ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

БРОШЮРА

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

При разработке брошюры использовалась информация, предоставленная Лигой безопасного Интернета и отделом защиты информации администрации Губернатора Ульяновской области

УЛЬЯНОВСК

2017

1 ВВЕДЕНИЕ

Нельзя отрицать того факта, что информационно-телекоммуникационная сеть «Интернет» все теснее проникает в нашу с вами жизнь. Для одних он стал источником знаний, для других используется в работе, кто-то нашел с помощью Интернета друзей, а кто-то даже смог наладить свою личную жизнь. Большинству из нас достаточно сложно представить день без онлайн-общения с друзьями, просмотра свежих новостей или новых роликов.

Это подтверждается и результатами социальных исследований. Так, согласно данным фонда «Общественное мнение», по состоянию на конец весны 2017 года общее количество пользователей сети Интернет в России в возрасте от 18 лет и старше составило 82,4 млн человек при суточной аудитории Интернета в 71,6 млн человек.

Вместе с тем следует помнить, что, несмотря на все преимущества, которые предоставляет нам Интернет, он может быть использован для нанесения вреда вам, вашим близким и вашему имуществу.

Различного рода мошенники, преследователи, разнообразные вирусы – все это представляет угрозу для каждого пользователя сети Интернет. Более того, количество подобных угроз постоянно растет.

Так, за один только второй квартал 2017 года Лабораторией Касперского было обнаружено **16 119 489** уникальных вредоносных программ, а за период с июля 2015 г. по июнь 2016 г. в России в **5,5 раза** выросло число несанкционированных снятий денежных средств со счетов держателей банковских карт через интернет-банкинг.

Появляются и совершенно новые опасности, такие как трагично прогремевшие на всю страну «группы смерти», представляющие серьезную опасность для физического и психологического здоровья детей.

Все это говорит о том, что при использовании Интернета необходимо проявлять крайнюю внимательность и осторожность.

Мы надеемся, что ознакомление с данной брошюрой позволит вам более грамотно подойти к пользованию информационно-телекоммуникационной сетью Интернет и избежать таким образом возможных опасностей.

1 ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ В СЕТИ ИНТЕРНЕТ

Помните! Ответственность за правонарушения в виртуальном пространстве наступает по реальным законам!

РАСПРОСТРАНЕНИЕ ЭКСТРЕМИСТСКИХ МАТЕРИАЛОВ В СЕТИ ИНТЕРНЕТ

С целью противодействия таким негативным явлениям, как экстремизм, ксенофобия, проявление нетерпимости разного толка, расовой, национальной или религиозной розни, связанной с насилием или призывами к насилию, был издан Федеральный закон № 114-ФЗ от 25 июля 2002 г. «О противодействии экстремистской деятельности», который определил, что на территории России запрещается издание и распространение печатных, аудио-, аудиовизуальных и иных материалов, содержащих признаки экстремистской деятельности. В статье 12 Федерального закона «О противодействии экстремистской деятельности» устанавливается прямой запрет на использование сетей связи общего пользования для осуществления экстремистской деятельности.

Незаконная информация экстремистского толка преследуется правоохранительными органами и в информационно-телекоммуникационных сетях общего пользования (Интернете), даже если носителя информации сложно обнаружить или по каким-то причинам он не может быть представлен в материальной форме (диск, накопитель, дискета и т.д.) следствию или суду. В основном это сайты, где возбуждаются вражда и ненависть к представителям других народов, содержатся призывы к осуществлению экстремистской деятельности, предложения об услугах киллеров, информация по приготовлению взрывчатых веществ.

Лица, виновные в незаконном изготовлении, распространении и хранении в целях дальнейшего распространения экстремистских материалов, привлекаются к административной либо уголовной ответственности.

ПРОПАГАНДА, НЕЗАКОННАЯ РЕКЛАМА НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ

В силу п. 1 статьи 6.13 Кодекса РФ об административных правонарушениях пропаганда либо незаконная реклама наркотических средств, психотропных веществ влечет наложение административного штрафа на граждан в размере от четырех тысяч до пяти тысяч рублей с конфискацией рекламной продукции и оборудования, использованного для ее изготовления; на должностных лиц – от сорока тысяч до пятидесяти тысяч рублей; на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, – от сорока тысяч до пятидесяти тысяч рублей с конфискацией рекламной продукции и оборудования, использованного для ее изготовления либо административное приостановление деятельности на срок до девяноста суток с конфискацией рекламной продукции и оборудования, использованного для ее изготовления; на юридических лиц – от

восьмисот тысяч до одного миллиона рублей с конфискацией рекламной продукции и оборудования, использованного для ее изготовления, либо административное приостановление деятельности на срок до девяноста суток с конфискацией рекламной продукции и оборудования, использованного для ее изготовления.

В соответствии с подп. «б» п. 2 статьи 228.1 Уголовного кодекса РФ сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть Интернет), – наказывается лишением свободы на срок от пяти до двенадцати лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до одного года либо без такового.

КЛЕВЕТА В СЕТИ ИНТЕРНЕТ

Сведения признаются порочащими честь, достоинство или деловую репутацию, если они не соответствуют действительности, причем бремя доказывания лежит на субъекте, их распространяющем, в соответствии с п. 1 ст. 152 ГК РФ. Порочащими являются сведения, содержащие утверждения о нарушении субъектом или организацией действующего законодательства или моральных принципов (о совершении нечестного поступка, неправильном поведении в трудовом коллективе, быту) и другие утверждения, порочащие производственно-хозяйственную и общественную деятельность, деловую репутацию, умаляющие честь и достоинство.

К распространению сведений, порочащих честь и достоинство граждан или деловую репутацию граждан и юридических лиц, Пленум Верховного Суда РФ относит в том числе и распространение в сети Интернет.

В соответствии со ст. 151 и 152 ГК РФ истец в суде может требовать:

1. пресечения дальнейшего распространения информации в Сети, а также ее опровержение тем же способом, которым она была распространена;

2. имущественной ответственности ответчика (компенсация морального вреда, возмещение убытков).

В соответствии с ч. 2 ст. 128.1. УК РФ клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, наказывается штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до одного года либо обязательными работами на срок до двухсот сорока часов.

МОШЕННИЧЕСТВО, СВЯЗАННОЕ С БЛОКИРОВАНИЕМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРОВ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ

В настоящее время достаточно распространенными являются случаи мошенничества, в основе которого лежит использование вредоносных программ с целью блокирования программного обеспечения компьютеров пользователей сети Интернет. С правовой позиции описанные деяния необходимо квалифициро-

вать по ст. 272 УК РФ – «неправомерный доступ к компьютерной информации», по ст. 273 УК РФ – «создание, использование и распространение вредоносных компьютерных программ», а в случаях когда, указанное правонарушение повлекло за собой хищение чужого имущества или приобретение права на чужое имущество, – по ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации».

ХИЩЕНИЯ, СОВЕРШАЕМЫЕ С ПОМОЩЬЮ СЕТИ ИНТЕРНЕТ И КОМПЬЮТЕРНОЙ ТЕХНИКИ

Цель финансовых преступлений, совершаемых в компьютерной сети, – получение незаконной выгоды с помощью компьютерных технологий.

В зависимости от специфики совершения такие деяния квалифицируются по ст. 158 УК РФ – «Кража», по ст. 183 УК РФ – «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», по ст. 187 УК РФ – «Неправомерный оборот средств платежей» и по ст. 272 УК РФ – «неправомерный доступ к компьютерной информации».

НАРУШЕНИЕ АВТОРСКИХ ПРАВ В СЕТИ ИНТЕРНЕТ

Творческое произведение, зафиксированное в цифровой форме, признается объектом авторского права. Данное правило означает, что порядок использования произведения в Интернете (даже если такое произведение, кроме как в Интернете, больше нигде не существует) является точно таким же, как и в случае использования любого произведения в реальном мире, а не в виртуальном.

За нарушение авторских и смежных прав, а также изобретательских и патентных прав на информационный объект (произведение), размещенный и распространяемый в сети Интернет, законодательством предусматриваются гражданско-правовая (пресечение противоправных действий, прекращение деятельности юридического лица или индивидуального предпринимателя, возмещение вреда в натуре, возмещение причиненных убытков, компенсация, арест и уничтожение контрафактных материалов без компенсации, уничтожение оборудования за счет нарушителя – ст. 12, 1082, 1302, 1252 ГК РФ; компенсация морального вреда – ст. 151 ГК РФ), административная (административный штраф, конфискация орудия или предмета правонарушения – ст. 7.12 КоАП РФ) и уголовная (штраф, арест, лишение свободы – ст. 146, 147 УК РФ) ответственность.

Кроме того, следует помнить, что программы, книги, музыку, которые пользователь ищет в Интернете с поисковым запросом «скачать бесплатно», могут содержать вирусы и подписки на контентные сервисы.

2 ПЕРСОНАЛЬНЫЕ ДАННЫЕ

2.1. Что такое персональные данные и почему они так важны?

Согласно Федеральному закону № 152-ФЗ «О персональных данных»:

Персональные данные *– любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).*

Т.е. персональные данные – это информация о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность. Таких идентифицирующих данных огромное множество, к ним относятся: фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.

Персональные данные не стоит путать с личными данными. Личные данные – это вообще совокупность всех данных о пользователе в Сети. Например, данные о геолокации, статистика по наиболее посещаемым интернет-страницам, фотографии и т.д.

Кому нужны ваши персональные данные?

* 80% преступников берут информацию в соцсетях.
* Личная информация используется для кражи паролей.
* Личная информация используется для совершения таких преступлений, как шантаж, вымогательство, оскорбление, клевета, киднеппинг, хищение.

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2.2. Как защитить свои персональные данные?

В абсолютном большинстве случаев мы сами указываем свои персональные данные при регистрации на сайтах, оформлении заказов в интернет-магазинах, заполнении профиля в социальных сетях или даже при составлении поискового запроса.

Обратите внимание, продолжая регистрацию на любом сайте, вы соглашаетесь с пользовательским соглашением, ставя «галочку» при заполнении его полей. Обычно этого достаточно, чтобы разрешить владельцам сайта использовать введенные вами данные при работе с его сервисами.

Таким образом, пользуясь сайтом или услугой, вы соглашаетесь на передачу и хранение ваших данных, будь то дата рождения, номер мобильного телефона, переписка и любые другие данные личного характера. Взамен их обязуются хранить в конфиденциальности и ни в коем случае не разглашать третьим лицам. Однако на деле это не всегда так – далеко не всегда сторона, ответственная за хранение ваших персональных данных, добросовестно выполняет свои обязанности. Кроме того, никто не защищен от взлома баз данных, содержащих персональную информацию, или простых ошибок и человеческой опрометчивости. Например, регистрируясь или авторизуясь на сайте через социальную сеть, вы разрешаете сайту получить ваши личные данные, и точно неизвестно, как он будет ими пользоваться. Точно так же любой ваш звонок в магазин или салон автоматически вносит ваш номер в базу пользователей этой компании.

Следование нескольким простым советам во многом сократит угрозу незаконного использования ваших персональных данных:

1. Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.
2. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.
3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат – действительно тот, за кого себя выдает.
4. При необходимости размещения объявления в Интернете воспользуйтесь временной сим-картой и выдуманным именем. Можно также воспользоваться услугой «Второй номер», которую предоставляют некоторые операторы мобильной связи. Эта услуга позволяет подключить в «Личном кабинете» второй номер только на прием звонков и СМС. Звонить с него не получится.
5. Используйте только сложные пароли, разные для разных учетных записей и сервисов. Пользователи, которые используют один и тот же пароль для всех сервисов, при компрометации хотя бы одного из сервисов могут потерять доступ ко всем своим учетным записям. Повторное использование паролей категорически запрещено.
6. Регулярно меняйте пароли, желательно не реже раза в месяц.
7. По возможности используйте двухфакторную авторизацию – это метод идентификации пользователя в каком-либо сервисе (как правило, в Интернете) при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения. На практике это обычно выглядит так: первый рубеж – это логин и пароль, второй – специальный код, приходящий по СМС или электронной почте.
8. Заведите себе два адреса электронной почты – частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках) и публичный – для открытой деятельности (форумов, чатов и так далее).

Что делать, если вы стали жертвой нарушения в области персональных данных?

В первую очередь вам необходимо обратиться в уполномоченный орган в сфере персональных данных – Роскомнадзор, а точнее, его территориальное Управление.

В целях объективного и полного рассмотрения вам необходимо указать следующую информацию:

1) перечень персональных данных, неправомерно обрабатываемых на сайтах в сети Интернет;

2) сведения о документе, удостоверяющем вашу личность (копии страниц паспорта), для подтверждения принадлежности персональных данных, неправомерно размещенных на сайтах в сети Интернет, к вам как к субъекту персональных данных;

3) точные и доступные адреса страниц сайтов (указатели страниц сайтов в сети Интернет – URL), содержащие незаконно обрабатываемые (размещённые) персональные данные, позволяющие осуществить просмотр данных страниц Управлением, а также снимки экрана с данными страницами, содержащие в себе полный адрес страницы сайта (URL) и даты публикации постов/сообщений, содержащих незаконно обрабатываемые (размещённые) персональные данные на текущий момент времени (дата) и другие сведения, подтверждающие нарушения требований законодательства в области персональных данных (видеозапись экрана с действиями, позволяющими зафиксировать нарушения и т.п.);

4) сведения, уполномочивающие вас представлять интересы физических лиц (копии доверенностей), персональные данные которых размещены на сайтах (в случае нарушения их прав как субъектов персональных данных).

Дополнительно следует представить (при наличии):

- сведения, подтверждающие факт направления вами в адрес администрации сайта (далее – оператор) требования об уничтожении ваших персональных данных с указанием на их незаконное получение (без согласия) оператором или с указанием того, что они не являются необходимыми для заявленной цели обработки (представляется при возможности направления указанного требования);
- ответ оператора на ваше требование об уничтожении ваших персональных данных (при наличии).

Обращаем внимание на то, что все имеющиеся сведения должны быть представлены в адрес Управления единовременно!

В случае если по результатам проверки Управление Роскомнадзора выявило нарушение, выдается предписание об его устранении.

Если Управление Роскомнадзора не увидело нарушения, вы можете обратиться в центральный аппарат данного ведомства.

Помимо этого, все субъекты персональных данных имеют право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Ответственность за нарушение законодательства о персональных данных предусматривается в соответствии со ст. 13.11 Кодекса об административных правонарушениях РФ.

3 МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ

3.1. Как действуют мошенники

Мошенники очень хорошо знают психологию людей и умело используют всю доступную информацию, включая ту, которую жертва мошенничества невольно выдаёт при общении. В организации телефонных махинаций участвуют несколько преступников. Очень часто в такие группы входят злоумышленники, отбывающие срок в исправительно-трудовых учреждениях.

Мошенники используют следующие мотивы:

- беспокойство за близких и знакомых;
- беспокойство за свой телефонный номер, счёт в банке или банковскую карту;
- желание выиграть крупный приз;
- любопытство – желание получить доступ к какой-либо информации;
- желание помочь больным детям или людям, пострадавшим от стихийных бедствий.

Социальные сети являются кладезем информации для мошенников. Размещая данные о себе на своих страничках, мы не задумываемся о том, кто может этим воспользоваться. Между тем именно благодаря нам самим мошенникам обычно не составляет труда узнать информацию о родственниках, контактах, увлечениях своей потенциальной жертвы и при выманивании денег внушить доверие знанием её личной жизни.

3.2. Виды интернет-мошенничества. Как защитить себя?

Наиболее распространенными видами мошенничества на данный момент являются:

Телефонное мошенничество

Существуют наиболее распространённые схемы телефонного мошенничества. Вариантов того, как представят вам их мошенники, очень много, но суть не меняется.

- **Обман по телефону.** С вас могут потребовать выкуп или взятку за освобождение якобы из отделения полиции или с места ДТП вашего родственника. Что делать: в этом случае главное не паниковать, позвонить самому родственнику, если не отвечает, то попытаться найти его через друзей и знакомых.

- **СМС-просьба о помощи.** Требование перевести определённую сумму на указанный номер с использованием обращения «мама», «друг», «сынок» и т.п. Что делать: не спешите переводить деньги, убедитесь, что в них действительно нуждается ваш родственник или знакомый.

- **Телефонный номер-грабитель.** Платный номер, за звонок на который со счёта списывается денежная сумма. Что делать: не перезванивайте на незнакомые или предложенные в СМС-сообщениях номера телефонов.

- **Выигрыш в лотерее, которую якобы проводит радиостанция или оператор связи.** Вас могут попросить оплатить пошлину, налог и т.п., перевести сумму на определённый счёт, сообщить пришедший на телефон код. Что делать: не спешите переводить деньги или сообщать какие-либо данные по телефону. Позвоните по официальным номерам (указанным в справочниках, на сайтах) компании – организатора лотереи или конкурса, убедитесь в том, что вас не обманывают.

- **Штрафные санкции и угроза отключения номера** якобы за нарушение договора с оператором вашей мобильной связи. Что делать: позвоните сами своему оператору по официальному номеру, уточните информацию.

- **Ошибочный перевод средств**. Вас попросят перевести якобы ошибочно переведённые средства, а затем дополнительно снимут деньги. Что делать: игнорируйте подобные сообщения или (если это телефонный разговор) посоветуйте для возврата ошибочно переведённой суммы обратиться к оператору связи.

Мошенничество с банковскими картами

Наиболее популярные способы мошенничества с банковскими картами:

- СМС-сообщение о блокировке банковской карты, о несанкционированном движении денежных средств, смене ПИН-кода, окончании срока действия карты и т.д. с требованием перейти по ссылке или перезвонить по указанному телефону.

- Телефонный звонок «работника банка», потенциального «покупателя» с предложением пройти к ближайшему банкомату и совершить манипуляции с банковской картой во избежание каких-либо последствий, внесения аванса и т.п.

Для сохранности ваших средств соблюдайте основные правила безопасности:

- Никому не сообщайте свой ПИН-код, даже работникам банка. Не вводите ПИН-код при работе в сети Интернет, он может потребоваться только мошенникам.
- СМС-сообщения по проводимым операциям по банковским картам рассылаются с определённых коротких номеров (Сбербанк – 900). Для связи с банком необходимо использовать официальные номера Контактного центра, указанные на банковской карте. Если в СМС-сообщении о блокировке карты, движении денежных средств указан другой номер, по которому предлагается позвонить, то это мошенники.
- В случае возникновения проблем у банкомата, не принимайте помощь посторонних, позвоните в Контактный центр банка по телефону, указанному на банкомате.
- Если к вам обратились по телефону, в Интернете, через социальные сети или другими способами и под различными предлогами пытаются узнать данные о вашей банковской карте (номер карты, трехзначный код на оборотной стороне карты), код, пришедший на ваш мобильный телефон, пароли или другую персональную информацию, будьте осторожны, это мошенники.
- При телефонном общении не совершайте никаких действий у банкомата по инструкции «работников банка», если только данный звонок не был инициирован лично вами.
- Не переходите по ссылкам в СМС-сообщениях.
- При получении СМС-сообщений о снятии денежных средств с вашей банковской карты немедленно обращайтесь в банк, блокируйте карту.

Мошенничество в социальных сетях

Мошенники активно пользуются социальными сетями и различными сервисами общения, например, сайтами знакомств.

Популярные способы мошенничества:

- **Распространение ссылок на вредоносное программное обеспечение, порнографические сайты, мошеннические ресурсы и приложения.** Пользователи социальных сетей часто сталкиваются со спамом, который приходит к ним в «личные сообщения» от имени «друзей» или незнакомых пользователей. Это означает, что аккаунты этих людей взломаны. *Как правило, ссылки в таких сообщениях сопровождаются завлекающим текстом, например: «Видела твои фото, я такого не ожидала, посмотри сам!..», «В этой базе данных есть вся информация на любого человека» и т.п.* Что делать*: никогда не переходите по подозрительным ссылкам. Для доступа в социальную сеть используйте уникальный пароль: он должен быть длинным, состоять из цифр и латинских букв. Лучше использовать разные пароли для разных социальных сетей и других* интернет-сервисов*. Не поддавайтесь на*

призыв кого-то из «администрации сайта» сообщить ваш логин и пароль под каким-либо предлогом. Регулярно меняйте пароль от социальной сети (хотя бы раз в месяц); остерегайтесь мошеннических сайтов с похожими по написанию названиями (vkontahte.ru, vk0ntalkte.ru и т.д.). Эти «фишинговые» страницы рассчитаны на невнимательность и на то, что вы сами предоставите мошенникам свой логин и пароль.

- **Знакомые незнакомцы.** В социальных сетях и на сайтах знакомств мошенники создают страницы, где указываются данные и размещаются фотографии вымышленных людей. С помощью этих страниц они знакомятся с другими пользователями сайта. Со временем мошенники входят в доверие, предлагают перейти собеседнику на более «близкое» общение и оставляют свой номер телефона. Самым безобидным последствием такого общения будет то, что номер окажется платным и с вашего счёта спишутся деньги.

- **Просьбы о финансовой помощи, благотворительные акции.** Мошенники часто используют такие поводы, поэтому, прежде чем перевести деньги для помощи, убедитесь, что вас не обманывают. Обратите внимание на наличие нескольких контактов (телефоны, электронная почта, странички в социальных сетях), наличие подтверждающих документов.

Мошенничество на сайтах бесплатных объявлений

Размещая объявления, или покупая что-либо на сайтах бесплатных объявлений (например, «Авито»), будьте внимательны и осторожны, так как мошенники очень часто используют их для обмана. Продавая что-то, вы желаете получить прибыль, но, столкнувшись с мошенниками, можете потерять все свои сбережения.

Как вас могут обмануть:

- **Оплата или предоплата за ваш товар**. Очень часто заинтересованные покупатели предлагают произвести оплату (если сумма незначительная) или предоплату за ваш товар, но сделать это могут по каким-либо причинам только на банковскую карту (находятся в другом городе, нет наличных денег, деньги на расчётном счету и т.п.), но при этом требуют сообщить не только номер карты и ФИО (больше для перевода ничего не требуется), но и другие данные. Помните, что если вас просят сообщить пришедший на телефон код, пройти к банкомату и совершить какие-то действия, вставив вашу карту (чтобы, например, подтвердить прохождение платежа), сообщить срок действия карты и трёхзначный код на оборотной стороне, то это мошенники. Прекращайте контакты с такими «покупателями» и, если успели сообщить какие-то данные, немедленно блокируйте банковскую карту, позвонив по указанному на ней номеру телефона.

- **Предоплата за покупаемый товар.** Покупая что-либо, будьте осторожны, если вас просят произвести предоплату. Вполне возможно, что получив её, «продавец» перестанет отвечать на ваши звонки.

- **СМС-сообщения со ссылкой.** На номер, который вы указали при публикации объявления о продаже или желании что-либо купить, может прий-

ти СМС-сообщение с предложением товара, обмена и ссылкой на этот товар. Если вы перейдёте по ссылке, то загрузите на свой телефон вредоносное программное обеспечение, которое позволит мошенникам получить доступ к вашим банковским картам.

Будьте осторожны, если вам предлагают:

- назвать номер банковской карты, трёхзначный код на оборотной стороне карты, ПИН-код;
- произвести манипуляции с банковской картой у банкомата;
- сообщить пришедший на телефон код;
- перевести сумму денег (аванс, залог, пошлина, налог, ошибочно переведённый платеж и т.п);
- перейти по ссылке в Интернете, в СМС- или ММС-сообщении на смартфоне;
- позвонить по указанному в СМС-сообщении номеру телефона;
- отправить ваш номер телефона;
- отправить СМС-сообщение на короткий номер;
- назвать пароли от ваших личных страничек в социальных сетях.

4 ЗАЩИТА ТЕХНИЧЕСКИХ УСТРОЙСТВ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

4.1. Понятие вредоносной программы

Одной из наиболее актуальных проблем при работе в сети Интернет является опасность заражения вашего технического устройства (компьютера, смартфона, планшета) вредоносными программами.

Вредоносная программа («вирус») – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам технического устройства или к информации, хранимой на нем, с целью несанкционированного использования ресурсов технического устройства или причинения вреда (нанесения ущерба) владельцу информации и/или владельцу технического устройства путём копирования, искажения, удаления или подмены информации.

Причины создания «вируса» могут быть самыми разными – развлечение, незаконное получение прибыли, кража аккаунтов социальных сетях и т.д. Важно помнить, что независимо от цели создателя вредоносной программы, каждый вирус представляет существенную опасность для любого из ваших технических устройств.

Ни в коем случае нельзя считать, что эта проблема не касается вас. Жертвой вредоносной программы может стать каждый.

4.2. Виды вредоносных программ и основные способы их распространения

В настоящее время выделены следующие основные виды вредоносных программ:

Файловые вирусы

До распространения в сети Интернет данный тип вирусов был наиболее часто встречающимся. Файловые вирусы заражают исполняемые файлы различных операционных систем. В наиболее распространенной на сегодня ОС Microsoft

Windows это исполняемые файлы (расширения .exe, .com), динамические библиотеки (.dll), командные файлы (.bat), драйверы устройств (.sys) и файлы сценариев (скрипты). Файловый вирус записывает свой код в «тело» поражаемого файла и при обращении к нему операционной системы перехватывает управление, после чего может совершать различные вредоносные действия: копировать свой код в другие файлы (размножаться), стирать другие файлы, искажать данные и т.д. После выполнения своего набора действий вирус передает управление другим программам, и пользователь может даже не подозревать, что на его ПК происходит какая-то деструктивная деятельность.

Загрузочные вирусы

Вирусы этого типа поражают загрузочные секторы (boot-области или Master Boot Record) загрузочных устройств (жестких дисков, дискет, flash-драйвов). Вирус (boot-вирус) заменяет собой загрузочный код, который выполняется при включении компьютера и таким образом получает управление еще до непосредственного запуска операционной системы. Получив управление, вирус может производить различные действия – например, загрузить свой код в оперативную память. Размножается вирус записью в загрузочную область других накопителей компьютера.

Макровирусы

Макрос – в принципе, тоже исполняемый файл, который, однако, работает только в своей программной среде – например, в приложениях Microsoft Office. Макровирусы поражающие документы Microsoft Office и являются наиболее распространенными. Они написаны на языке Visual Basic, который используется в приложениях семейства Office. Вирус записывает себя в DOT-файл, в котором содержатся все глобальные макросы, часть из которых он подменяет собой. После этого все файлы, сохраненные в приложении (например, Excel), уже будут содержать макровирус. При запуске зараженного макроса выполняются различные вредоносные действия с данными (искажение, удаление). Конечно, это далеко не полный перечень видов компьютерных вирусов. Классифицировать их можно и по другим принципам, например, по способу заражения или по алгоритму действия. Тем не менее нам кажется, что для базового понятия о компьютерных вирусах приведенной информации достаточно.

Сетевые черви (worms)

Основная особенность этого типа вредоносных программ – распространение через компьютерные сети, умение использовать сетевые протоколы передачи данных. Наиболее распространенным видом сетевых червей являются почтовые черви (e-mail worms). Заразиться ими можно при открытии приложения к электронному письму с червем или при переходе по html-ссылке, приведенной в данном письме. Зачастую пользователей побуждают необдуманно открывать приложения писем или интернет-ссылки в письмах.

При активизации кода червя происходит его размножение – начинается рассылка червя по другим адресам электронной почты с зараженного компьютера. Для определения списка адресатов червь может использовать адресную книгу программы – почтового клиента или даже сканировать файлы на жестком диске в

поисках адресов e-mail будущих жертв. В настоящий момент появились сетевые черви, которые могут распространяться и через службы мгновенных сообщений (интернет-пейджеры), например, такие как ICQ.

Трояны (Trojans)

Один из самых опасных типов вредоносных программ на сегодня. Трояны – это вредоносные программы, которые обычно маскируются под какое-либо безобидное программное приложение: вьюверы картинок, скринсейверы, дисковые утилиты, обновление операционной системы и т.д. Попав обманным путем на компьютер жертвы, трояны в зависимости от своего назначения могут выполнять различные действия: обеспечивать злоумышленнику возможность удаленного администрирования ПК жертвы, воровать пользовательские пароли от различных сервисов (в том числе и коммерческих), несанкционированно скачивать какие-либо файлы и т.д. и т.п. Иногда о присутствии троянской программы может свидетельствовать необычное поведение ПК: самопроизвольно раскрывающиеся окна, зависания, заметное замедление скорости работы компьютера.

Программы для взлома (хакерские программы)

Существует еще целый класс программ, которые не угрожают непосредственно компьютеру, на котором исполняются, а используются для атаки на другие сетевые ресурсы или взлома. Подробно они описаны в вирусной энциклопедии Касперского.

Основными способами распространения вирусов являются:
Интернет

Глобальная информационная сеть Интернет на сегодняшний день является основным источником распространения всех видов вредоносных программ. Именно поэтому при работе в Интернете необходимо уделять больше внимания вопросам безопасности.

Вирус может попасть на ваше техническое устройство при следующих обстоятельствах:

- при посещении сайта, содержащего зловредный код;
- при скачивании вредоносных программ, маскирующихся под различное программное обеспечение;
- при скачивании через peer-to-peer сеть (например, торренты).

Электронная почта

Достаточно часто почтовые сообщения, поступающие в почтовый ящик пользователя, используются для распространения вредоносных программ. При открытии такого письма и при сохранении на диск вложенного в письмо файла вы можете заразить данные на вашем компьютере.

Внешние носители информации

Не секрет, что для передачи информации по-прежнему широко используются цифровые диски, разнообразные карты памяти и другие внешние носители информации. При работе с ними также необходимо помнить о безопасности – запуская какой-либо файл, расположенный на внешнем носителе, вы можете поразить данные на вашем техническом устройстве вирусом и, незаметно для себя, распространить вирус на диски вашего компьютера.

Уязвимости в программном обеспечении

Так называемые «дыры» (эксплойты) в программном обеспечении являются основным источником хакерских атак. Уязвимости позволяют получить хакеру удаленный доступ к вашему компьютеру, а следовательно, к вашим данным, к доступным вам ресурсам локальной сети, к другим источникам личной или конфиденциальной информации.

4.3. Профилактика

Важнейшим средством защиты технических устройств от воздействия вредоносных программ является профилактика. Вот несколько простых советов по ее проведению:

- Важно пользоваться только лицензионными программами и операционными системами. Любая нелицензионная программа – потенциальная угроза для безопасности вашего технического устройства, т.к. она может содержать различных «вредителей». Если приобрести лицензионную версию программы вам представляется проблематичным, стоит задуматься об использовании бесплатных аналогов.
- Необходимо проводить регулярные обновления программного обеспечения. Каждая новая версия программы стремится исправить уязвимости предыдущей версии, тем самым делая ваше техническое устройство более защищённым от негативного вмешательства.
- Самое главное – использовать специальные средства защиты, такие как антивирус и файервол. Именно два этих компонента во многом обеспечивают безопасность вашего технического устройства.

Антивирус, как и все остальное используемое вами программное обеспечение, должен быть легальным и постоянно обновляться. В противном случае он вряд ли обеспечит надлежащую защиту. Это связано с тем, что каждый антивирус имеет собственную базу вредоносных программ, которые он умеет распознавать – своеобразный «чёрный список». К сожалению, количество выявляемых вредоносных программ в мире за 10 лет увеличилось в 208,3 раза и превысило 300 тыс. в сутки[1]. Поэтому важно своевременно обновлять антивирус, ведь иначе он не распознает вирус и пропустит его на ваше техническое устройство.

То же касается и файервола. Это специальный фильтр, который контролирует доступ к Интернету с того или иного устройства. Во-первых, он может блокировать попытки вирусов подключаться к сети с вашего компьютера. Например, мешать боту общаться со своим хозяином. Во-вторых, он знает, у каких сайтов хорошая репутация, а каким доверять не стоит. «Черные» и «белые» списки файервола, как и антивируса, должны быть свежими. Тогда он сумеет вовремя остановить вас, если вы соберетесь перейти по подозрительной ссылке.

Однако определять заражённые сайты наверняка файервол не умеет. Поэтому для гарантии большей безопасности можно установить дополнительные сервисы, которые бы блокировали переходы на опасные страницы (Google Public DNS, Яндекс. DNS и др.).

---

1. https://rns.online/it-and-media/Kolichestvo-viyavlyaemih-kompyuternih-virusov-v-mire-za-10-let-viroslo-v-200-raz--2017-04-18/

5 ИНТЕРНЕТ И РЕБЕНОК. ПАМЯТКА РОДИТЕЛЮ

5.1. Ваш ребенок в киберпространстве

Нельзя спорить с тем фактом, что сеть Интернет предоставляет современным детям огромные возможности для развития, обучения, виртуального общения со сверстниками, получению важной информации об окружающем их мире.

Отвечая этому запросу, в Сети был создан такой сегмент, как «детский Интернет» – совокупность обучающих и развлекательных сайтов, предоставляющих широкие возможности для полезного и увлекательного времяпрепровождения. На таких площадках дети могут свободно общаться со своими ровесниками, играть в игры, читать сказки и смотреть мультфильмы.

Вместе с тем следует помнить, что в большинстве случаев Интернет – далеко не самое подходящее место для ребенка.

Постоянно растет количество негативных интернет-ресурсов. Так, за период 2016 – 2017 гг. в России было заблокировано более 3000 сайтов, на которых содержались экстремистские материалы. По данным американского исследовательского центра TopTenReviews, 12% всех сайтов (24,8 млн) содержат материалы для взрослых.

Помимо этого, появляются и новые интернет-угрозы. Дети, часто не задумываясь, рассказывают своим онлайн-друзьям, где они живут или по какому графику работают их родители, отправляют дорогостоящие SMS мошенникам и часами сидят в социальных сетях, что не может не сказаться на их психическом и физическом здоровье. Кроме того, в последнее время участились случаи преследования и запугивания детей через различные интернет-сервисы. По данным нескольких опросов, в среднем каждый второй подросток сталкивался с унижениями и оскорблениями в Сети.

Любой родитель должен со всей внимательностью относиться к данной проблеме и обеспечить своему ребенку безопасное использование сети Интернет.

5.2. Возможные угрозы для вашего ребенка

Как мы уже сказали ранее, Интернет содержит различные угрозы, с которыми может столкнуться ваш ребенок. Предлагаем вам ознакомиться с наиболее распространёнными из них на данный момент:

1. Контентные риски

Контентные риски связаны с потреблением информации, которая публикуется в Интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент.

- **Неподобающий контент**

В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анарексии и булимии, суицида, азартных игр и наркотических веществ.

- **Незаконный контент**

Незаконный контент *– это контент, нарушающий местные, региональные законы и морально-этические принципы.*

В Российской Федерации под данное понятие попадают материалы сексуального характера с участием детей и подростков, порнографический контент, описания насилия, в том числе сексуального, экстремизм и разжигание расовой ненависти, призывы к суициду, материалы, распространяющиеся с нарушением авторских прав, информация о способах приобретения или изготовления наркотических веществ.

2. Электронная безопасность

Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в Сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн-мошенничество и спам.

- **Вредоносные программы**

Вредоносные программы *– это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы-шпионы, нежелательное рекламное ПО и различные формы вредоносных кодов.*

- **Спам**

Спам *– это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный интернет-трафик. Также нежелательная почта может содержать в виде самозапускающихся вложений вредоносные программы.*

- **Кибермошенничество**

Кибермошенничество *– это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести*

к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя с целью получить материальную прибыль.

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя контакты педофилов с детьми и киберпреследования.

- **Незаконный контакт**

Незаконный контакт *– это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.*

- **Киберпреследования**

Киберпреследование *– это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование.*

Приложение: результаты пилотного онлайн-опроса по проблемам безопасности Интернета для детей и подростков, проведенного Лигой безопасного Интернета (март – июль 2017 года)

	Виды информационных угроз	Процент от общего числа упоминаний среди родителей	Процент от общего числа упоминаний среди педагогов и психологов
1	Побуждение к суициду, группы смерти, игры типа «Синий кит», «Тихий дом» и т.п.	20,8%	20,3%
2	Материалы со сценами насилия, жестокости, агрессивным поведением и т.п.	17,7%	15,9%
3	Материалы эротического содержания, порнография	13,3%	12,5%
4	Материалы о наркотиках, психотропных веществах и т.п.	10,5%	9,5%
5	Вовлечение в экстремистские и террористические группы, секты и т.п.	10,0%	13,9%
6	Демонстрация употребления алкоголя, табака и т.п.	6,4%	6,4%
7	Реклама, в том числе спам	6,3%	3,6%

8	Вредные онлайн-игры	4,2%	3,3%
9	Воровство, мошенничество с помощью онлайн-технологий, киберпреступность	2,7%	1,5%
10	Сюжеты о войнах и катастрофах в новостях и т.п.	2,2%	1,0%
11	Бранная речь, нецензурная и сниженная лексика и т.п.	1,3%	1,0%
12	Другое	4,6%	11,1%

5.3. Ключевые проблемы обеспечения безопасности

На данный момент можно выделить несколько ключевых проблем, которые могут сделать использование ребенком Интернета небезопасным. К ним относятся:

Неосведомлённость детей

Несомненно, именно этот момент является ключевым при обеспечении интернет-безопасности детей. Ребенок будет вести себя в Интернете гораздо более ответственно, если будет иметь верные представления о возможных рисках и последствиях своих действий. Родители могут во многом положиться на разумное отношение своего ребёнка к Сети, если они уверены в том, что он знает, что делает. Однако надо понимать, что это относится лишь к детям, достигшим определённого возраста, и совсем не означает, что родители, учителя или опекуны могут полностью самоустраниться от вопроса безопасности ребёнка.

Неосведомлённость взрослых

К сожалению, даже многие родители, опекуны не имеют полного представления о том, каким рискам подвергается их ребёнок в Сети. Неосведомлённость варьируется от недооценивания рисков до чрезмерной опеки и паники, спровоцированной тревожными сообщениями в СМИ. Обе крайности пагубны, взрослые могут эффективно защищать ребёнка лишь в том случае, если имеют полное и верное представление об онлайновых рисках для их детей.

Недостаточная техническая грамотность взрослых и детей

Несмотря на то что многие дети быстро осваивают новые технологии и программы, не многие из них озабочены собственной безопасностью. Ребёнок может отключить антивирус, файервол или программу родительского контроля, если ему покажется, что они ограничивают его возможности в онлайне, и если взрослый не позаботится о том, чтобы запретит ему такие действия. Таким образом, с технической точки зрения взрослым следует изучить все возможности обеспечения безопасности ребёнка с помощью компьютерных программ (семейных фильтров, блокираторов рекламы, антивирусов и файерволов), установить и должным образом настроить все необходимые программы. Детям же необходимо разъяснить необходимость и важность таких программ.

Проблемы доверия

Это также крайне важный аспект безопасности. Ребёнок должен знать, что он может доверять вам, что вы поможете ему при возникновении трудной ситуации, объясните, как правильно себя вести, и главное, что не будете обвинять его. Большинство детей не склонны рассказывать родителям о неприятных происшествиях в Сети, опасаясь, что те сочтут, что дети сами спровоцировали такую ситуацию, и накажут их либо ограничат доступ в Интернет. Кроме того, если ребёнок чувствует, что ему некому доверять в реальной жизни, он будет более склонен делиться своими проблемами с незнакомцами в онлайне, искать их дружбы и поддержки.

5.4. «Группы смерти». Как уберечь ребенка?

В 2016 году стало известно о деятельности так называемых «групп смерти» – групп в социальных сетях, в которых подростки играют в своеобразную игру, итогом которой является подготовленный суицид. Обычно в названиях этих групп присутствуют метафоры про китов, а в содержании находятся депрессивные песни, мрачные картинки с порезанными венами или изображением китов, а также грустные цитаты. В «игре» каждый ребёнок должен выполнить ряд заданий, которые позволяют перейти на следующий уровень. Задания могут быть совершенно жуткими: например, сфотографировать свою руку с порезами. После прохождения таких заданий ребёнку присваивается номер, а также сообщается дата и способ самоубийства. Дети начинают вести обратный отсчёт на своих страницах в социальных сетях.

Как уберечь ребенка от «групп смерти»?

1. Разговаривайте с ребенком

Для того, чтобы подросток не попал под влияние деструктивных групп, нужно делать только одно – разговаривать с ним о том, что такое «хорошо», а что такое «плохо». Когда с детства у ребёнка есть чётко сложившееся мнение об этих понятиях, его не заинтересуют призывы к насилию или суицидальному поведению.

2. Учите ребенка мыслить критически

Один из важнейших критериев, не позволяющих попасть подросткам в «группы смерти», – наличие критического мышления. **Подросток должен уметь самостоятельно фильтровать поступающую ему информацию, уметь анализировать её, сопоставлять с другой информацией, составлять собственное мнение.** Именно наличие критического мышления позволяет и взрослым людям не повестись на провокации и не попасть в секты.

3. Следите за изменениями в поведении ребенка

Заботливые и внимательные родители всегда заметят, что с ребёнком что-то происходит. Резкое падение успеваемости, изменение музыкальных пристрастий, круга общения, появление новых увлечений – ко всему этому нужно относиться внимательно и обязательно разговаривать с ребёнком. **Жизнью ребёнка нужно искренне интересоваться, а не контролировать. Важно не нарушать личные**

границы подростка, не читать его переписки и не проверять группы в социальных сетях, ребёнок сам всё расскажет родителям, если в семье есть доверительные отношения. Подросток должен чувствовать поддержку родных, а родители должны дать понять, что примут его любого, со всеми проблемами, комплексами и недостатками. Если у ребёнка есть твёрдая уверенность в своей семье, то «группы смерти» ему будут не интересны.

Если же случилось так, что ребенок отдалился от вас, стал потерянным, замкнутым, начал отказываться от еды и не спать по ночам, но при этом не хочет обсуждать с вами свою жизнь, то вам стоит присмотреться внимательнее к его поведению.

Вас должно насторожить:

- появление порезов и шрамов на теле ребенка;
- желание подростка дарить и раздавать свои вещи, в том числе и те, что особенно памятны для него;
- поведение ребенка, похожее на поведение перед отъездом (например, он наводит порядок в комнате, спешит закончить какие-то дела, встретиться с родственниками, которых давно не видел, раздать долги).

Кроме того, по статистике 80% подростков, совершивших суицид, говорили родителям о своем нежелании жить, но взрослые не воспринимали эти слова всерьез. Так что если ребенок внезапно изменил свое поведение, попытайтесь вспомнить, не звучали ли от него раньше угрозы покончить с собой.

Что нужно делать родителям?

1. Попробуйте вывести ребенка на разговор

Как уже было сказано выше, ни в коем случае нельзя шпионить за ребенком и тайно читать его личные сообщения в социальных сетях. Зато можно попробовать вывести подростка на разговор «окольными» путями: посмотреть фильм о самоубийстве или рассказать о книге на эту тему и потом предложить ребенку поделиться своим мнением.

2. Всегда поддерживайте разговор с ребенком, о чем бы он ни был

Если ребенок не хочет говорить с вами о своих проблемах, но хочет говорить о какой-нибудь компьютерной игре или о музыке, то поддерживайте эти разговоры. Если вы будете искренне интересоваться жизнью подростка, то вам будет легче вернуть его доверие.

3. Придумайте ребенку занятие

Если ваш сын или дочь проводят в Интернете слишком много времени, засыпают с телефоном, сидят в социальных сетях во время завтрака и ужина, и, как вам кажется, совсем выпадают из реальности, не ругайте его за это, а попытайтесь придумать ему альтернативное занятие: предложите вместе сходить на пробный урок по скалолазанию или в турпоход, на мастер-класс по украшению тортов или созданию моделей – а вдруг ребенка затянет новое увлечение сильнее, чем виртуальная реальность? Тогда у него не будет необходимости искать единомышленников в социальных сетях.

4. Чаще обедайте вместе

Подумайте, давно ли вы собирались семьей за одним столом или же каждый ужинает в разное время, когда ему удобно? В семьях, где принято вместе принимать пищу, дети реже чувствуют себя одинокими и, следовательно, реже задумываются о самоубийстве. Для подростка важно быть частью чего-то целого, так пусть этим целым будет для него семья.

5. Не бойтесь обращаться к специалистам

Если между вами и ребенком нет доверительных отношений, а между тем перечисленные выше тревожные сигналы присутствуют в поведении подростка, необходимо обратиться к психологу. Экстренную помощь вам могут оказать по детскому телефону доверия **8 800 200-01-22**. Он бесплатный и анонимный. Позвонить туда может как взрослый, так и ребенок, поэтому поделитесь этой информацией с дочерью или сыном. У детского телефона доверия есть свои сайт – http://telefon-doveria.ru. Если вам трудно говорить о проблеме по телефону, то на сайте вы можете пообщаться с психологом в чате.

Куда обращаться?

Если вы обнаружили в Интернете группу или сайт, призывающий к самоубийству, можете сообщить об этом в Роскомнадзор по ссылке http://eais.rkn.gov.ru/feedback/ и заполнить все поля в форме. Пожаловаться можно и в Лигу безопасного Интернета http://www.ligainternet.ru/hotline/

5.5. Родительский контроль

Родительский контроль – программное обеспечение электронных средств, используемых детьми и подростками, направленных на защиту их влияния от негативного Интернет-пространства. К сожалению, в России программы родительского контроля не получили массового распространения. Вместе с тем родительский контроль предоставляет большое количество полезных возможностей.

Что можно сделать с помощью родительского контроля?

1. Установить временные интервалы работы компьютера;

2. Управлять разрешениями на запуск и установку различных программ или игр;

3. Формировать «белый список», «черный список»;

4. Использовать безопасный поиск по запрещённым словам;

5. Просматривать экран компьютера ребенка по сети (удаленная перезагрузка и выключение);

6. Контроль за посещением ресурсов Интернета;

7. Получение отчета о посещенных страницах по электронной почте.

На сегодняшний день существует большое количество вариантов родительского контроля. При выборе одного из них необходимо обратить внимание на несколько факторов:

1. Какие функции родительского контроля вы планируете использовать: про-

сто ограничить время и посещение сайтов с противозаконным и неэтичным контентом или же хотите установить тотальную слежку.

2. Возраст ребенка и его навыки работы с компьютером.

3. Какое программное обеспечение уже установлено на вашем компьютере (ОС, антивирус).

Способы родительского контроля:

Родительский контроль средствами операционной системы Windows

Родительский контроль – удобная функция для родителей, которая появилась в последних версиях ОС от Microsoft.

Владельцы ПК на базе ОС Windows имеют возможность бесплатно установить и использовать программу Family Safety («Семейная безопасность») из пакета Windows Essentials. Чтобы сделать это, достаточно пару раз щелкнуть мышью на сайте Microsoft. Естественно, для работы потребуются учетная запись Microsoft, а также версия операционной системы не ниже Windows Vista. После установки программы можно будет выбрать учетную запись и ввести для нее ограничения. Если компьютером одновременно пользуются несколько человек, для детей следует создавать отдельные учетные записи.

Контроль учетных записей с помощью «Семейной безопасности» осуществляется в особой зоне сайта Microsoft, где позволительно очень гибко настраивать все типы фильтрации и ограничений. Также система ведет журнал активности, благодаря чему легко узнать, когда ребенок сел за компьютер и сколько времени провел за ним.

Эта функция позволяет:

- оградить детей от нежелательного содержимого;
- сделать браузер для детей более безопасным;
- наложить запрет на запуск определенных приложений и игр;
- ограничить время, проводимое детьми за ПК.

Родительский контроль в браузере

При использовании детьми интернет-браузеров, родительский контроль может быть осуществлен с помощью таких браузеров, как:

– **браузер Google Chrome** имеет функцию родительского контроля, которая осуществляется через управление контролируемым профилем. При использовании такого родительского контроля в браузере вы сможете регулировать поведение вашего ребенка в Интернете.

– **детский браузер Гогуль** – бесплатное расширение для браузера *Mozilla Firefox* для родительского контроля и ограничения детей в Сети от нежелательного контента. Имеется каталог «белых», разрешённых к просмотру детьми сайтов, остальные будут блокироваться по умолчанию.

Родительский контроль средствами антивирусов

Некоторые антивирусы имеют возможность установки ограничения доступа к определенным сайтам в Интернете.

Родительский контроль Kaspersky Internet Security – это компонент программы, позволяющий установить для каждой учетной записи на компьютере ограничения доступа использования компьютера и Интернета. С его помощью можно контролировать: запуск различных программ; использование Интернета (ограничение использование Интернета по времени); посещение веб-сайтов в зависимости от их содержимого; загрузку файлов из Интернета в зависимости от их категории; переписку с определенными контактами в социальных сетях.

Модуль родительского контроля «Доктор Веб» помогает ограничить доступ пользователей компьютера к определенным сайтам в сети Интернет, локальным файлам или папкам, ресурсам локальной сети. Администратор компьютера может сам задать список запрещенных сайтов или воспользоваться постоянно обновляемыми тематическими списками, предоставляемыми компанией «Доктор Веб».

Родительский контроль на уровне провайдера

Некоторые провайдеры, предоставляющие доступ в Интернет, оказывают дополнительные услуги по защите от запрещённого контента. Услуга, как правило, платная. Подключается в «Личном кабинете» или при обращении к оператору связи.

Родительский контроль на Wi-Fi-роутере

При подключении к Интернету через Wi-Fi-роутер можно воспользоваться встроенной в него функцией Parental Control (Родительский контроль). Такая функция есть не на всех роутерах.

Настройка родительского контроля предоставляет возможность создавать правила доступа к сайтам для каждого компьютера или мобильного устройства, которое подключается через точку доступа (устройства распознаются по MAC адресу). Можно также запретить доступ к определённым сайтам или разрешить только к некоторым для всех устройств, которые работают через один и тот же роутер.

Специальные программы для родительского контроля

Специальные программы для родительского контроля обладают рядом преимуществ перед остальными способами, так как предоставляют больший объем возможностей:

- анализ содержимого страниц на присутствие запрещенных слов;
- блокирование доступа к сайтам из «черного» списка;
- ограничение использования Интернета по времени;
- просмотр экрана компьютера ребенка по сети (удаленная перезагрузка и выключение);
- режим «Безопасный поиск» в поисковых системах;
- запись адресов посещенных сайтов в файл-журнал;
- отсылка отчета о посещенных страницах по электронной почте;
- автоматическая деактивация программы для администраторов программы;
- специальные функции для работы с программой через локальную сеть;
- контроль запуска игр.

Примеры программ:

Crawler Parental Control 1.1

KidsControl 2.02

ParentalControl Bar 5.22

КиберМама

KinderGate

ОдинДома

КиберЦензор

Родительский контроль на смартфонах

Установить родительский контроль на мобильном устройстве вашего ребенка достаточно просто – можно воспользоваться специальной программой (например, **Safe Lagoon**) или подключить у мобильного оператора специальную услугу «Детский Интернет».

Помните, что ни один из перечисленных способов не гарантирует на 100% защищенность вашего ребенка от опасностей современного Интернета. Важно приложить усилия к тому, чтобы дети в силу воспитания сами не стремились к поиску запрещенного контента, знали о возможных последствиях всех своих действий в Интернете.

Советы по управлению безопасностью детей при работе с Интернетом:

- Старайтесь держать компьютеры с подключением к Интернету в общих комнатах, в которых можно легко осуществлять визуальный контроль над тем, что делает ваш ребенок в Интернете.
- Создайте при участии детей свод домашних правил пользования Интернетом и требуйте его неукоснительного соблюдения.
- Приучите детей посещать только те сайты, которые вы разрешили.
- Используйте средства блокирования нежелательного материала как дополнение, но не замену к родительскому контролю.
- Создайте семейный электронный ящик, на который будет приходить вся ваша электронная почта, вместо того чтобы позволять детям иметь собственные адреса.
- Научите детей советоваться с вами перед раскрытием информации через электронную почту, чаты, доски объявлений, регистрационные формы и личные профили.
- Маленьким детям не следует пользоваться чатами – слишком велика опасность. Только когда ваш ребенок подрастет, можно разрешить общаться там, где есть контроль над сообщениями (или, говоря компьютерным языком, «модерация»).
- Научите детей не загружать программы, музыку или файлы без вашего разрешения.

- Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.
- Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится.
- Если, несмотря на все меры предосторожности, ваши дети познакомились в Интернете со злоумышленником, не вините их. Вся полнота ответственности всегда лежит на правонарушителе. Предпримите решительные действия для прекращения дальнейших контактов ребенка с этим лицом.

6 ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В СЕТИ «ИНТЕРНЕТ»

1. Приложите максимум усилий к защите ваших технических устройств:

- регулярно обновляйте операционную систему;
- используйте лицензионную антивирусную программу;
- применяйте файервол;
- создавайте резервные копии важных файлов;
- используйте надёжные пароли;
- периодически меняйте пароли на самых важных для вас сайтах;
- скачивайте программы только с официальных источников;
- не посещайте подозрительные сайты;
- закрывайте сомнительные всплывающие окна;
- не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они ни были.

2. При работе с электронной почтой:

- никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их, выбрав команду в меню сообщений.
- никогда не отвечайте на спам;
- никогда не пересылайте «письма счастья» и другой подобный спам. Вместо этого сразу удаляйте такие письма.

3. Защите самих себя:

- не вводите личную и конфиденциальную информацию на непроверенных и подозрительных сайтах;
- внимательно относитесь к собеседникам в Интернете, сообщайте важную информацию только проверенным людям;
- при работе за компьютером, к которому имеют доступ другие люди, не сохраняйте пароли в браузере.

4. Соблюдайте правила:

- помните, что в виртуальном пространстве ответственность наступает по реальным законам;
- уважительно и добросовестно относитесь к другим пользователям сети Интернет.

По вопросам в сфере персональных данных
Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор):

Справочно-информационный центр:

8 (495) 983-33-93 (пн-чт 9:00-18:00, пт 9.00-16:45)

Управление Роскомнадзора по Ульяновской области

Отдел по защите прав субъектов персональных данных, надзора в сфере массовых коммуникаций и информационных технологий:

8 (8422) 21-42-07
E-mail:rsockanc73@rkn.gov.ru

По обращениям, относительно деятельности мошеннических интернет-ресурсов, создания использования и распространения вредоносного программного обеспечения, неправомерного доступа к компьютерной информации, хищениям, совершенным с использованием поддельных банковских карт, электронных платежных систем и систем дистанциооного банковского обслуживания

УМВД России по Ульяновской области
8 (8422) 42-29-60, 67-88-00432071,
г. Ульяновск, ул. К. Маркса, 31/108
8 (8422) 67-88-88 – «горячая линия»
https://73.мвд.рф

Общественная приемная МВД РФ
Выбрать пункт «Управление К МВД России»

https://mvd.ru/request_main

Информация для проведения уроков безопасного Интернета в школах
Лига безопасного интернета

http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachers-detail.php?ID=3652

Брошюра «Информационная безопасность в сети Интернет»

Проект реализуется за счет средств, выделенных по результатам конкурсного отбора социально ориентированных некоммерческих организаций для предоставления субсидий из бюджета муниципального образования «Город Ульяновск»

Брошюры изданы для бесплатного распространения.

Изготовитель: ООО «Центр коммуникаций Поволжья», 432011, г. Ульяновск, ул. Радищева 90, офис 1.
Объем: 36 стр. Печать офсетная. Тираж: 3000 экземпляров. Заказ №1. Подписано в печать 18.10.2017