МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
безопасность детей в Интернете посредством технических средств

Оглавление

Введение

Интернет позволяет детям получить доступ к играм, фильмам, разнообразной информации, общаться со сверстниками, тем самым предоставляя широкие возможности личностного, творческого, интеллектуального развития ребенка. Но эти преимущества сопровождаются и рядом Интернет-угроз, таких как: вредоносные программы, мошенничество, кибербуллинг, запрещенный возрастным цензом контент, Интернет-зависимость.

Используя современные технические средства возможно предпринять некоторые шаги, которые помогут защитить детей от опасностей в Интернете. Однако, не следует забывать при этом, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются ваши дети за компьютером, планшетом или смартфоном.

Интернет-угрозы

Вредоносные программы

К вредоносным программам относятся угрозы, способные нанести значительный ущерб работе компьютера или мобильного устройства, перехватить персональные данные, в том числе пароли от банковских систем. Какие действия ребенка могут привести к появлению вредоносных программ:

загрузка файлов с внешних источников или носителей (флэшки, диски, компьютеры в сети);

переход на вредоносный сайт;

загрузка файлов с файлообменных ресурсов;

загрузка пиратских материалов (игры, музыка, видео);

установка «бесплатного» ПО, в результате чего может появиться нежелательная реклама, в том числе вплывающие окна и рекламные программы;

ввод персональных данных на сайтах.

Как защитится:

установка антивирусных программ;

установка (использование) программ (сервисов) родительского контроля;

установка обновлений на компьютер, мобильное устройство;

использование сложных паролей;

внимательное изучение различных аспектов использование сервисов или программного обеспечения.

Мошенничество

К мошенничеству относятся угрозы, способные нанести значительный финансовый ущерб, привести к краже или нежелательному распространению персональных данных, в том числе пароли от банковских систем.

Какие действия ребенка могут привести к угрозе мошенничества:

переход на вредоносный сайт, в том числе интернет-магазины;

общение с мошенниками в Интернете посредством социальных сетей, форумов, по телефону, в том числе смс.

использование платного контента (игры, приложения, подписки);

Как защититься:

установка (использование) программ (сервисов) родительского контроля;

использование виртуальных карт (не основных) для оплаты товара или контента;

блокировка оплаты сервисов посредством мобильного телефона ребенка;

внимательное изучение различных аспектов использование сервисов или программного обеспечения.

Кибербуллинг

Под этим понятием подразумеваются угрозы, оскорбления и другие проявления агрессии в Интернете. Можно выделить следующие формы кибербуллинга:

исключение - форма кибербуллинга аналогична бойкоту: жертву намеренно исключают из отношений и коммуникации. При этом возможны самые разнообразные проявления исключения (ребенка могут не допускать к играм, встречам, совместным разговорам онлайн или другим совместным занятиям с его друзьями).

домогательство - постоянная и умышленная травля при помощи оскорбительных или угрожающих сообщений, отправленных ребенку лично или как часть какой-либо группы.

аутинг - преднамеренная публикация личной информации ребенка с целью его унизить, при этом произведенная без его согласия.

кибersталкинг - реальная угроза для безопасности и благополучия ребенка. В частности, этим термином могут называться попытки взрослых связаться с детьми и подростками через Интернет с целью личной встречи и дальнейшей сексуальной эксплуатации.

фрейпинг - получение контроля над учетной записью ребенка в социальных сетях и публикация нежелательный контента от его имени.

поддельные профили –скрытие личности под вымышленными профилями в социальных сетях, чужими адресами электронной почты, телефонными номерами.

диссинг - передача или публикация порочащей информации о жертве онлайн.

обман - пытка завоевать доверие ребенка, чтобы тот рассказал ему какую-либо персональную информацию, которую обидчик затем публикует в Интернете.

троллинг - намеренная провокация при помощи оскорблений или некорректной лексики на интернет-форумах и в социальных сетях.

кетфишинг - воссоздание профиля жертвы в социальных сетях на основе украденных фотографий и других персональных данных.

Как защититься:

установка (использование) программ (сервисов) родительского контроля;

Запрещенный возрастным цензом контент

К нему относится информация о наркотиках, суициде, причинении себе вреда, в том числе посредством некомпетентных рекомендаций (сюда же

входят рекомендации по похудению) и сексуальных извращениях, порнографии. Информация о перечисленных угрозах распространяется посредством определенных сайтов, социальных сетей и рекламных баннеров. Информация о детской порнографии, сексуальных извращениях зачастую содержится на файлообменных ресурсах, а также в торрентах в виде вкраплений, отдельных страниц.

Надзорным органом, осуществляющим за блокировку сайтов в российской доменной зоне, является Роскомнадзор.

Как защитится:

установка (использование) программ (сервисов) родительского контроля;

установка (использование) программ фильтрации контента.

Интернет-зависимость

К ней относится навязчивое стремление использовать Интернет и избыточное пользование им, проведение большого количества времени в сети. Интернет-зависимость не является психическим расстройством по медицинским критериям. Несет угрозу, в том числе летального исхода, посредством переутомления или длительной концентрациии ребенка, а также отрывом от реальности. Выделяются следующие виды зависимости:

навязчивый веб-серфинг (информационная перегрузка) — бесконечные путешествия по Интернету, поиск информации;

пристрастие к виртуальному общению и виртуальным знакомствам — большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Интернете;

игровая зависимость — навязчивое увлечение компьютерными играми по Интернету;

навязчивая финансовая потребность — игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернет-аукционах;

пристрастие к просмотру фильмов через Интернет.

Как защитится:

установка (использование) программ (сервисов) родительского контроля.

Средства защиты от Интернет-угроз

Антивирусные программы

Установка антивирусной программы — одна из обязательных составляющих защиты от Интернет-угроз, при этом сегодня есть возможность обезопасить все цифровые устройства семьи, имеющие выход в Интернет, за один прием. Существуют как платные, так и бесплатные версии программ, однако, необходимо всегда помнить что, каждый антивирус имеет свои достоинства и недостатки. Однако, если своевременно обновлять антивирусные базы, то антивирус станет надежным защитником Вашего компьютера от вредоносного программного обеспечения.

Наиболее популярные антивирусы:

Платные: Dr.Web, Kaspersky, ESET Nod32

Бесплатные: Avast, AVG, 360 Total Security.

Стоит добавить, что даже у платных антивирусов есть бесплатные и весьма эффективные утилиты (Dr.Web CureIT!), а также бесплатные версии с минимальным набором функций (Kaspersky Free).

Обновление программ

Своевременное обновление программного обеспечения является одним из эффективных инструментов защиты компьютеров и мобильных устройств. Злоумышленники используют уязвимости приложений в корыстных целях, а разработчики приложений ведут активную работу по устранению уязвимостей, поэтому своевременное обновление программ обеспечит повышение защищенности приложений

Пароли

Использование паролей — самый распространенный способ авторизации пользователей в Интернете. При составлении надежных паролей рекомендуется придерживаться следующих правил:

пароль должен содержать не менее восьми символов;

используйте различные наборы символов (цифры, латинские буквы (заглавные, прописные), специальные символы («$», «?», «!», «<», «>». «”», «#», «%», «@» и другие) .

пароли для разных веб-сервисов не должны совпадать;

не используйте в качестве пароля: общеупотребительные слова и устойчивые словосочетания, наборы символов, представляющие собой комбинации клавиш, расположенных подряд на клавиатуре (qwerty, 123456789, qazxsw и т. п.), персональные данные (имена и фамилии, даты рождения (свою и родственников), клички домашних животных).

Для создания надежных паролей и создания возможности их надежного хранения на компьютере или мобильном устройстве возможно использовать менеджеры паролей (например, Kaspersky Password Manager, 1Password, LastPass, iCloud Keychain). Менеджеры паролей обычно используют выбранный пользователем основной пароль, чтобы сформировать ключ, используемый для зашифровки хранимых паролей. Этот основной пароль должен быть достаточно сложным, чтобы устоять при атаках злоумышленников. Если основной пароль будет взломан, то будут раскрыты все хранимые в базе данных программы пароли. Это демонстрирует обратную связь между удобством использования и безопасностью: единственный пароль может быть более удобен, но если он будет взломан, то поставит под угрозу все хранимые пароли.

Программы родительского контроля

Большинство программ (сервисов) родительского контроля включают в себя фильтрацию контента — возможность блокировать доступ к веб-сайтам соответствующих нежелательных категорий, таких как порнография, насилие, ненависть и т.п. Однако, этот тип фильтрации будет работать только если он не зависит от браузера и требует фильтрации всего защищенного трафика (HTTPS). Если нет фильтрации HTTPS, то не обделенный умом подросток сможет обойти защиту при помощи анонимизирующих прокси-сайтов типа MegaProxy или Hide My Ass.

Еще одной общей функцией этих сервисов является возможность составления расписания доступа в Интернет. Некоторые приложения позволяют родителям установить еженедельный график для доступа в Интернет, можно установить расписание пользования компьютером в целом, или же ставит ограничения и на Интернет, и на компьютер.

Если у ребенка имеется возможность получить доступ к Интернету с других устройств (планшет, смартфон) следует устанавливать программы родительского контроля и на них.

Прежде чем выбрать определенную программу родительского контроля, убедитесь, что она поддерживает все типы устройств, находящихся в вашем доме. Не все из них совместимы с Mac OS, Android и IOS. Проверьте также, чтобы не было проблем с ограничениями по количеству детских профилей или устройств.

Если установка родительских программ на все устройства кажется вам слишком сложной, тогда рассмотрите вариант защиты сразу всех посредством одного решения (например, Kaspersky Safe Kids).

По мере того как дети становятся старше, фильтрация контента может показаться бессмысленной поскольку ребенок активно взаимодействует с внешним миром посредством социальных сетей, медиаконтента (музыка, фильмы, сериалы, блоги и т.д.).

Среди программ родительского контроля присутствуют трекеры социальных сетей. С их помощью вы сможете ограничить просмотр постов и сообщений, содержащих неуместные фразы или те, которые покажутся вам неприемлемыми. В большинстве случаев для установки трекеров социальных медиа нужно знать учетные данные вашего ребенка, или же придется уговорить ребенка войти в систему и затем установить приложение трекера. Обязательно получите на это согласие от ребенка, разъясните важность роли родителей в воспитании и безопасности ребенка.

У некоторых программ родительского контроля имеется возможность отслеживать звонки и SMS (без отображения самого текста сообщения и содержания звонков), которые поступают на смартфон ребенка.

Поскольку современные мобильные устройства содержат GPS или ГЛОНАСС приемники у программ родительского контроля появилась возможность отслеживать местоположение ребенка (функция геолокации), некоторые программы позволяют устанавливать геолокационный периметр, в котором, как ожидается, ребенок будет находиться в определенный период времени, – и если он его покинет, родителям придет уведомление.

В большинстве систем родительского контроля, вы можете выбрать, как получать уведомления — посредством смс или электронной почты, когда ваш ребенок пытается посетить заблокированный сайт, делает запись, используя сомнительную лексику, или иным образом нарушает ваши запреты. Некоторые из этих инструментов позволяют детям удаленно запросить родительский ответ для разблокирования конкретного сайта, или получить дополнительное время в Интернете, чтобы закончить домашнее задание.

В большинстве случаев вы управляете родительской системой контроля, зайдя в интернет-консоль. С помощью консоли можно настроить параметры, просмотреть отчеты о проделанной работе или ответить на запрос ребенка. И любые изменения, которые вы вносите, начинают действовать при подключении устройств к интернету.

Наиболее популярные программы родительского контроля:

Norton Family Parental Control; Kaspersky Safe Kids; ESET Parental Control, SkyDNS.

Заключение

Защитить ребенка от всевозможных интернет-угроз невозможно. Даже созданный вокруг него защищенный периметр не гарантирует, что в той или иной ситуации он из него не выйдет, а, следовательно, будет подвержен угрозе. Очень важно научить ребенка правильно реагировать на угрозу, привлекать к ней внимание взрослых, развивать медиаграматность.