ФОРУМ ЦИФРОВОЙ БЕЗОПАСНОСТИ
(НЕДЕЛЯ БЕЗОПАСНОГО РУНЕТА - 2020)

ПОВЫШЕНИЕ КОМПЕТЕНТНОСТИ ПЕДАГОГОВ В ВОПРОСАХ ЦИФРОВОЙ БЕЗОПАСНОСТИ ДЕТЕЙ И ПОДРОСТКОВ

ТИМОФЕЕВА ЛИЛИЯ ЛЬВОВНА

к.п.н., доцент кафедры развития образовательных систем Института развития образования, г. Орел
Автор *парциальной программы* «Формирование культуры безопасности у детей 3—8 лет»,
соавтор пособий *предметной линии* «Окружающий мир» (УМК «Школа России»)

Научные подходы к обеспечению безопасности детей и подростков

Научные подходы к обеспечению безопасности человека по-разному трактуют функции индивида, возможности социальных систем:

- ***ограждающий подход*** (устранение опасностей или перемещение человека в безопасную среду);
- ***обучающий подход*** (формирование навыков безопасного поведения, обучение предвидению, распознаванию опасностей, способам поведения в опасных ситуациях);
- ***образовательный подход*** (формирование компетентности или готовности к распознаванию, предвидению, уклонению и преодолению опасностей как личностного образования, системы качеств, необходимых для успешного самообеспечения безопасности);
- ***личностно-развивающий подход*** (формирование личностной зрелости на основе поддержки становления ценностно-смысловой сферы человека и качеств субъекта жизни, устойчивости к негативным воздействиям, способности превращать опасности в фактор собственного развития)

Н.А. Лызь

Научные подходы к обеспечению безопасности детей и подростков

- ***безопасность как всесторонняя защита –*** системное понимание условий, приводящих к возникновению опасностей и их минимизация (J. Reason; C. Vincent, S. Taylor-Adams, N. Stanhope);
- ***теория высокой надежности и безопасности*** ориентирована на достижение безотказной работы системы в неопределенных и сложных условиях (K. Roberts, D. Rousseau);
- ***теория динамики и безопасности системы*** (A. Amalberti) отражает динамическое системное представление о безопасности и риске, психологические оценки поведенческих факторов, лежащих в основе нарушений (A. Amalberti);
- ***безопасность как коллективная осознанность*** предполагает постоянство усилий всех заинтересованных сторон для прогнозирования и сдерживания непредвиденных негативных обстоятельств (K. Weick, K. Sutcliffe, D. Obstfeld);
- ***безопасность как устойчивость*** – подход, фокусирующийся на повышении адаптивности индивида, развитии у него устойчивости в проблемных ситуациях (E. Hollnagel, D. Woods, N. Leveson).

Комплекс мер по обеспечению информационной безопасности детей и подростков

1) ***правовая защита***, заключающаяся в создании нормативно-правовой базы регулирования общественных отношений в этой области;
2) ***технологическая защита***, направленная на создание технических способов блокировки нежелательного контента, ограничения доступа к отрицательной информации, технические возможности осуществления родительского контроля за временем пребывания ребенка в сети и качественный анализ сайтов и интернет-сообществ, посещаемых детьми;
3) ***психолого-педагогические методы***, направленные на работу с ребенком по формированию его медиа и компьютерной грамотности, стратегий поведения при встрече с нежелательным контентом и опасными знакомыми в сети Интернет, формирование критического мышления по отношению к информации, получаемой в сети и др.

Е.М. Шпагина, Р.В. Чиркина

Готовность педагога обеспечивать информационную безопасность обучающихся

Количественный аспект. Для эффективного решения проблем защиты детей от угроз, связанных с воздействием информации, необходимо обеспечить охват не менее 70 процентов педагогических работников специальным обучением, направленным на повышение уровня их знаний и навыков в сфере информационной безопасности.

«Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учетом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности» (разработаны в соответствии с пунктом 8 приказа № 88 Минкомсвязи России от 27 февраля 2018 года «Об утверждении плана мероприятий по реализации Концепции ин-формационной безопасности детей на 2018—2020 годы»)

Качественный аспект. Требования профессионального стандарта «Педагог»

- необходимые знания,
- трудовые действия,
- необходимые умения.

Необходимые знания

Специфика детской популяции

- воздействие огромного прессинга неранжированной, чаще хаотической информации, что определяет изменения восприятия, сознания, мышления ребенка;
- значительные изменения в развитии потребностно-мотивационной и эмоционально-волевой, ценностной сфер;
- формирование качественно нового типа социализации, передачи знаний, противостоящего стационарному образованию, принципиально меняющего роль взрослого, преобладающие каналы восприятия детьми информации, моделей поведения и деятельности;
- интенсивная примитивизация сознания детей, рост цинизма, грубости, жестокости, агрессивности, за которыми кроются внутренние глубинные переживания ребенка — неуверенность, одиночество, страх, инфантилизм, эгоизм, духовная опустошенность *(по Д.И. Фельдштейну);*
- наблюдаются феномены изменения идентичности человека, появления виртуальных сообществ, новых форм агрессивного поведения (кибербуллинг, использование Интернета для реализации насильственных действий в реальности), кибераддикции *(Е.М. Шпагина, Р.В. Чиркина),* восприятие детьми «цифровой жизни» как реальной.

Необходимые знания

Угрозы, связанные с воздействием информации. Киберугрозы

1) Технологические угрозы, которые могут включать распространение вредоносных, шпионских программ, риск взлома.
2) Угрозы, связанные вредным или оскорбительным содержанием, с которым индивид сталкивается в сети Интернет.
3) Угрозы преследования, включающие в себя любую форму нежелательных контактов, внимания, издевательства, насилия, связанные с коммуникацией в сети Интернет.
4) Угрозы, определяющие возникновение рисков социализации и негативных изменений в развитии личности детей и подростков, нанесение вреда их физическому и (или) психическому здоровью.
5) Угрозы, сопряженные с ситуацией раскрытия личной или конфиденциальной информации, персональных данных.

Необходимые знания

Пути обеспечения информационной безопасности

- цели и задачи работы по защите детей от информации, причиняющей вред их здоровью и развитию;
- приоритетные направления, принципы и технологии обеспечения информационной безопасности, представленные в нормативных документах федерального и регионального уровней;
- роль информации в развитии детей и подростков, ее влияние на процессы социализации в разные возрастные периоды;
- подходы к формированию информационной культуры и медиаграмотности, повышению адаптивности детей к негативному влиянию информации;
- компоненты информационной среды, типовые информационные угрозы;
- критерии оценки и способы осуществления экспертизы информационной продукции, технические и программные средства защиты обучающихся.

Необходимые знания

Причины возникновения и факторы эскалации детской агрессии

- нарушение требований психологической безопасности в условиях семьи и в образовательной организации (во взаимодействии со сверстниками и педагогами);
- личностные особенности, неудовлетворительное состояние физического и психического здоровья обучающихся;
- неудовлетворенность базовых потребностей (в безопасности, самореализации, уважении, признании, общении, принадлежности к коллективу);
- недостаток положительных эмоций, преобладание запретов, объектная позиция обучающихся;
- неэффективность воспитательной работы в целом и ее направления, нацеленного на формирование детского коллектива с точки зрения теорий коллективного осознания и устойчивости;
- отсутствие правил взаимодействия, четко сформулированных и неукоснительно соблюдаемых в отношении всех участников образовательных отношений;
- недостаточных уровень компетентности педагогов (специалистов) в области обеспечения кибербезопасности детей, локализации конфликтных ситуаций, негативных проявлений в общении;
- влияние видеоигр, коммуникации в социальных сетях (A.K. Przybylski, N. Weinstein. 13.02.2019. https://doi.org/10.1098/rsos.171474).

Необходимые знания

Признаки детей, подвергшихся насилию

- частые пропуски уроков или прогулы в определенные дни или определенных уроков; опоздания на занятия, отказ от участия во внеурочных мероприятиях без объективных причин или по надуманным причинам;
- частые жалобы на плохое самочувствие на уроках;
- замкнутость, уход в себя, избегание друзей, одноклассников, самоизоляция или изоляция со стороны других обучающихся;
- резкое снижение успеваемости, потеря интереса к учебе и другой деятельности;
- недоверие к сверстникам и взрослым, низкая самооценка, неуверенность в себе;
- резкие и беспричинные перепады настроения; рассеянность, невнимательность, забывчивость, неспособность концентрироваться;
- постоянное или частое состояние тревожности, напряженности; пугливость, боязнь громких звуков и резких движений;
- постоянное или частое плохое настроение, состояние угнетенности, подавленности, или, наоборот, гиперактивности, раздражительности, агрессивности;
- частая потеря или порча личных вещей (мобильного телефона, рюкзака, учебников и др.), синяки, ссадины, порванная или измятая одежда;
- отказ объяснить причины вышеописанных состояний и поведения или явно неправдоподобные объяснения. *(Предотвращение насилия в образовательных организациях. Барнаул, 2017).*

Необходимые умения

Общепрофессиональные умения

- создавать условия, обеспечивающие психологическую безопасность индивида;
- обеспечивать субъектную позицию ребенка (подростка) в образовательном процессе, выстраивать доверительные взаимоотношения с учетом личностных особенностей обучающихся;
- развивать мотивационную сферу учения, обеспечивать удовлетворенность базовых потребностей;
- эффективно осуществлять воспитательную работу.

Специфические умения, связанные с вопросами цифровой безопасности

- способность ориентироваться в информационных потоках, идентифицировать потенциальные угрозы, связанные с отбором, оценкой и защитой информации, запрещенной для распространения среди детей;
- способность анализировать, оценивать и выбирать аппаратно-программные средства защиты информации в целях формирования инфобезопасной среды образовательной организации;
- готовность эффективно использовать комплекс мер противодействия несанкционированному информационному воздействию на личность учащегося с учетом правовых основ, разработанных аппаратно-программных средств защиты информации и экономической целесообразности. *(Ю.И. Богатырева)*

Необходимые меры

- Принятие решений об обязательной подготовке педагогов по вопросам обеспечения информационной безопасности детей и подростков.
- Разработка эффективных программ обучения будущих и действующих специалистов.
- Подготовка региональных тьюторов для обучения педагогов на уровне регионов.
- Проведение обучающих мероприятий ведущими специалистами страны в области обеспечения информационной (в частности, цифровой) безопасности детей и подростков в дистанционном режиме.
- Создание в регионах экспертных советов по обеспечению безопасности детей в инфосфере.
- Подготовка консультантов по обеспечению безопасности детей в инфосфере (information ecosystem), работающих на базе органов управления образованием, уполномоченных по правам человека, ППМС-центров, центров реабилитации и др.