных опасных признаков и их соотнесение с типом социальных киберугроз несовершеннолетних.
Примеры заданий:

Провести анализ банка предложенных ситуаций «Социальные киберугрозы несовершеннолетних в социальных сетях», размещенный на странице курса виртуальной обучающей среды http://68cdo.ru/moodle и выявить признаки социальных киберугроз несовершеннолетних в социальных сетях. Обсудить полученные результаты в группе.

Количество попыток: не ограничено

Раздел программы: Тема 2.6 Технологические киберугрозы несовершеннолетних в социальных сетях
Форма: практическая работа
Описание, требования к выполнению:
Условия организации практической работы: работа проводится в микрогруппах 5-6 человек. Слушателям предлагается банк ситуационных заданий «Технологические киберугрозы несовершеннолетних в социальных сетях», размещенный на странице курса виртуальной

обучающей среды http://68cdo.ru/moodle. На основе предложенных ситуаций, слушатели проводят анализ и выявляют признаки технологических видов киберугроз несовершеннолетних. Слушатели обсуждают полученные результаты в группе.
Критерии оценивания:
правильность выявленных опасных признаков и их соотнесение с типом технологических киберугроз несовершеннолетних.
Примеры заданий:

Провести анализ предложенного банка ситуационных заданий «Технологические киберугрозы несовершеннолетних в социальных сетях», размещенного на странице курса виртуальной обучающей среды http://68cdo.ru/moodle. Выявить признаки технологических видов киберугроз несовершеннолетних в социальных сетях. Обсудить полученные результаты в группе.

Количество попыток: не ограничено

Раздел программы: Раздел программы: Модуль 3. Проектирование образовательной деятельности по формированию кибербезопасного поведения несовершеннолетних в социальных сетях Тема 3.1 Методические приемы, механизмы, формы профилактики кибербезопасности несовершеннолетних в соцсетях
Форма: практическая работа
Описание, требования к выполнению:
Условия организации практической работы: работа проводится в микрогруппах 5-6 человек. На основе рассмотренных ранее киберугроз (психологических, социальных, технологических) для несовершеннолетних: слушатели выбирают один из видов киберугроз; осуществляют отбор приемов, механизмов, форм профилактики для выбранного вида киберугроз; осуществляют подготовку методических или дидактических материалов для проектируемого занятия/мероприятия по профилактике кибербезопасности обучающихся в соцсетях; обсуждают полученные результаты в группе.
Критерии оценивания:
педагогическая целесообразность выбора приемов, механизмов, форм профилактики киберугроз; полнота, логичность подготовленных методических/дидактических материалов для проектируемого занятия/мероприятия по профилактике кибербезопасности обучающихся в соцсетях.
Примеры заданий:

На основе рассмотренных ранее киберугроз (психологических, социальных, технологических) для несовершеннолетних: выбрать один из видов киберугроз; осуществить отбор приемов, механизмов, форм профилактики для выбранного вида киберугроз; подготовить методические или дидактические материалы для проектируемого занятия/мероприятия по профилактике кибербезопасности обучающихся в соцсетях; обсудить полученные результаты в группе.

Количество попыток: не ограничено

Раздел программы: Тема 3.2 Меры защиты несовершеннолетних от киберугроз в соцсетях
Форма: практическая работа
Описание, требования к выполнению:
Условия организации практической работы: работа проводится в микрогруппах 5-6 человек. Слушателям предлагается кейс «Меры защиты несовершеннолетних от киберугроз в соцсетях», размещенный на странице курса виртуальной обучающей среды http://68cdo.ru/moodle. Слушатели осуществляют выбор мер защиты обеспечения кибербезопасности, способов организации кибербезопасной работы обучающихся в социальных сетях.
Критерии оценивания:
соответствие способов организации кибербезопасной работы обучающихся в социальных сетях

мерам защиты обеспечения кибербезопасности. Педагогическая целесообразность по их применению, аргументированность, грамотности речи.
Примеры заданий:

На основе анализа кейса «Меры защиты несовершеннолетних от киберугроз в соцсетях», размещенного на странице курса виртуальной обучающей среды http://68cdo.ru/moodle . Осуществить выбор мер защиты обеспечения кибербезопасности, способов организации кибербезопасной работы обучающихся в социальных сетях; аргументировать свой выбор.

Количество попыток: не ограничено

Раздел программы: Тема 3.3 Планирование и организация деятельности обучающихся по защите от киберугроз
Форма: практическая работа
Описание, требования к выполнению:
Условия организации практической работы: работа проводится в микрогруппах 5-6 человек. Слушатели разрабатывают дорожную карту мероприятий по защите киберугрозы с позиции социальных ролей участников образовательных отношений. Слушатели обсуждают полученные результаты в группе.
Критерии оценивания:
соответствие теме задания, логичность, педагогическая целесообразность выбора мероприятий дорожной карты с позиции социальных ролей участников образовательных отношений.
Примеры заданий:

Разработать дорожную карту мероприятий по защите от киберугроз с позиции социальных ролей участников образовательных отношений. Обсудить полученные результаты в группе.

Количество попыток: не ограничено

Раздел программы: Тема 3.4 Проектирование образовательного мероприятия по кибербезопасности с использованием цифровых инструментов и сервисов
Форма: практическая работа
Описание, требования к выполнению:
Условия организации практической работы: работа проводится в микрогруппах 5-6 человек. Каждый участник микрогруппы работает за компьютером, под руководством преподавателя проходит регистрацию на одном из цифровых сервисов (Wizer.me, Инфограмм), осваивает возможности сервиса. Разрабатывает задание по теме занятия, с помощью предложенных цифровых сервисов, необходимых для проектирования занятия/ сценария мероприятия по киберпрофилактике в социальных сетях. Слушатели обсуждают полученные результаты в группе.
Критерии оценивания:
соответствие теме задания, логичность, педагогическая целесообразность по использованию цифровых инструментов и сервисов, необходимых для проектирования занятия/ сценария мероприятия по киберпрофилактике в социальных сетях.
Примеры заданий:

Разработать задания по киберпрофилактике в социальных сетях для обучающихся с помощью предложенных (Wizer.me, Инфограмм), цифровых инструментов и сервисов, необходимых для проектирования занятия/ сценария мероприятия по киберпрофилактике в социальных сетях. Обсудить полученные результаты в группе.

Количество попыток: не ограничено

Раздел программы: Тема 3.4 Проектирование образовательного мероприятия по

кибербезопасности с использованием цифровых инструментов и сервисов
Форма: самостоятельная работа
Описание, требования к выполнению:
Условия организации практической работы: Каждый слушатель выбирает из разработанной дорожной карты одно из мероприятий и проектирует технологическую карту занятия/сценария мероприятия по киберпрофилактике в социальных сетях. Выполненную работу, размешает в личном кабинете слушателя на платформе дистанционного обучения.
Критерии оценивания:
соответствие теме задания, логичность, педагогическая целесообразность по использованию цифровых инструментов и сервисов, необходимых для проектирования занятия/ сценария мероприятия по киберпрофилактике в социальных сетях.
Примеры заданий:

Выбрать из разработанной дорожной карты одно из мероприятий. Разработать технологическую карту занятия/сценария мероприятия по киберпрофилактике в социальных сетях. Выполненную работу, разместить в личном кабинете слушателя на платформе дистанционного обучения.

Количество попыток: не ограничено

Итоговая аттестация

Итоговая аттестация осуществляется по совокупности результатов всех видов контроля, предусмотренных программой.

Раздел 4. Организационно-педагогические условия реализации программы

4.1. Организационно-методическое и информационное обеспечение программы

Нормативные документы

1. Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2021).
2. Указ Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года».
3. Приказ Министерства просвещения РФ от 2 декабря 2019 г. № 649 «Об утверждении Целевой модели цифровой образовательной среды».
4. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 г. № 436-ФЗ(с изм. и доп., вступ. в силу с 01.07.2021).
5. Федеральный закон от 8 июня 2020 г. № 177-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации».

Литература

1. Артамонов, В. А. Кибербезопасность в условиях цифровой трансформации /В. А. Артамонов, Е.В. Артамонова //Цифровая трансформация, 2021. № 4 (17). С.42–51.
2. Артамонова Е.Г., Калинина Н.В., Ефимова О.И., Салахова В.Б. Обеспечение психологической безопасности в детско-подростковой среде. Методические рекомендации для психологов общеобразовательных организаций /Под ред. Л.П. Фальковской - М.: ФГБНУ «Центр защиты прав и интересов детей», 2018. 36 с.

3. Белоусов А.Д. Угрозы сети Интернет для несовершеннолетних пользователей: психологический анализ и профилактика: монография. - М.: Проспект, 2019. 80 с.
4. Бочавер А.А., Хломов К.Д. Кибербуллинг: травля в пространстве современных технологий /Психология. Журнал Высшей школы экономики, 2018. №3. С. 171-191.
5. Калинина Н.В. Субъектно-ориентированный подход к профилактике интернет-рисков в образовательной среде // Социальная педагогика. 2019. №3. С. 24-28.
6. Кирюхина Д.В. Кибербуллинг среди молодых пользователей социальных сетей // Современная зарубежная психология. 2019. Том 8. № 3. С. 53–59.
7. Солдатова Г. У., Чигарькова С. В., Дренева А. А., Илюхина С. Н. Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете: Учебно-методическое пособие. – М.: Когито-Центр, 2019. 176 с.
8. Хломов К.Д., Давыдов Д.Г., Бочавер А.А. Кибербуллинг в опыте российских подростков // Психология и право. 2019 Т. 9. № 2. С. 276–295.

Электронные обучающие материалы

Интернет-ресурсы

1.Безопасный Интернет для детей: законодательство, советы, международный опыт.URL: http://i-deti.org/(дата обращения: 04.02.2022).

2.Единый урок безопасности в сети Интернет. URL: https://www.xn--d1abkefqip0a2f.xn--p1ai/ (дата обращения: 04.02.2022).

3.Информационный портал о всех видах зависимостей, связанных с компьютерными и мобильными устройствами .URL: http://netaddiction.ru (дата обращения: 04.02.2022)

4. «Кибербезопасность для детей и взрослых - Российская Электронная школа». URL: https://resh.edu.ru/page/cyber-project(дата обращения: 04.02.2022).

5. Центр безопасного Интернета в России, горячая линия по безопасному Интернету. URL: http://www.saferunet.ru/(дата обращения: 04.02.2022).

6.«Основы кибербезопасности от Сбербанка». URL: https://promo.sber.ru/kidssafety(дата обращения: 04.02.2022).

7. Центр безопасного Интернета в России. URL: http://www.saferunet.ru/(дата обращения: 04.02.2022).

8.Официальный сайт «Лига безопасного Интернета».URL: http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/(дата обращения: 04.02.2022).

4.2. Материально-технические условия реализации программы

Технические средства обучения

Условием полноценной реализации программы в дистанционной интерактивной форме является наличие у слушателя курсов персонального компьютера, оснащенного аудиоколонками, микрофоном и веб-камерой, имеющего широкополосный выход в Интернет, с установленной программой MicrosoftLync и операционной системой не ниже Windows 8.

Для обеспечения интерактивного взаимодействия со слушателями в рамках данных занятий используются возможности сети Интернет, программы MicrosoftLync, Сферум (или иного программного обеспечения, обладающего аналогичным функционалом).

Самостоятельная работа слушателей в офлайн-режиме предусматривает изучение учебных материалов и выполнение заданий, размещенных на странице курса виртуальной обучающей среды Moodle на сайте Центра дистанционного образования ТОИПКРО http://68cdo.ru/moodle

и доступных зарегистрированным слушателям.