Согласовано:
Директор Городского студенческого пресс-центра Санкт-Петербурга

_____ Туголукова Е.Н.
«__» _____ 2021 г.

Утверждено:
Председатель Воспитательного совета Учебно-методического объединения Комитета по науке и высшей школе по среднему профессиональному образованию Санкт-Петербурга

_____ Корабельников С.К.
«__» _____ 2021 г.

Методические рекомендации

Основные советы по безопасности в социальных сетях для родителей несовершеннолетних обучающихся

Санкт-Петербург 2021

Авторы разработки:

- Эрендженов Артур Александрович, преподаватель информатики, СПБ ГБПОУ «Санкт-Петербургский архитектурно-строительный колледж».
- Ляшко Илья Анатольевич, заместитель директора по воспитательной работе, ФГБОУ ВО СПбГУПТД Колледж технологии, моделирования и управления.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Сегодня все больше и больше компьютеров, смартфонов, планшетов подключается к работе в сети Интернет. Все большее количество детей получает возможность работать в Интернете. Тем острее встает проблема обеспечения безопасности наших детей в Интернете. Интернет представляет собой огромное количество информации, причем далеко не всегда безопасной. В связи с этим и с тем, что возраст, в котором человек начинает работать с Интернет, становится все моложе, возникает проблема обеспечения безопасности детей. Первые, кто могут им в этом помочь, это родители.

Родители должны быть информированы не только о возможной опасности для ребенка, но и способах обеспечения его безопасности в сети Интернет. Следует понимать, что, подключаясь к Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как разрешить ему выход в Интернет.

Раздел 1. ЧЕМ ОПАСЕН ИНТЕРНЕТ

- **Угроза заражения вредоносным ПО.** Для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, флэш-накопители и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.
- **Доступ к нежелательному содержимому.** Сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, т.к. на многих сайтах отображаются всплывающие окна содержащие любую информацию, чаще всего порнографического характера;
- **Контакты с незнакомыми людьми с помощью чатов или электронной почты.** Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи;
- **Неконтролируемые покупки.** Несмотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот день, когда эта угроза может стать весьма актуальной.

Раздел 2. ЧЕМ ОПАСЕН БЕСПЛАТНЫЙ WI-FI.

Опасность №1. Анализ трафика

Владелец Wi-Fi точки или человек, который получил к ней доступ, может просматривать весь трафик, который проходит через неё. И с помощью анализатора пакетов данных (например, Wireshark или CommView) узнавать, на какие страницы люди заходили с подключенных устройств и что вводили в формы на сайтах, которые используют протокол http. Это могут быть данные для входа, тексты писем, сообщения на форумах.

Еще с помощью анализатора трафика можно украсть cookie-файл с идентификатором сессии, который можно использовать для входа на некоторые сайты под аккаунтом жертвы.

Опасность №2. «Фальшивые» страницы для кражи паролей

Когда человек подключается к Wi-Fi в общественном месте, то его могут направлять на страницу для подтверждения своей личности по номеру телефона или авторизации через соцсети. Все введенные на этих страницах данные владелец точки может собирать для личного пользования.

Также человек, у которого есть доступ к управлению роутером, может настроить, например, перенаправление с facebook.com на сайт facebb00k.com, на котором будет размещена копия главной страницы популярной соцсети, созданная для воровства паролей.

Опасность №3. Заражение вредоносными программами

Таким же образом человека можно перекидывать не только на фишинговые сайты, но и на страницы для скачивания троянов и вирусов, которые могут похитить с компьютера множество ценной для мошенника информации (пароли, документы). Результат зависит от того, насколько жертва заботится о безопасности своего компьютера.

Раздел 3. СПИСОК ПРОГРАММ – ФИЛЬТРОВ:

Для персонального компьютера:

1. **PowerSpy 2008** -программу удобно использовать, чтобы узнать, чем заняты дети в отсутствие родителей.
2. **iProtectYouPro** - программа-фильтр интернета, позволяет родителям ограничивать по разным параметрам сайты, просматриваемые детьми.
3. **KidsControl** - контроль времени, которое ребенок проводит в интернете.
4. **CYBERsitter** - дает возможность ограничивать доступ детей к нежелательным ресурсам в Интернете.
5. **КиберМама 1.0b** - КиберМама проследит за временем работы, предупредит ребенка о том, что скоро ему нужно будет отдохнуть и приостановит работу компьютера, когда заданное вами время истечет.
   КиберМама поддерживает следующие возможности:
   - Ограничение по суммарному времени работы
   - Поддержка перерывов в работе
   - Поддержка разрешенных интервалов работы
   - Возможность запрета интернета
   - Возможность запрета игр/программ

Для смартфонов:

1. **Kaspersky Safe Kids**
   В числе его функций:

- Фильтрация веб-контента.
- Фильтрация поиска (позволяет исключить из поисковой выдачи сайты с нежелательным содержимым).
- Блокировка устройства в установленное время (за исключением звонков).
- Определение географического месторасположения (родитель может узнать, где находится ребенок).
- Мониторинг использования устройства и оправка отчетов на телефон или электронную почту родителя.

2. **Norton Family parental control (Symantec)**
   Norton Family имеет почти такой же набор возможностей, как и продукт Касперского. И также выпускается в платном и бесплатном вариантах.
   В бесплатной версии доступны:

- Функция контроля за посещением веб-сайтов (ведение журнала).
- Фильтрация веб-контента.
- Немедленное предупреждение родителей о нежелательных действиях ребенка.

  В платной дополнительно присутствуют возможности выборочно управлять доступом к приложениям, создавать отчет об использовании устройства за 90 дней, получать на электронную почту еженедельные или ежемесячные сводки о времени, проведенном ребенком за устройством, и о действиях на нем.

3. **Bitdefender Parental Control**
   Набор возможностей Bitdefender Parental Control несколько шире. В бесплатной версии доступны:
- Мониторинг использования устройства (какие сайты ребенок посещал, какие приложения запускал).
- Контроль звонков и SMS-сообщений.
- Мониторинг поисковых запросов.
- Защита программы от удаления.

  Премиум-вариант Parental Control'а от Bitdefender включает:
- Наблюдение за аккаунтом ребенка в соцсети Facebook.
- Отслеживание географического месторасположения.
- Блокировка нежелательных звонков и SMS.
- Блокировка веб-контента и приложений.
- Ограничение времени пользования устройством.

  Дополнительный функционал больше подойдет родителям младших школьников, которые длительное время находятся вне дома.

4. **SafeKiddo Parental Control**
   SafeKiddo Parental Control, пожалуй, один из самых функциональных и гибких инструментов родительского контроля, но платный (от $5.95 за квартал).

   В числе его возможностей:
- Безопасный поиск во всех популярных браузерах.
- Индивидуальные настройки блокировки сайтов (черные и белые списки).
- Ограничение веб-серфинга по времени (можно создать расписание на каждый день недели).
- Дистанционное управление настройками и правилами (со смартфона взрослого).
- Ограничение времени пользования устройством.

  Несмотря на обилие функций, пользоваться SafeKiddo довольно просто. Кроме того, с его помощью можно контролировать нескольких детей, используя для каждого отдельные правила.

5. **Kids Zone Parental Controls**
   Kids Zone Parental Controls удобно использовать для создания детям отдельных профилей на устройстве, которым пользуется взрослый. Предназначена программа в основном для малышей. Выпускается в бесплатном и платном вариантах.

   С помощью Kids Zone вы сможете:
- Создать на своем телефоне или планшете индивидуальный профиль для каждого ребенка, установить им персональные обои на рабочий стол. В профилях детей будут отображаться только те приложения, которые вы разрешите.
- Защитить настройки программы от изменений с помощью пин-кода.
- Ограничить время пользования устройством.

- Заблокировать исходящие звонки и СМС.
- Запретить доступ в Интернет.
- Запретить скачивание и установку программ из Google Play и других источников.
- Заблокировать доступ к параметрам устройства и личным данным аккаунта родителя.
- Вести мониторинг использования устройства детьми.
- Снимать блокировку нажатием одной кнопки (когда нужно ответить на звонок).

Раздел 4. ПЕДАГОГИЧЕСКИ-ВОСПИТАТЕЛЬНЫЕ РЕКОМЕНДАЦИИ

Социальные сети стали неотъемлемой частью жизни, позволяющей сегодня решать не только коммуникативные, но и другие задачи. Молодое поколение вырастает «с телефоном в руках». Поэтому для подростков социальные сети – естественная среда жизни, а не виртуальная. С этой точки зрения к ним нужно относиться как к обычной части жизни подростка и предоставлять то личное пространство, какое мы привыкли уважать «в обычной жизни», оффлайн.

Одно из наиболее эффективных средств воспитания – личный пример. Социальные сети не исключение. Важный шаг к грамотному и безопасному поведению подростка в Интернете – родительский пример грамотной коммуникации. Это позволит Вам иметь авторитет в вопросах пользования электронными ресурсами. Вот несколько рекомендаций по этикету в социальных сетях:

- уделите внимание фотографиям, размещаемым на персональной странице – фотографии с продуманным ракурсом и простым вниманием к деталям в Интернете это аналог опрятного вида в оффлан;
- не распространяйте «игрушечные» репосты, сообщения (например, требующие переслать 10-ти людям, а если вернётся 5, то…), в сегодняшнем информационном поле они выглядят наивно;
- для сохранения полезной информации используйте закладки или функцию отправки сообщения самому себе, не засоряйте страницу хаотичными репостами;
- вместо немых репостов стоит писать авторские посты, так Вы покажете личное внимание к тому, о чём хотите публично высказаться (время написания поста – отличный фильтр, позволяющий понять, действительно ли сообщение стоит того, чтобы его публиковать);
- следите за грамотностью.

Чтобы предостеречь подростка от опасных коммуникаций в Интернете, стоит провести доверительные разговоры на следующие темы:

1. В социальных сетях часто пишут мошенники. Это может быть личное сообщение от незнакомого человека или от лица друга, чью страницу взломали. Мошеннические сообщения от взломанного знакомого можно

распознать по непривычному обращению, нехарактерной манере письма. Если это сообщение от незнакомого человека, то мошенника выдают даты добавления фотографий, публикаций постов (они, как правило, публикуются подряд в одну дату с разницей в 1-2 минуты).

2. Люди могут использовать социальные сети для знакомства, нахождение единомышленников, объединения по интересам. Если «в друзья стучится» человек с таким мотивом, стоит внимательно оценить содержание его страницы, продумать обоснованность такого знакомства и отдавать себе отчёт, зачем оно лично Вам.

3. Часто можно встретиться с агрессией в комментариях. Прежде, чем оставить свой комментарий (поставив себя под прицел комментаторов), стоит подумать: зачем я его пишу? Готов ли я ответить за ту мысль, которую высказываю публично? Есть ли необходимость её написать? Почему я хочу оставить комментарий?

Соблюдение этих рекомендаций не защитит от всех опасностей сети Интернет (как соблюдение ПДД автоматически не защищает человека от экстремальных ситуаций на дороге), но сократит предпосылки для их появления.

ЗАКЛЮЧЕНИЕ

Не стоит думать, что Интернет – это безопасное место, в котором дети могут чувствовать себя защищенными. Необходимо понимать, что использование только средств воспитательной работы без организации технического контроля и ограничений и наоборот – использование репрессивных средств контроля без организации воспитательной работы – это бесполезное занятие. Только в единство данных средств может помочь организовать безопасное нахождение несовершеннолетних в сети Интернет и наиболее эффективно оградить их от влияния злоумышленников.

СПИСОК РЕСУРСОВ

1. Азбука безопасности. В Интернете http://azbez.com/safety/internet
2. Акции детского портала Tvidi.Ru."Правила безопасности в сети Интернет"http://www.fid.su/projects/saferinternet/year/actions/tvidi/
3. Анкета «Интернет и пятиклассники». http://ludmilakarnazhitska.blogspot.com/2010/11/blog-post_21.html
4. Безопасность детей в Интернете http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html
5. Копилочка активных методов обучения http://www.moi-universitet.ru/ebooks/kamo/kamo/
6. Материалы сайта «Интернешка» http://interneshka.net/
7. Статья