Памятка терминов и определений для детей и родителей «Безопасный интернет»

Молодежный отряд содружества Туры «МОСТ»
Тюмень, 2018

Антивирусная программа(антивирус) - специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики - предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Интернет-аддикция - феномен психологической зависимости от сети Интернет, который проявляется в своеобразном уходе от реальности, при котором процесс навигации по сети Интернет затягивает субъекта настолько, что он оказывается не в состоянии полноценно функционировать в реальном мире.

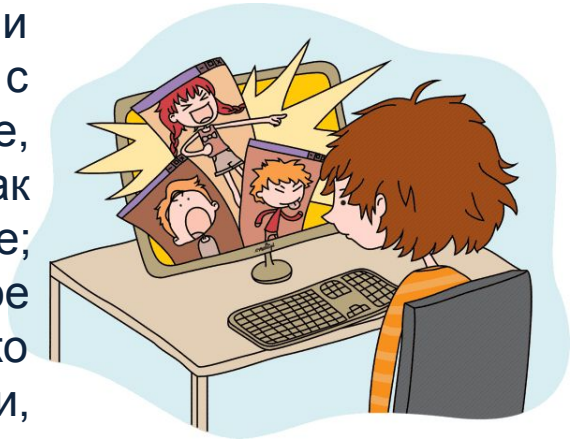
Информационная безопасность - защита информации, ее источников и средств передачи и распространения от потерь, искажения или неправильного (случайного или сознательного) использования (защита данных, защита источника от несанкционированного доступа, средства и способы борьбы с компьютерными вирусами, резервное копирование и архивация данных).

Иформационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Информационная продукция для детей - информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей.

Кибермошенничество - один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный и финансовый ущерб.

Киберпреследование (или кибер-буллинг) - это преследование пользователя сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью различных интернет-сервисов. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами; запугивание; подражание; хулиганство (интернет- троллинг); социальное бойкотирование. По форме буллинг может быть не только словесным оскорблением. Это могут быть фотографии, изображения или видео жертвы, отредактированные так, чтобы быть более унизительными.



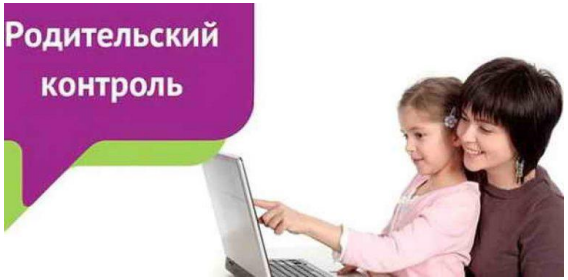
Кибертерроризм - использование виртуального пространства для совершения актов насилия, а также другие деяния, посягающие на общественную безопасность.

Конфиденциальная информация – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Контентные риски - это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д. интернет-мошенничества, целью которого является получение какой-либо выгоды путем установления личных отношений через Интернет.

Приватный режим - это такой режим просмотра веб-страниц, при котором в браузере не остаётся никаких следов пребывания как для самих страниц, так и для других пользователей. Его ещё называют режим инкогнито.

Программа «Родительский контроль» - программа, ограничивающая время пребывания ребенка за компьютером, запрет на определенные игры и сайты.



Средства блокирования - методы и технологии, ограничивающие доступ к серверам и сайтам, на котором находится нежелательный материал, таким образом он становится полностью недоступным для пользователя.

Фильтрация интеренет-контента- устройство или программное для фильтрации сайтов по их содержимому, не позволяющее получить доступ к определённым сайтам или услугам сети Интернет. Целью таких устройств или программ является ограничение доступа в Интернет для школ, предприятий, религиозных организаций и т.д.

Электронные (кибер-) риски - это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д. Вредоносное ПО (Программное Обеспечение) использует широкий спектр методов для распространения и проникновения в компьютеры, не только через компакт-диски или другие носители, но и через электронную почту посредством спама или скачанных из Интернета файлов.

Используемые источники

1. Федеральный закон от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющий вред их здоровью и развитию».

2. Федеральный закон от 27.07.2006 N 149-ФЗ
«Об информации, информационных технологиях и о защите информации».

3. blog.zabedu.ru
Доклад на тему «Фильтрация контента в Интеренете. Анализ мировой практики».

4. www.vocabulary.ru