

6.16. КОМПЬЮТЕР, ИНТЕРНЕТ И КИБЕРБЕЗОПАСНОСТЬ ДЕТЕЙ ДОШКОЛЬНОГО ВОЗРАСТА

РАЗБИРАЕМСЯ В ГЛАВНОМ



- Как правильно развивать, учить и воспитывать ребенка в условиях всеобщей компьютеризации, информатизации и цифровых технологий?
- Как уберечь детей от киберопасностей современного цифрового общества?
- Какой он, современный ребёнок, появившийся на свет в эпоху цифровых технологий?

- Каким образом влияет на детей необходимость постоянного пополнения знаний и умений для оперирования информацией?

- Что может дать ребёнку общество, всё больше развивающееся в глобальных сетях, представляющее собой некий «коллективный разум»?

Основные понятия

Цифровое общество – общество, инфраструктура которого функционирует посредством цифровых технологий, к которым относят все то, что связано с электронными вычислениями и преобразованием данных: гаджеты, электронные устройства, технологии, программы.

Цифровая среда – многофункциональное пространство, созданное с помощью цифровых технологий. Цифровая среда для ребенка дошкольного возраста представляет собой виртуальное пространство способное моделировать и транслировать информацию в доступной форме. Характеристиками цифровой среды для детей дошкольного возраста являются «направленность на обучение и развитие ребенка», «информационная безопасность» и «защита от киберугроз».

Информационная безопасность – «...состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию»¹.

Киберугроза – это незаконное проникновение в личное цифровое пространство через носитель данных (гаджет) с целью причинения вреда (материального, физического, психологического).

Рекомендуемые формы и темы просвещения родителей

- *родительские собрания, тематические встречи-обсуждения с передачей опыта, дискуссии:* «Как выбрать полезную компьютерную игру?», «Защита ребенка от деструктивной информации», «Организация кибербезопасной среды дошкольника», «Интернет-зависимость – как избежать?»;
- *родительское собрание:* «Телевидение в жизни семьи и ребенка»;
- *конкурс семейных девизов:* «Скажем «Нет» вредным привычкам!» (пищевые привычки, гаджеты и сеть интернет);
- *визуальная информация:* памятки;
- *буклеты;*
- *практикумы:* «Как отказаться от гаджетов, или что такое цифровой детокс?», «Вред и польза гаджетов у детей», «Профилактика зависимостей».

В современном мире в разы увеличилось не только количество и доступность продуктов технического прогресса, изменились их функциональные возможности. Дети сильно изменились под воздействием информационно-технического прогресса общества.

¹ Ст.2 п.4 Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ».

Марк Пренски в 2001 году ввел такое понятие, как «аборигены цифрового общества». Аборигены цифрового общества представляют собой поколение, родившееся и развивающееся в уже существующих условиях новых технологий. Они привыкли ко всем видам цифровых игр и инструментов, которые являются неотъемлемой частью их жизни. Цифровая деятельность для них – естественная среда обитания. Они понимают ценность цифровой технологии (мгновенный отклик, доступность, свободный доступ) и могут пользоваться ей без специальной подготовки. Имеют множество новых и впечатляющих компетенций: обладают интуитивным владением информатикой, компьютерами, электронными устройствами и мобильным оборудованием. Им не требуется читать руководство пользователя, и они не просят уроков по использованию компьютера. Это – поколение технологической акселерации, интернета и социальных сетей, являющиеся носителями «цифрового» языка. Вырастая в таком окружении, они думают и обрабатывают информацию совершенно другим способом, нежели предыдущие поколения: изменились алгоритмы мышления.

Это настолько радикальное изменение, что образовался большой разрыв между их поколением и предыдущими. Отсюда происходит часть проблем с родителями и преподавателями. Особенно остро этот конфликт поколений ощущается в образовании. Разрешение данного конфликта намечается не в стремлении старшего поколения «догнать», а в переходе «от компьютерной грамотности к информационной культуре» для молодого поколения. Где старшее поколение, выполняя социальный заказ нового общества, берет на себя важную функцию формирования у сегодняшних детей культуры использования информационных коммуникационных технологий и средств массовой информации, как части общей культуры человека, учитывая при этом возрастные и психологические особенности детей, сохраняя их психическое и физическое здоровье.

Специалисты предупреждают: постоянное воздействие негативных факторов современной цифровой среды в конечном счете может привести к снижению уровня психологической и личностной зрелости ребенка. Отмечают опасность задержки развития сферы воображения, при восприятии информации выраженную ориентацию на наглядность. Вызывает опасение формирование коммуникативных умений и навыков, слабость произвольной сферы и искажение восприятия мироустройства. К факторам риска также относятся и киберугрозы, с которыми дети встречаются в цифровом пространстве.

В целом, последствия неуправляемого и необдуманного взаимодействия детей с цифровым миром можно разделить на несколько категорий:

1. *негативное влияние на психику ребенка;*

Самые распространенные жалобы этой категории: эмоциональная неустойчивость; агрессивное поведение ребенка; снижение самооценки; развитие компьютерной зависимости; отказ от других видов деятельности и др.

2. *нарушение физического здоровья ребенка;*

Ухудшение зрения; нарушения опорно-двигательного аппарата и осанки; головные боли; трудность с засыпанием и др.

3. *социальная дезадаптация личности;*

Проблемы в установлении взаимоотношений со сверстниками; напряженность отношений с родителями и взрослыми; снижение качества формирования навыков учебной деятельности; появление антисоциального поведения и др.

4. *угроза жизни ребенка от преступников.*

В цифровом пространстве сложно узнать с кем ребенок общается. Преступники создают профиль, в котором представляют себя как сверстника и начинают общаться с ребенком на увлекательные темы. Уговаривают ребенка встретиться с ним в реальности.

Отметим наиболее **частые киберугрозы**, с которыми встречаются дети:

– *Нежелательный контент.*

К нежелательному контенту относится все то, о чем ребенку не следовало бы узнавать, как можно долгое время. К этой категории относятся порносайты, информация, пропагандирующая агрессивное поведение, алкоголизм, употребление наркотиков, самоубийство и многое другое. Нежелательный контент самая частая угроза, с которой сталкиваются дети в интернет-пространстве. При этом дети редко делятся с родителями своими открытиями.

– *Развитие пристрастия к азартным играм.*

Вопреки мнению, что дети сами «перерастут» игровую зависимость, это случается довольно редко. Чаще всего одни игры сменяются другими. Времени и потребности заниматься чем-либо еще становится все меньше.

– *Различные виды мошенничества.*

Фишинг (у детей пытаются разными способами узнать конфиденциальную информацию, номера и пароли банковских карт родителей и т.д.), непреднамеренная трата денег (во многих первоначально бесплатных онлайн-играх игрокам предлагается купить за деньги различные опции, дающие ощутимые преимущества в игре).

– *Вирусные атаки.*

Способствуют не только поломке компьютера, возможна кража конфиденциальной информации, личная переписка и многое другое, что в последствии может служить для преступников предметом шантажа.

– *Доступ к личной информации.*

Необходимо знать, что домашняя сеть не безопасна. Любая информация, которую вы размещаете или ищете, доступна любому. Особенно осторожно следует относиться к той информации, которую сами родители размещают в социальных сетях.

– *- Кибергруминг*

Прямая угроза жизни и здоровью детей от незнакомцев, предлагающих личные встречи через интернет-пространство. Общась в социальной сети с ребенком, преступник вызывает интерес и устанавливает эмоциональную связь с целью сексуального насилия и/или убийства.

*Рекомендованные действия родителей детей дошкольного
возраста по обеспечению кибербезопасности ребенка*

ПРАВИЛА КИБЕРБЕЗОПАСНОСТИ СПЕЦИАЛИСТЫ СОВЕТУЮТ

- Ограничьте время, которое ребёнок проводит в сети.
- Используйте средства обеспечения безопасности в Интернет-пространстве.
- Объясняйте детям, что нельзя принимать за правду всё то, что есть в Интернете.
- Избегайте самостоятельного использования Интернет пространства ребенком до 7 лет.
- Убедите ребенка не называть свое реальное имя и фамилию в Интернет-пространстве.
- Читайте специальную литературу, посвященную вопросам кибер и информационной безопасности
- Познакомьте ребенка с существующей маркировкой по возрасту (0+, 6+, 12+ и т.д.).

