Рабочая программа

дополнительной профессиональной программы повышения квалификации «Формирование медиаграмотности и информационной культуры обучающихся в условиях образовательной организации»

Государственная политика в сфере общего образования Российской Федерации. Законодательство Российской федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию (лекция - 5 ч. практическое занятие - 2ч.)

Лекция.·Государственная политика в сфере общего образования Российской Федерации. Цели и ключевые задачи Российской Федерации в сфере образования. Суть цифровой трансформации образования. Нормативное регулирование информационной безопасности обучающихся. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.10.2012 года № 436-ФЗ. Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 01.12.2020 г. № 644 «О плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021 – 2027 годы».

Способы обеспечения информационной безопасности обучающихся в образовательной организации. Локальные акты образовательной организации, направленные на обеспечение медиабезопасности обучающихся.

Практическая работа.·Подготовка отчета по основным нормативно-правовым актам Российской федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию. Цель: анализ и систематизация нормативно –правовых документов в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию. Результат: систематизация нормативно-правовой документации в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

Современные информационные угрозы и обеспечение информационной безопасности обучающихся

Виды информационных угроз. (лекция - 4 ч. практическое занятие - 2 ч.)

Лекция.·Воздействие информационной среды на социализацию современных детей и молодёжи (формирование зависимости, виртуализация сознания, «клиповое мышление»). Понятие «угроза информационной безопасности» и классификация угроз Понятие «угроза информационной безопасности». Классификация угроз. Технические угрозы (возможность повреждения ПО, информации, нарушение ее конфиденциальности или взлома аккаунта, хищения паролей и персональной информации). Коммуникационные угрозы (кибербуллинг,рекрутинг в опасные и экстремистские сообщества и др.). Контентные угрозы (закрытые группы смерти, группы «вписки» и др.). Потребительские угрозы (риск приобретения товара низкого

качества, подделок, контрафактной и фальсифицированной продукции, хищение денежных средств злоумышленником через онлайн-банкинг и т.д.)
Практическая работа.·Анализа аккаунтов в социальных сетях с целью выявления распространения информации, склоняющей к деструктивному поведению. Цель: совершенствование навыков выявления прямых и косвенных признаки деструктивного поведения на основании медиаконтента представленного на станице в социальной сети. Результат: формирование умения анализировать медиаконтент на предмет наличия информации склоняющей несовершеннолетних к деструктивному поведению.
Обеспечение информационной безопасности обучающихся в условиях образовательной организации (лекция - 4 ч. практическое занятие - 2 ч.)
Лекция.·Способы обеспечения информационной безопасности обучающихся в образовательной организации. Локальные акты образовательной организации, направленные на обеспечение медиабезопасности обучающихся. Методы защиты от вредоносного ПО. Требования к информационной безопасности при работе в общедоступных сетях Wi-fi.
Санитарно - гигиенические требования к организации занятий с использованием цифровых средств обучения. Алгоритм работы образовательной организации по мониторингу аккаунтов обучающихся в социальных сетях с целью выявления информации, склоняющей к деструктивному и противоправному поведению
Практическая работа.·Обеспечение информационной безопасности обучающихся в условиях образовательной организации. Решение кейсов. Цель: отработка навыков анализа проблемной ситуации и определение стратегии по обеспечению информационной безопасности обучающихся в образовательной организации, на основании представленной информации.
Результат: формирование умения оценивать информационные риски ситуации и выработка стратегии по обеспечению информационной безопасности обучающихся в условиях образовательной организации.
Развитие медиаграмотности и информационной культуры обучающихся
Медиаграмотность и информационная культура, способы формирования. (лекция - 6 ч.)
Лекция.·Информационная культура личности как часть общей культуры современного человека. Формирование у обучающихся навыков безопасного использования цифровых технологий. ·Понятие «персональные данные». Виды персональных данных. «Цифровые следы» и идентификация пользователей сетей. ·Средства защиты персональных данных. Приватность и личные границы в сети Интернет. Правила безопасных коммуникаций в сети Интернет.

Алгоритм действий при столкновении с ситуациями кибербуллинга, вовлечения в деструктивные Интернет-сообщества.
Технология девиантологического анализа медиапродукции (практическое занятие -4 ч.)
Практическая работа.·Проведение девиантологического анализа медиапродукции кинофильма/мультфильма/музыкального видеоклипа. Цель: совершенствование навыков анализа медиаконтента на предмет наличия деструктивных посылов для организации профилактической работы с обучающимися Результат: отработка практических навыков применения методики девиантологического анализа медиапродукции, оценка медиаконтентана предмет деструктивных посылов.