

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ
**«Интернет-угрозы: что собой представляют и как их
обнаружить»**

Автор:

Есяян Манушак Кимиковна,
старший вожатый МБОУ СОШ №2 г.Донецка

Памятка разработана на основе материалов НЦПТИ «Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет»

2018 г.

РОДИТЕЛЬ ДОЛЖЕН ЗНАТЬ ...

Современный мир невозможно представить без информационных технологий и сети Интернет. Наравне с большим количеством положительных сторон Интернет таит в себе и множество угроз. Поэтому большую актуальность в наше время приобретают вопросы Интернет-безопасности. При этом процесс обеспечения информационной безопасности основывается на умениях родителя и ребенка увидеть, понять и нейтрализовать угрозу, исходящую от информационного воздействия.

Интернет-угрозы можно разделить на 4 группы:

- электронные угрозы;
 - контентные риски;
 - коммуникационные риски;
 - кибермошенничество и вредоносные программы.
- Электронные угрозы - это кража личных данных, взламывание личных страниц.
 - Вредоносные программы и кибермошенничество – различные вирусы, фишинг (когда вам рассылают письма с поддельных сайтов банков), фейковые Интернет-магазины – это «клоны» Интернет-магазинов, когда создается сайт популярного магазина (в ссылке сайта может быть изменена всего лишь одна буква и многие этого просто не замечают).
 - Коммуникационные риски – связаны с Интернет-общением.
 - Контентные риски – информация, носящая вредный, нежелательный, а также противоправный характер, оказывающая, в первую очередь, отрицательное влияние на духовное, нравственное развитие ребенка; содержащая в себе пропаганду деструктивного, противоправного, поведения, вредных привычек, суицида и др.

Контентные риски для детей и подростков подразделяются на следующие виды:

- материалы экстремистской и террористической направленности;
- материалы наркотической направленности,
- информация суицидального характера;
- пропаганда нацистской символики;
- запрещенные в РФ экстремистские материалы;
- материалы и символика организаций, признанных в РФ запрещенными;
- материалы порнографического характера;
- пропаганда деструктивного, противоправного поведения.

Словарь «тревожных» терминов для родителей

Скулшутинг - или по-английски «*school shooting*». Этот термин применяется к массовым убийствам учащихся, которое производится одним учеником или кем-то посторонним, проникшим в школу с оружием (**скулшутер** – лицо, осуществляющее подобное нападение).

Интернет-троллинг - форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже.

Кибербуллинг (от англ. *bull* («бык»)) - это травля человека по интернету. Цель виртуального террора – нанесение психологического вреда. Интернет-троллинг и кибербуллинг в чем-то схожи, однако последний вид имеет более серьезные последствия.

Киберсуицид - это самоубийство, которые совершается в результате знакомства и общения через Интернет.

«**Флешмоб-киберсуицид**» – это общение ранее не знакомых суицидально настроенных лиц с целью совершения самоубийств.

Онлайнкиберсуицид – совершение самоубийства в реальном времени, перед камерой или обсуждение процесса самоубийства в чате.

Флейм (от англ. *flame* — огонь, пламя) — «спор ради спора», обмен сообщениями в местах многопользовательского сетевого общения (напр. интернет-форумы, чаты, социальные сети и др.), представляющий собой словесную войну.

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.

Социальное бойкотирование – игнорирование участника группы, беседы, форума другими участниками.

«**Группы смерти**» – сообщества в социальной сети, распространяющие суицидальные игры среди пользователей, целевую аудиторию представляют дети и подростки.

«**Синий кит**» (или «**море китов**», «**тихий дом**») - существующая игра, финальной целью которой является совершение самоубийства. «**Куратор**» – лицо, которое ищет и привлекает новых игроков, является ведущим смертельной игры, назначающим задания и следящим за их выполнением.

Хеппислепинг (в переводе «счастливое хлопанье») – избиение людей с целью того, чтобы сделать видео, разместить его в Интернете и набрать большое количество просмотров.

«Беги или умри» — опасная игра, суть которой заключается в том, что ребенок перебегает дорогу в минимальной близости от автомобиля. В это время другой подросток снимает все происходящее на телефон. После они выкладывают свои «подвиги» в соцсети.

Зацепинг - это способ передвижения на поезде, при котором человек цепляется к вагонам снаружи за различные поручни, лестницы, подножки и другие элементы. К опасной информации для жизни и здоровья детей можно также отнести демонстрацию руфинга или не спортивного паркура.

Руфинг (руферы) – современная городская субкультура, приверженцы которой посещают крыши различных зданий и строений. Большинство руферов пользуются социальными сетями, в основном Вконтакте и твиттером. Любят делать фотографии с высоты и выкладывать их на доступные сайты. С 2017 года вовлечение детей в «руфинг» и «зацепинг» совершеннолетними может рассматриваться как уголовно наказуемое деяние, так как Роскомнадзор расценивает данные культуры как скрытые формы суицидального поведения.

Родитель! Не забудь установить фильтр! :)

Быть может, вы слышали о такой службе, как *«Родительский контроль»*? Именно с помощью данного программного средства вы можете надежно защитить ваших детей от часто имеющей место ситуации — «пока еще рано».

Шаг №1: Создаем новую учетную запись.

Для того чтобы добавить нового пользователя в систему, зайдите в меню «Пуск» — «Панель управления» — «Учетные записи пользователей» — «Управление...». Слева в нижней части окна кликните по одноименному пункту «Создание...». Введите имя нового пользователя и завершите процесс добавления нажатием нижерасположенной клавиши подтверждения.

Внимание!

Чтобы задействовать все параметры безопасности Интернета, так как система Windows 7 имеет некоторые ограничения по функционалу, рекомендуется произвести загрузку дополнительного компонента родительского контроля, а именно *«Семейная безопасность»*. Скачать данное приложение можно абсолютно бесплатно с официального сайта Windows Live. Однако для корректной работы данного сервиса необходимо зарегистрироваться в системе, что, в общем-то, займет всего несколько минут вашего времени. Вместе с тем вы получите потрясающий инструмент мониторинга и контроля. Кстати, в операционной системе Windows 8 оговариваемый компонент интегрирован в операционную систему.

Шаг №2: Настройка безопасности Интернета.

После установки выбранного компонента зайдите в меню «Пуск» и активируйте иконку *«Семейная безопасность»*. Введите регистрационные данные в соответствующие чек-боксы. Выберите созданную вами учетную запись для ребенка и перейдите по ссылке, отраженной в верхней части окна. После того как вы попадете на страницу «Семейная безопасность», активируйте учетную запись вашего ребенка и выполните соответствующие настройки.

Шаг №3: В открывшемся окне вы можете задать соответствующие параметры безопасности Интернета конкретно для своего ребенка.

«Веб-фильтр» — можно ограничивать доступ к определенным ресурсам интернет-сети. Также у родителей появляется возможность (следующий одноименный инструмент) создавать *«белые и черные списки» сайтов*. Обратите внимание на то, что фильтры могут сочетаться друг с другом. Например, созданные вами списки разрешенных или запрещенных сайтов также корректно будут учитываться службой, которая осуществляет контроль основными средствами защиты. *«Создание отчетов»* — опция, которая позволяет вам (администратору) просматривать краткую информацию о том, на

какие сайты заходил ребенок и сколько времени он там проводил, а также какие программы он загружал из Сети или использовал на компьютере. **«Ограничение времени»** — вам предоставляется право устанавливать лимит на использование интернет-трафика, согласно указанным часам активности. То есть система безопасности берет интернет-подключение полностью под свой контроль. **«Ограничение игр и приложений»** — два независимых инструмента, с помощью которых вы можете закрыть ребенку доступ на использование того или иного программного продукта.

Браузер - твой друг! ;)

Опция «защита поисковой выдачи»

Данная опция продумана разработчиками популярных браузеров; она защитит ребёнка во время поиска информации. Можно воспользоваться **«Семейным поиском»** от **Яндекс**, который фильтрует поисковые запросы и не выдаёт результаты, не предназначенные ребёнку.

Защита основана на том, что по умолчанию все новые открытые вкладки в браузере используют в качестве домашней страницы поисковую систему Яндекс с Семейным фильтром. Вероятнее всего, что ребёнок не будет переходить на другие поисковые системы, а воспользуется уже предложенным с фильтрацией.

Google Chrome

1. Войдите в настройки браузера: Верхний правый значок из трёх горизонтальных линий -> Настройки.
2. Выберите: Начальная группа -> Следующие страницы.
3. Нажмите Добавить, в поле Добавить страницу впишите <http://family.yandex.ru>
4. Нажмите ОК.

Mozilla Firefox

1. Войдите в настройки браузера: Правка -> Настройки.
2. Во вкладке Основные выберите: При запуске Firefox Показать домашнюю страницу.
3. В поле Домашняя страница укажите: <http://family.yandex.ru>.
4. Нажмите ОК.

Opera

1. Войдите в настройки браузера: Opera -> Настройки -> Общие настройки.
2. Во вкладке Основные выберите: При запуске Начать с домашней страницы.
3. В поле Домашняя укажите: <http://family.yandex.ru>
4. Нажмите ОК.

Родители, обнаружить Интернет-угрозы вам помогут ключевые слова:

Перечень ключевых слов для поиска/обнаружения признаков пропаганды идеологии терроризма и террористических материалов:

- джихад
- муджахед / моджахед / маджахед / муджахидин
- муртады
- кафиры
- куфр
- неверные
- вилайят
- имарат
- халифат
- мушрики
- мунафики
- названия запрещенных террористических организаций (полный список <http://nac.gov.ru/terroristicheskie-i-ekstremistskie-organizacii-i-materialy.html>).

Ключевые слова для обнаружения материалов с признаками **националистического экстремизма:**

- 1312 или АСАВ
- 14/88
- 23/16, White power (НС-скинхеды)
- RaHoWa (Racial Holy War)
- Жиды
- Зига
- Москали
- Скины
- Хачи
- Гои
- Кацапы

Ключевые слова для поиска/обнаружения информации **наркотической направленности:**

- *легальные порошки, курительные миксы, курительные смеси купить, курительные смеси, кодеин, коделак, спайс, спайс купить, поторчать на смесях, каннабиноид LTI-558, каннабиноид LTI-696 (MN-25,PB-22), трип, гарик, курануть порошок мн-25, накуриться реагента, под кайфом, прикуренный, курить синтетику, под дудосом, каннабиноид*

w-001 , W-001F 10 грамм, курево, крол, канаб, канабинойд, спайсы, соли, миксы, закладка, ищем закладчиков, ищем курьеров, работа курьер, кристаллы, дудка, лсд, бульбик, бонг.

Ключевые слова для обнаружения приверженности идеям скулшутинга:

#ЛевБиджаков

#Школа127

#колумбайн + #стрелок

#schoolshooters

#скулшутинг

#ДиланКлиболд , #Дилан , #Клиболд

#ЭрикХаррис , #Эрик , #Харрис , #Росляков, #ВладРосляков

Ключевые слова для обнаружения вовлеченности в смертельно-опасные игры и «группы смерти»:

По степени вовлеченности в игру:

- хочет вступить в игру:

#хочу_в_игру

#хочу_играть

#ищу_куратора

#разбуди_меня_в_4:20

#4:20

#harmselfie

- уже играет:

#синий_кит

#морекитов

#киты_плывут_вверх

#я_в_игре

#синий

#игра

#ня_пока

#49 (или с любой цифрой от 1 до 50 (в некоторых случаях до 56) обозначающей день игры)

#млечный_путь

#тихий_дом

#f53, #f57, #f58, #d28

#z17 #F53 #f54 #57 #58 #6/38 #зелёныйкот #оранжеваясобака #*50*

#FoxDead #DK_1281 #exit #terminal_1281 #храмсмерти #deletedsky

#млечный_путь #краснаясова #f48 #FL57

#u27 #977 #заблудший977 #soul977 #u19 #L13 #YG4 #Новый_путь #L13

#YG4

#РинаПаленкова