УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И НАУКИ ЛИПЕЦКОЙ ОБЛАСТИ

ГАУДПО ЛИПЕЦКОЙ ОБЛАСТИ
«ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ»

Методические рекомендации для педагогических работников и родительской общественности по обеспечению информационной безопасности детей в сети Интернет

Авторы-составители:

Мещерякова Е.М., тьютор отдела организационно-методической работы ЦНППМПР ГАУДПО ЛО «ИРО», Ю.В. Грибцова, методист отдела организационно-методической работы ЦНППМПР ГАУДПО ЛО «ИРО»

Рассмотрено
на заседании учебно-методического
объединения «Управление в системе ОО»
Протокол № 4 от «23» декабря 2024 г.

Липецк
2024

Введение

Цифровая революция коренным образом изменила жизнь общества, и дети оказались в самом центре этих перемен. Интернет, некогда воспринимавшийся как исключительно полезный инструмент, сегодня представляет собой сложную и многогранную среду, наполненную как невероятными возможностями, так и значительными опасностями для несовершеннолетних.

Актуальность настоящих методических рекомендаций по обеспечению информационной безопасности детей в сети Интернет обусловлена рядом взаимосвязанных факторов, требующих пристального внимания со стороны общества, родителей и педагогов.

Выделяют шесть факторов:

1. Распространение цифровых технологий и ранний доступ к интернету. Современные дети получают доступ к интернету и мобильным устройствам в всё более раннем возрасте. Они проводят значительную часть времени онлайн, используя социальные сети, онлайн-игры и другие цифровые платформы. Этот ранний и часто неконтролируемый доступ делает их уязвимыми перед различными угрозами, которые они не всегда способны распознать и предотвратить самостоятельно.

2. Рост киберпреступности и новые формы угроз. Интернет стал площадкой для различных видов киберпреступности, причем её масштабы и изощренность постоянно растут. Кибербуллинг, онлайн-мошенничество, распространение вредоносного контента, онлайн-хищники – всё это представляет реальную угрозу для детей. Новые технологии и платформы постоянно генерируют новые виды угроз, требующие постоянного анализа и адаптации методов защиты.

3. Психологические последствия. Воздействие негативного онлайн-контента, кибербуллинга и других форм интернет-преследований может иметь серьёзные психологические последствия для детей. Это может привести к депрессии, тревожным расстройствам, снижению самооценки, социальной изоляции, а в тяжелых случаях – даже к суицидальным мыслям.

4. Отсутствие должного уровня осведомленности. Многие родители и педагоги не в полной мере осознают все риски, связанные с использованием

интернета детьми. Недостаток знаний и навыков в области информационной безопасности приводит к тому, что дети остаются без должной защиты.

5. Законодательные и этические аспекты. Законодательство, регулирующее информационную безопасность детей, часто отстает от темпов развития технологий. Кроме того, существует ряд этических вопросов, связанных с мониторингом онлайн-активности детей и балансом между безопасностью и правом на частную жизнь.

6. Трансграничный характер угроз. Киберпреступность носит глобальный характер. Это означает, что угрозы для детей могут исходить из любой точки мира, что значительно усложняет их предотвращение и расследование.

К сожалению, не существует единой, общепринятой и строго формализованной классификации информационных угроз в сети Интернет. Различные исследователи и организации используют различные подходы, часто пересекающиеся и дополняющие друг друга. Однако, можно выделить наиболее часто встречающиеся категории, которые охватывают большинство известных угроз.

Каждый раздел настоящих методических рекомендаций соответствует категории информационных угроз в сети Интернет.

В разделах с 1 по 6 содержится информация, позволяющая различать вид информационной угрозы, знать её феномен с разных аспектов, определять признаки вовлечения: явные и скрытые, поведенческие и онлайн-признаки, идеологические и мировоззренческие.

В разделе 7 содержатся рекомендации, позволяющие обеспечить информационную безопасность детей в семье и образовательной организации.

В разделе 8 содержатся рекомендуемые современные ресурсы по информационной безопасности для учеников (видеолекции, проекты. Исследования. Уроки. Книги и др.), созданные при поддержке государства, профильных фондов, центров, ведущих цифровых компаний, в том числе с официальных сайтов организаций Липецкой области, рекомендуемых к сотрудничеству и взаимодействию.

Раздел 9 содержит список используемых нормативных документов.

СОДЕРЖАНИЕ

1. Социальные угрозы

1.1. Экстремальные увлечения молодежи

Увлечение экстремальным досугом само по себе не является угрозой, но его онлайн-проявления могут создавать серьезные риски. Интернет, с одной стороны, предоставляет огромные возможности для получения информации, общения с единомышленниками и организации мероприятий, связанных с экстремальными видами спорта и отдыха. С другой стороны, он же становится площадкой для распространения опасного контента, стимулирования неоправданного риска и подражания, что может привести к травмам или смерти.

Вот основные аспекты, делающие увлечение экстремальным досугом угрозой в сети Интернет:

- **Романтизация риска:** Интернет часто наполнен видеозаписями и фотографиями, изображающими экстремальные виды деятельности в романтизированном или героическом свете. Это может побуждать к неоправданному риску и неадекватному оценке своих способностей. Подростки и молодые люди особенно уязвимы к такой пропаганде.
- **Недостаточная информация о безопасности:** онлайн-сообщества и форумы, посвященные экстремальным видам спорта, могут содержать неполную или неверную информацию о технике безопасности. Недостаток знаний и опыта может привести к серьезным травмам или смерти.
- **Влияние пиара и рекламы:** экстремальные виды спорта часто продвигаются через яркие видеоролики и фотографии в социальных сетях. Такой маркетинг может создавать иллюзию легкости и доступности экстремальных деятельностей, не уделяя достаточного внимания рискам.
- **Подражание:** видеролики с захватывающими кадрами экстремального досуга стимулируют подражание. Люди, не имеющие достаточного опыта и подготовки, могут пытаться повторить виденное на видео, что может привести к несчастным случаям.

- **Отсутствие контроля и регуляции:** в онлайн-пространстве сложно контролировать распространение небезопасного контента и предотвратить участие неподготовленных людей в опасных деятельностях.
- **Онлайн-вызовы и челленджи:** экстремальные челленджи и онлайн-вызовы в социальных сетях могут стимулировать опасное поведение, побуждая к необдуманным действиям и риску ради популярности.

Виды экстремальных досуговых предпочтений подростков

Руфинг – прогулки по крышам высотных зданий, а также по другим сооружениям (вышкам, опорам ЛЭП и т. д.).

Зацепинг – проезд вне салона электрички или трамвая (на крыше, на подножке).

Роупджампинг - прыжки с высоты с использованием специального каната (троса), прикрепленного к телу прыгуна.

Паркур – перемещение и преодоление попадающихся на пути препятствий (стен, лестниц и т.д.), сочетает в себе множество сложных и опасных трюков: кувырки, прыжки с опорой на руки.

Диггерство – спуск и изучение подземных коммуникаций (бункеры, колодцы, шахты, тоннели метро, водосточные системы, бомбоубежища и пр.).

Скайуокинг – покорение самых высоких точек в городе без специального снаряжения.

Сталкерство – посещение и изучение заброшенных мест.

Акрострит – уличная акробатика, предполагающая выполнение сложных и опасных трюков: стойка на голове, прыжки с возвышенностей, сальто.

Бейскламбинг – подъем на большую высоту без страховки.

Признаки вовлечения

Явные признаки:

- **Изменение поведения:** появление рискованного поведения, не характерного для подростка ранее. Это может проявляться в форме неоправданной агрессии, импульсивности, пренебрежения безопасностью.
- **Новые знакомства:** появление новых друзей или онлайн-знакомств, которые делят интерес к экстремальным видам досуга. Обратите внимание на их возраст и поведение.
- **Изменение круга интересов:** резкий сдвиг интересов в сторону экстремальных видов спорта, туризма или других рискованных занятий. Подросток может посвящать большую часть своего времени изучению информации по этой теме.
- **Покупка специального оборудования:** появление необычного для подростка оборудования или снаряжения, которое может быть связано с экстремальными видами досуга.
- **Участие в рискованных мероприятиях:** участие в мероприятиях, которые представляют угрозу для жизни и здоровья, без необходимой подготовки и обеспечения безопасности.
- **Рассказы о своих подвигах:** подросток может хвастаться своими достижениями в экстремальных видах досуга, при этом не уделяя внимания рискам и опасностям.

Скрытые признаки:

- **Изменение онлайн-активности:** появление новых подписок на каналы YouTube или группы в социальных сетях, посвященные экстремальным видам досуга.
- **Секретность:** подросток может стать более закрытым и скрытным, не желающим делиться информацией о своих планах и деятельности.

- **Проблемы со сном:** нарушение сонного цикла, бессонница могут быть связаны с возбуждением и переживаниями, связанными с экстремальными видами досуга.
- **Изменение в отношениях:** напряжение в отношениях с семьей и друзьями из-за недостатка времени или постоянного стремления к приключениям.
- **Финансовые затраты:** неожиданные и подозрительные финансовые расходы, связанные с покупкой оборудования или участием в мероприятиях.

1.2. Феномен «Колумбайн» («Скулшутинг»)

Термин «Колумбайн» (в контексте интернет-угроз) стал синонимом школьной стрельбы (скулшутинга) и обозначает не саму стрельбу как событие, а определенный тип угрозы, связанной с планированием и вдохновением подобных актов насилия в онлайн-пространстве. Он не является отдельной угрозой, а скорее обозначает феномен, включающий несколько аспектов:

- **Глорификация насилия:** в интернете существует множество материалов, восхваляющих или романтизирующих школьные стрельбы. Это может включать видеоролики, изображения, тексты, посвященные стрелкам и их действиям. Такая глорификация может служить вдохновением для других людей, испытывающих подобные мысли.
- **Распространение идеологии ненависти:** онлайн-платформы часто используются для распространения идеологии ненависти и экстремизма, которые могут послужить почвой для планирования насильственных актов. Это может включать в себя расистские, сексистские или другие формы нетерпимости.
- **Создание онлайн-сообществ:** существуют онлайн-сообщества, где общаются люди, испытывающие агрессию и ненависть, а также те, кто планирует или мечтает о совершении насильственных актов. Эти сообщества могут

служить площадкой для обмена идеями, планами и поддержки друг друга в их намерениях.

- **Имитация и подражание:** некоторые люди могут пытаться повторить или скопировать действия стрелков из прошлых школьных стрельб. Это может быть мотивировано желанием получить известность, внимание или отомстить.
- **Доступность информации:** Интернет предоставляет доступ к информации о том, как совершить насильственные акты, включая инструкции по изготовлению оружия и планированию атак.

Признаки вовлечения

Поведенческие признаки:

Резкое изменение поведения: появление агрессии, изоляции, депрессии, резких перепадов настроения, апатии, отсутствие интереса к прежним увлечениям.

- **Обособление:** подросток может стать закрытым, избегать общения с семьей и друзьями, проводить много времени в своей комнате за компьютером.
- **Обсессия насилием:** появление интереса к темам насилия, смерти, оружия, терроризма. Это может проявляться в просмотре соответствующего контента в интернете, чтении книг и статей на эти темы.
- **Глорификация стрелков:** идеализация личности стрелков из прошлых школьных стрельб, восхищение их действиями.
- **Создание рисунков и творчества на тематику насилия:** наличие рисунков, стихов, историй, видеороликов, содержащих сцены насилия, оружия или смерть.
- **Общение с подозрительными людьми:** появление новых друзей или онлайн-знакомств, которые делят интерес к насилию и экстремизму.

- **Угрозы на реальность:** прямые или косвенные угрозы насилием в отношении себя или других. Это могут быть устные угрозы, записи в дневнике или сообщения в интернете.
- **Поиск информации об оружии и взрывчатке:** попытки найти информацию о том, как изготовить или приобрести оружие, взрывчатые вещества или другие средства нанесения вреда.
- **Планирование актов насилия:** появление планов или записей, свидетельствующих о планировании насильственных действий.

Онлайн-признаки:

- **Посещение подозрительных сайтов и форумов:** подросток может посещать сайты и форумы, посвященные насилию, экстремизму и школьным стрельбам.
- **Участие в онлайн-группах:** участие в онлайн-группах, где прославляется насилие или обсуждаются планы насильственных действий.
- **Просмотр соответствующего контента:** просмотр видеороликов, пропагандирующих насилие, и другого подозрительного контента.

2. Социально-психологические угрозы

2.1. Экстремистская деятельность

Экстремистская деятельность в интернете представляет собой серьезную угрозу, так как он предоставляет мощные инструменты для распространения экстремистской идеологии, вербовки новых членов и планирования террористических актов. Опасность заключается в следующих аспектах:

1) Пропаганда и вербовка:

- **Распространение экстремистской идеологии:** Интернет позволяет экстремистским группам быстро и широко распространять свою пропаганду, используя различные платформы: социальные сети, форумы, мессенджеры,

видеохостинги. Они используют привлекательные для определенных групп населения лозунги, манипулируют эмоциями и используют различные методы психологического воздействия.

- **Целенаправленная вербовка:** экстремистские организации активно ищут новых членов онлайн, используя социальные сети для поиска уязвимых лиц, например, подростков, людей, испытывающих чувство одиночества или социальной изоляции, или тех, кто ищет смысл жизни.
- **Онлайн-радикализация:** постоянное воздействие экстремистской пропаганды может привести к радикализации пользователей, усиливая их ненависть и агрессию по отношению к определенным группам людей или государству.

2) Планирование и координация:

- **Планирование терактов и других преступлений:** Интернет используется для координации действий экстремистских групп, планирования терактов и других преступных актов. Закрытые чаты и форумы позволяют обмениваться информацией, координировать действия и обсуждать стратегию.
- **Обучение и инструктаж:** онлайн-платформы служат для распространения инструкций по изготовлению взрывных устройств, использованию оружия и других методов насилия.

3) Дезинформация и фейковые новости:

- **Распространение дезинформации:** экстремистские организации используют интернет для распространения ложной и искаженной информации, с целью манипулирования общественным мнением, подрыва доверия к государственным институтам и провоцирования социальных конфликтов.
- **Создание фейковых новостей:** фейковые новости и манипуляции используются для достижения политических или идеологических целей экстремистских организаций.

4) Труднодоступность и скрытность:

- **Использование криптографии и анонимных сетей:** экстремисты используют шифрование и анонимные сети (например, Tor), чтобы избежать обнаружения и преследования правоохранительными органами.
- **Использование кодировки и символики:** для скрытой коммуникации могут использоваться специальные коды и символы, понятные только членам экстремистских групп.

Признаки вовлечения

Идеологические и мировоззренческие признаки:

- **Резкое изменение мировоззрения:** появление новых, радикальных взглядов, не совпадающих с прежними убеждениями подростка или семейными ценностями. Это может проявляться в форме резкой критики существующего строя, властей, религиозных или этнических групп.
- **Обострение националистических или религиозных чувств:** чрезмерная приверженность к своей национальности или религии, нетерпимость к другим культурам и религиям.
- **Идеализация экстремистов:** появление восхищения или идолопоклонства по отношению к экстремистским лидерам или деятелям.
- **Отрицание общепринятых норм и законов:** оправдание насилия и экстремизма, отрицание значения законов и правил общежития.
- **Пропаганда насилия и нетерпимости:** распространение экстремистских идей среди своих знакомых и друзей.

Поведенческие признаки:

- **Изменение круга общения:** появление новых друзей или знакомств, придерживающихся экстремистских взглядов.
- **Секретность:** подросток становится более закрытым, скрывает свои дела и общение.

- **Изменение интересов:** резкая смена интересов в сторону экстремистской идеологии и пропаганды.
- **Резкое изменение поведения:** появление агрессии, раздражительности, депрессии, потеря интереса к учебе и другим видам деятельности.
- **Участие в незаконных акциях:** участие в несанкционированных митингах, демонстрациях или других акциях протеста.
- **Поддержка экстремистских организаций:** финансовая или иная поддержка экстремистских организаций.
- **Изучение методов ведения боевых действий:** поиск информации о методах ведения боевых действий, изготовлении взрывных устройств или других видах военного дела.

Онлайн-признаки:

- **Посещение экстремистских сайтов и форумов:** подросток посещает сайты и форумы, пропагандирующие экстремистские идеи.
- **Участие в экстремистских группах в социальных сетях:** участие в онлайн-группах, где распространяются экстремистские материалы и идеи.
- **Распространение экстремистского контента:** подросток распространяет экстремистские материалы через социальные сети или другие онлайн-каналы.

2.2. Суицидальные сообщества

Суицидальные сообщества в интернете представляют собой серьёзную угрозу, особенно для подростков и молодых людей, испытывающих эмоциональные трудности или склонность к самоповреждению. Эти сообщества, часто скрытые и существующие на различных платформах (форумы, социальные

сети, мессенджеры), объединяют людей, имеющих суицидальные мысли или склонность к самоповреждению. Угроза заключается в нескольких аспектах:

- **Нормализация суицидальных мыслей**

В таких сообществах суицидальные мысли и самоповреждение часто представляются как нормальное или даже желательное поведение. Общение с людьми, разделяющими подобные взгляды, укрепляет эти мысли и может подтолкнуть к действию.

- **Подстрекательство к суициду**

В некоторых сообществах могут присутствовать пользователи, активно подстрекающие к совершению суицида или самоповреждения, часто используя манипулятивные техники и психологическое давление.

- **Создание «культуры смерти»**

В таких сообществах формируется специфическая культура, где смерть романтизируется, а суицид представляется как решение всех проблем. Это может быть особенно опасно для молодых людей с низкой самооценкой и отсутствием поддержки в реальной жизни.

- **Распространение методов суицида**

В этих сообществах может происходить обмен информацией о методах совершения суицида, что делает их более доступными и увеличивает риск летального исхода.

- **Отсутствие контроля и модерации**

Многие суицидальные сообщества существуют в «серых зонах» интернета, где модерация слаба или отсутствует вовсе. Это позволяет распространяться опасной информации и деструктивному влиянию без каких-либо ограничений.

- **Затрудненное выявление**

Распознать суицидальные сообщества не всегда просто. Они часто маскируются под группы поддержки или сообщества по интересам, используя завуалированный язык и скрытую символику.

- **Усиление чувства изоляции**

Хотя такие сообщества создают иллюзию поддержки, они на самом деле могут усиливать чувство изоляции и безнадежности, усугубляя суицидальные наклонности.

Признаки вовлечения

Поведенческие признаки:

- **Резкое изменение настроения и поведения:** появление депрессии, апатии, раздражительности, агрессии, резких перепадов настроения, бессонницы или, наоборот, чрезмерной сонливости.
- **Изоляция и отстраненность:** подросток может избегать общения с семьей и друзьями, замыкаться в себе, терять интерес к прежним увлечениям и занятиям.
- **Самоповреждающее поведение:** появление порезов, ожогов, других телесных повреждений, нанесение себе увечий.
- **Употребление психоактивных веществ:** попытки справиться с состоянием с помощью алкоголя, наркотиков или других психоактивных веществ.
- **Разговоры о смерти и самоубийстве:** прямые или косвенные упоминания о смерти, самоубийстве, желании умереть. Это могут быть разговоры, записи в дневнике, сообщения в социальных сетях.
- **Прощальные записки:** написание прощальных писем или сообщений близким людям.
- **Изменение внешнего вида:** неухоженность, отказ от личной гигиены.
- **Потеря интереса к жизни:** подросток может выражать пессимистические взгляды на будущее, отсутствие целей и планов.
- **Поиск информации о самоубийстве:** попытки найти информацию о методах самоубийства в интернете или из других источников.

Онлайн-признаки:

- **Посещение просуицидальных сайтов и форумов:** подросток может посещать сайты и форумы, где обсуждаются темы самоубийства и суицидального поведения. Обращайте внимание на группы в социальных сетях с подобной тематикой.
- **Участие в онлайн-группах, пропагандирующих суицид:** вступление в онлайн-сообщества, где прославляется суицид или обсуждаются методы самоубийства.
- **Создание контента с просуицидальной тематикой:** публикация рисунков, стихов, видеороликов или других материалов, содержащих сцены самоубийства или пропагандирующих суицид.
- **Общение с пользователями, пропагандирующими суицид:** подросток может общаться в онлайн-пространстве с людьми, которые поощряют его суицидальные намерения.

3. А.У.Е. (Арестантский Уклад Единый)

Субкультура, зародившаяся в местах лишения свободы и распространившаяся в интернете, представляющая собой серьёзную угрозу для подростков и молодёжи. Она пропагандирует криминальный образ жизни, культивирует насилие, жестокость и презрение к закону. Интернет стал мощным инструментом для распространения идеологии АУЕ, позволяя ей выходить за пределы тюрем и влиять на неокрепшие умы. Опасность АУЕ заключается в следующем:

- **Рекрутирование несовершеннолетних:** АУЕ активно вербует подростков и молодёжь через социальные сети, мессенджеры и другие онлайн-платформы. Используются привлекательные для подростков образы силы, братства и принадлежности к «крутому» сообществу. Часто используется манипуляция и психологическое давление.
- **Пропаганда насилия и криминала:** в Интернете распространяется большое количество контента, прославляющего криминальный мир, насилие и

жестокость. Это формирует у подростков искажённое представление о реальности и может подтолкнуть к совершению противоправных действий.

- **Формирование криминального мировоззрения:** АУЕ пропагандирует презрение к закону, правоохранительным органам и общественным нормам. Это может привести к формированию у подростков антиобщественного поведения и склонности к совершению преступлений.
- **Создание замкнутых сообществ:** в Интернете создаются закрытые группы и сообщества, где происходит обмен идеологическими материалами, подстрекательство к противоправным действиям и разработка планов совершения преступлений.
- **Использование символики и кодов:** АУЕ использует специфическую символику и кодировку сообщений, что затрудняет обнаружение и пресечение противоправной деятельности.
- **Влияние на реальный мир:** идеология АУЕ не ограничивается виртуальным пространством и активно проявляется в реальной жизни. Это может привести к участию подростков в преступной деятельности, насильственным действиям и другим правонарушениям.

Признаки вовлечения

Поведенческие признаки:

- **Резкое изменение поведения:** появление агрессии, жестокости, неуважения к старшим, нарушения дисциплины в школе или дома.
- **Изменение круга общения:** появление новых друзей, которые демонстрируют агрессивное поведение, используют специфическую терминологию и символику АУЕ.
- **Использование символики АУЕ:** ношение одежды или аксессуаров с символикой АУЕ (например, татуировки, рисунки, надписи на одежде). Обращайте внимание на рисунки, надписи в тетрадях или на личных вещах.

- **Использование терминологии АУЕ:** использование в речи специфических слов и выражений, характерных для АУЕ.
- **Проявление культуры «блатных» и «зеков»:** подражание поведению, манерам и образу жизни заключенных.
- **Интерес к криминальной культуре:** появление интереса к криминальной литературе, фильмам и музыке, прославляющим жизнь в зоне.
- **Защита криминальных ценностей:** оправдание криминальных деяний, противоправного поведения, негативное отношение к закону и правоохранительным органам.
- **Попытки вовлечения других подростков:** попытки вовлечь своих сверстников в АУЕ или пропаганда идей АУЕ среди друзей.
- **Физическая сила и угрозы:** использование физической силы для установления своего доминирования в школе или вне школы.
- **Шантаж и вымогательство:** попытки вымогательства денег или вещей у других подростков.

Онлайн-признаки:

- **Посещение сайтов и сообществ АУЕ:** просмотр материалов АУЕ в интернете, общение на форумах и в группах, посвященных АУЕ.
- **Распространение символики АУЕ в онлайне:** использование символики АУЕ в аватарках, статусах в социальных сетях или в других онлайн-материалах.

4. Груминг и секстинг

Груминг и секстинг – это две тесно связанные угрозы в сети Интернет, особенно опасные для детей и подростков. Они часто идут рука об руку, при этом груминг используется как инструмент для подготовки к секстингу и дальнейшей сексуальной эксплуатации.

Груминг – это процесс постепенного завоевания доверия ребенка или подростка со стороны взрослого с целью сексуальной эксплуатации. Онлайн-

среда предоставляет преступникам уникальные возможности для осуществления груминга:

- **Анонимность:** преступники могут скрывать свою личность и использовать фальшивые профили в социальных сетях или мессенджерах.
- **Доступность:** они могут постоянно поддерживать контакт с жертвой, используя различные цифровые каналы.
- **Манипуляция:** они умело манипулируют чувствами ребенка, завоевывая его доверие и создавая иллюзию дружеских или романтических отношений.
- **Постепенность:** процесс груминга занимает время. Преступник постепенно выстраивает отношения с ребенком, завоевывая его доверие и подготавливая его к сексуальной эксплуатации.
- **Использование технологий:** преступники используют видеозвонки, игры, обмен фотографиями и видео для установления контакта и манипуляции ребенком.

Секстинг – это обмен интимными фотографиями или видеороликами через цифровые каналы. В контексте груминга, секстинг часто используется как шаг к дальнейшей эксплуатации:

- **Шантаж:** преступник может шантажировать ребенка, угрожая опубликовать интимные материалы, если он откажется от дальнейшего взаимодействия.
- **Вымогательство:** преступник может требовать деньги или другие услуги в обмен на неразглашение интимных материалов.
- **Распространение:** интимные фотографии и видео могут быть распространены среди других лиц, что приведет к публичному унижению и серьезным психологическим травмам.

Признаки груминга

- **Новые онлайн-знакомства:** появление новых друзей или онлайн-знакомств, особенно взрослых людей, с которыми подросток проводит много времени онлайн. Обращайте внимание на скрытность общения.

- **Изменение поведения:** подросток становится более скрытным, закрытым, избегает общения с семьей и друзьями, проводит много времени онлайн.
- **Получение подарков и денег:** подросток получает подарки, деньги или другие материальные блага от взрослого человека, которого он знает онлайн.
- **Сексуально окрашенные разговоры:** подросток участвует в онлайн-разговорах сексуального характера со взрослым человеком.
- **Повышенное внимание к себе:** взрослый проявляет чрезмерное внимание к подростку, делает комплименты, выражает восхищение, манипулирует его самооценкой.
- **Доверительные отношения:** взрослый настаивает на исключительной близости отношений, на доверии и секретности, выстраивает с подростком доверительные отношения.
- **Манипуляции и шантаж:** взрослый использует манипуляции, угрозы или шантаж, чтобы контролировать подростка и заставить его делать то, что он хочет.

Признаки секстинга

- **Скрытность использования гаджетов:** подросток старается скрывать свое общение в онлайне, закрывает экран компьютера или телефона, когда к нему подходят.
- **Наличие фотографий и видео интимного характера:** обнаружение на гаджетах подростка фотографий или видео интимного характера, которые он сам сделал или получил.
- **Необычные сообщения:** получение или отправка сообщений сексуального характера через различные каналы связи (SMS, мессенджеры, социальные сети).
- **Стресс и тревога:** подросток может испытывать стресс, тревогу или депрессию, связанные с секстингом.

- **Внезапное изменение поведения:** подросток может резко измениться в поведении после того, как отправил или получил интимные фотографии или видео.
- **Чувство вины и стыда:** подросток может испытывать чувство вины и стыда из-за участия в секстинге.

5. Социально-технологические угрозы

5.1. Кибербуллинг

Кибербуллинг – это форма преследования и издевательств, осуществляемая с использованием цифровых технологий. Он представляет собой серьезную угрозу для подростков и молодых людей, так как может иметь разрушительные последствия для их психического здоровья и благополучия. В отличие от традиционного буллинга, кибербуллинг имеет ряд особенностей, усугубляющих его негативное воздействие.

Ключевые характеристики кибербуллинга:

- **Анонимность:** зачастую буллеры скрывают свою личность, что позволяет им действовать безнаказанно и с большей агрессивностью. Анонимность затрудняет выявление и наказание обидчиков.
- **Доступность:** жертва может подвергаться преследованию в любое время и в любом месте, где есть доступ к интернету. От этого нет убежища. Буллинг может преследовать жертву 24/7.
- **Распространение:** информация, распространяемая в интернете, может быстро распространиться среди широкой аудитории, увеличивая масштабы травли и унижения. Удаление информации часто бывает невозможным или очень сложным.
- **Постоянство:** онлайн-издевательства могут сохраняться в интернете на неопределенный срок, нанося постоянный эмоциональный ущерб жертве. Скриншоты и видео могут долго циркулировать, постоянно напоминая о травле.

- **Многогранность:** кибербуллинг может принимать различные формы: текстовые сообщения (оскорбления, угрозы), посты в социальных сетях (оскорбительные комментарии, фальшивые профили), распространение компрометирующих фотографий или видео (доксинг, секстинг), намеренное исключение из онлайн-групп.

Формы кибербуллинга:

- **Прямое преследование:** оскорбления, угрозы, шантаж, обращение с оскорблениями.
- **Непрямое преследование:** распространение слухов и сплетен, создание фейковых профилей, унизительные комментарии.
- **Исключение из групп:** умышленное удаление из онлайн-групп или игнорирование.
- **Доксинг:** публикация личной информации жертвы без ее согласия.
- **Стимпинг:** создание фейковых аккаунтов для преследования.
- **Сайбершейминг:** публичное унижение и осуждение.
- **Кибersталкерство:** постоянное преследование в онлайн-среде.

Последствия кибербуллинга:

- **Психическое здоровье:** депрессия, тревога, низкая самооценка, стресс, самоповреждение, суицидальные мысли.
- **Физическое здоровье:** проблемы со сном, головные боли, расстройства пищевого поведения.
- **Социальная адаптация:** изоляция, трудности в общении, снижение успеваемости.

Признаки кибербуллинга

Поведенческие признаки:

- **Изменения в настроении:** ребенок становится более раздражительным, тревожным, депрессивным, апатичным, либо демонстрирует резкие перепады настроения.

- **Избегание общения:** ребенок может избегать общения с семьей и друзьями, отказываться от совместных прогулок и мероприятий.
- **Проблемы со сном:** рарушение сна, бессонница или, наоборот, чрезмерная сонливость.
- **Изменения в академической успеваемости:** снижение успеваемости в школе, отказ от участия в учебном процессе.
- **Физические симптомы:** головные боли, боли в животе, тошнота, другие соматические проявления стресса.
- **Изменение аппетита:** снижение или повышение аппетита.
- **Самоповреждение:** появление порезов, ожогов, других телесных повреждений.
- **Ухудшение самооценки:** ребенок может говорить о себе негативно, выражать чувство безнадежности и беспомощности.
- **Скрытность использования гаджетов:** ребенок старается скрывать свое общение в онлайне, закрывает экран компьютера или телефона, когда к нему подходят.

Онлайн-признаки:

- **Резкое изменение онлайн-активности:** ребенок может внезапно прекратить общение в социальных сетях или играх, избегать онлайн-встреч с друзьями.
- **Нежелание пользоваться гаджетами:** ребенок может отказываться пользоваться гаджетами или быть более раздражительным во время пользования ими.
- **Необычные сообщения:** получение угроз, оскорблений, издевательств через социальные сети, мессенджеры или игры.
- **Появление незнакомых номеров или пользователей:** в истории сообщений ребенка могут появиться незнакомые номера или пользователи, с которыми он активно общается.

5.2. Наркоторговля в Даркнет

Наркоторговля в Даркнет представляет собой серьезную угрозу, поскольку она обеспечивает анонимность и скрытность для продавцов и покупателей наркотиков, значительно затрудняя работу правоохранительных органов. Это создает ряд проблем:

- **Анонимность и скрытность:** Даркнет, благодаря своей анонимной инфраструктуре (например, Tor), позволяет продавцам и покупателям наркотиков скрывать свои личные данные и местоположение. Это значительно усложняет расследование и пресечение преступной деятельности.
- **Глобальный характер:** торговля наркотиками в Даркнет имеет глобальный характер, преодолевая географические границы и национальное законодательство. Это делает ее особенно трудно контролируемой.
- **Разнообразие наркотиков:** в Даркнет можно найти практически любые виды наркотиков, включая синтетические вещества и новые психоактивные вещества (НПВ), информация о которых может быть ограничена. Это представляет дополнительную опасность для покупателей, которые могут не знать о действии и потенциальных последствиях употребления таких веществ.
- **Легкость доступа:** для доступа к наркотикам в Даркнет не требуется сложных технических навыков. Многие сайты имеют интуитивно понятный интерфейс и принимают криптовалюты, что делает покупку наркотиков относительно простой.
- **Реклама и пропаганда:** продавцы наркотиков в Даркнет активно продвигают свой товар, используя различные маркетинговые стратегии, включая рекламу на других сайтах и форумах.
- **Связь с другими видами преступности:** наркоторговля в Даркнет часто связана с другими видами преступной деятельности, такими как отмывание денег, киберпреступления и терроризм.

Признаки вовлечения

Поведенческие признаки:

- **Изменение поведения:** резкое изменение поведения, нехарактерное для подростка. Это может проявляться в агрессии, раздражительности, депрессии, апатии, резких сменах настроения, потеря интереса к учёбе и прежним увлечениям.
- **Изменение круга общения:** появление новых друзей, с которыми подросток проводит много времени и о которых он неохотно рассказывает.
- **Скрытность:** подросток становится более скрытным, закрытым, избегает общения с семьей и друзьями.
- **Проблемы со сном:** нарушение сна, бессонница или, наоборот, чрезмерная сонливость.
- **Изменения в академической успеваемости:** снижение успеваемости в школе, пропуски занятий, отказ от учёбы.
- **Физические симптомы:** необъяснимые физические симптомы, например, расширенные или суженные зрачки, покраснение глаз, тремор рук, необычный запах от тела или одежды.
- **Изменение аппетита:** снижение или повышение аппетита.
- **Небрежный внешний вид:** неухоженность, отказ от личной гигиены.
- **Финансовые проблемы:** просьбы о деньгах, пропажа денег из дома, кражи денег или вещей.
- **Необычные предметы:** появление необычных предметов в комнате подростка (шприцы, трубки, пакеты, необычные порошки).
- **Изменение речи:** невнятная речь, замедленная или ускоренная речь.

Онлайн-признаки:

- **Поиск информации о наркотиках:** поиск информации о наркотиках в интернете.
- **Общение в онлайн-группах:** общение в онлайн-группах, где обсуждается употребление наркотиков.
- **Использование специфической терминологии:** использование в речи специфических слов и выражений, связанных с наркотиками

6. Психологические и техно-психологические угрозы

6.1. Феномен онлайн-игровой зависимости

Онлайн-игровая зависимость представляет собой серьёзную угрозу, влияющую на психическое и физическое здоровье, социальную адаптацию и образование. Интернет, с его доступностью и разнообразием онлайн-игр, значительно усиливает эту угрозу. Ключевые аспекты проблемы:

- **Легкий доступ:** онлайн-игры доступны практически круглосуточно, из любого места с доступом в интернет. Это создает идеальные условия для развития зависимости, так как пользователь может играть в любое время, не ограничиваясь временем и местоположением.
- **Постоянная стимуляция:** многие онлайн-игры разработаны таким образом, чтобы постоянно стимулировать игрока, используя механизмы поощрения и награды. Это может приводить к постоянному желанию играть и трудностям с самоконтролем.
- **Социальная изоляция:** зависимость от онлайн-игр часто приводит к социальной изоляции. Игроки проводят много времени в виртуальном мире, пренебрегая реальной жизнь, общением с друзьями и семьей.
- **Физические проблемы:** проведение много времени за компьютером может привести к различным физическим проблемам, таким как нарушение зрения, остеохондроз, ожирение, и нарушение сонного цикла.
- **Психические проблемы:** онлайн-игровая зависимость часто сопровождается депрессией, тревогой, низкой самооценкой и другими психическими расстройствами.
- **Проблемы в образовании и работе:** зависимость может привести к снижению успеваемости в школе или университете.
- **Финансовые проблемы:** игроки могут тратить значительные суммы денег на покупку виртуальных предметов, донат и сами игры.

- **Семейные конфликты:** зависимость от онлайн-игр может привести к серьёзным семейным конфликтам из-за недостатка внимания к близким людям и проблем с коммуникацией.

Признаки вовлечения

Поведенческие признаки:

- **Чрезмерное время за играми:** подросток проводит за играми значительно больше времени, чем планировал или чем это допустимо для его возраста и обязанностей (учеба, сон, общение с семьей). Это может быть несколько часов в день или даже большую часть суток.
- **Пренебрежение другими сферами жизни:** подросток пренебрегает школьными обязанностями, домашними делами, личной гигиеной, встречами с друзьями и семьей ради игры. Ухудшение успеваемости в школе, пропуски занятий становятся частыми.
- **Изменение настроения:** резкие перепады настроения, раздражительность, агрессия, депрессия, апатия вне игры. Возможны вспышки гнева при попытке прервать игру.
- **Проблемы со сном:** бессонница, нарушения сна, сонливость в течение дня из-за ночных игровых сессий.
- **Физические проблемы:** головные боли, боли в спине, проблемы со зрением, остеохондроз из-за длительного сидения за компьютером.
- **Социальная изоляция:** подросток может избегать общения с семьей и друзьями в реальном мире, предпочитая виртуальное общение с игровыми товарищами.
- **Ложь и скрытность:** подросток может скрывать от родителей или других взрослых сколько времени он проводит за играми, заниматься этим тайно.
- **Финансовые проблемы:** подросток может тратить деньги на внутриигровые покупки, не сообщая об этом родителям, или просить деньги на игру.

Онлайн-признаки:

- **Чрезмерная активность в онлайн-играх:** подросток постоянно находится онлайн, играет в игры почти без перерывов.
- **Негативные онлайн-взаимодействия:** подросток может вступать в конфликты с другими игроками или быть жертвой онлайн-буллинга.
- **Зависимость от определенных игр:** подросток сосредоточен только на одной или нескольких играх, игнорируя другие интересы и возможности.

6.2. Онлайн-мошенничество

Онлайн-мошенничество представляет собой широкий спектр преступных деяний, совершаемых с использованием сети Интернет для обмана и хищения денег, личной информации или других ценных ресурсов у жертв. Это динамично развивающаяся область преступности, постоянно адаптирующаяся к новым технологиям и методам защиты.

Основные характеристики онлайн-мошенничества:

- **Широкий спектр методов:** онлайн-мошенничество включает множество различных методов, от простых скамов до сложных кибератак.
- **Глобальный охват:** преступники могут действовать из любой точки мира, обойдя географические границы и юрисдикции.
- **Анонимность:** Интернет позволяет мошенникам скрывать свою личность и местоположение, усложняя расследование и привлечение к ответственности.
- **Масштабируемость:** онлайн-платформы позволяют мошенникам одновременно обманывать большое количество людей, распространяя свои схемы через электронную почту, социальные сети и другие каналы.

- **Постоянная эволюция:** мошенники постоянно разрабатывают новые методы обмана, адаптируясь к усилению безопасности и изменениям в технологиях.

Основные виды онлайн-мошенничества:

Фишинг — это тип онлайн-мошенничества, при котором злоумышленники пытаются получить конфиденциальную информацию, такую как пароли, номера кредитных карт, данные банковских счетов и другую личную информацию, притворяясь доверенными источниками. Они часто используют поддельные веб-сайты, электронные письма или сообщения, чтобы обмануть жертв.

Фрейпинг — это метод мошенничества, при котором злоумышленник предлагает пользователю что-то бесплатно (или по очень низкой цене) с целью получить его доверие и впоследствии обмануть. В онлайн-среде это может проявляться в виде:

Псевдо-благотворительность — это создание ложных благотворительных организаций или использование имени настоящих благотворительных организаций для выманивания денег у доверчивых людей. Признаки псевдо-благотворительности:

Признаки вовлечения

Финансовые признаки:

- **Необъяснимые расходы:** неожиданное исчезновение денег с карты или электронного кошелька ребенка.
- **Просьбы о деньгах:** ребенок начинает чаще просить деньги у родителей, причем его объяснения могут казаться неправдоподобными или неполными.
- **Покупки в онлайн-магазинах:** появление в истории покупок неизвестных или подозрительных товаров или услуг.

Поведенческие признаки:

- **Скрытность:** ребенок становится более скрытным в своем общении с родителями, скрывает свои онлайн-активности.
- **Изменение настроения:** ребенок может стать более тревожным, раздражительным, депрессивным или апатичным.
- **Избегание общения:** ребенок может избегать общения с родителями и другими членами семьи.
- **Необычные онлайн-знакомства:** ребенок может рассказывать о новых знакомствах в онлайне, особенно если эти люди старше его или их личность вызывает подозрение.
- **Участие в азартных играх:** ребенок может рассказывать об участии в онлайн-азартных играх или о попытке выиграть что-то ценное.
- **Необычные подарки:** ребенок может получить необъяснимые подарки от неизвестных людей.

Онлайн-признаки:

- **Необычная онлайн-активность:** ребенок проводит много времени онлайн с неизвестными людьми или в подозрительных группах.
- **Нежелание делиться информацией:** ребенок отказывается рассказывать о своих онлайн-активностях.
- **Подозрительные сообщения:** в истории сообщений ребенка могут появиться подозрительные сообщения от неизвестных людей или сообщения с угрозами.
- **Установка подозрительных программ:** на устройстве ребенка могут появиться подозрительные программы, которые он не устанавливал сам.

7. Рекомендации по профилактике и противодействию современным информационным угрозам

7.1. Рекомендации родителям (законным представителям) по обеспечению информационной безопасности детей в семье

Профилактика и противодействие современным информационным угрозам требуют совместных усилий семьи и образовательной организации. Только комплексный подход, объединяющий образовательные, воспитательные и профилактические меры, может обеспечить эффективную защиту детей.

Работа по профилактике современных информационных угроз, которую может обеспечить семья, должна строиться на доверии, открытом общении и активном участии всех членов семьи. Она должна быть гибкой и адаптироваться к изменениям в жизни подростка и развитию новых технологий.

1) Открытое общение и доверие:

- **Регулярные беседы:** создайте атмосферу, где подросток может свободно общаться с родителями о своих проблемах, чувствах и мыслях, не боясь осуждения. Проводите регулярные беседы о жизни подростка, его интересах и отношениях с друзьями.
- **Активное слушание:** учитесь активно слушать подростка, показывая ему, что вы заинтересованы в его жизни и готовы поддержать его.
- **Демонстрация безусловной любви:** дайте подростку понять, что вы его любите и принимаете безусловно, независимо от его проблем и поступков.

2) Обучение кибербезопасности и цифровой грамотности:

- **Беседы о рисках:** проводите беседы о различных видах онлайн-угроз: кибербуллинг, онлайн-мошенничество, груминг, секстинг, экстремистские группы, пропаганда насилия (включая «Колумбайн»), суицидальные группы, АУЕ. Объясните подростку, какие риски существуют и как их избегать.
- **Практические навыки:** научите подростка практическим навыкам кибербезопасности: безопасному пользованию социальными сетями, распознаванию фишинговых ссылок, защите личных данных, блокировке нежелательных пользователей.
- **Мониторинг онлайн-активности (деликатно):** следите за онлайн-активностью подростка, но делайте это тактично и с уважением к его личной жизни. Важно найти баланс между контролем и доверием.

3) Формирование здоровых ценностей и интересов:

- **Поддержка здорового досуга:** помогите подростку найти здоровые и интересные занятия вне онлайн-пространства: спорт, творчество, волонтерство, хобби, общение с друзьями в реальном мире.
- **Развитие самооценки:** помогите подростку развивать высокую самооценку, чтобы он не был уязвим к влиянию сверстников и манипуляциям.
- **Профилактика стресса и депрессии:** научите подростка здоровым способам справляться со стрессом и негативными эмоциями. При необходимости обращайтесь за помощью к специалистам (психолог, психиатр).

4) Установление границ и правил:

- **Семейные правила пользования гаджетами:** совместно с подростком разработайте четкие правила пользования гаджетами и интернетом. Эти правила должны быть реалистичными и последовательными.
- **Ограничение времени онлайн:** ограничьте время, которое подросток проводит онлайн, и контролируйте его активность.
- **Защита персональных данных:** объясните важность защиты персональных данных и не разглашать их в онлайне.

5) Своевременное обращение за помощью:

- **При подозрении на проблемы:** при появлении подозрительных признаков (изменения в поведении, необычная онлайн-активность, депрессия) немедленно обращайтесь за помощью к специалистам.
- **Знание контактной информации:** убедитесь, что подросток знает, куда обращаться за помощью в случае угроз или неприятных ситуаций онлайн.

Важно создать атмосферу открытости и доверия, где подросток будет чувствовать себя в безопасности и сможет обратиться за помощью в любое время.

7.2. Рекомендации по обеспечению информационной безопасности детей в образовательной организации

Работа образовательной организации по обеспечению информационной безопасности детей в сети Интернет должна быть комплексной и системной, строиться на принципах сотрудничества с родителями и с учетом возрастных особенностей детей.

1) Образовательные мероприятия:

- **Внедрение уроков цифровой грамотности:** разработка и внедрение в учебный план специальных уроков или модулей, посвященных безопасности в интернете. Темы должны включать:
  - Основы безопасного поиска информации.
  - Защита личных данных (пароли, конфиденциальность).
  - Распознавание онлайн-мошенничества.
  - Безопасное общение в сети.
  - Ответственное использование социальных сетей.
  - Распознавание пропаганды и дезинформации.
  - Защита от онлайн-насилия.
  - Последствия неправомерных действий в сети.
- **Использование интерактивных методов:** применение ролевых игр, дискуссий, кейсов и других интерактивных методов для повышения эффективности обучения.
- **Обучение педагогических работников:** педагоги также должны быть обучены основам кибербезопасности и уметь распознавать признаки возможных проблем у учащихся.

2) Воспитательные мероприятия:

- **Развитие критического мышления:** поощрение критического мышления, способности анализировать информацию и выявлять пропаганду.
- **Пропаганда здорового образа жизни:** поощрение здорового образа жизни, спорта, творчества и других позитивных видов деятельности, чтобы снизить риск вовлечения в деструктивные сообщества.

3) Профилактические мероприятия:

- **Информационные кампании:** проведение информационных кампаний для учащихся и родителей о современных онлайн-угрозах и способах защиты. Использование плакатов, буклетов, видеороликов и других наглядных материалов.
- **Родительские собрания и семинары:** организация родительских собраний и семинаров, посвященных вопросам кибербезопасности и безопасного использования интернета детьми.
- **Сотрудничество с родителями:** создание системы обратной связи с родителями для своевременного выявления и решения проблем.

4) Технические меры:

- **Фильтры контента:** использование специальных программ для фильтрации нежелательного контента на школьных компьютерах и в сетях (с учетом баланса между безопасностью и правом на доступ к информации).
- **Безопасные сети Wi-Fi:** использование защищенных сетей Wi-Fi со строгими паролями в школе.
- **Мониторинг сетевой активности:** мониторинг сетевой активности на предмет подозрительной деятельности (в соответствии с законодательством о защите персональных данных).

5) Организационные меры:

- **Разработка и внедрение политики кибербезопасности:** разработка и внедрение четкой политики кибербезопасности в образовательной организации, регламентирующей использование интернета и цифровых устройств учащимися и сотрудниками.
- **Процедуры реагирования на инциденты:** разработка и внедрение четких процедур реагирования на случаи кибербуллинга, онлайн-мошенничества и других информационных угроз. Это включает в себя алгоритм

действий при обнаружении проблемы, назначение ответственных лиц и способы документирования инцидентов.

- **Сотрудничество с правоохранительными органами:** взаимодействие с правоохранительными органами в случаях серьезных преступлений в интернете.

6) Постоянное совершенствование:

- **Мониторинг новых угроз:** постоянный мониторинг новых онлайн-угроз и адаптация программ к изменениям в цифровом мире.
- **Обратная связь:** сбор отзывов от учащихся, родителей и преподавателей для постоянного совершенствования программ по информационной безопасности.

В заключение следует подчеркнуть, что обеспечение информационной безопасности детей в сети Интернет – это комплексная задача, требующая совместных усилий родителей, педагогов, разработчиков цифровых продуктов и государственных органов. Не существует универсального решения, и эффективность мер зависит от постоянного мониторинга ситуации и адаптации к новым вызовам, которые постоянно появляются в быстроразвивающемся цифровом мире.

Успешная защита детей требует не только технических решений, таких как установка антивирусных программ и фильтров, но и воспитания цифровой грамотности, развития критического мышления и умения распознавать опасности онлайн. Дети должны понимать риски, связанные с общением с незнакомцами, распространением личной информации и участием в сомнительных онлайн-активностям. Важно формировать у них навыки безопасного поведения в сети, способность оценивать достоверность информации и умение обращаться за помощью в случае возникновения проблем.

Роль родителей и педагогов в этом процессе неоценима. Они должны быть активными участниками жизни ребенка в цифровом пространстве, проводить

профилактические беседы, мониторить онлайн-активность (разумеется, с уважением к личной жизни ребенка), и быть готовыми оказать помощь и поддержку в случае возникновения трудностей.

Вместе мы можем создать более безопасную и здоровую цифровую среду для наших детей, позволяя им пользоваться преимуществами Интернета, минимизируя при этом риски. Постоянное обучение, диалог и совместные действия – ключ к успеху в этой важной задаче. Только объединенными усилиями мы сможем обеспечить нашим детям безопасность и комфорт в цифровом мире.

8. Рекомендуемые информационные ресурсы

Рекомендуем совместный просмотр и изучение ресурсов детям, родителям и педагогам. Данные ресурсы по информационной безопасности актуальны на дату создания настоящих методических рекомендаций и содержат методические материалы, видеолекции, проекты, исследования, уроки, книги, тренажёры для детей родителей и учителей, созданные при поддержке государства, профильных фондов, центров, ведущих цифровых компаний, в том числе с официальных сайтов организаций Липецкой области, рекомендуемых к сотрудничеству и взаимодействию.

1. Материалы родителям и педагогам от Лиги безопасного интернета

Режим доступа: https://ligainternet.ru/o-nas/

- Защита персональных данных детей. Анимационный ролик
- Безопасность школьников в сети Интернет. Видеоролик от Видеоуроки в Интернет
- Брошюра для учеников младших классов «Азбука информационной безопасности» от Лаборатории Касперского
- Материалы к урокам безопасного интернета

- Как обеспечить безопасность детей в Интернете. Рекомендации патртнеров Google: «Центра безопасного интернета», Линии помощи «Дети Онлайн»
- «Киберпреступность — очень доходный бизнес». Интервью с главой антивирусной компании
- 6 самых вредоносных приложений для смартфонов
- Тест родительских контролей от Anti-Malware.ru. Результаты данного теста должны помочь родителям выбрать наиболее качественную защиту для их детей, осваивающих просторы глобальной сети.

2. ЛООО «Поиск пропавших детей» г. Липецк. Режим доступа: https://poiskdeteilip48.ucoz.ru/

3. Липецкий областной Центр общественного здоровья и медицинской профилактики Режим доступа: http://uzalo48.lipetsk.ru/obl/obl-med-prof

4. ГУЗ «Липецкий областной наркологический диспансер». Тренинговый центр «Подросток». Программа тренингов, позволяющая сформировать навыки общения, планирования поступков, распознавания опасных ситуаций и уверенного отказа от использования неизвестных веществ.

Режим доступа: http://uzalo48.lipetsk.ru/obl/obl-nark-disp

5. Методические рекомендации Центра «СемьЯ»

Режим доступа: https://xn--48-mlc2ax2eva.xn--p1ai/metodicheskie-razrabotki/

- Суицид. Помощь подросткам
- Буллинг. Причины, последствия, помощь
- Рекомендации учителям при работе с трудными подростками
- Профилактика буллинга, скулшутинга и кибераддикции в образовательных организациях
- Новенький в классе. Советы педагогу
- Педагогам о старших подростках
- Плохое поведение. Рекомендации педагогам
- Работа с трудными подростками в кризисных ситуациях

- Рекомендации по проведению Больших психологических игр
- Рекомендации учителям 5 классов
- Методические рекомендации по профилактике суицида среди несовершеннолетних
- Памятка по безопасности на железной дороге и объектах железнодорожного транспорта

6. Учебно-методический центр по гражданской обороне и защите от чрезвычайных ситуаций Липецкой области. Режим доступа: http://umcgochs48.ru/

7. Методические рекомендации по реализации мер, направленных на обеспечение безопасности детей в сети «Интернет». Управление «К» МВД России. Режим доступа: https: мвд. рф

8. Дидактическая интерактивная педагогическая игра «Это не игра», разработана ФГАОУ ДПО «Академия Минпросвещения России»

9. Навигатор профилактики девиантного поведения - 2022 Режим доступа: https://mgppu.ru/about/publications/deviant_behaviour

10. Инструкция к Навигатору профилактики и описание памяток для классных руководителей, педагогов и специалистов по различным видам девиантного (отклоняющегося) поведения обучающегося ВЕРСИЯ 2022. Режим доступа: https://uo-sayansk.ru/doc/profilaktika/navigator2023.pdf

11. Информационный ресурс некомерческой организации «Лига безопасного интернета». URL: http://www.ligainternet.ru

12. Информационный ресурс «Дети России Онлайн». URL: http://detionline.com

13. Всероссийский урок безопасного Интернета. -2023 г. URL: https://ligainternet.ru/translyatsiya-vserossijskogo-uroka-bezopasnogo-interneta/

14. Что рассказать детям о кибербезопасности/ Раздел «Кибербезопасность — это просто!» сайт Госуслуг URL: https://www.gosuslugi.ru/life/details/cyber_security_for_kids?categoryCode=Internet_and_communication

15. Образовательный онлайн-проект DigitaLogia от компании «Ростелеком» и Центра молодежных инженерных и научных компетенций «Кванториум». URL: https://www.company.rt.ru/social/cyberknowledge/digitalogia/

16. Проекты Альянса по защите детей в цифровой среде»: методические материалы исследования, книги, подкасты 2022. URL: https://internetforkids.ru/projects/

17. Станислав Макаров Прекрасный, опасный, кибербезопасный мир: книга по кибербезопасности. - 2021 г. [Электронный ресурс] URL: https://www.company.rt.ru/social/cyberknowledge/book_cybersecurity/

18. Онлайн-курс: видеолекции для родителей «Как защитить ребенка от рисков в интернете?» от Ростелекома. [Электронный ресурс] URL: https://www.company.rt.ru/social/cyberknowledge/cyber-lessons/

19. Всероссийский образовательный проект в сфере цифровой экономики «УРОК ЦИФРЫ» от ведущих технологических компаний: Яндекса, «Лаборатории Касперского», Фирмы «1С», госкорпорации Росатом, VK, Благотворительного фонда «Вклад в будущее», Авито и Группы Астра.2024 г.— [Электронный ресурс] URL: https://kids.kaspersky.ru/

20. Просветительский проект «Цифровой ликбез»: видеоролики для детей и взрослых от ведущих цифровых компаний-лидеров: VK, Благотворительный фонд Сбербанка «Вклад в будущее», СКБ Контур, «Лаборатория Касперского», Авито. [Электронный ресурс] URL: https://digital-likbez.datalesson.ru/

21. Проект «Готов к цифре» от Университета 2035, Минцифры России, Цифровой экономики о безопасном и эффективном использовании цифровых технологий для людей самых разных уровней цифровых компетенций // Сервис готовности к цифровой экономике «Стань успешнее вместе с цифрой». [Электронный ресурс] URL: https://xn--b1abhljwatnyu.xn--p1ai/

22. Проект «КиберЗОЖ» от Минцифры России и компании SOLAR [Электронный ресурс] URL: https://xn--90aiddcl6ao.xn--p1ai/

23. Проект «Кибербуллинг» от Минцифры России и компании SOLAR [Электронный ресурс] URL: https://xn----9sbbihqekoax4a5b.xn--p1ai/

24. Проект «Выучи свою роль» от Минцифры России и компании SOLAR [Электронный ресурс] URL: https://xn--b1aarnoanfq4b3bvw.xn--p1ai/

25. Проект «прокачай скилл защиты» от Минцифры России и компании SOLAR [Электронный ресурс] URL: https://xn--80aaa1aecdfdla2amoux8e1b1b.xn--p1ai/

26. Кибербезопасность Для Детей И Взрослых //Государственная образовательная платформа «Российская электронная школа» [Электронный ресурс] URL: https://resh.edu.ru/page/cyber-project

27. Digital-квесты для подростков: безопасность в сети и первая профессия//Фонд «Национальные ресурсы образования» [Электронный ресурс] URL: https://nro.center/projects/digital-kvesty-dlja-podrostkov-bezopasnost-v-seti-i-pervaja-professija/

28. Методические разработки от ФГБУ «Центр защиты прав и интересов детей», 2024. [Электронный ресурс] URL: https://fcprc.ru/metodicheskie-razrabotki/

29. Олимпиада «Безопасный интернет» для учеников 1–11 классов от ООО «Учи.ру» [Электронный ресурс] URL: https://safenet.uchi.ru/

Список используемых источников

Нормативные документы

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_140174/

2. Федеральный закон от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_108808/;

3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (последняя редакция) URL: ttps://www.consultant.ru/document/cons_doc_LAW_61798/

4. Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ URL: http://www.kremlin.ru/acts/bank/24154

5. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» URL: http://www.kremlin.ru/acts/bank/41460

6. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» URL: http://www.kremlin.ru/acts/bank/10638

7. Приказ № 644 «О плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021–2027 годы» URL: https://digital.gov.ru/ru/documents/7382/

8. Постановление Главного государственного санитарного врача Российской Федерации от 28.09.2020 № 28 "Об утверждении санитарных правил СП 2.4. 3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи». URL: http://publication.pravo.gov.ru/document/view/0001202012210122

9. 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//Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: http://surl.li/sbcczp

10. Распоряжение Правительства РФ от 28.04.2023 N 1105-р «Об утверждении Концепции информационной безопасности детей и признании

утратившим силу Распоряжения Правительства РФ от 02.12.2015 N 2471-р». URL: https://www.consultant.ru/law/hotdocs/80196.html

11. Концепция информационной безопасности детей в Российской Федерации, утверждённая распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р. URL: http://static.government.ru/media/files/0vjjsdBmSsIdUZ4c8Z2eOAiGkCbCf7OJ.pdf

12. Методические рекомендации для несовершеннолетних, родителей (законных представителей) несовершеннолетних, наглядные информационные материалы по безопасному использованию сети «Интернет» в целях предотвращения преступлений, совершаемых с ее использованием, как самими несовершеннолетними, так и в отношении них. Методические рекомендации/Авторы: Артамонова Е.Г., Бородина А.С., Мелентьева О.С. - М.: ФГБУ «Центр защиты прав и интересов детей», 2021 − 35 стр.