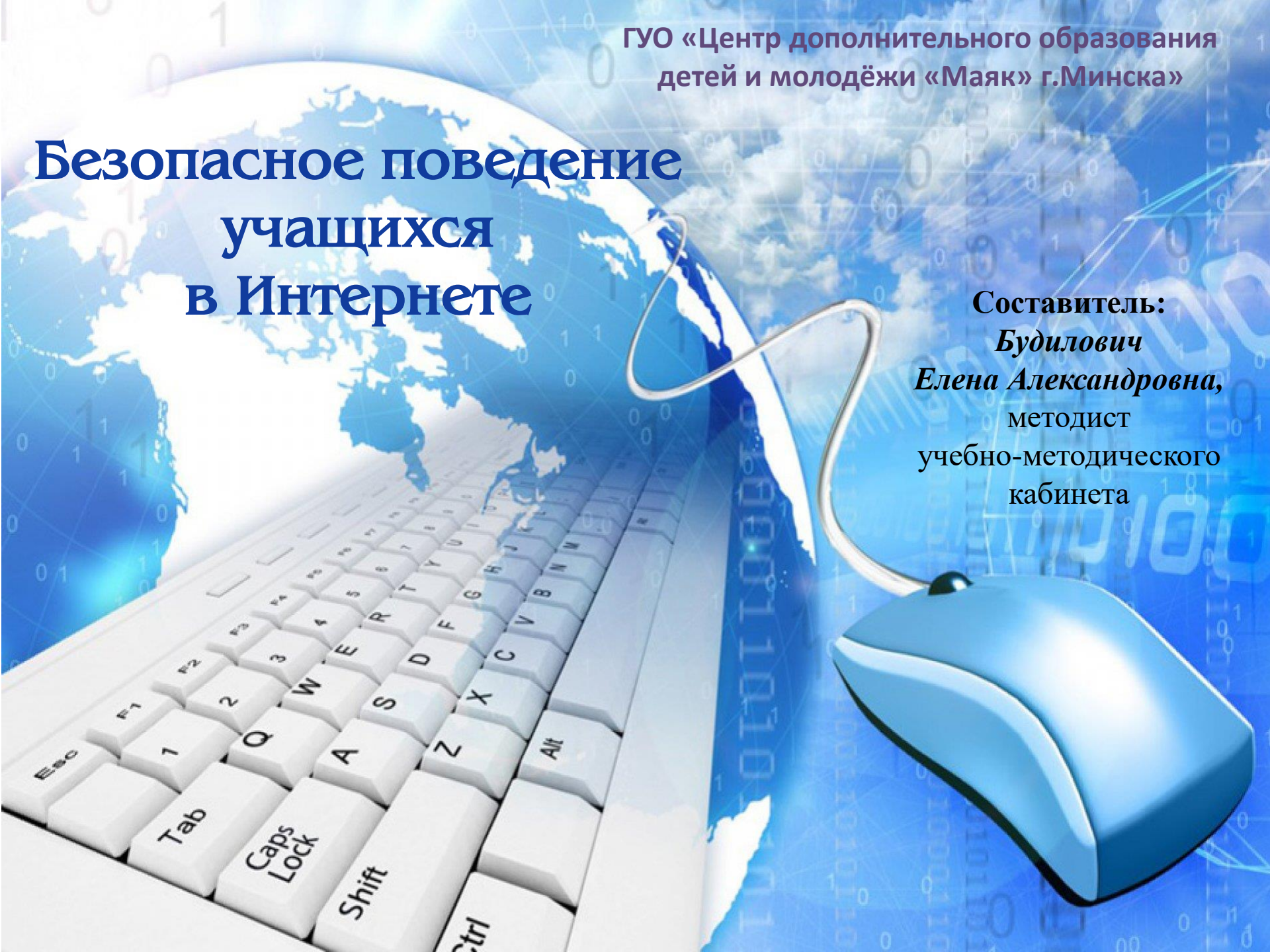
ГУО «Центр дополнительного образования
детей и молодёжи «Маяк» г.Минска»

Безопасное поведение учащихся в Интернете

Составитель:
Будилович
Елена Александровна,
методист
учебно-методического
кабинета



В наши дни мы все проводим много времени в интернете, в том числе дети и подростки. Каждый родитель хочет, чтобы дети чувствовали себя в безопасности, находясь в сети, ведь в интернете есть вещи, которых следует опасаться. Опасны не только вирусы и хакеры, которые могут украсть личную информацию; помимо них существует кибербуллинг (травля), неприемлемый контент и онлайн-хищники, нацеленные на детей и подростков.

Детям и подросткам интернет необходим для выполнения школьных заданий, общения с учителями и другими учениками, интерактивных игр и выполнения других задач. Это прекрасное место для обучения и общения. Но родители должны быть в курсе того, что их дети видят и слышат в Интернете, с кем общаются и что рассказывают о себе.

Обеспечение информационной безопасности понимается как состояние защищённости детей и учащейся молодёжи, при котором минимизирован риск, связанный с причинением информацией вреда здоровью, нормальному физическому, интеллектуальному, психическому, духовному и социальному развитию детей и учащейся молодёжи.

Данные исследований:

- ✓ **90%** детей ежедневно заходят в интернет;
- ✓ каждый **3-ий** из них находится в сети **от 3 до 5 часов**;
- ✓ каждый **6-ой** ребенок – **от 5 до 8 часов**.

Особенности общения в сети

- ✓ невидимость субъекта коммуникации;
- ✓ анонимность;
- ✓ слабая регламентированность поведения;
- ✓ разнообразие сред общения, видов деятельности и способов самопрезентации;
- ✓ внешние воздействия мало влияют на поведение, что благоприятствует проявлению в поведении индивидуальных различий.

Ощущение вседозволенности

Интернет – это…

- «…место, где можно сделать всё, что хочется»?
- «…свободное пространство, где по своему усмотрению можно делать всё, что пожелаешь»?
- «… просто свобода!»?
- «…сеть, в которой можно всё»?
- «…место, где все чувствуют себя свободнее и увереннее»?

- «…свободный виртуальный мир, где есть абсолютно всё»?

Правила поведения в социальных сетях: как улучшить имидж

Не рекомендуется:

- просить о репосте;
- спамить;
- излишне увлекаться селфи;
- репостить фейки (запрещено);
- часто выкладывать фото мест, где Вы побывали;
- отмечать друзей на фотографиях без спроса;
- отмечать друзей в постах и поздравлениях без спроса;
- страдать «напоказ»;
- злоупотреблять хэштегами;
- добавлять в группы друзей без спроса.

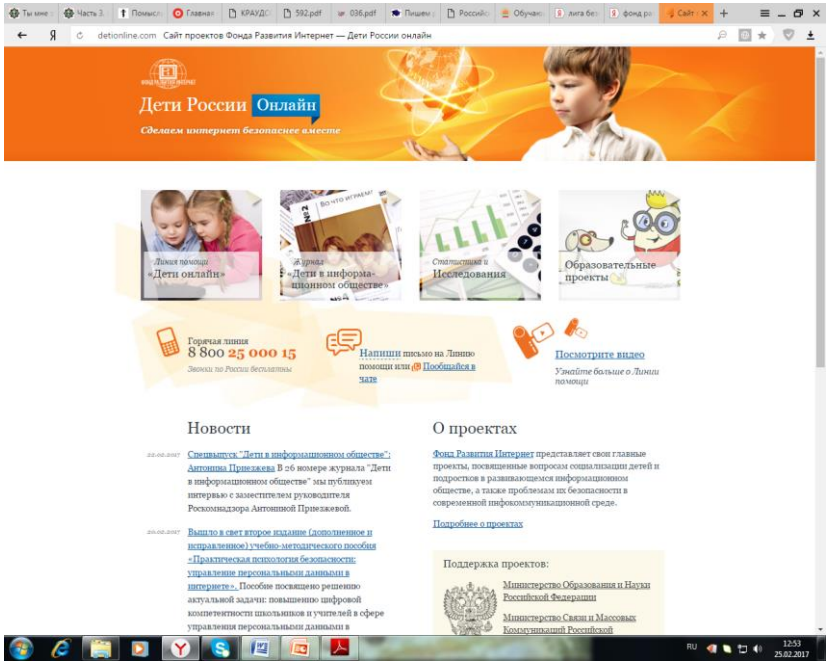
http://www.spb.kp.ru/daily/26515.7/3531703/

Необходимо:

- следить за фоном на снимках;
- писать грамотно, без сокращений.

НЕТИКЕТ

- Нетикет - это сетевой этикет или правила поведения в сети. Интернет практически не регулируется законами, за исключением тех случаев, когда к нему прямо применимы законы, действующие в "реальной жизни". Однако существуют некоторые традиции и культура интернет-сообщества, которых придерживается большинство пользователей.
- Сеть - это публичное место. В нем "ходят" разные люди, в том числе и дети. Уважайте окружающих. Если вы новичок, ведите себя как в гостях - будьте готовы изучить и понять чужие правила и принципы, прежде чем устанавливать свои.



http://detionline.com/

Нетикет

Нетикет (*net* + *etiquette*) – правила хорошего тона при общении в Интернете.

Электронная почта:

- тема сообщения, приветствие, подпись
- не набирать предложения заглавными буквами
- не посылать большие файлы без договоренности
- не пересылать исполняемые файлы (*.exe)
- не использовать нецензурных и жаргонных выражений

Форумы:

- прочитать список вопросов и ответов (FAQ, ЧаВо)
- не отклоняться от темы форума *(off-topic* – «вне темы»*)*
- не набирать предложения заглавными буквами
- не оскорблять участников

Чаты:

- не встревать в чужой разговор
- не обижаться, если он ушел

ПРАВИЛА БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ ДЛЯ ДЕТЕЙ

Никогда не рассказывай о себе незнакомым людям в Интернете: где ты живешь и учишься, не сообщай свой номер телефона. Не говори никому, где работают твои родители и номера их телефонов.

Всегда спрашивай родителей о непонятных вещах, которые ты встречаешь в Интернете. Они расскажут тебе, что можно делать, а что нет.

Никогда не отвечай на сообщения от незнакомцев в Интернете и не отправляй им смс. Если незнакомый человек предлагает встретиться или пишет тебе оскорбительные сообщения — сразу скажи об этом родителям!

Если в Интернете ты решил скачать картинку, игру или мелодию, а тебя просят отправить смс — не делай этого! Ты можешь потерять деньги, которые мог бы потратить на что-то другое.

Если ты регистрируешься на сайте, в социальной сети или в электронной почте, придумай сложный пароль, состоящий из цифр, больших и маленьких букв и знаков. Помни, что твой пароль можешь знать только ты и твои родители.

Ключевые коммуникационные риски в Интернете для детей

- общение с незнакомцами;
- агрессия в Интернете;
- троллинг;
- кибербуллинг;
- секстинг;
- груминг.

Троллинг *– (англ. trolling означает «ловлю рыбы на блесну»)* нарушение этики сетевого взаимодействия, выражающееся в виде проявления различных форм провокационного, агрессивного, издевательского и оскорбительного поведения.

Прямой троллинг:

- оскорбления участников;
- нарушение правил ресурса;
- подстрекание.

Замаскированный троллинг:

- сообщения не по теме;
- возвращение к другой острой теме;
- завуалированные негативные сообщения.

Кибербуллинг – агрессивные, умышленные, социально негативные действия, совершаемые систематически на протяжении длительного времени одним или несколькими лицами с использованием электронных или цифровых средств коммуникации, в отношении того, кто не имеет возможности защитить себя в актуальной ситуации.

http://www.klicksafe.de/ueber-klicksafe/downloads/weitere-spots/uk-childnet-lets-fight-it-together-english/
http://old.digizen.org/cyberbullying/kim.aspx?video
http://old.digizen.org/cyberbullying/teacher.aspx
http://old.digizen.org/cyberbullying/rob.aspx
http://old.digizen.org/cyberbullying/mum.aspx

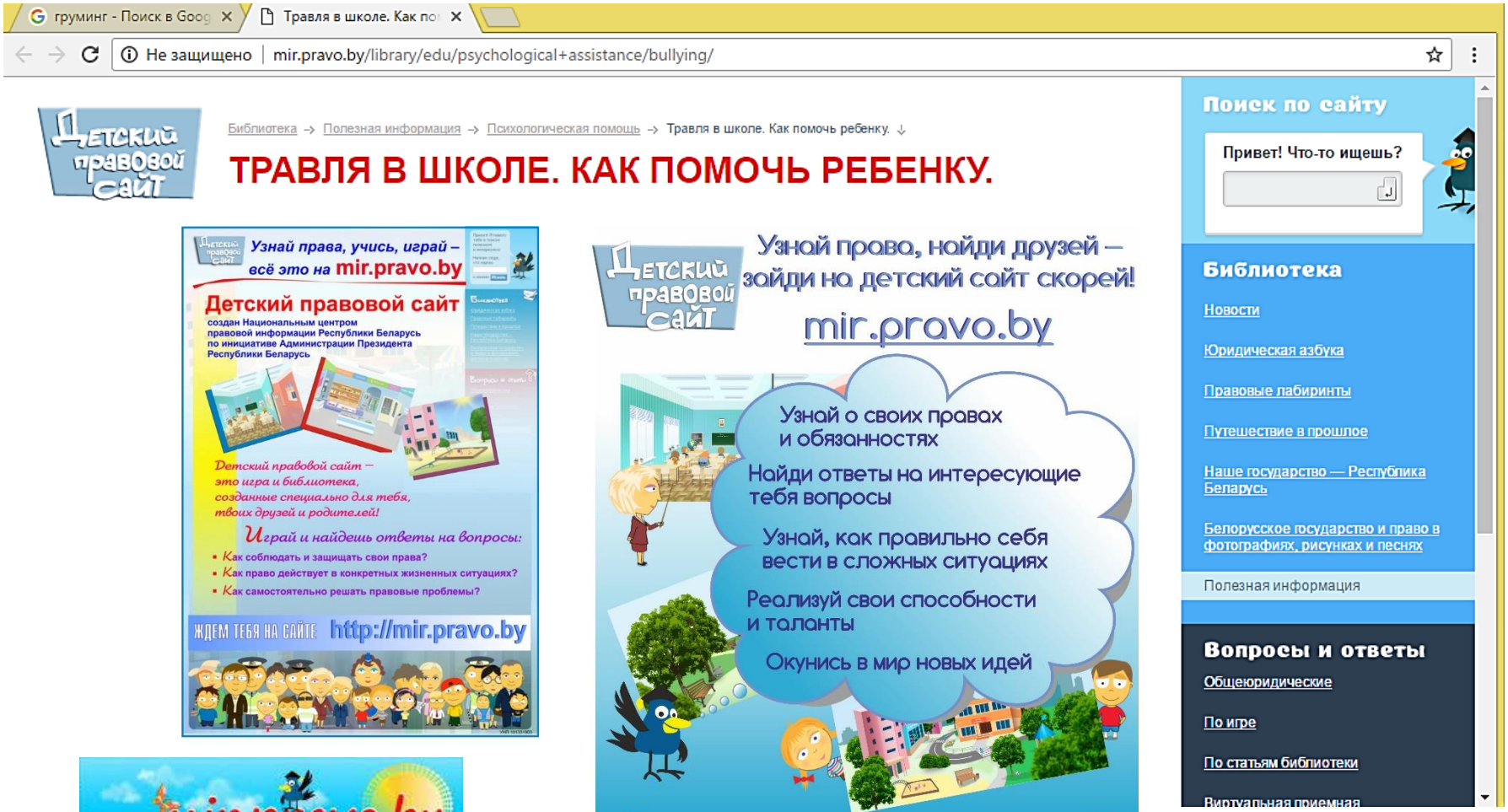
Секстинг (англ. *sexting*) – пересылка личных фотографий, сообщений интимного содержания посредством современных средств связи: сотовых телефонов, электронной почты, социальных интернет-сетей.

В некоторых странах, в частности в США и Австралии, секстинг является уголовным преступлением, если на интимных фотографиях изображён несовершеннолетний; это рассматривается как детская порнография – причём виновными считаются оба: как человек, отправивший фотографии, так и получивший их – это классифицируется как производство и хранение детской порнографии соответственно. Кроме того, лицу, пославшему свои фотографии в обнажённом виде, могут быть предъявлены обвинения в сексуальном домогательстве.

Термин **«груминг»** происходит от английского слова *«grooming»*, которое буквально переводится как «уход», «забота». Оно передаёт основную суть метода интернет-хищников: создать у ребёнка ощущение, что о нём заботятся, им искренне интересуются, вызвать у него ощущение психологической связи. Груминг включает в себя завоевание доверия ребёнка или подростка на основе его или её интересов. Эти интернет-хищники чрезвычайно ловко манипулируют людьми. Иногда для преследования и соблазнения ребёнка используются подарки, деньги, даже билеты на транспорт, чтобы завлечь его туда, где интернет-хищник сможет совершить сексуальное насилие над ним или ней.

Такие события даже могут фотографироваться или сниматься на видео, или, если встреча происходит не в реальном мире, интернет-хищник может принуждать ребёнка создавать изображения сексуального характера со своим участием или участием своих друзей, или принять участие в действиях сексуального характера, используя веб-камеру для их трансляции. Многие дети и подростки, которые вовлечены в такие виды преступных отношений, в определённой степени испытывают недостаток эмоциональной зрелости или имеют низкую самооценку. Это может сделать их восприимчивыми к такому роду манипуляциям и запугиваниям. Также они могут не торопиться рассказать взрослым о своих встречах, испытывая замешательство или страх потерять доступ в интернет. В некоторых случаях они запуганы интернет-хищниками, и им приказано держать эту связь или то, что случилось, в тайне.

Детский правовой сайт www.mir.pravo.by



Рекомендации для родителей по преодолению контентных рисков

- ✓ Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определённой тематикой. Настройки браузера устанавливаются бесплатно. На сайте каждого разработчика можно найти подобную информацию в разделе «Безопасность». Специальные программы, называемые системами родительского контроля, позволяют родителям самим решать, какое содержимое в интернете могут просматривать их дети, отсекать «плохие» сайты в соответствии с введенными настройками. Такие программы позволяют смотреть отчёты о том, какие сайты посещал ребёнок, сколько времени пользовался интернетом, устанавливать ограничения пользования компьютером и интернетом по времени.
- ✓ Создайте на компьютере несколько учётных записей, когда каждый пользователь сможет входить в систему независимо и иметь собственный уникальный профиль. Учётная запись администратора позволяет контролировать системные настройки и устанавливать новое программное обеспечение, ограничивая в таких правах других пользователей компьютера. Создавайте для работы надёжные и защищённые пароли.
- ✓ Поддерживайте доверительные отношения с вашим ребёнком, чтобы всегда быть в курсе с какой информацией он сталкивается в сети.

Попав случайно на какой-либо опасный, но интересный сайт, ребёнок с большой вероятностью из любопытства захочет познакомиться и с другими подобными ресурсами. Важно заметить это как можно раньше и объяснить, ребёнку, чем именно ему грозит просмотр подобных сайтов, а также обновить настройки безопасности браузера или программного фильтра.

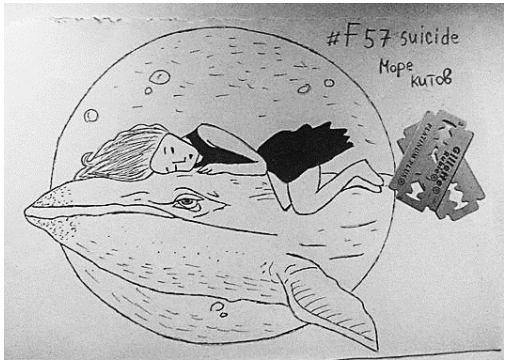
- ✓ Объясните детям, что далеко не всё, что они могут прочесть или увидеть в интернете – правда. Необходимо проверять информацию, увиденную в интернете. Для этого существуют определённые правила проверки достоверности информации. Признаки надёжного сайта, информации которого можно доверять, включают: авторство сайта, контактные данные авторов, источники информации, аккуратность представления информации, цель создания сайта, актуальность данных. Расскажите об этих правилах вашим детям.
- ✓ Помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую может быть гораздо конструктивнее, чем постоянное отслеживания посещаемых сайтов и блокировка всевозможного контента.

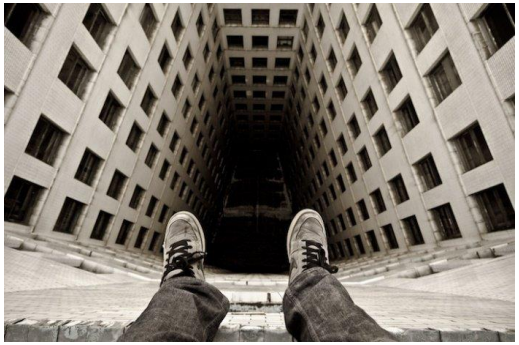
Внимание! Опасно!

«Группы смерти» в сети

Киты и бабочки

http://ligainternet.ru/publications/publication.php?ID=13737
http://ligainternet.ru/publications/publication.php?ID=13021
http://ligainternet.ru/publications/publication.php?ID=13023





udf.by МЧС предупреждает родителей подростков и водителей: в соцсетях активизировались новые "группы смерти" » UDF.B...

группы смерти белоруссия — Яндекс: нашлось 42 млн результатов

UDF.BY
unity • democracy • freedom

ГЛАВНАЯ | МУЛЬТИМЕДИА | ПОЛИТИКА | ЭКОНОМИКА | ОБЩЕСТВО | КУЛЬТУРА | ТЕХНОЛОГИИ | В МИРЕ | СПОРТ | БЕЗ ГАЛСТУКА | МНЕНИЕ

Радыё Свабода

БАЯВАЯ НОЧЫЯ: БУДАЎНІЧЫЯ РАБОТЫ ЛЯ КУРАПАТАЎ ПРЫПЫНЕНЫЯ НА ТЫДЗЕНЬ, ЛЯГЕР ЗАСТАЕЦЦА, — ВЫНІКІ ПЕРАМОВАЎ У ГАРВЫКАНКАМЕ

МЧС предупреждает родителей подростков и водителей: в соцсетях активизировались новые "группы смерти"

5 февраля 2017, 14:21

Снимок носит иллюстративный характер

Министерство по чрезвычайным ситуациям Беларуси предупредило о том, что в социальных

добавить новость на UDF.BY

ПРОСТУДА МЕР
по данным НИИ ГРИППА
ЭПИДЕМИЯ МОЖЕТ БЫТЬ В ТВОЁМ ГОРОДЕ!
50%

Последние комментарии

Petr Petrov минуту назад
Ну и , если добавить вдогонку, аргументация очень слабая, на уровне пятиклассника средней школы. ещё

RU 17:28 01.03.2017

ВНИМАНИЕ! ОПАСНО!

Смотрим в соцсети

- на личной стене появляются цифры, начиная от 50 и меньше
- состоит в группах, содержащих в названии следующее: «Киты плывут вверх», «Разбуди меня в 4.20», f57, f58, «Тихийдом», «Рина», «Няпока», «Море китов», «50 дней до моего...»
- размещает фотографии самоунижения, оскорбления себя в разных и порой даже жестоких формах, вплоть до нанесения себе травм, в частности, порезов
- сохраняет фотографии, снятые с высоты (крыш, чердаков и т.п.)
- внимание на хэштеги: #домкитов, #млечныйпуть, #150звёзд, #ff33, #d28, #хочувигру
- в переписке с друзьями на личной стене есть фразы «разбуди меня в 4.20», «я в игре»

Что это за «группы смерти» и почему о них все говорят?

В 2016 году в соцсетях появились группы, где детей склоняют к суициду в режиме онлайн. То есть, заставляют покончить с собой и снять это на камеру, выложить в сеть. В таких группах работают профессиональные психологи, которые планомерно доводят детей до самоубийства.

Как это работает?

Модераторы групп смерти часто сами находят подростков, которые уже и так страдают от депрессии и не скрывают своих суицидальных настроений на личной странице в соцсетях (слушают депрессивную музыку, публикуют кровавые фотографии, увлекаются субкультурой эмо, частью которой считаются суицидальные наклонности). А потом начинают жёсткое и манипулятивное психологическое воздействие на подростков.

Например, пишут: «Ты девочка? Тебя предали друзья? Бросил парень? Часто слушаешь грустную музыку? Тогда подписывайся на «киты плывут вверх», – так модераторы зазывают детей в свое сообщество.

Модераторы предлагают им помощь, постепенно заражают их «философией китов» и втягивают их в смертоностный квест (игру), последний этап которого – суицид. Если не покончишь с собой, считай, что квест не пройден.

Когда администратор группы уверен в том, что ребёнок готов к самоубийству, создаётся аудио с музыкой, в котором ребёнок выступает в главной роли, и оговариваются все проблемы, которые он озвучил «проводнику». Единственный выход из всех проблем, который озвучивается в этом «произведении», – совершить самоубийство. Ребёнок слушает аудиозапись и делает последний шаг. Видеозаписи в дальнейшем продаются в сети интернет или в Darknet.

Самое страшное, что родители детей, которые погибали в результате такого квеста, не замечали никаких странностей в поведении своего ребёнка.

Какова идеология и символика «групп смерти»?

Символ групп смерти – киты, и фанаты и члены таких сообществ называют себя «китами». Эти животные ассоциируются у идеологов «групп смерти» со свободой, в том числе – свободой покончить с собой. Подростков восхищает, что такие большие и сильные животные могут выбрасываться на берег, отверженные океаном (родителями, обществом, любимым человеком), и совершают суицид. Такая смерть считается красивой.

Согласно описаниям из групп смерти, киты просыпаются или умирают в 4.20 утра. В это время подростки встают, чтобы получить от модераторов группы очередное задание квеста – порезать себя, оставить синяки, ожоги или ссадины на теле. И так до тех пор, пока не остается последнее задание квеста – убить себя. И всё это – обязательно снять на камеру.

Но группы смерти бывают разными, и иногда модераторы таких сообществ используют в качестве символа бабочек (живут всего день) или единорогов.

Как ещё детей доводят до самоубийства?

«Группы смерти» постоянно эволюционируют. Появляются всё новые и более изощрённые способы склонить подростка к суициду.

Так, в Республике Беларусь стремительно распространялась опасная игра среди подростков **«Беги или умри»**. Суть её в том, чтобы на мобильный телефон снять, как игроки перебегают дорогу как можно ближе к транспортному средству, которое движется. Уже есть жертвы.

А ещё недавно родителей ошарашил рецепт превращения детей в огненную фею, который рассылают детям по SMS. Ребёнку предлагается включить ночью все конфорки газовой плиты, не поджигая, и иди спать, чтобы утром стать феей огня из Винкс. Эта «игра» также родом из соцсети «Вконтакте». Комментаторы не исключают, что такое сообщение могло прийти и из одной из так называемых групп китов.

Как отличить фейк?

Можно следовать классическому журналистскому подходу четырёх шагов.

1. *Подтверждение информации как минимум в трёх независимых друг от друга источниках («Правило трёх»).*
2. *Сопоставление полученной информации с уже известной по этой теме.*
3. *Проверка достоверности полученной информации у авторитетных экспертов.*
4. *Запрос у источника информации дополнительных деталей, подтверждающих истинность основного сообщения.*

- *Особые возможности Интернета*
- Можно выяснить статус документа, рейтинг источника и его популярность, частоту использования данного материала другими источниками, получить сведения о компетентности и статусе автора материала с помощью специальных поисковых сервисов Интернета, проанализировать сайт, на котором находится информация, оценить квалификацию его авторов и т. п.

Договоритесь с ребенком, сколь времени он будет проводить в Интернете. Для каждого возраста должна быть своя норма.

Приучите детей, что нельзя раскрывать свои личные данные в Интернете. Помогите ребенку придумать псевдоним не раскрывающий никакой личной информации.

Объясните детям, что в Интернете человек может быть не тем, за кого он себя выдает.

Расскажите ребенку, что такое Интернет. Объясни, что Интернет – это в первую очередь помощник в поиске информации и в образовании.

Ребенок может столкнуться с негативной информацией (наркотики, порнография). Он должен рассказать об этом родителям.

Расскажите ребенку о мошенничестве в Сети – розыгрышах, лотереях, тестах. Приучите его никогда без ведома взрослого не отправлять СМС, чтобы получить куда-то доступ или информацию из Интернета.

Беседуйте с детьми об их виртуальных друзьях. Если ребенок хочет встретиться с Интерент-другом в реальной жизни, то перед этим он обязательно должен посоветоваться с родителями.

9 ПРИЗНАКОВ ИНТЕРНЕТ-ЗАВИСИМОСТИ:

1. ПОСТОЯННОЕ ЖЕЛАНИЕ БЫТЬ ОНЛАЙН
2. РАЗДРАЖИТЕЛЬНОСТЬ ПРИ НЕВОЗМОЖНОСТИ ВЫЙТИ В ИНТЕРНЕТ
3. НЕЖЕЛАНИЕ ОТВЛЕКАТЬСЯ ОТ ВИРТУАЛЬНОГО ПРОСТРАНСТВА
4. РАССТРОЙСТВО ВНИМАНИЯ
5. ПРЕНЕБРЕЖЕНИЕ ЛИЧНОЙ ГИГИЕНОЙ
6. ОТКАЗ ОТ ПИЩИ ИЛИ СИСТЕМНОЕ НЕРЕГУЛЯРНОЕ ПИТАНИЕ
7. ОТКАЗ ОТ ОБЩЕНИЯ В РЕАЛЬНОЙ ЖИЗНИ
8. ГОТОВНОСТЬ ВКЛАДЫВАТЬ ВСЕ СВОБОДНЫЕ ДЕНЬГИ В КОМПЬЮТЕР И ИНТЕРНЕТ
9. КОНФЛИКТЫ С ОКРУЖАЮЩИМИ ЛЮДЬМИ

Самые распространённые виды вредоносных программ

- ***Вирус*** – это программа, которая способна заражать другие программы, модифицируя их так, чтобы они включали в себя копию вируса.
- ***Троянский конь*** – программа, которая содержит скрытый или явный программный код, при исполнении которого нарушается функционирование системы безопасности.
- ***«Червяк»*** – программа, распространяемая в системах и сетях по линиям связи.
- ***«Жадная» программа*** – программа, которая захватывает (монополизирует) отдельные ресурсы вычислительной системы, не давая другим программам возможности их использовать.
- ***«Бактерия»*** – программа, которая делает копии самой себя и становится паразитом, перегружая память ПК и процессор.
- ***«Логическая бомба»*** – программа, приводящая к повреждению файлов или компьютеров (от искажения данных до полного уничтожения данных).
- ***«Лазейки»*** – точка входа в программу, благодаря которой открывается доступ к некоторым системным функциям.
- ***Снифферы*** – *(программы, перехватывающие сетевые пакеты)*, программы подбора паролей, атаки на переполнение буфера.

Угрозы, вызванные нарушениями в работе сети

- Пользователь может потерять доступ к данным, хранящимся на распределённых серверах (в «облаке»), информации в сети интернет, общению с коллегами и друзьями.
- Кража конфиденциальных данных и заражение устройства вредоносным ПО.
- Кража личных данных – вид мошенничества, в результате которого происходит хищение личной информации, к примеру, паролей, имён пользователей, банковских данных, номеров кредитных карточек и т.д.
- Параметры доступа к финансовым системам, интернет-пейджерам и сайтам, адресам электронной почты, паролям к онлайн-играм. Для осуществления кражи чаще всего используются вредоносные программы или методы социального инжиниринга.

Рекомендации по технической безопасности

1. При загрузке интернет-сайта удостовериться, что адрес сайта начинается с комбинации https:// – это значит, что соединение с веб-сайтом зашифровано.
2. При подключении через общедоступную сеть Wi-Fi нельзя пользоваться платёжными системами и другими важными сервисами.
3. Необходимо использовать надёжные пароли – это важный элемент защиты, позволяющий значительно повысить безопасность онлайн-транзакций. Ключевые элементы надёжности пароля – длина и сложность. Идеальный пароль – это длинная комбинация различных знаков, которая включает в себя буквы и цифры, а также знаки пунктуации и символы.
4. Не использовать один и тот же пароль для доступа в различные аккаунты.
5. Регулярно изменять свои пароли.
6. Важно обеспечить защиту для записанных паролей. Быть внимательным к тому, где хранятся или записываются пароли.
7. Регулярно обновлять браузер и операционную систему.
8. Внимательно следить за тем, какие веб-сайты открываются и что загружается. Это относится к музыке, фильмам, файлам, плагинам и дополнениям для браузера и т. д.

9. Остерегаться всплывающих окон, которые предлагают установить ПО или устранить неполадки.
10. Устанавливать ПО только из надёжных источников.
11. Пользоваться только авторитетными ресурсами, такими как встроенный магазин приложений или сайт разработчика, а не сторонними сайтами для загрузки ПО.
12. В случае обнаружения подозрительных признаков работы ПК после загрузки из сети интернет (устройство медленно работает, появляются всплывающие окна), нужно немедленно удалить ПО и проверить систему с помощью последней версии антивирусной программы.

Составитель:
Будилович Елена Александровна,
методист учебно-методического кабинета

Государственное учреждение образования
«Центр дополнительного образования детей и молодёжи «Маяк» г.Минска»

220006, г.Минск, пер. Полевой, 2а
Тел.: 373-24-10
E-mail: lencvr@minsk.edu.by
Сайт: https://mayak.minskedu.gov.by