1. Необходимо в комплексе рассматривать все существующие угрозы:
2. - технологические угрозы, сопряженные с распространением вредоносных, шпионских программ, риском взлома защитных систем персонального компьютера;
3. - угрозы, связанные вредным или оскорбительным содержанием, с которым индивид сталкивается в сети Интернет;
4. - угрозы преследования обучающихся, включающие в себя любую форму нежелательных контактов, внимания, издевательства, насилия, связанные с коммуникацией в сети Интернет;
5. - угрозы, сопряженные с ситуацией раскрытия личной или конфиденциальной информации, персональных данных;
6. - угрозы, определяющие возникновение рисков социализации и негативных изменений в развитии личности детей и подростков, нанесение вреда их физическому и (или) психическому здоровью информацией, независимо от источника ее получения. В соответствии с выделяемыми группами угроз определяются основные действия по обеспечению информационной безопасности детей в образовательной организации. Выделяют такой комплекс мер: - правовая защита обучающихся, заключающаяся в создании нормативно- правовой базы регулирования общественных отношений в области обеспечения информационной безопасности; - технологическая защита, направленная на создание технических способов блокировки нежелательного контента, ограничения доступа к отрицатель-ной информации, технические возможности осуществления родительского контроля за временем пребывания ребенка в сети и качественный анализ сайтов и интернет-сообществ, посещаемых детьми; - 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