**Безопасность подростков в сети Интернет.**

Виртуальная реальность: возможности и опасности. Основные правила медиабезопасности для родителей и подростков. Профилактика интернет-рисков. Как уберечь ребенка от опасностей в социальных сетях.

За сравнительно небольшой промежуток времени количество пользователей сети Интернет в Республике Беларусь превысило пять миллионов человек. Сегодня по плотности проникновения широкополосного доступа на 100 человек Беларусь вышла на среднеевропейские показатели, а по скорости – на третье место в мире. Указанные темпы проникновения информационных технологий во все сферы жизнедеятельности человека наряду с имеющей место не квалифицированностью определенной части пользователей являются предпосылкой возрастающего количества компьютерных инцидентов.

Особо проблемной видится ситуация использования возможностей компьютерных технологий и сети Интернет наиболее неподготовленными категориями пользователей, такими как дети и подростки, а также лица преклонного возраста.

Когда мы говорим о такой категории пользователей как дети, необходимо констатировать ряд причин, по которым именно они могут стать участниками (жертвами, виновниками, соучастниками) Интернет-происшествий.

1. Необходимо обратить внимание на особенности развития психологии ребенка, наивность его мышления, отсутствие критического подхода к фактам и событиям.
2. Следует отметить тот факт, что пользователями компьютерной техники (компьютерами, планшетами, смартфонами, телевизорами с функциями SmartTV и т.д.) становятся дети с младшего школьного возраста, наряду с этим отсутствует какая-либо система их подготовки к этому..

Таким образом, мы находимся в ситуации, когда ребенку с учетом его психофизиологических особенностей предоставляется неограниченный доступ к мощному инструменту обработки и обмена информацией, при этом отсутствуют системные механизмы обучения эффективному и безопасному использованию этого инструмента.

Ведение профилактической работы среди детей сотрудниками образовательных учреждений, представителями иных заинтересованных субъектов профилактики, может иметь определенный эффект в отношении детей старшего школьного возраста, но когда мы говорим о детях, делающих первые шаги в глобальной паутине, нужна постоянная индивидуальная работа с ребенком.

Основные риски и угрозы, которые могут возникнуть при использовании сети Интернет ребенком:

* вероятность совершения ребенком правонарушений в сфере информационной безопасности;
* вероятность совершения в отношении ребенка правонарушений в сфере информационной безопасности;
* вероятность совершения ребенком либо в отношении ребенка иных преступлений с использованием сети Интернет;
* возможность заражения компьютера при работе в сети Интернет вредоносными программами;
* возможность ознакомления ребенка с нежелательной информацией;
* возможность вовлечения в незаконный оборот наркосодержащих и психотропных веществ в сети Интернет;
* возможность вовлечения в сообщества деструктивного толка;
* грумминг;
* секстинг;
* кибербуллинг;
* возможность возникновения Интернет-зависимости.

Рассмотрим их подробнее.

* При использовании сети возможно совершение ребенком правонарушений в сфере информационной безопасности.
* Уголовным кодексом предусмотрен ряд преступлений, имеющих отношение к сфере высоких технологий.

***Совершение в отношении ребенка правонарушений в сфере информационной безопасности.***

Каждый пользователь компьютерной техники, сети Интернет автоматически становиться обладателем определенной компьютерной информации, которая хранится на жестких дисках компьютеров, в памяти мобильных телефонов на съемных носителях, в облачных хранилищах, которая содержится в учетных записях пользователей на различных Интернет-сайтах, например, в электронной почте, в социальных сетях, Интернет-дневниках. Все активнее в нашу жизнь входят электронные платежи в сети Интернет. При небрежном подходе к организации безопасности хранения и использования такой информации, ее владелец, в данном случае ребенок, может стать жертвой противоправных деяний третьих лиц, направленных на завладение и совершение неправомерных деяний по отношению к этой информации.

***Совершение ребенком либо в отношении ребенка иных преступлений с использованием сети Интернет.***

Необходимо понимать, что компьютер и Интернет – это всего лишь инструмент, в том числе используемый для совершения противоправных деяний. Такие давно известные правонарушения, как мошенничество, распространение клеветнических сведений, оскорбление, распространение материалов порнографического содержания, информации экстремистского содержания, разжигание межнациональной, межрасовой, межконфессиональной вражды и т.д. в настоящее время достаточно часто совершаются с использованием сети Интернет, что в некоторых случаях является дополнительным квалифицирующим признаком совершаемого преступления. Дети, пользуясь сетью Интернет и находясь в состоянии мнимой анонимности, умышленно либо по незнанию могут совершать такие деяния. Одновременно и ребенок должен быть проинструктирован на случай совершения в отношении него каких-либо противоправных деяний в сети.

***Возможность заражения компьютера при работе в сети Интернет вирусами.***

Вредоносные программы – различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения на компьютеры, не только через внешние носители информации, но и через электронную почту посредством спама или скачанных из интернета файлов.

***Возможность ознакомления   ребенка с  нежелательной информацией.***

Сеть Интернет является источником огромного количества информации, как полезной для ребенка, так и нежелательной, способной нанести непоправимый вред находящейся на этапе становления психике. К такой информации относят следующую тематику: наркомания, ярко выраженное насилие, экстремизм, жестокое обращение с детьми, оккультные и псевдорелигиозные организации и учения, аборты, азартные игры, порнография, знакомства, оружие, половое воспитание, алкоголь, табак и т.д.

***Вовлечение детей в незаконный оборот наркосодержащих и психотропных веществ в сети Интернет.***

В настоящее время Интернет стал основной площадкой нелегального оборота наркотических средств и психотропных веществ. Он предоставляет возможность ребенку как получить большой объем информации о наркотиках, так и практически не выходя из дома на условиях анонимности приобрести наркотики, психотропные вещества, курительные смеси. Также не исключена возможность вовлечения детей в преступные схемы распространения таких веществ.

***Возможность вовлечения детей в сообщества деструктивного характера.***

В сети Интернет активно ведут деятельность различные оккультные и псевдорелигиозные организации, сообщества пользователей деструктивной направленности. Неокрепшая психика ребенка зачастую является целью их деятельности. Периодически появляются сообщества в социальных сетях, ориентированные исключительно на детей, предлагающие в игровой форме осуществлять определенные действия, которые в итоге могут привести к угрозе психическому и физическому здоровью, а также в некоторых случаях и жизни ребенка.

***Груминг –*** это установление дружеского и эмоционального контакта с ребенком в Интернете для его дальнейшей сексуальной эксплуатации. Работают преступники по следующей схеме: лицо, заинтересованное в интимной связи с несовершеннолетним, представляется в сети другим человеком, зачастую сверстником, втирается в доверие к ребенку и настаивает на личной встрече. Последствия для поддавшегося на уговоры ребенка могут быть очень плачевны.

***Секстинг***– пересылка личных фотографий, сообщений интимного содержания посредством сотовых телефонов, электронной почты, социальных сетей. Опасны возможные последствия участия детей в таких действиях. Переписка с неизвестным пользователем, которым может оказаться взрослый человек, страдающий педофилией, чревата совершением в отношении ребенка преступлений на сексуальной почве. Распространение интимных фотографий зачастую используется преступниками для шантажа, известны случаи детских суицидов на данной почве.

***Кибербуллинг, или Интернет-травля*** – намеренные оскорбления, угрозы и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени. При этом такие действия могут совершаться сообща членами какого-либо Интернет-сообщества, в котором состоит ребенок, либо лицами, преследующими хулиганские мотивы. Проблемой в данном случае являются последствия психологического воздействия на ребенка.

***Интернет-зависимость*** – навязчивое желание войти в Интернет, находясь офлайн и неспособность выйти из Интернета, будучи онлайн. По своим симптомам Интернет-зависимость ближе к зависимости от азартных игр. Для этого состояния характерны следующие признаки: потеря ощущения времени, невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером, досада и раздражение при невозможности выйти в Интернет.

Как видим, представленный и далеко не исчерпывающий список угроз в сети позволяет констатировать, что неподготовленному ребенку при работе в сети Интернет может быть причинен существенный вред.

Встает вопрос, каким образом этот вред можно предотвратить. И здесь необходимо сделать вывод, что основным инструментом профилактики является планомерная и целенаправленная работа родителей с детьми с момента, когда они делают первые шаги в глобальную паутину, до момента, когда знания и психика детей достигают уровня, позволяющего обеспечить самоконтроль.

Родители должны обладать достаточным уровнем подготовки в части пользования компьютером, а также методикой воспитания подрастающего пользователя сети Интернет.

***На различных этапах становления личности и с приобретением опыта работы в сети используются различные подходы к обеспечению безопасности детей в Интернете, при этом необходимо учитывать следующие основные положения:***

* Интернет – не отдельный виртуальный мир, а всего лишь составляющая часть реальности, соответственно в сети Интернет действуют те же моральные и правовые ограничения, что и в повседневной жизни. В сети недопустимы поступки, которые непозволительны в реальности.
* Анонимность в сети Интернет, во-первых, является мнимой, поскольку личность любого пользователя сети может быть установлена. Во-вторых, ребенку необходимо объяснять, что его собеседник также находится в состоянии такой анонимности, поэтому к указанным им сведениям о себе, выложенным фотографиям, текстам сообщений всегда необходимо относиться критично.
* Использование сети Интернет может нести некоторые опасности (вредоносные программы, небезопасные сайты, Интернет-мошенники и др.), поэтому каждое действие должно быть подкреплено соображениями безопасности. Недопустимо совершение действий, в безопасности которых ребенок не уверен.
* Установите с ребенком доверительные отношения и положительный эмоциональный контакт в вопросе использования сети Интернет. Оговорите с ребенком критический уровень опасности, когда решение в возникшей проблемной ситуации должно приниматься родителями (иным доверенным лицом, обладающим достаточным опытом и познаниями, например, старшим братом или сестрой) либо по согласованию с ними.
* Установленные для ребенка правила работы в сети Интернет должны соответствовать возрасту и развитию Вашего ребенка. Применение слишком мягких правил на начальном этапе освоения сети ребенком может повысить риск возникновения у ребенка различных угроз. В то же время слишком жесткие правила либо запреты для ребенка, обладающего достаточным опытом и знаниями, могут повлечь игнорирование им всяких правил и использование выхода в сеть Интернет без какого-либо контроля родителей.
* Ребенку для работы в сети Интернет должен быть предоставлен в пользование компьютер со специфически настроенными параметрами. Он должен быть оснащен поддерживаемой производителем версией операционной системы с установленными актуальными обновлениями. В обязательном порядке на компьютере должно быть установлено и настроено актуальное антивирусное программное обеспечение, установлен и настроен сетевой экран. Родителями должен контролироваться перечень установленного на компьютере программного обеспечения и его настройки. При необходимости на компьютере должно быть установлено специальное программное обеспечение, позволяющее контролировать и ограничивать деятельность ребенка в Интернете. Используйте лицензионное программное обеспечение.
* В настоящее время наблюдается бурный рост информационных технологий и сети Интернет, в частности. В связи с этим программные, организационные меры обеспечения безопасности постоянно развиваются. Родители должны быть нацелены на саморазвитие в данной сфере и корректировать поведение детей в соответствии со складывающимися условиями.

***Рекомендации  родителям***

***Интернет с детьми различных возрастных групп.***

***Для детей от 7 до 10 лет***

* Оптимальной формой ознакомления ребенка в таком возрасте с сетью Интернет будет совместная работа с ребенком за компьютером.
* Приучите детей:
* посещать только те сайты, которые Вы разрешили;
* советоваться с Вами, прежде чем совершить какие-либо новые действия, раскрыть личную информацию;
* сообщать Вам, если ребенка что-то встревожило либо было непонятно при посещении того либо иного сайта.

Запретите:

* скачивать файлы из Интернета без Вашего разрешения;
* общаться в Интернете с незнакомыми Вам людьми;
* использовать средства мгновенного обмена сообщениями без Вашего контроля.

Постоянно беседуйте с детьми на тему использования ими сети Интернет: о действиях, посещенных сайтах, возможных новых знакомых.

***Для детей от 10 до 13 лет***

* В данном возрасте ребенок уже обладает определенными навыками и познаниями о работе в сети, не готов к постоянному личному контролю со стороны взрослых, однако все еще требует контроля.

Рекомендации:

* создайте ребенку на компьютере собственную учетную запись с ограниченными правами;
* используйте средства фильтрации нежелательного контента;
* напоминайте о конфиденциальности личной информации;
* приучайте ребенка спрашивать разрешение при скачивании файлов из Интернета, при скачивании и установке программного обеспечения;
* поощряйте желание детей сообщать Вам о том, что их тревожит или смущает в Интернете;
* настаивайте на том, чтобы ребенок позволял Вам знакомиться с содержимым его электронной почты, учетных записей в социальных сетях, перепиской в средствах мгновенного обмена сообщениями;
* расскажите об ответственности за недостойное поведение в сети Интернет.
* На данном этапе могут активно использоваться программные средства родительского контроля, к которым можно отнести следующие инструменты:
* услуга родительского контроля провайдера, оказывающего услугу доступа в сеть Интернет, позволяющая ограничить доступ к Интернет сайтам, содержащим нежелательный контент;
* функции родительского контроля, встроенные в операционную систему (ограничение времени работы компьютера, ограничение запуска программ, в том числе игр);
* функции родительского контроля, встроенные в некоторые антивирусы (например Kaspersky Internet Security, Norton Internet Security), позволяющие контролировать использование компьютера, запуск различных программ (попытки запуска запрещенных программ блокируются), использование Интернета (ограничение по времени), посещение веб-сайтов в зависимости от их содержимого, загрузку файлов из Интернета, переписку с определенными контактами через Интернет мессенджеры и социальные сети, пересылку персональных данных, употребление определенных слов и словосочетаний в переписке через мессенджеры;
* специализированное программное обеспечение, предназначенное для выполнения функций родительского контроля, например, КиберМама, KidsControl, TimeBoss и другие.