ПОСОБИЕ ПО ЗАЩИТЕ МОЛОДЕЖИ В ОНЛАЙН СРЕДЕ

Ташкент – 2016

В настоящее время, когда Интернет *(INTERNET, сокращённое от INTERconnected NETworks – объединённые сети)* – глобальная всемирная телекоммуникационная сеть становится частью жизни человека с самого раннего возраста, защита детей является важнейшей проблемой, которая срочно требует глобальной скоординированной реакции. Сеть Интернет трансгранична и содержит в себе как полезную информацию, так и большое количество негативной, деструктивной информации, несовместимой с моральными и этическими нормами, которые отрицательно влияют на сознание и нравственное воспитание молодого подрастающего поколения.

Настоящее руководство несет рекомендательный характер и разработано на основе результатов исследований по проблемам безопасности детей в сети Интернет, в рамках инициативы Центра обеспечения информационной безопасности и адресовано пользователям-подросткам и их родителям.

Цель – не изолировать ребенка от Интернета,
а создать полноценный инструмент для его развития

Интернет играет очень значительную роль в воспитании ребенка, так как модели поведения, нормы жизни, образ мыслей, картина мира – все то, одним словом, что и называется воспитанием, в большой степени черпается ребенком в сети. Иногда родители считают, что дома за компьютером их ребенок в безопасности, однако, в виртуальном мире детей также могут поджидать определенные риски, угрозы и опасности. Чтобы понять, как защитить себя от рисков и угроз, уберечь себя от опасности, специалисты по информационной безопасности подготовили некоторые несложные правила и рекомендации, на которые следует обратить особое внимание и помнить при работе с Интернетом.

РИСКИ – в сети существуют три основных типа:

Контентный риск – присутствие в сети различных материалов (текстов, изображений, аудио-, видео файлов, ссылок), содержащих противозаконную, неэтичную и вредную информацию (насилие, жестокость, безнравственность, нецензурную лексику, разжигание расовой, этнической и межнациональной розни, терроризм и религиозный экстремизм, пропаганду наркотических и психотропных препаратов, суицид, азартные игры), негативно сказывающуюся на моральном и духовном воспитании молодого поколения.

Коммуникационный риск – возникает в процессе межличностного общения в сети Интернет с незнакомыми (малознакомыми) пользователями. Анонимность и уверенность в своей безнаказанности некоторых пользователей приводит к оскорблениям, троллингу, кибербуллингу, домогательствам и шантажу в сети.

Технический риск – повреждение ПО или хищение конфиденциальной, личной информации, посредством вредоносных программ (вирусы, боты, шпионские программы) и кибермошенничество.

УГРОЗЫ – специалисты классифицировали основные виды угроз, которым подвергаются дети во «всемирной паутине», что несомненно, может отразиться на их психике.

1. Легкая доступность к нежелательным сайтам и материалам (фото, видео, аудио и публикации) содержащие сцены жестокости, насилия, безнравственность, аморального поведения, информацию о наркотиках, о призывах к противоправным действиям, расовую и этническую ненависть.

2. Общение, переписка, знакомство с незнакомыми людьми посредством электронной почты, социальных сетей и различных сомнительных форумов.

3. Процесс не контролируемых покупок через Интернет и бесконтрольное времяпровождения за онлайн играми, с которыми также имеют дело дети в Интернете.

ОПАСНОСТИ – эксперты по информационной безопасности выделили **5** наиболее важных типов опасности, пренебрежение к которым может негативно отразиться на детях.

1. Потеря родительского авторитета вследствие бесконтрольного пользования Интернетом.

Зачастую родители оставляют подростка один на один с всемирной сетью, посчитав его взрослыми, или просто, лишь бы ребенок был отвлечен чем-то и не мешал родителям. Это первый шаг к тому, что молодые люди начинают бесконтрольно пользоваться Интернетом, что впоследствии приводит к тому, что дети перестают слушать родителей, врать им и огрызаться.

2. Перевёрнутая система культур, идей, идеологий.

Дети постоянно ищут способы самовыражения, свое место в обществе. Они остро нуждаются в ощущении своей независимости и самостоятельности. И на этом пути, распространяемая и пропагандируемая в сетях Интернет перевёрнутая система культур, так называемых субкультурных течений, как «готы», «эмо» и т.д., идеология религиозно-экстремистского толка представляют особую опасность для молодых людей, у которых ещё не сформирована личность. Кроме этого, зачастую в сети можно услышать песни (клипы), содержащие мат, наполненные тоской, пессимизмом и отвращением к людям, песни с тюремными «понятиями». В сюжетах некоторых песен прослеживается противостояние с обществом, презрение к закону, драки, криминальные разборки, убийства, наркотический кайф, и тому подобное. Влияние такого рода искусства «нулевой» художественной ценности, описывать нет смысла.

3. Анонимное Интернет-общение.

Онлайн-общение отличается по своей природе от «живого» общения. Тут совсем другие нормы и правила поведения, другие этические стандарты, другие регуляторы. В форумах, чатах, сообществах происходит общение с неизвестными людьми, и анонимность подталкивает людей к вседозволенному поведению и высказываниям в Интернете, которые никогда бы они себе не позволили в реальном мире. Анонимное общение может привести к оскорблениям, кибербуллингу, унижениям и домогательствам в сети.

Знакомства в Интернете явно относятся к тем критериям, которые родители просто обязаны контролировать во имя безопасности ребенка, в том числе и физической.

4. Потеря персональных данных.

В большинстве случаев утечка персональных данных происходит из-за излишней доверчивости и открытости пользователей, в основном детей и подростков, в сети Интернет. Это случается в чатах, форумах при заполнении анкет, при совершении онлайн-покупок, а также при регистрации в социальных сетях. Этот набор персональных данных, лакомый кусочек для злоумышленников, которые могут воспользоваться ими в корыстных и противоправных целях. Особенно хочется отметить то, что основным местом утечки персональных данных являются аккаунты (страничка) в социальных сетях. Многие молодые пользователи в них выкладывают в свободный доступ всё, начиная от имени и года рождения (номер телефона, школы, адреса проживания, места, где они любят бывать, описывают свое настроение и характер), до личных фото в огромном количестве.

5. Игромания.

Онлайн-игры действительно увлекательны, их разработчики сделали все, чтобы пользователь как можно дольше оставался в игре. Современные онлайн-игры требуют много времени для прохождения определенных этапов и предлагают бесконечное развитие персонажей, что приводит к полному погружению молодых пользователей в игру. Подростки нуждаются в самовыражении и самореализации, что они и находят в

играх. Это может привести к психологическому расстройству – зависимости. Многие дети начинают пропускать учёбу, забывают поесть, не спят, проводя время за игрой.

6. Повреждение программного обеспечения, посредством вредоносных программ (вирусы, спамы, шпионские программы, фишинги).

Интернет-мошенники часто пользуются доверчивостью и незнанием молодых пользователей о разного рода атак, путем внедрение вредоносных программ на компьютеры пользователя. Так, переход по незнакомым ссылкам, скачивание программ и других мультимедийных файлов с неизвестных сайтов, чтение писем от непонятных «друзей», может привести к заражению компьютера вирусами, что приведет в конечном итоге к негативным последствиям.

Компьютерный вирус – это вид вредоносной программы, способный создавать копии самого себя и внедряться в код других программ, а также распространять свои копии по разнообразным каналам связи. Целью вируса является нарушение работы компьютера, удаление файлов, блокирование работы пользователей и т. п.

Шпионские программы – это программы, которые скрытным образом устанавливаются на компьютер с целью сбора информации о конфигурации компьютера, пользователе, пользовательской активности, а также производящие другие действия: изменение настроек, установка программ без ведома пользователя, перенаправление действий пользователя.

Спам – массовая рассылка писем содержащих вредные материалы.

Фишинг – письмо или ссылка, которое обычно маскируется под официальное сообщение. Для того, чтобы жертва не догадалась об обмане, оформление сайта или письма, имитируется под оформление официального варианта.

Исходя из вышеизложенного, мы хотим предложить несколько простых советов по Интернет-безопасности, которые помогут защитить детей и подростков в Интернете.

Однако, учитывая, что каждый ребенок, это индивидуальная личность и к каждому нужен свой подход, специалисты поделили детей и подростков на следующие возрастные категории:

1) **7-10 лет** – в данном возрасте познание ребенка самое активное и требует контроля в предоставлении правильной информации, у них только формируется информационное сознание. Большинство пользователей данной возрастной группы только научились читать и до конца не понимают, на какой сайт они вошли и с каким контентом могут столкнуться. Дети в основном пытаются найти что-то красочное и интересное, в частности интерес вызывают красочные игры и мультфильмы. Поэтому, пользование детьми 7–10 лет Интернетом должно все время контролироваться родителями или взрослыми. Целесообразно фильтровать информацию в сети Интернет или частично ограничить те ресурсы, которые вредны для подрастающего поколения. Например, путем создания списка безопасных веб-сайтов или использование фильтрующих программ, которые подходят данному возрасту. Цель состоит в том, чтобы научить данную возрастную группу основам безопасности в Интернете, этикету и пониманию правильности той или иной информации.

2) **10-13 лет** – данный промежуток очень важен, поскольку он является сложным переходным возрастом для ребенка. Данная категория отличается тем, что дети начинают многое осознавать, и становятся, наиболее любопытными. В этом возрасте уже не детское любопытство толкает их к поискам других стереотипов, что важно учитывать и при Интернет общении. Так, наряду с играми и поиском информации в сети, данная группа молодых людей активно пользуется социальными сетями и чатами в поиске новых друзей.

3) **13-16 лет** – данная категория состоит из подростков. Она охватывает обширный круг и требует особого подхода, учитывая то, что именно в этом возрасте подросток формируется как личность, как полноправный член общества. Эта категория молодых людей активно пользуется Интернетом. Интернет для них это большая база информации,

средство общения с друзьями и сверстниками, а также место, где можно провести досуг. Огромное количество молодых людей в этом возрасте пользуется социальными сетями и приложениями мгновенных сообщений (мессенджерами).

Главной проблемой в этом возрасте является то, что родители зачастую перестают контролировать своих детей, посчитав их уже достаточно взрослыми. Этот возраст можно считать возрастом «информационного голодания», когда подросток становится старше и ему хочется знать всё и даже больше. Выход в онлайн для многих является частью повседневной жизни.

На сегодняшний день, к сожалению, ещё не разработана норма времяпрепровождение детей и подростков в сети Интернет. Мнение специалистов расходятся.

Средняя продолжительность непрерывной работы в Интернете, по мнению большинства психологов, врачей, педагогов должна быть следующей:

- ✓ **7-10 лет** – 1 час в день
- ✓ **10-13 лет** – 1,5 часа в день
- ✓ **13-16 лет** – 2 часа в день

Стоит также отметить, что за время нахождение ребенка перед экраном, необходимо делать перерывы не менее 10 минут. Так безопасное времяпрепровождение молодежи различного возраста в Интернете направленно на защиту подростков и детей от «Интернет-зависимости» или от таких болезней как ухудшение зрения (синдром «сухого глаза»), искривление позвоночника (скалиоз), нарушения осанки (сутулость), которые, как правило, вызываются длительным нахождением за компьютером.

Предложения по защите для возрастной группы 7-10 лет

- прежде, чем начать поиск, нужно иметь четкое представление о том, что вы ищете;
- не заходите на незнакомые сайты, не переходите по незнакомым ссылкам и не делитесь ссылками на такие веб-сайты;
- если вы попали или зашли на сайт со взрослым контентом или материалами, которые вызывают у вас негативное отношение, то попытайтесь сразу покинуть данный сайт;
- не загружайте файлы и не устанавливайте их сами, попросите взрослых сделать это;
- не принимайте условия, не заполняйте анкеты или другие требования;
- добавьте в «избранное» те ресурсы, которыми вы часто пользуетесь и на которых правильный и достоверный контент;
- если вам стали приходить сообщения от незнакомых людей или с сайтов с некорректным и грубым содержанием, игнорируйте и блокируйте их.

При любых обстоятельствах, если что-то вас беспокоит или вызывает сомнения, обсудите это с родителями.

Рекомендации родителям данной категории детей:

– объясните детям, что им разрешено, а что запрещено делать в Интернете;

– ограничьте время нахождения ребенка в сети, и постарайтесь проводить время за компьютером вместе с ним;

– внесите нежелательные сайты в «черный список» браузера.

Многие продукты для обеспечения безопасности в Интернете сочетают в себе возможности антивирусной защиты и расширенные функции родительского контроля, которые помогают защитить детей, когда те находятся в Интернете;

– если детям разрешено использовать программы мгновенного обмена сообщениями или посещать Интернет-чаты, расскажите им об опасностях общения или отправки сообщений людям, которых они не знают и которым не доверяют;

– попросите детей рассказывать обо всем, что вызывает у них неприятные чувства или дискомфорт при посещении Интернета.

Предложения по защите детей для возрастной группы 10–13 лет

• при поиске нужной информации, необходимо иметь четкое представление о том, что вы ищете;

• не заходите на незнакомые сайты, не переходите по незнакомым ссылкам, адреса которых получены из недостоверных источников,

• не принимайте письма или приглашения от незнакомого человека, а также не делитесь ссылками на такие веб-сайты;

• если вы попали или зашли на сайт, где размещены публикации, видео, аудио или фотоматериалы с «недетским» содержанием (сцены безнравственности, насилия, жестокости), то попытайтесь сразу покинуть данный ресурс;

• не загружайте незнакомые файлы и не устанавливайте их без согласия родителей;

• не принимайте условия, не заполняйте анкеты или другие требования на малознакомых сайтах и различных ссылках;

• храните свои персональные данные конфиденциально. Не размещайте свои личные данные в открытом доступе (ф.и.о, адрес, телефон, г.р.);

• храните свои пароли в секрете, не разглашайте их, не посылайте друзьям, знакомым. Создайте трудно подбираемый пароль с использованием цифр, букв и символов.

• используйте «ник» вместо своего настоящего имени, если вы играете в онлайн-игры или находитесь в незнакомом чате с большим количеством пользователей;

• будьте осторожны с тем, с кем общаетесь, знакомитесь в онлайн среде. Не принимайте предложения дружбы, если вы действительно не знайте этого человека и не уверены в нем. Человек может притвориться тем, кем на самом деле не является;

• если вам стали приходить сообщения от незнакомых людей или с сайтов с некорректным и грубым содержанием, игнорируйте и заблокируйте тех, кто оскорбляет вас в сети или пишет что-то пугающее. Не поддавайтесь на провокации.

При любых обстоятельствах, если что-то вас беспокоит или вызывает сомнения, обсудите это с родителями.

Рекомендации родителям данной категории детей:

– поговорите с вашим ребенком, расскажите, про отрицательные стороны бесконтрольного пользования сетью Интернет, объясните, что ему разрешено, а что запрещено делать в Интернете;

– ограничьте время нахождения ребенка в сети, контролируйте посещаемые им ресурсы или постарайтесь проводить время за компьютером вместе с ним;

– если детям разрешено использовать программы мгновенного обмена сообщениями или посещать Интернет-чаты, расскажите им об опасностях общения или отправки сообщений людям, которых они не знают и которым не доверяют;

– если ребенок пользуется социальными сетями, создайте аккаунт сами (знайте их логин и пароль), контролируйте размещаемую вашим ребенком информацию на своей страничке;

– спрашивайте и будьте в курсе о всех виртуальных друзьях ваших детей. Объясните вашему ребенку, что нельзя встречаться с онлайновый другом в реальной жизни, наедине;

– внесите нежелательные сайты в «черный список» браузера или установите функцию «родительский контроль» на вашем компьютере. Это поможет избежать посещения вредных сайтов в ваше отсутствие;

– попросите детей рассказывать обо всем, что вызывает у них неприятные чувства или дискомфорт при посещении Интернета.

Предложения по защите для возрастной группы 13–16 лет

• при работе в поисковиках ищите только ту информацию, которая действительно вам нужна;

• пользуйтесь информацией только из достоверных источников и проверенных сайтов. Всегда дважды проверяйте информацию из других надежных источников;

• не посещайте малознакомые веб-сайты или те, которые вызывают у вас недоверие.

• не переходите по незнакомым ссылкам и не делитесь ссылками на такие веб-сайты, адреса которых получены из недостоверных источников, в письмах или приглашениях от незнакомого человека;

• если вы попали на сайт с нежелательным контентом, где размещены материалы (видео, аудио, фото или другая информация) вызывающие у вас негативное чувству, то попытайтесь сразу покинуть данный ресурс;

• не загружайте файлы с малознакомых или непроверенных ресурсов, не устанавливайте их без согласия родителей;

• не соглашайтесь и не принимайте условия, не дочитав их до конца;

• не заполняйте анкеты или другие требования на незнакомых сайтах и различных ссылках;

• не размещайте свои персональные данные в открытом доступе (ф.и.о., адрес, телефон, г.р.). Личные данные должны быть конфиденциальны;

• запомните, Интернет это ваш «цифровой отпечаток». Загруженные вами персональные данные, видео, аудио ролики или изображения хранятся там постоянно. Эти данные могут быть использованы в корыстных целях другими пользователями.

• не разглашайте, не делитесь и не посылайте друзьям, знакомым свои пароли и логины. Храните их в секрете. Создайте трудно подбираемый пароль с использованием цифр, букв и символов;

• используйте «ник» вместо своего настоящего имени, если вы играете в онлайн-игры или находитесь в незнакомом чате с большим количеством пользователей;

• будьте осторожны с тем, с кем общаетесь, знакомитесь в онлайн среде. Не принимайте предложения дружбы, если вы действительно не знайте этого человека и не уверены в нем;

• если вам стали приходить спам-сообщения от незнакомых людей или с сайтов, удаляйте их не читая и не открывая. Они могут содержать вирусы;

• если кто-то оскорбляет вас в сети или пишет что-то пугающее, не поддавайтесь на провокации, проигнорируйте и заблокируйте их.

При любых обстоятельствах, если вы видите, что что-то вас беспокоит, обсудите это с родителями.

Рекомендации родителям данной категории детей:

– по возможности контролируйте время нахождения ребенка в сети и посещаемые им ресурсы или постарайтесь проводить время за компьютером вместе с ним;

– поговорите с вашим ребенком, расскажите, про отрицательные стороны бесконтрольного пользования сетью Интернет, объясните, что ему разрешено, а что запрещено делать в Интернете;

– расскажите детям, что онлайновый друг может оказаться совсем другим человеком, не таким, каким его или ее представляли;

– если ребенок хочет встретиться с виртуальным другом в реальной жизни, объясните ему, что он должен пойти на встречу не один, а позвать с собой кого-то надежного (взрослого), для того чтобы избежать любой проблемы в случае, если встреча обернется разочарованием;

– попросите своего ребенка не совершать покупок с помощью Интернет-магазина, не посоветовавшись с взрослыми;

– если ребенок пользуется социальными сетями, попросите его поделиться информацией размещенной в его аккаунте, а также логин и пароль, контролируйте размещаемую и потребляемую вашим ребенком информацию на своей страничке;

– попросите детей рассказывать обо всем, что вызывает у них неприятные чувства или дискомфорт при посещении Интернета.

Заключение

Описание рисков, угроз и опасностей в Интернет-среде приведённые и освещенные в данном руководстве могло создать ложное впечатление об Интернете как о полностью вредной, разрушительной среде. Конечно, это не так. В Интернете есть много полезной, познавательной и интересной информации, правильное, рациональное и грамотное использование которой даст пользователю большую базу знаний, умений и навыков в различных сферах. А задача родителей состоит в том, чтобы научить ребенка грамотно пользоваться всеми положительными возможностями «виртуальной сети». Для этого необходимо тщательно проверять информацию и учить этому детей, формировать у детей нормальную систему ценностей, адекватную картину мира, знакомить их с подлинной великой наукой и подлинным великим искусством. Вместе с этим, у пользователей из числа молодого поколения необходимо **развивать и формировать «Интернет-культуру».**

Интернет-культура – предусматривает культуру потребления, освоения и передачи информации любого содержания и источника. Интернет-культура – это осознанное ограничение доступа к негативной информации в Интернет сети, влияющую на общественное сознание, направленную на смену конституционного строя, в том числе содержащих религиозно-экстремистскую, террористическую, порнографическую, насилия, жестокость и другую вредную информацию. В основе Интернет – культуры лежат общепринятые нравственные требования к общению, неразрывно связанные с признанием неповторимости и ценности каждой личности.

Незнание Интернет-культуры может привести к неограниченному общению пользователей в Интернете и социальных сетях, обмену непроверенной и неподтверждённой информации с «анонимными» пользователями. Данная тенденция может привести к таким часто встречающимся негативным последствиям в Интернете, как киберпреступность, кибербуллинг.

Вместе с этим, хочется отметить, что доверительные отношения с детьми, открытый и доброжелательный диалог зачастую может быть гораздо конструктивнее, чем постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.

Методичка разработана в Центре Обеспечения информационной безопасности при Министерстве по развитию информационных технологий и коммуникаций Республики Узбекистан, и утверждена совместным постоновлением Министерства по развитию информационных технологий и коммуникаций, Министерства Народного образования, и Высшего и средне - специального образования, от 7 апреля 2016 года № 14-03-, 24- и 22-қ/қ.