МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ НЕСОВЕРШЕННОЛЕТНИХ, РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ) НЕСОВЕРШЕННОЛЕТНИХ, НАГЛЯДНЫЕ ИНФОРМАЦИОННЫЕ МАТЕРИАЛЫ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ СЕТИ «ИНТЕРНЕТ» В ЦЕЛЯХ ПРЕДОТВРАЩЕНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ЕЕ ИСПОЛЬЗОВАНИЕМ, КАК САМИМИ НЕСОВЕРШЕННОЛЕТНИМИ, ТАК И В ОТНОШЕНИИ НИХ

(Ленинградская область)

Авторский коллектив:

А.Н. Кивалов, специалист центра цифровой трансформации и развития цифровой образовательной среды ГАОУ ДПО «ЛОИРО», доктор технических наук, профессор

В.И. Колыхматов, проректор по цифровой трансформации и обеспечению деятельности ГАОУ ДПО «ЛОИРО», доцент кафедры педагогики и психологии ГАОУ ДПО «ЛОИРО», кандидат педагогических наук

М.А. Горюнова, профессор кафедра естественно-научного, математического образования и ИКТ ГАОУ ДПО «ЛОИРО», кандидат педагогических наук, доцент

ВВЕДЕНИЕ

В современных условиях в Российской Федерации обеспечение благополучного и безопасного детства стало одним из основных национальных приоритетов. В соответствии с Конституцией РФ государство обязано создавать все условия, способствующие всестороннему духовному, нравственному, интеллектуальному и физическому развитию детей. Социализация несовершеннолетних, ее совершенствование с учетом потребностей семьи и государства определяется целом рядом нормативных документов, в том числе Федеральным законом «Об основных гарантиях прав ребенка в Российской Федерации», Федеральным законом «Об образовании в Российской Федерации», Федеральным законом «Об основах системы профилактики правонарушений в Российской Федерации» и др.

Особого внимания со стороны государства в настоящее время требуют случаи опасного поведения среди подростков, активного бесконтрольного распространение деструктивных идеологий и иной информации разрушительного характера. Ситуация усложняется тем, что распространение подобной информации не ограничивается географией района, населенного пункта или региона. Сети «интернет» сделали возможной и доступной массовую коммуникацию, участниками которой может стать неограниченное число людей из самых разных регионов земного шара. Помимо позитивного контекста именно сеть «интернет» является основным способом распространения деструктивных идеологий. Свобода и открытость интернет-среды несет в себе сложность, связанную с защитой от разного рода посягательств.

Имеют место случаи размещения в сети «интернет» видеосюжетов со сценами побоев, истязаний и иных насильственных действий в отношении малолетних детей и подростков, что значительно усугубляет психологические

травмы жертв. Кроме того, сам факт распространения в информационно-телекоммуникационных сетях подобных видеоматериалов способствует культивированию насилия среди несовершеннолетних и провоцирует их на подобные съемки.

Соответственно вопрос по безопасному использованию сети «Интернет» в целях предотвращения преступлений, совершаемых с ее использованием, как самими несовершеннолетними, так и в отношении них становится одним из важнейших и острых не только в нашей стране, но и во всем мире. Развитие всевозможных компьютерных технологий в значительной степени опережает развитие, как базы юридического регулирования, так и формирования норм и правил, допустимого и категорически невозможного в виртуальной среде.

Для использования возможностей интернета во благо, а не в разрушение, взрослым важно знать все по безопасному использованию сети интернет и что может угрожать психологическому благополучию и даже жизни детей. Задача родителей (законных представителей) несовершеннолетних в обучении безопасности состоит, также как и в реальной жизни, в осознанном выборе соответствующих ресурсов и в знании техники безопасности при работе в сети интернет. Методические рекомендации для несовершеннолетних, родителей (законных представителей) несовершеннолетних, наглядные информационные материалы по безопасному использованию сети «Интернет» в целях предотвращения преступлений, совершаемых с ее использованием, как самими несовершеннолетними, так и в отношении них являются одним из инструментов решения этой задачи.

1. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ НЕСОВЕРШЕННОЛЕТНИХ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ СЕТИ «ИНТЕРНЕТ»

1.1. Правила по использованию паролей

Имена пользователей и пароли создаются для доступа на сайт школы, игровые сайты, в социальные сети, для публикации фотографий, совершения покупок в Интернете и других операций.

Согласно исследованиям 75 процентов детей в возрасте от 8 до 9 лет сообщают свои пароли другим лицам, 66 процентов девочек в возрасте 7-12 признались, что сообщали свой пароль другим лицам.

Первое правило безопасности при работе в Интернете: пароли следует держать в секрете. Научитесь хранить свои пароли столь же бережно, как информацию, которую вы хотите защитить.

Правила, которые несовершеннолетние должны знать и соблюдать:

- Никогда не сообщайте свои пароли другим. Не показывайте никому свои пароли, даже друзьям.
- Обеспечьте защиту для записанных паролей. Будьте внимательны к тому, где вы храните или записываете пароли. Не храните пароли в рюкзаке или бумажнике. Не оставляйте данные о паролях в местах, где вы бы не хотели оставить информацию, защищенную с их помощью. Не храните пароли в файле на компьютере. Преступники ищут там в первую очередь.
- Никогда не предоставляйте свой пароль по электронной почте или в ответ на запрос по электронной почте. Любое сообщение электронной почты, в

котором вас просят указать пароль или перейти на веб-сайт, чтобы проверить пароль, может представлять собой разновидность мошенничества, которая называется фишингом.

К ним относятся запросы с сайтов, вызывающих доверие, которые вы можете постоянно посещать. Мошенники часто создают поддельные сообщения электронной почты, содержащие такие же логотипы как и на реальных сайтах и написанных таким языком, чтобы не вызывать сомнения в своей достоверности.

- Не вводите пароли на компьютерах, которые вы не контролируете. Не пользуйтесь общедоступными компьютерами в школе, библиотеке, в интернет-кафе или в компьютерных лабораториях, кроме как для анонимного просмотра страниц в Интернете.

Не используйте эти компьютеры с учетными записями, где требуется вводить имя пользователя и пароль. Преступники могут за очень небольшие деньги приобрести устройства, регистрирующие нажатия клавиш, которые устанавливаются в течение нескольких секунд. С помощью подобных устройств злоумышленники могут собирать информацию, вводимую на компьютере, через Интернет.

1.2. Безопасная работа в общедоступных сетях Wi-Fi

С помощью WI-Fi можно получить бесплатный интернет-доступ в общественных местах: кафе, отелях, торговых центрах и аэропортах. Так же является отличной возможностью выхода в Интернет. Но многие эксперты считают, что общедоступные WiFi сети не являются безопасными.

Основные советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
4. Не используй публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту;
5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

1.3. Безопасное использование социальных сетей

Социальная сеть – это сайт, который предоставляет возможность людям осуществлять общение между собой в интернете. Чаще всего в них для каждого человека выделяется своя личная страничка, на которой он указывает о себе различную информацию, начиная от имени, фамилии и заканчивая личными фотографиями. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Сайтами социальных сетей можно пользоваться только теми, которые

предназначены для детей, такими как Webkinz или Club Penguin, или сайтами, предназначенными для взрослых, такими как Windows Live Spaces, YouTube, MySpace, Flickr, Twitter, Facebook и другие. Все вопросы по использованию сайтов должны согласовываться с родителями (законными представителями) несовершеннолетних.

Социальные сети используются для общения с лицами, которые могут проживать на другом конце земного шара, или со своими знакомыми, с которыми они каждый день видятся в школе. Многие из этих сайтов социальных сетей могут просматриваться всеми, кто имеет доступ в Интернет. В результате публикации ими некоторой информации они могут стать уязвимыми для фишинговых сообщений, киберугроз и похитителей в Интернете.

Некоторые советы несовершеннолетним, которые помогут безопасно пользоваться сайтами социальных сетей:

- Рассказывайте своим родителям по поводу общения в социальных сетях. Рассказывайте им, если встретится в Интернете то, что вызывает у вас беспокойство, неудобство или страх. Они могут рассказывать вам о таких вещах и помогут успешно разрешить сложившуюся ситуацию.
- Определите правила работы в Интернете. Как только вы стали самостоятельно пользоваться Интернетом, согласуйте с родителями правила пользования Интернетом. В этих правилах должно быть определено, какие можно использовать сайты социальных сетей и каким образом.
- Соблюдайте возрастные ограничения. Рекомендуемый возраст для регистрации на сайтах социальных сетей обычно составляет 13 и более лет. Если вы не достигли этого возраста, не пользуйтесь данными сайтами.
- Учитесь оценивать сайты. Оцените сайты, которые планируете использовать, и убедитесь, что понимаете политику конфиденциальности и правила поведения. Узнайте, существует ли на сайте контроль со стороны администратора над публикуемым содержимым.
- Не встречайтесь с теми, с кем вы общались только по сети. В современных условиях несовершеннолетние подвергаются реальной опасности во время личной встречи с незнакомыми людьми, с которыми вы общались только по сети. Старайтесь ипользовать сайты для общения с друзьями.
- Указывайте свои имена. Указывайте только свое имя или псевдоним и ни в коем случае не использовать псевдонимы, которые могли бы привлечь нежелательное внимание. Не публикуйте полные имена своих друзей.
- Относитесь с осторожностью к информации в профиле. На многих сайтах социальных сетей вы можете присоединяться к общественным группам, включающих учеников определенной школы. Будьте осторожны, предоставляя информацию, по которой вас можно легко идентифицировать, например любимое животное - талисман, увлечение, место проживания и др. Если указано слишком много информации, то вы можете подвергаться киберугрозам, атакам со стороны интернет-преступников, интернет-мошенников или краже личных данных.
- Защищайте свою страничку сайта. Некоторые сайты позволяют защитить вашу страницу с помощью пароля или другими способами, чтобы ограничить круг посетителей, разрешив его только определенным лицам. С помощью различных средств, например Windows Live Spaces вы можете настроить

разрешения, указав тех, кто может посещать вашу страничку или сайт. При этом возможны самые различные настройки – от всех пользователей Интернета до ограниченного списка людей.

- Следите за деталями на фотографиях. Фотографии могут раскрывать много личной информации. Не публикуйте фотографии себя или своих друзей, на которых имеются четко идентифицируемые данные, такие как названия улиц, государственные номера автомобилей или название школы на одежде.
- Не выражайте своих эмоций перед незнакомцами. К предупреждению не общаться с незнакомыми людьми напрямую по сети важно добавить предупреждение о необходимости не выражать своих эмоций при написании журналов и стихотворений и др., в которых часто выражают сильные чувства. Написанное вами сможет прочесть любой, кто имеет доступ в интернет, и злоумышленники часто ищут эмоционально уязвимых детей.
- Помните об интернет-угрозах. Помните, что детям может угрожать через Интернет. Следует сразу же сообщить родителям, учителю или другому взрослому человеку, которому вы доверяете, о всех смущающих вас моментах. Кроме того, очень важно помнить, что общаться по сети необходимо точно так же, как общаются лично. При общении в интернете относитесь к другим людям так же, как и вы хотели бы, чтобы относились к самим.
- Удаление страницы в сети. Если вы отказываетесь соблюдать установленные правила для защиты безопасности, то родители могут обратиться на веб-сайт социальной сети, которую вы используете, с просьбой удалить вашу страницу. Они могут также использовать средства фильтрации интернет-содержимого (например, Функции семейной безопасности Windows Live).

Основные правила работы в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
3. Защищай свою репутацию – держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

1.4. Основные советы по безопасной работе с электронной почтой

Электронная почта – это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в

компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Надо выбрать правильный почтовый сервис. В Интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;

Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;

Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

Если есть возможность написать самому свой личный вопрос, используй эту возможность;

Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

1.5. Рекомендации по безопасности при написании блогов

Практика написания блогов (сокращение от англ. "web log" – дневник в сети) или личного интерактивного журнала очень быстро стала популярной среди подростков, многие из которых ведут свои блоги без ведома родителей или законных представителей.

Социальные сети сейчас обошли по популярности блоги среди большинства подростков, однако многие несовершеннолетние по-прежнему ведут свой блог на своем сайте социальной сети. Недавние исследования показали, что на сегодняшний день примерно половину всех блогов пишут подростки, при этом каждые двое из троих указывают свой возраст, каждые трое из пяти сообщают о месте своего проживания и дают контактную информацию, а каждый пятый указывает свое полное имя. Разглашение подробной личной информации сопряжено с риском.

Несмотря на то, что ведение блога дает возможные преимущества, включая развитие навыков письма и общения, очень важно научиться информационной безопасности их писания еще до того, как вы начнете этим заниматься.

Некоторые советы:

- Прежде чем опубликовать материалы в интернете, тщательно просмотрите, что вы планируют опубликовать. Внешне безобидную информацию, собрав воедино, злоумышленники могут проанализировать и понять очень многое из того, что блогер не хотел бы распространять.
- Насколько комфортно вы будете чувствовать себя, показывая различные материалы незнакомцу. Если имеются сомнения, исключите такие материалы.
- Проведите оценку службы блогов и выясните, обеспечивает ли она возможность написания личных блогов, защищенных с помощью паролей.
- Сохраните интернет-адрес своего блога и покажите его своим родителям.

- Просматривайте другие блоги, отыскивая положительные примеры для подражания.

1.6. Основные советы по безопасной работе с электронными деньгами

Электронные деньги – это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги. Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные – это те, в которых разрешается проводить операции без идентификации пользователя, а в не анонимных идентификации пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, StROng!;
4. Не вводи свои личные данные на сайтах, которым не доверяешь.

1.7. Основные советы по борьбе с фишингом

Фишинг или кража личных данных с помощью интернет-мошенничества, главная цель фишинг которого состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установи надежный пароль (PIN) на мобильный телефон;
6. Отключи сохранение пароля в браузере;

7. Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

1.8. Основные советы по борьбе с кибербуллингом

Кибербуллинг или виртуальное издевательство - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
2. Управляй своей киберрепутацией;
3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
5. Веди себя вежливо;
6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

1.9. Основные советы для безопасности мобильного телефона

Современные смартфоны и планшеты содержат в себе вполне широкий функционал и могут конкурировать со стационарными компьютерами. Однако средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасного использования мобильного телефона:

1. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
3. Необходимо обновлять операционную систему твоего смартфона;
4. Используй антивирусные программы для мобильных телефонов;
5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;

7. Периодически проверяй какие платные услуги активированы на твоем номере;

8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ) НЕСОВЕРШЕННОЛЕТНИХ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ СЕТИ «ИНТЕРНЕТ»

2.1. Общие советы родителям (законным представителям) о безопасности в интернете

Прежде всего, как рассказать детям о безопасности в интернете, родители должны сами познакомиться с основными сведениями о потенциально опасных сайтах и приложениях.

Методические рекомендации о работе с детьми по безопасности в интернете:

- Спросите ребенка, какие приложения и веб-сайты он использует. Попросите ребенка научить вас использовать и показать свои любимые приложения, игры или веб-сайты. Это поможет вам понять, как они работают, и выявить потенциальные риски с худшими приложениями для детей.
- Обсудите с вашим ребенком все возможные проблемы. Если вы опасаетесь, что ребенок использует неподходящее для детей и подростков приложение или сайт, поделитесь с ним своим беспокойством. По возможности принимайте совместное с ребенком решение, чтобы он понимал причины, по которым не следует использовать то или иное приложение.
- Будьте честны и откровенны с ребенком. Поговорите с ним о последствиях ненадлежащего использования технологий. Расскажите ему о кибербуллинге, взломе, социальной инженерии и онлайн-ухаживаниях.
- Убедите ребенка, что с вами всегда можно поделиться. Скажите ребенку, что вы не будете остро реагировать, если он сообщит вам о том, что видел в Интернете: например, неприятные комментарии, материалы сексуального характера или изображения насилия. Скажите также, что вы бы предпочли, чтобы он сообщил об этом вам, а не держал в себе. Покажите, как можно блокировать нежелательный контент или сообщать о нем.
- Установите границы, но будьте реалистом. Устанавливаемые границы использования интернета должны зависеть от возраста ребенка и того, что приемлемо в вашей семье. Границы могут включать согласование следующих правил: сколько времени ребенок может проводить в сети и когда, не писать текстом вещи, которые он не сказал бы в лицо, не отправлять личные изображения, не сообщать вам пароль, чтобы вы могли проверить телефон ребенка.
- Настройте родительский контроль. Настройте или пересмотрите параметры родительского контроля и интернет-фильтры. Родительский контроль предназначен для защиты детей от неприемлемого контента в

интернете. Его можно использовать по-разному, например, чтобы обеспечить детям доступ только к соответствующему возрасту контенту, установить время использования устройства, отслеживать активность и не допустить передачу личной информации посторонним.

- Убедитесь, что на устройстве ребенка установлены последние версии антивирусных программ. Антивирусные программы защищают устройства от внешних атак, находят и уничтожают потенциальные угрозы для системы и предупреждают о них. Новые вирусы появляются постоянно, и разработчики регулярно улучшают антивирусы, чтобы они оставались эффективными.
- Убедитесь, что для ребенка установлены настройки максимальной конфиденциальности. Почти все приложения для социальных сетей имеют настраиваемые параметры конфиденциальности. Изучите их и вместе с ребенком настройте профили.

2.1. Методические рекомендации для родителей с учетом возрастных категорий детей

Обучение интернет-безопасности необходимо с раннего возраста. Можно использовать средства, чтобы ограничить доступ к содержимому, веб-сайтам и действиям, а также принимать активное участие в действиях ребенка в Интернете, однако рекомендуется всегда быть рядом с детьми, когда они используют Интернет, пока они не достигнут 10-летнего возраста.

Советы по безопасности при использовании Интернета вместе с ребенком в возрасте от 2 до 10 лет:

1. Никогда не рано начинать формировать открытое и позитивное общение с детьми. Желательно поговорить с ними о компьютерах, ответить на их вопросы и удовлетворить любопытство.
2. Всегда сидите за компьютером вместе с детьми данного возраста, когда они подключаются к Интернету.
3. Установите четкие правила по использованию Интернета.
4. Настаивайте на том, чтобы несовершеннолетние не разглашали своей личной информации, например свое реальное имя, адрес, номер телефона или пароли, людям, которых они встречают в Интернете.
5. Если на сайте детей просят указать свое имя, чтобы персонифицировать веб-материалы, помогите детям придумать псевдоним для работы в Интернете, который бы не выдавал никакой личной информации.
6. Используйте средства семейной безопасности для создания соответствующих профилей для каждого члена семьи, а также для обеспечения фильтрации интернет-содержимого.

Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер.

7. Все члены семьи должны показывать пример детям, которые только начинают пользоваться Интернетом.

В возрасте от 11 до 14 лет несовершеннолетние хорошо разбираются во всех вопросах, связанных с Интернетом, однако все равно рекомендуется следить и контролировать их, чтобы оградить детей от неподобающих материалов. Можно

воспользоваться средствами интернет-безопасности, которые ограничивают доступ к содержимому и сайтам, а также предоставляют информацию о действиях в Интернете. Проследите за тем, чтобы несовершеннолетние в этом возрасте понимали, какую личную информацию не следует разглашать в Интернете.

Постоянно находиться рядом с детьми в этом возрасте, чтобы контролировать их использование Интернета, практически нецелесообразно. Можно использовать следующие средства: Функции семейной безопасности Windows Live, средства родительского контроля Windows и Windows Vista.

Советы по безопасности, которые следует учитывать при подключении к Интернету вместе с ребенком в возрасте 11-14 лет:

1. Важно формировать открытое и позитивное общение с детьми. Поговорите с ними о компьютерах, ответьте на их вопросы и удовлетворите любопытство.
2. Установите четкие правила по использованию Интернета.
3. Настаивайте на том, чтобы несовершеннолетние не разглашали своей личной информации, например свое реальное имя, адрес, номер телефона или пароли, людям, которых они встречают в Интернете.
4. Если на сайте детей просят указать свое имя, чтобы персонифицировать веб-материалы, помогите детям придумать псевдоним для работы в Интернете, который бы не выдавал никакой личной информации.
5. Используйте средства семейной безопасности для создания соответствующих профилей для каждого члена семьи, а также для обеспечения фильтрации интернет-содержимого.
6. Настройте средний уровень в средстве семейной безопасности, который накладывает некоторые ограничения на содержимое, сайты и действия в Интернете.
7. Компьютеры, подключенные к Интернету, следует устанавливать в открытом месте, где можно легко контролировать действия детей.
8. Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер.
9. Попросите детей рассказать, не ощущали ли они неудобство или страх от уведенного в Интернете или в ходе общения с другими людьми. Проявляйте спокойствие и напомните детям, что их никогда не накажут за то, что они вам расскажут. Похвалите их и попросите их сообщить вам, если то же самое повторится еще раз.

Подростки в возрасте от 15 до 18 лет должны иметь практически неограниченный доступ к содержимому, сайтам или действиям. Они хорошо разбираются с тем, как использовать Интернет, однако родителям все равно следует напоминать им о соответствующих правилах безопасности. Родители всегда должны быть готовы помочь своим детям-подросткам разобраться, какие сообщения являются непристойными, а также избегать опасных ситуаций. Родителям рекомендуется напоминать детям-подросткам о том, какую личную информацию не следует предоставлять через Интернет.

Советы по безопасности, которые рекомендуется выполнять, когда ваши несовершеннолетние-подростки используют Интернет:

1. Старайтесь по-прежнему поддерживать как можно более открытое общение внутри семьи и позитивное отношение к компьютерам. Обсуждайте с детьми их общение, друзей и действия в Интернете точно так же, как другие действия и друзей.

Просите детей-подростков рассказывать вам, если что-то или кто-то в Интернете доставляет им чувство неудобства или страха. Если вы подросток и вам не нравится что-то или кто-то в Интернете, расскажите об этом.

2. Создайте список семейных правил использования Интернете дома. Укажите виды сайтов, которые можно посещать без ограничений, время подключения к Интернету, расскажите, какую информацию не следует разглашать в Интернете, а также предоставьте инструкции по общению с другими в Интернете, включая общение в социальных сетях.

3. Компьютеры, подключенные к Интернету, должны находиться в открытом месте, а не в спальне ребенка-подростка.

4. Изучите средства фильтрации Интернет-содержимого (такие как Windows Vista, средства родительского контроля Windows и Функции семейной безопасности Windows Live) и используйте их в качестве дополнения к контролю со стороны родителей.

5. Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер.

6. Следите за тем, какие сайты посещает ваш ребенок-подросток и с кем он общается. Просите их пользоваться контролируемыми чатами, настаивайте на том, чтобы они использовали только общедоступные чаты.

7. Настаивайте на том, чтобы они никогда не соглашались на встречу с друзьями, с которыми они познакомились в Сети.

8. Научите детей не загружать программы, музыку или файлы без вашего разрешения. Обмен файлами и использование текста, изображений или рисунков с веб-сайтов может привести к нарушению авторских прав и может быть незаконным.

9. Поговорите со своими детьми-подростками о содержимом в Интернете, предназначенном для взрослых, и порнографии, а также укажите им позитивные сайты, посвященные вопросам здоровья и сексуальности.

10. Помогите им защитить себя от спама. Проинструктируйте своих детей-подростков никогда не давать свой адрес электронной почты при общении в Интернете, не отвечать на нежелательные почтовые сообщения и пользоваться фильтром электронной почты.

11. Знайте, какие сайты ваши несовершеннолетние-подростки посещают чаще всего. Убедитесь, что ваши несовершеннолетние не посещают сайты, содержащие оскорбительные материалы, и не публикуют свою личную информацию. Следите за тем, какие фотографии публикуют ваши несовершеннолетние-подростки и их друзья.

12. Учите своих детей отзывчивости, этике и правильному поведению в Интернете. Они не должны использовать Интернет для распространения сплетен, клеветы или запугивания других.

13. Проследите за тем, чтобы несовершеннолетние спрашивали у вас, прежде чем совершать финансовые операции в Интернете, включая заказ,

покупку или продажу товаров.

14. Обсудите со своими детьми-подростками азартные игры в Интернете, а также потенциальные риски, связанные с ними. Напомните им о том, что азартные игры в Интернете являются незаконными.

3. ИНФОРМАЦИЯ И НАГЛЯДНЫЕ ИНФОРМАЦИОННЫЕ МАТЕРИАЛЫ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ СЕТИ «ИНТЕРНЕТ»

3.1. Потенциально опасные для детей приложения и сайты

Набор приложений и веб-сайтов, которые используют дети и подростки, постоянно растет. Многие из них безопасны и предназначены для развлечения, однако отдельные приложения для детей могут быть источником определенных рисков. Опасности включают нежелательное общение с незнакомцами, непреднамеренное раскрытие личной информации и кибербуллинг (травля в интернете). Важно осознавать риски и разрешать детям использовать только приложения, соответствующие их возрасту и обстоятельствам.

Далее описаны потенциально опасные для детей приложения и веб-сайты.

Tik Tok очень популярен среди детей и подростков; количество загрузок приложения превышает 1,65 миллиарда. Tik Tok позволяет пользователям создавать, публиковать и просматривать короткие музыкальные клипы, его еще называют «караоке цифровой эпохи». Возможность добавлять специальные эффекты к видео способствует творческому самовыражению.

Безопасность Tik Tok для детей

- Когда в приложении регистрируются пользователи в возрасте от 13 до 15 лет, их учетные записи по умолчанию являются закрытыми. Это означает, что только друзья могут комментировать их видео. Только пользователи старше 16 лет могут вести прямые эфиры и обмениваться сообщениями, и только пользователи старше 18 лет могут покупать, отправлять и получать виртуальные подарки.
- Однако в приложении отсутствует возможность проверки возраста. Предполагается, что пользователи укажут фактическую дату рождения.
- Приложение поощряет активность, а многие пользователи желают продемонстрировать свои таланты, в результате чего мошенники с помощью лести и комплиментов могут легко выйти на контакт с подростками.
- Некоторые родители выразили обеспокоенность по поводу использования ненормативной лексики в отдельных видео (хотя приложение запрещает пользователям искать нежелательный контент, например, по словам «секс» или «порно»).
- Родители также могут использовать для контроля ограниченный режим или режим семейной безопасности, позволяющий связать свою учетную запись с учетной записью ребенка и полностью контролировать настройки.

Официальные возрастные ограничения: 13+

Omegle – это бесплатный чат, позволяющий общаться с другими пользователями без регистрации. Маркетинговый слоган приложения: «Общайтесь с незнакомцами!» Приложение подбирает в качестве собеседника случайного пользователя, вошедшего на сайт из любой точки мира.

Предлагается использовать текстовый или видеочат. В приложении предусмотрены теги интересов, позволяющие общаться с пользователями, имеющими схожие интересы. Популярность приложения резко возросла во время пандемии коронавируса в 2020 году.

Чаты анонимны, если вы не раскроете свою личность. В начале диалога люди идентифицируются как «вы» и «незнакомец». При возникновении неловкости и дискомфорта можно остановить чат, нажав кнопку «Стоп» и выйдя с сайта или начав новый чат с другим пользователем.

Безопасность Omegle для детей

- Приложение Omegle не скрывает опасностей, о чем говорится в явном виде: «Известно, что злоумышленники используют Omegle, поэтому будьте осторожны».
- Тем не менее, в Omegle не предусмотрено четких инструкций по безопасности и родительского контроля для защиты детей.
- В Omegle дети могут общаться с незнакомцами любого возраста. Чтобы обезопасить детей, важно обсудить с ними, какие опасности имеются на таких сайтах, как Omegle. Лучшая защита – объяснить детям кто и как может использовать такие сайты с преступными намерениями.
- Основные родительские опасения по поводу этого приложения связаны с возможностью кибербуллинга и онлайн-ухаживания.
- Omegle не имеет функции блокировки пользователей, хотя предлагает сообщать о ненадлежащем поведении.
- Omegle блокирует пользователей за жестокость и ненадлежащее поведение на основе их IP-адресов. Однако такую блокировку можно обойти с использованием общедоступного программного обеспечения, такого как виртуальная частная сеть (VPN).

Официальные возрастные ограничения: 13+

Houseparty – это приложение для дружеского общения в видеочатах, как один на один, так и в группах до 8 человек с помощью видео в реальном времени и текстовых сообщений в чат-группах. Также в рамках чат-группы можно играть в игры.

Безопасность Houseparty для детей

- Согласно правилам, для создания учетной записи Houseparty пользователям должно быть не менее 13 лет, но проверка возраста не выполняется – пользователи просто вводят дату рождения.
- В приложении нет предварительного просмотра, видео транслируется в прямом эфире, поэтому дети не защищены от просмотра неприемлемого контента.
- В приложении отсутствует родительский контроль.
- По умолчанию Houseparty не настроен как закрытый. Это означает, что при использовании приложения друзья (или друзья друзей, которых вы, возможно, не знаете) могут автоматически начать с вами видеочат без вашего согласия.
- Они также видят, в каких звонках и с кем вы участвуете, и могут присоединиться без приглашения.
- Пользователи могут отправлять ссылки в чат и делать скриншоты.

Официальные возрастные ограничения: 13+

Tellonyn – это анонимное приложение для обмена сообщениями, описываемое как «самое честное место в Интернете».

Оно позволяет пользователям задавать вопросы друг о друге и отвечать на них, не раскрывая личности, и стало очень популярным среди учеников средних и старших классов.

Безопасность Tellonyn для детей

- Контент создается пользователями и является анонимным. Сообщалось, что встречались случаи кибербуллинга, угрозы насилия и обсуждались темы для взрослых, включая секс, наркотики и алкоголь (если не установлены фильтры).
- В приложении отсутствует проверка возраста, хотя возрастное ограничение приложения в App Store – 17+.
- По умолчанию учетные записи являются открытыми, то есть с ребенком могут общаться, в том числе, незнакомцы.
- Есть функция, которая позволяет пользователям передавать данные о своем местоположении. По умолчанию она отключена, но рекомендуется проверить, действительно ли она отключена у ребенка.
- В приложении есть средства отчетности и блокировки, а также правила сообщества, которым должны следовать пользователи.

Официальные возрастные ограничения: в условиях использования Tellonym указано, что пользователи должны быть старше 13 лет, но App Store оценивает это приложение как лиц старше 17 лет.

Snapchat – это приложение, позволяющее пользователям отправлять фотографии и видео, которые исчезают после получения. Фильтры и специальные эффекты в приложении позволяют изменять изображения.

Безопасность Snapchat для детей

- Согласно условиям использования Snapchat, минимальный возраст для регистрации не должен быть менее 13 лет. Однако, как и для описанных выше приложений, проверка возраста не предусмотрена.
- Многие дети считают, что изображения в Snapchat нельзя сохранять и распространять, поэтому спокойно обмениваются фотографиями, чего не сделали бы в противном случае. Однако пользователи могут сделать снимок экрана до того, как изображение исчезнет в приложении, а на серверах Snapchat изображения хранятся до 30 дней.
- Некоторые родители выражали озабоченность по поводу материалов, не соответствующих возрасту детей, и маркетинговых приемов для сбора пользовательских данных, замаскированных под викторины.

Официальные возрастные ограничения: 13+

YOLO – это аббревиатура фразы "You Only Live Once" – «Живем всего лишь раз». Это приложение для анонимных вопросов и ответов в Snapchat. Пользователи могут публиковать анонимные вопросы и комментарии к историям Snapchat, а также присоединять изображения.

После привязки приложения к учетной записи Snapchat, пользователю предлагается получать анонимные сообщения и создавать вопросы, чтобы получать «честные сообщения» от других пользователей.

Безопасность YOLO для детей

- Элемент анонимности в этом других подобных приложениях позволяет использовать его для агрессии, а иногда и для излишне честных комментариев. Ранее магазины приложений Apple и Google запрещали аналогичные анонимные приложения из-за возможностей для кибербуллинга и разжигания ненависти.
- Существует возможность сообщать о нарушителях, но невозможно их заблокировать, поскольку все пользователи анонимны. Алгоритмы приложения должны отслеживать оскорбительные сообщения, а в условиях использования говорится о недопустимости нежелательного контента. Если поступило сообщение об оскорбительном комментарии, он подлежит удалению.
- В приложении отсутствует ясное описание, как осуществляется передача пользовательских данных.

Официальные возрастные ограничения: 13+

Kik – это бесплатное приложение для обмена текстовыми сообщениями, в котором нет ограничений на количество символов или сообщений. Оно позволяет регистрировать имена пользователей и отправлять текстовые сообщения незнакомцам, не сообщая номер мобильного телефона. На этой платформе пользователи могут обмениваться фотографиями, видео и играми.

Безопасность Kik для детей

- Приложение позволяет детям общаться с незнакомцами в сети. Идентификация пользователей осуществляется только по имени пользователя (не связанным с номером телефона). Kik опережает другие приложения в плане обеспечения анонимности.
- Критике подвергается комбинация анонимности, что позволяет пользователям искать профили по возрасту, и возможности отправлять изображения, которые не хранятся на телефонах.
- В Kik нет родительского контроля.
- В 2018 году по данным BBC, только в Великобритании приложение Kik Messenger использовалось в 1100 случаях сексуального насилия над детьми. Это создает Kik репутацию одного из худших приложений для детей.

Официальные возрастные ограничения: 13+

Discord – это популярное среди геймеров приложение для голосового и текстового чата. Геймеры используют для общения во время игры и обмена советами на игровых серверах.

Некоторые игры, такие как Fortnite, имеют официальные проверенные сервисы Discords, для общения фанатов.

Безопасность Discord для детей

- На сайте Discord доступна информация для родителей и опекунов по обеспечению безопасности детей.
- В Discord также есть функция «Keep Me Safe» для автоматической блокировки неприемлемых изображений, отправляемых в личных сообщениях. Ее необходимо включить, когда ребенок создает учетную запись. Однако эта функция не проверяет текст, поэтому дети могут получать сообщения, содержащие нецензурную лексику.
- Можно изменить настройки конфиденциальности для ребенка, чтобы с

ним не смогли общаться незнакомцы, но у ребенка сохранится доступ к общим серверам. На общедоступных серверах ребенок может найти изображения, видео и комментарии, способные расстроить его.

- Можно с легкостью заблокировать пользователя прямо в приложении, щелкнув его профиль.
- Сообщать об отдельных фрагментах контента несколько сложнее. Для этого нужно отправить в Discord само сообщение и ссылку на сообщение, изображение или видео, о которых вы хотите сообщить.

Официальные возрастные ограничения: 13+

Twitch – это популярный среди геймеров сайт потокового вещания, который позволяет пользователям транслировать игровой процесс, чтобы другие могли смотреть и комментировать его в режиме реального времени. Пользователи также могут воспроизводить запись игр и общаться с другими игроками.

Присоединиться к игре, транслируемой на Twitch, невозможно, но можно общаться с другими пользователями, которые смотрят игру, в чате в реальном времени.

Безопасность Twitch для детей

- В случае прямой трансляции всегда есть вероятность встретить нецензурную лексику и неприемлемые изображения, поскольку трансляция не отредактирована.
- В популярных трансляциях с высокой посещаемостью чат Twitch приобретает хаотичный характер, поскольку все пользователи набирают текст одновременно, пытаясь пообщаться с любимыми стримерами. На более крупных каналах эти чаты могут превратиться в соревнование «кто кого перекричит», с кибербуллингом и разжиганием ненависти. Когда это происходит, модераторы изо всех сил стараются сдержать перегруженный чат.
- Если ваш ребенок ведет прямые трансляции, убедитесь, что игра, которую он транслирует, соответствует возрасту, и что чат находится под контролем, чтобы не привлекать нежелательного внимания.
- Если ребенок в основном смотрит прямые трансляции других игроков, лучше всего изучить этих игроков и их каналы, и убедиться, что эти трансляции соответствуют его возрасту.

Официальные возрастные ограничения: 13+

Tumblr – это сайт микроблогов, который позволяет пользователям делиться фотографиями, видео, короткими блогами, гифками и ссылками, а также имеет встроенную функцию чата. Здесь дети и подростки могут общаться и делиться увлечениями – размещать сообщения о шоу или фильмах, которые им нравятся.

Безопасность Tumblr для детей

- В 2018 году Tumblr запретил порнографический контент, но на платформе все еще можно найти изображения сексуального характера. Также сообщается о публикациях в поддержку анорексии, членовредительства и другом неприемлемом контенте.
- Родительский контроль недоступен, но есть параметры конфиденциальности, которые можно настроить для ребенка.

Официальные возрастные ограничения: 16+

Instagram, Популярность Instagram, вероятно, выше, чем у других приложений для обмена фотографиями. Пользователи размещают в ленте фотографии, которые можно редактировать с помощью фильтров, и истории, доступные в течение 24 часов. Instagram принадлежит Facebook. Пользователи Instagram, как правило, подписываются на друзей, родственников и знаменитостей. В Instagram также есть функция прямых эфиров.

Безопасность Instagram для детей

- Приложение имеет встроенные функции, для автоматического удаления оскорбительных слов и комментариев. Можно добавить собственный список нежелательных слов. Однако в приложении все еще можно найти контент для взрослых и неприемлемые комментарии (хотя есть способ отметить неприемлемый контент для проверки).
- Некоторые пишут в Instagram грубые или неприятные комментарии. Это называется «троллинг» и часто осуществляется анонимно.
- Пользователи могут изменить настройки, чтобы не скрыть свое местоположение или заблокировать определенных подписчиков. Однако многие небрежно относятся к настройкам и общаются с незнакомцами.

Официальные возрастные ограничения: 13+

WhatsApp – популярное приложение для обмена сообщениями, позволяющее пользователям отправлять текст, видео, фото, выполнять звонки и общаться в видеочатах по всему миру.

Безопасность WhatsApp для детей

- Дети и подростки могут общаться только с лицами из списка контактов на своем телефоне. Однако приложение позволяет делиться контентом, который может не соответствовать их возрасту. Это актуально, если друзья добавляют их в групповые чаты, и в конечном итоге у детей появляются контакты людей, с которыми они никогда не встречались лично.
- Следовательно, они смогут связаться с незнакомым человеком и оказаться незащищенными от контента, размещенного этим человеком.
- Пользователи не могут контролировать, кто добавляет их в групповой чат, но они всегда могут контролировать свое участие в чате: из чата можно выйти в любой момент.
- Рекомендуется рассказать ребенку, что если в групповом чате находятся незнакомые люди или люди, с которыми он чувствует себя неловко, следует выйти из чата и обсудить это с родителями.

Официальные возрастные ограничения: 16+

YouTube описывает YouTube Kids как «замкнутую среду, в которой дети могут исследовать YouTube», что упрощает задачи контроля со стороны родителей или опекунов.

По сути, это отдельная версия популярного сайта для распространения видео, ориентированная непосредственно на детей. Одна из его лучших функций – это таймер, позволяющий установить ограничения на то, сколько времени дети играют в приложении.

Безопасность YouTube Kids для детей

• Приложение по большей части является безопасным, поскольку его алгоритм направлен на фильтрацию контента, не подходящего для детей; действия алгоритма дополняются модераторами. Тем не менее, существует небольшая вероятность того, что фильтры пропустят контент, изображающий наготу или насилие.

• Поступали сообщения о видеороликах, которые выглядели как детские, но явно таковыми не являлись. Это были видеоролики с детскими названиями, начинающиеся со знакомых персонажей из детских телешоу (таких как Свинка Пеппа), которые затем становились странными и даже тревожными. Некоторые видео были специально отмечены тегами, чтобы обмануть алгоритм YouTube.

• YouTube предупреждает, что дети могут увидеть нежелательный контент, и что вы можете заблокировать или сообщить о неприемлемых видео.

• При отсутствии премиум-версии будет показана реклама, в том числе нездоровой пищи и продуктов, которые возможно, являются нежелательными для ребенка.

Официальные возрастные ограничения: 4+

3.2. Выбор антивирусного решения для безопасности в интернете

Существует множество факторов, которые необходимо учитывать при выборе оптимального антивируса в соответствии с имеющимися потребностями. Когда на карту поставлена безопасность информации, в том числе персональных данных, стоит уделить некоторое время оценке каждого антивирусного продукта. Некоторые антивирусы можно скачать бесплатно и попробовать, прежде чем доверять им свои данные.

Более того, при активном использовании интернета, электронной почты, систем мгновенного обмена сообщениями и других веб-услуг, важно выбрать антивирус, использующий специальные технологии защиты данных, которые вы вводите в интернете.

• Критерии выбора оптимальной защиты от вредоносных программ

К сожалению, не все антивирусы обеспечивают требуемый уровень защиты от вредоносных программ. Даже 10 самых популярных на рынке антивирусных программ, если их оценить по приведенным ниже критериям, могут получить очень разные баллы.

• Надежность

Даже самый качественный антивирус может оказаться абсолютно бесполезным, если он конфликтует с другим программным обеспечением, работающим на компьютере. Если в результате такого конфликта возникает сбой или временная остановка процессов антивирусной защиты, система может стать уязвимой.

• Удобство использования

Если для повседневной работы антивируса требуются особые навыки, он может оказаться непрактичным для многих пользователей. Любой антивирусный продукт, который неудобен в использовании, задает пользователю слишком много вопросов или требует принятия сложных решений, увеличивает возможность «ошибок оператора». В некоторых случаях, если антивирусом слишком сложно управлять, пользователь может просто отключить его.

• Комплексная защита

Антивирусная программа должна обеспечивать постоянную защиту для всех компьютеров, всех типов файлов и всех элементов сети, которые могут стать целью вредоносной атаки или других вредоносных программ . Программа должна уметь обнаруживать вредоносный код и обеспечить безопасность всех каналов передачи данных на компьютере, включая электронную почту, интернет, FTP и т.д.

• Качество защиты

Антивирусы должны уметь работать в постоянно меняющейся агрессивной среде с новыми вирусами, червями и троянцами, которые становятся все сложнее. Кроме этого, антивирусные программы могут включать новые способы борьбы с угрозами. Качество защиты частично зависит от следующих факторов:

• Эффективность обнаружения угроз

Для эффективности обнаружения угроз и обеспечения надежной защиты компьютера антивирус должен:

обнаруживать вредоносные программы самого разного рода — в идеале, все имеющиеся вредоносные программы;

обнаруживать новые модификации известных вредоносных программ;

обнаруживать вредоносное программное обеспечение, упакованное в архив (т.е. исполняемые файлы, модифицированные утилитами архивирования), а затем проверять содержимое архивов и установочных пакетов.

• Частота и регулярность обновлений.

Поскольку киберпреступники становятся активнее и постоянно запускают новые более сложные вредоносные программы, крайне важно, чтобы антивирус регулярно обновлялся компанией-разработчиком. Без регулярных обновлений выбранный антивирус не сможет быстро реагировать на новую вредоносную программу.

• Возможность вылечить зараженый компьютер

Существует ряд причин, по которым вредоносная программа могла заразить компьютер с уже работающим на нем антивирусом. Например:

если пользователь не включил автоматическое обновление антивируса и не загрузил вручную последнее обновление антивирусной базы данных;

если антивирус на компьютере не был произведен одним из ведущих антивирусных вендоров.

В этих обстоятельствах, если пользователь, наконец, обновляет антивирусную базу данных или устанавливает более эффективное антивирусное решение, на его компьютере может быть обнаружено вредоносное ПО. В этом случае пользователь должен убедиться в том, что вредоносная программа правильно удалена из системы.

• Эффективная защита без снижения производительности

Все программное обеспечение, которое работает на компьютере, естественным образом создает определенную нагрузку на ресурсы компьютера. Антивирус не является исключением. Поэтому важно выбрать антивирус, который обеспечивает нужный уровень защиты компьютера без значительного снижения его производительности.

3.3 Комплексные решения кибербезопасности на устройствах детей

Для надежного обеспечения кибербезопасности на устройствах детей целесообразно использовать комплексные решения. В качестве одного из решений кибербезопасности на устройствах детей представляется возможным использование Kaspersky Safe Kids, которое разработано специально для защиты детей в интернете. Оно состоит из двух приложений: одно нужно установить на устройство ребенка, второе – на смартфон родителя, чтобы просматривать отчеты и менять настройки. Встроенный родительский контроль даже позволяет управлять временем, которое дети проводят перед экраном на разных устройствах.

Непрерывная защита ваших детей с помощью Kaspersky Safe Kids:

1. Отслеживание по GPS

Определение местонахождения ребёнка. Назначение безопасной области нахождения ребёнка и получение уведомлений, если ребёнок покидает её.

Отслеживание и определение местонахождения ребенка в режиме реального времени на цифровой карте в вашем приложении.

Установление безопасного периметра на карте и отправка уведомлений в случае выхода ребенка за его пределы.

2. Контроль экранного времени

Ежедневный контроль времени, проведенного ребенком за экраном каждого устройства, в соответствии с его расписанием и вашим стилем воспитания.

Ограничение экранного времени в день и блокировка устройства при достижении этого ограничения.

Запрет использования устройств в определенное время, например, когда ребенок должен делать домашнее задание.

3. Фильтры веб-сайтов и приложений

Блокировка доступа к сайтам для взрослых и составление списка сайтов и приложений, которые ребенку можно посещать только с вашего разрешения.

Блокирование доступа к нежелательным приложениям и веб-сайтам, например, из категорий Азартные игры, Насилие и Оружие.

Контроль времени использования приложений и составление списка приложений, для открытия которых ребенку нужно ваше разрешение

Отчеты о публикациях на страничке ребенка и изменениях в списке его друзей Вконтакте

4. Безопасный поиск на YouTube

Проверяйте историю поиска на YouTube и защищайте детей от взрослого контента.

Просмотр истории поиска на YouTube – будьте уверены, что поведение вашего ребенка в сети безопасно.

Блокирование поисковых запросов, связанных с алкоголем, курением и азартными играми.

3.4 Рекомендуемые интернет-ресурсы для несовершеннолетних, родителей (законных представителей) несовершеннолетних, наглядных информационных материалов по безопасному использованию сети «Интернет»

Информационно-методические материалы:

Твоя психологическая безопасность (Памятка): https://fcprc.ru/wp-content/uploads/2019/05/6.-Tvova-psihologicheskava-bezopasnost- pamyatk-dlya-

detej .pdf

Как защитить ребенка от интернет-рисков (Памятка): https://fcprc.ru/wp-content/uploads/2019/05/5.-Kak-zashhitit-detei-ot-internet-riskov- pamvatka-roditelvam.pdf

Родителям о психологической безопасности детей и подростков (Памятка): https://fcprc.ru/wp-content/uploads/2019/05/4.Roditelvam-o-psihologicheskoi-bezopasnosti-detei-i-podrostkov-pamvatka.pdf

Применение медиативных и восстановительных технологий в сфере предупреждения деструктивных проявлений среди несовершеннолетних: https://fcprc.ru/wp-content/uploads/2021/05/Primenenie-mediativnvh-i-vosstanovitelnvh- tehnologii-v-sfere-preduprezhdeniva-destmktivnvh-provavlenii-sredi- nesovershennoletni compressed.pdf

Работа с родителями обучающихся образовательных организаций по проведению профилактической деятельности с несовершеннолетними, склонными к суицидальному поведению. Методические рекомендации для педагогов-психологов и социальных педагогов образовательных организаций: https://fcprc.ru/wp-content/uploads/2021/04/Rabota-s-roditelvami-obuchavushhihsva-obrazovatelnvh- organizatsii-po-provedenivu-profilakticheskoi-devatelnosti-s-nesovershennoletnimi- sklonnvmi-k-suitsidalnomu-povedenivu.pdf

Дополнительная общеразвивающая программа интерактивных занятий для детей, подростков и молодежи по вопросам ненасильственных методов разрешения споров и конфликтов «Курс юного переговорщика»: http://iac.dagminobr.ru/files//2021/kurs voung pereg.pdf

Программа экстренной и пролонгированной психологической помощи детям, оказавшимся в трудной жизненной ситуации: https ://fcprc.ru/ spec-value-of-life/metodicheskie-materialv-dlva-spetsialistov/

Профилактика интернет-рисков: методические рекомендации для педагогов и родителей: https://fcprc.ru/wp-content/uploads/2019/05/3-Razvitie-ustojchivosti-k-internet-riskam.pdf

Психологическая безопасность детей и подростков в образовательной среде: рекомендации для руководителей, педагогов, психологов образовательных организаций:

https://fcprc.ru/wp-content/uploads/2019/05/1.-Metodicheskie-rekomendatsii-po-obespecheniyu-psihologicheskoj-bezopasnosti-obrazovatelnoj-sredy-dlya-rukovoditelej-OO.pdf

Информационно-методические материалы по профилактике криминализации образовательной сред: https: //fcprc.ru/wp-content/uploads/2020/01/Profilaktika- kriminalizatsii-obrazovatelnoj-sredy red.-2.pdf

Методические комплексы для психологического сопровождения обучающихся общеобразовательных организаций, в том числе программы развития социально-эмоциональных навыков учащихся: https://vbudushee.ru/library/psy umk/

Интерактивные материалы, статьи и полезные ресурсы для родителей:

Наглядно-методическое пособие для родителей «Формула семьи»: https://fcprc.ru/materials-category/informatsionno-metodicheskie-materialy-dlya-roditelej/

Статья об осознанном родительстве:

https: //растимдетей .рф/articles/uchimsya-osoznannomu-roditelstvu

Видео про безопасность в интернете в рамках акции УРОКБЕЗОПАСНОСТИ.РФ: https://www.youtube.com/watch?v=W XwekfKdnY ()

Блог «Лаборатории Касперского»: http s: //www. kaspersky .ru/blog/di gital - literacy- for-everyone/9004/

Онлайн-родительское собрание «Пространство социальных сетей - без риска для детей» (Сценарий и презентация): https://fcprc.ru/spec-value-of-life/metodicheskie-materialy-dlya-spetsialistov/

Вебинары

Электронный каталог вебинаров для педагогов, психологов и родителей обучающихся «Психологическая безопасность и благополучие в семье, школе, социуме»:https://fcprc.ru/value-of-life/elektronnvi-katalog-vebinarov-dlva-pedagogov-psihologov-i-roditelei-obuchavushhihsva-psihologicheskava-bezopasnost-i-blagopoluchie- v-seme-shkole-sotsiume/

«Особенности подросткового возраста с точки зрения психологии, социологии и этологии: подростковая девиантность»: https: //fcprc.ru/webinars/osobennosti- podrostkovogo-vozrasta-s-tochki-zreniva-psihologii-sotsiologii-i-etologii-podrostkovava- deviantnost/

«8 правил безопасного общения с подростками: как родителям реагировать на «трудное» поведение ребенка»: https://fcprc.ru/webinars/8-pravil-bezopasnogo-obshheniva-s-podrostkami-kak-roditelvam-reagirovat-na-trudnoe-povedenie-rebenka/

«Консультирование по вопросам детско-родительских отношений, девиантного поведения несовершеннолетних»:

https://fcprc.ru/webinars/konsultirovanie-po-voprosam-detsko-roditelskih-otnoshenii-deviantnogo-povedeniva-nesovershennoletnih-sostovalos-29-aprelva-2020-g/

«Давай договоримся! Развиваем навыки конструктивного диалога»: https: //www.voutube. com/watch?v=Rx 1 xPhVLWhl

«Ресурсы родителей»: https: //fcprc.ru/webinars/resursv-roditelva/

«Психология зависимого поведения»: https: //fcprc.ru/webinars/psiholo giva-zavisimogo-povedeniva/

«Территория онлайн - без стресса»: https://www.voutube.com/watch?v=t 1P3z5iwi U

ЗАКЛЮЧЕНИЕ

В современных условиях необходимо уделять большое внимание вопросам информационной безопасности и постоянно совершенствовать свои технологические решения. Не менее важная задача для каждого из нас – научиться и научить других людей, прежде всего несовершеннолетних, пользоваться новыми современными технологиями так, чтобы они смогли защитить себя и нашу семью.

Необходимо защищать компьютеры при помощи современных технологий подобно тому, как мы защищаем двери в наших домах. Наше поведение должно защищать от опасностей Интернета.

Для детей и их родителей (законных представителей) существует

бесплатная линия помощи «Несовершеннолетние онл@йн» http://detionline.com. Если ребенка оскорбляют и преследуют в интернете или ребенок стал жертвой сетевых мошенников, столкнулся с опасностью во время пользования сетью Интернет, если вы обеспокоены безопасностью ребенка при его работе в интернете, обратитесь на бесплатную линию помощи «Несовершеннолетние онл@йн». Эксперты помогут решить проблему, а также проконсультируют по вопросу безопасного использования детьми мобильной связи и интернет. Консультации проводят психологи и технические специалисты МГУ имени М.В. Ломоносова, Федерального института развития образования МОН РФ и МГТУ им. Баумана.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Есаков С.А. Возрастная анатомия и физиология (курс лекций). — Ижевск: УдГУ, 2010. — 196 с.
2. Крайг Г., Бокум Д. Психология развития. — 9-е издание. — СПб.: Питер, 2005. — 940 с: ил. — (Серия «Мастера психологии»).
3. Карабанова О.А. Возрастная психология. Конспект лекций/Издательство «Айрис-пресс», 2005 г. — 239 с. : табл.
4. Протопопова Е.Г., Казенная Е.В. Нападения на учебные заведения: феномен «скулшутинг» и психологические аспекты безопасности образовательной среды // Образование личности / ред. Е.Г. Артамонова // АНО «ЦНПРО» — 2019. — №1. — С.12-19.
5. Рыбакова Л.А., Бабынина Т.Ф. Дети группы риска: особенности развития, психолого-педагогические технологии работы с детьми группы риска: Учебное пособие. — Казань: Бриг, 2015. — 199 с. : ил.
6. Данные «Лаборатории интеллектуального анализа больших данных социальных медиа» ЦНТИ МФТИ и «Крибрум», разработчика платформы многофакторного мониторинга социальных медиа в режиме реального времени. — М.: АО «Крибрум», 2019. — 40 с.
7. Основы кибербезопасности «Лаборатория Касперского» [Электронный ресурс]. - URL: https://csr.kaspersky.com/education/main.htm! (дата обращения 10.12.2021 г.)
8. Материалы, представленные на круглом столе «Защита детей от интернет- контента, наносящего вред их психическому, физическому, духовному и нравственному здоровью», проходившем в Общественной палате Российской Федерации 11.06.2021 г.
9. Материалы, представленные Н. Касперской на форуме «Цифровая гигиена. Молодежь в сети», проходившей 28.03.2019 г. на площадке пресс-центра МИА «Россия Сегодня».
10. Методические материалы по признакам девиаций, действиям специалистов системы образования в ситуациях социальных рисков и профилактике девиантного поведения обучающихся. М: МГППУ, 2018 г., [Электронный ресурс]. - URL: https://mgppu.ru/about/publications/deviant behaviour (дата обращения 10.10.2021 г.)