**МКДОУ «Детский сад с.Аялизимахи»**

**Доклад на тему: «Безопасность в сети Интернет»**



**Воспитатель: Шихшунатова Р.М.**

**Аялизимахи2022**

**Введение**

Проблема обеспечения информационной безопасности детей в информационных сетях становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

Всеобщая информатизация и доступный, высокоскоростной Интернет уравнял жителей больших городов и малых деревень в возможности получить качественное образование.

Доступ молодежи к информационным ресурсам сети Интернет дает возможность студентам пользоваться основным и дополнительным учебным материалом, необходимым для обучения в колледже, выполнять домашние задания, самостоятельного обучаться. Благодаря таким ресурсам у них появляется возможность узнавать о проводимых олимпиадах, конкурсах, и принимать в них активное участие. Использование Интернета в образовательном процессе достаточно обширно: это использование электронной почты; поиск в сети нужной информации; создание собственных вебстраниц; рассылка; обмен опытом; ответы на типичные вопросы; совместные проекты студентов и преподавателей.

Между тем существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье молодежи, порождающих проблемы в поведении у психически неустойчивых подростков и представляющих для них угрозу. Бесконтрольный доступ к Интернету может привести к:

* + Интернет – зависимости;
	+ знакомству с человеком с недобрыми намерениями;
	+ заражению вредоносными программами при скачивании файлов;
	+ неправильному формированию нравственных ценностей;
	+ нарушению нормального развития подростка.

В связи с этим необходимо направить все усилия на защиту молодежи от информации, причиняющей вред их здоровью и развитию. Воспитательная работа в этом направлении, знание студентом элементарных правил отбора информации, а также умение ею пользоваться способствует развитию системы защиты прав молодежи.

Медиаграмотность определяется в международном праве, как грамотное использование инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке студентов и их преподавателей в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг.

Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на молодежь с использованием сети Интернет.

Обеспечение государством информационной безопасности молодежи, защита их физического, умственного и нравственного развития во всех аудиовизуальных медиауслугах и электронных СМИ – требование международного права.

Согласно российскому законодательству информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Обсуждение со студентами колледжа данной проблемы (беседы во время кураторских часов, анкетирование) позволило сделать вывод, что время, проводимое подростками-пользователями в Сети, становится значимой частью их распорядка дня, а Интернет — тем фактором, который определяет образ жизни. Большинство родителей объясняет детям о том, как пользоваться интернетом, однако дети недопонимают и не воспринимают большинство угроз, таящихся в интернете.

**Основные опасности Интернет-общения**

Потребность в информации — одна из базовых естественных потребностей человека. От этой потребности человек часто получает удовольствие. А при получении удовольствия, человек часто получает зависимость — это уже опасность интернета. Но информацией вполне можно «отравиться». Можно потреблять вредную информацию и серьезно навредить своему духовному здоровью. Как и пища, любая информация оказывает то или иное воздействие на человека — сильное или слабое, полезное или вредное, спасительное или абсолютно разрушительное. Так как информация неизбежно оказывает воздействие на человека, значит, она должна фильтроваться. Если взрослый человек справляется с этой задачей (хотя не всегда и не каждый), то подросток этого делать еще не умеет.

Раньше авторитет родителей был очень высок. Но сейчас ситуация меняется. Авторитетом пользуется тот, кто даёт удовольствие: то есть телевизор, интернет, видеоигры, видеоклипы и видеоинформация.

Отсутствие странички в социальной сети уже, скорее, исключение. Все стараются завести себе страницу – это модно и почти обязательно. Подросток, еще не умея фильтровать поступающую информацию, не имея еще устойчивых социальных моделей, получил доступ к социальным сетям, форумам, чатам, сайтам знакомств, онлайн-играм, информационным сайтам и блогам самого разного качества и содержания. На него буквально хлынул огромный, мощный поток самой разной информации. Он стал с ней взаимодействовать, зачастую один на один. Ситуация особенно обострилась в последние годы — с распространением планшетов и смартфонов. Таким образом, доступ в Интернет становится переносным и фактически неконтролируемым.

Зададимся вопросом: «Что подросток может взять из Интернета и телевидения в реальную жизнь?».

Чтобы дать объективную оценку влиянию Интернета на молодого человека, необходимо подчеркнуть многие положительные моменты.

В Интернете можно проявить свое творчество. На страницах социальных сетей, на специальных сайтах пользователи часто размещают свои стихи, рисунки, прозу, музыку. И сразу получают обратную связь в виде комментариев, лайков.

Интернет — большая библиотека: достаточно электронных книг по разным направлениям, что позволяет находить информацию как для обучения, так и для личностного роста.

Для того чтобы ориентироваться в интернет-пространстве, нужно учиться. Безопасно и полезно путешествовать по просторам интернета можно только при условии повышения компьютерной грамотности и соответствующей мотивации.

Интернет помогает устанавливать связи с пользователями из разных мест. Это одно из основных преимуществ интернет-пространства — отсутствие географических границ.

Интернет экономит наше время. Доступность ресурсов позволяет сэкономить время на поиск информации, общение. Однако остается проблема правильного распределения сэкономленного времени. Некоторые подростки жалуются, что не успевают ничего сделать из-за социальных сетей — все время кому-то отвечают. Решить эту проблему можно, составив режим дня, график использования Интернета. Однако главная проблема – это те опасности и угрозы, которые несет в себе Интернет-общение, особенно для людей, незащищенных и слабо представляющих его реальную угрозу.

Выделим основные опасности Интернет-общения:

1. Конфликтное, агрессивное общение.
2. Психологическое давление, оскорбления и унижения.
3. Несчастные случаи, вызванные желанием повторить увиденные рискованные трюки.
4. Извращения, насилие, сексуальные домогательства.
5. Вступление в радикальные группировки (правый сектор, ИГИЛ), экстремизм.
6. Мошенничество, вымогательство.
7. Приобретение зависимости от пропаганды наркотиков, алкоголя, курения.
8. Призывы причинить себе вред (от пропаганды суицида до опасных экспериментов над собой).
9. Безопасность доступа в Сеть и кража личных данных техническими средствами.
10. Незаконный сбор персональных данных несовершеннолетних и (или) распространение их в открытом доступе.
11. Уныние – как следствие беспрерывных развлечений и несоответствия реальности выработанным желаниям.
12. Ложные приоритеты и ценности (например, деньги важнее дружбы и человеческих качеств).
13. Безответственное поведение (например, нежелание учиться, а желание постоянно развлекаться и получать удовольствие)

Чем отличается общение в Интернете от реального общения? В виртуальном общении не работает важнейший механизм —врожденная способность чувствовать то, что чувствует собеседник, активно сопереживать. Опасность тут возникает лишь тогда, когда виртуальное общение с другом вытесняет живое. Тут запросто можно наткнуться на пропаганду фашизма и неонацизма, призывы к насилию, воровству и прочим противоправным действиям. Причем, в силу специфики социальных сетей, достаточно того, чтобы чем-то подобным заинтересовался кто-нибудь из друзей и нажал на «поделиться». То есть можно именно наткнуться на нехороший контент, не занимаясь его поиском целенаправленно.

А что же родители, понимают ли они опасность интернета? Каждый третий родитель знает, что дети видят изображения сексуального характера в Интернете, потому что видят их сами. В то же время, они почти не имеют представления о том, что дети становятся жертвами агрессивного поведения или могут быть агрессорами сами.

Также родители очень мало знают о том, что их дети встречаются с теми, с кем познакомились в Интернете. Очень часто, к сожалению, родительская бдительность спит: ведь ребенок дома, сидит за компьютером. Родители, не понимая опасностей онлайн-жизни, добровольно допускают посторонних людей с очень разными намерениями к воспитанию ребенка (например, в интернете можно договориться о покупке наркотиков, получить преждевременное растление и т.д.)

Что дети думают о родителях? Треть детей отмечает, что не ощущают со стороны родителей никакой поддержки, хотя сами родители при этом считают, что помогают своему ребенку. Получается, родитель теряет авторитет у ребенка, конкурируя с самыми разными людьми «с того конца Интернет-кабеля», то есть теряют возможность воспитывать своего ребенка.

Таким образом, модели поведения, нормы, образ мыслей, картина мира — все то, что и называется воспитанием, в большой степени черпается ребенком в сети (фильмы, видеоклипы, фото).

В настоящее время молодежи насаждается страсть к развлечениям, в то время как подросткам остро не хватает социализации. При этом не формируются жизненно необходимые навыки труда в коллективе, совместного творчества, подростки не привыкают добровольно брать на себя ответственность.

Если тенденция продолжится, то совсем скоро подрастающая личность будет формироваться уже в первую очередь Интернетом и лишь во вторую — общественным воспитанием.

**Классификация Интернет-угроз**

1. **Электронная безопасность**

Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн-мошенничество и спам

1. **Вредоносные программы**

Вредоносные программы - это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы-шпионы, нежелательное рекламное программное обеспечение и различные формы вредоносных кодов.

1. **Спам**

Спам - это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный интернет-трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений, вредоносные программы.

1. **Кибермошенничество**

Кибермошенничество - это один из видов киберпреступлений, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя, с целью получить материальную прибыль. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг.

1. **Коммуникационные риски**

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя контакты педофилов с детьми и киберпреследования.

1. **Контентные риски**

Контентные риски связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент.

1. **Неподобающий контент**

В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

1. **Незаконный контакт**

Незаконный контакт - это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.

1. **Киберпреследования**

Киберпреследование - это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование.

Бесконтрольное распространение нежелательного контента противоречит целям образования и воспитания молодежи.

 Отказываться от благ информационных технологий бессмысленно, но бесконтрольный доступ детей к Интернету может привести к:

* Киберзависимости
* Заражению вредоносными программами при скачивании файлов
* Нарушению нормального развития ребенка
* Неправильному формированию нравственных ценностей
* Знакомству с человеком с недобрыми намерениями

**Информационная безопасность**

Согласно российскому законодательству **информационная безопасность детей**– это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

Безопасность детей одна из главных задач цивилизованного общества, поэтому обеспечивать безопасность в Интернете должны все, кто причастен к этому обществу. И так по порядку:

* Правительство. Должны быть законы, которые смогли бы оградить детей от вредной информации в Интернете. Так в России все школы обязали установить программы контентной фильтрации в классах информатики.
* Поисковики. Многие поисковые сервисы такие как Yandex, Ramler имеют в своем арсенале большое количество настроек, помогающих родителям оградить детей от нежелательного контента в Интернете. Также есть поисковые системы, предназначенные специально для детей.
* Семья. Конечно же никто так сильно не отвечает за безопасность детей в Интернете, как сами родители. Ведь только родители могут полностью контролировать своих детей.
* Образовательные учреждения. Защита учащихся от информационных угроз и рисков Интернет-ресурсов связана с формированием медиа-грамотности. В образовательных учреждениях данная задача может решаться педагогами с использованием различных форм медиа-образования.

**Медиа-грамотность** определяется в международном праве как грамотное использование учащимися и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей, подростков и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг. Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет.

**Медиа-образование** выполняет важную роль в защите от негативного воздействия средств массовой коммуникации, способствует осознанному участию подростков и детей в медиасреде и медиакультуре, что является одним из необходимых условий эффективного развития гражданского общества.

Защиту подростков от информации, причиняющей вред их здоровью и безопасности, прежде всего, семья и образовательное учреждение. Проведение занятий по медиа-безопасности планируется в образовательных учреждениях на постоянной основе.

**Цель проведения занятий по медиа-безопасности** – обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

К информации, запрещенной для распространения среди молодежи, относится информация:

1. Побуждающая к совершению действий, представляющих угрозу жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству.
2. Способная вызвать желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством.
3. Обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом.
4. Отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи.
5. Оправдывающая противоправное поведение.
6. Содержащая нецензурную брань.
7. Содержащая информацию порнографического характера.

Также значимой является совместная работа с родителями по формированию у них базовых знаний, связанных с правилами безопасного пользования Интернет-ресурсами

**Рекомендации, которые могут помочь в решении проблемы безопасного пользования Интернет-ресурсами.**

**Как защитить несовершеннолетнего от нежелательного контента в Интернете:**

* Приучите ребенка немедленно сообщать о появлении нежелательной информации подобного рода.
* Объясните, что далеко не все, что можно прочесть или увидеть в Интернете – правда. Приучите детей спрашивать о том, в чем они не уверены.
* Старайтесь спрашивать об увиденном в Интернете. Зачастую, открыв один сайт, появляется желание познакомиться и с другими подобными ресурсами.

**Необходимо быть осторожными при знакомстве с новыми людьми в Интернете**

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др.

Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы.

Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие, пытается узнать личную информацию и договориться о встрече.

**Предупреждение груминга:**

* Следите за информацией, которую ты выкладываешь в Интернете. Не выкладывайте свои личные данные в Интернете (домашний адрес, номер телефона, место учебы, любимое место прогулки, время возвращения домой и т.д.). Любая информация может быть использована против вас, в том числе в корыстных и преступных целях.
* Используйте псевдоним при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), пользовании онлайн играми и других ситуациях.
* Не размещайте и не посылай свои фотографии незнакомцам.
* Будьте осторожны при общении с незнакомыми людьми. Старайтесь рассказывать как можно меньше информации о себе.

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

**Предупреждение кибербуллинга:**

* При общении в Интернете необходимо быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать.
* Правильно реагируйте на обидные слова или действия других пользователей;
* Нельзя использовать Сеть для хулиганства, распространения сплетен или угроз;

Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребенку опасность и, тем более, не всегда знают, как ее предотвратить.

Родителям следует обратить внимание на ряд признаков в поведении ребенка, которые могут свидетельствовать о том, что ребенок стал жертвой кибербуллинга:

* **Беспокойное поведение**. Даже самый замкнутый ребенок будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти на учебу – самые явные признаки того, что ребенок подвергается агрессии.
* **Неприязнь к Интернету**. Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.
* **Нервозность при получении новых сообщений**. Негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб

**Предупреждение кибермошенничества:**

* Ознакомьтесь сами и проинформируйте детей о самых распространенных методах мошенничества и научите их советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете.
* Установите на компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.

**Безопасное совершение покупок в Интернет-магазинах:**

* прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности;
* необходимо познакомиться с отзывами покупателей;
* проверьте реквизиты и название юридического лица – владельца магазина;
* уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs);
* поинтересуйтесь, выдает ли магазин кассовый чек;
* сравните цены в разных интернет-магазинах;
* позвоните в справочную магазина;
* обратите внимание на правила интернет-магазина;
* выясните, сколько точно вам придется заплатить.

**Как распознать интернет и игровую зависимость:**

Сегодня в России все более актуальны проблемы так называемой «интернет-зависимости» (синонимы: интернет-аддикция, виртуальнаяаддикция) и зависимости от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, в случае, если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Согласно исследованиям Кимберли Янг, предвестниками интернет-зависимости являются:

* навязчивое стремление постоянно проверять электронную почту;
* предвкушение следующего сеанса онлайн;
* увеличение времени, проводимого онлайн;
* увеличение количества денег, расходуемых онлайн.

Если Вы считаете, что Ваши близкие, в том числе дети, страдают от чрезмерной увлеченности компьютером, это наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь. Помощь может быть оказана как в специальных терапевтических группах, так и стационарно, с использованием специальных медицинских процедур.

**Как научить ребенка не загружать на компьютер вредоносные программы:**

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными и даже использовать Ваш компьютер для распространения вируса, рассылать от Вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

* установите на компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения;
* используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр;
* периодически старайтесь полностью проверять компьютеры;
* делайте резервную копию важных данных;
* старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

**Пять правил безопасного пользования электронной почтой:**

1. Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их, выбрав команду в меню сообщений.
2. Никогда не отвечайте на спам.
3. Применяйте фильтр спама поставщика услуг Интернета или программы работы с электронной почтой (при наличии подключения к Интернету).
4. Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.
5. Никогда не пересылайте «письма счастья». Вместо этого сразу удаляйте их.

**Заключение**

Формирование информационной культуры и безопасности – процесс длительный и сложный, но важный и необходимый. Задача взрослых (педагогов, родителей) – формирование разносторонней интеллектуальной личности, высокий нравственный уровень которой будет гарантией ее информационной безопасности. А для этого необходимо повышать квалификацию педагогов по вопросам информационной безопасности, чтобы уметь оперативно ориентироваться и ориентировать детей в вопросах безопасного поведения в Интернете. Регулярно проводить родительский всеобуч по вопросам кибербезопасности и работать не вдогонку, а на опережение.

Ребенок не станет пропадать в Интернете, если он занят очень интересным для него делом, если его реальный мир намного ярче и увлекательней мира виртуального. Нужно развивать способности и тягу ребенка к реальным действиям и достижениям: кружки, факультативы, секции, дополнительное образование. К тому же настоящие социальные навыки, настоящая культура формируется только в совместном интересном труде. Если не направить позитивную энергию ребенка — она будет поглощена Интернетом, а ребенок останется опустошенным, бесцельно блуждающим по бесконечному Интернет пространству в ожидании от него чуда.

Мир меняется, наши дети отличаются от нас, какими мы были в том же возрасте, но ценность семьи для них остается по-прежнему очень высокой. Обратите внимание на своих детей! Интересуйтесь их жизнью, станьте им друзьями. И, возможно, реальное пространство станет для ваших детей более притягательным, чем виртуальное.