СОЗДАНИЕ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СРЕДЫ ДЛЯ ДЕТЕЙ И ПОДРОСТКОВ

ЦИФРОВОЕ ПОСОБИЕ ДЛЯ РОДИТЕЛЕЙ И ПРЕПОДАВАТЕЛЕЙ

Подготовлено при активной поддержке:

4N6 DELTA FORENSICS

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ

КАК СОЗДАТЬ БЕЗОПАСНУЮ ИНФОРМАЦИОННУЮ СРЕДУ ДЛЯ РЕБЕНКА?

Пособие для аналоговых родителей в цифровом мире.

В этом пособии мы осветили для Вас следующие вопросы:

1. Как противостоять или недопустить травлю в Интернете.
2. Как не стать жертвой мошенников.
3. Как избежать вовлечения ребенка в незаконную деятельность.
4. Как ограничить получение нежелательной для ребенка информации.
5. Как избежать склонения ребенка к действиям сексуального характера.
6. Как избежать пристрастия ребенка к азартным играм и как контролировать, во что и сколько играют Ваши дети.
7. Какие виды ответственности предусмотрены действующим законодательством за преступления в Интернете?

ПРЕДИСЛОВИЕ ОТ АВТОРОВ ПОСОБИЯ:

Николай Дорин

Руководитель компании по расследованию киберпреступлений «Delta Forensics»

@nikolay.dorin

Задача любого родителя – вложить в руки ребенка современные инструменты, позволяющие развиваться и добиваться успеха. От того, как Ваш ребенок научится использовать технологии и работать с информацией зависит станет ли техника его помощником или постоянным вредителем.

Евгения Глебова

Когнитивный психолог. Клинический психолог. Преподаватель Института развития образования Краснодарского края. Врач высшей категории.

@evgeniya.psychologist

Помните – ребенок, это чистый лист бумаги, что вы на нем напишите, то и будет зафиксировано. Но если вы впишите слишком мало информации, то там ее напишут другие, посторонние люди и исправить это будет крайне сложно!

Рада Сахаренкова

Заведующая сектором по продвижению библиотечно-информационных технологий МУК ЦБС города Краснодара

@glambookworm

Информационная гигиена - залог гармоничного существования детей и родителей в информационном обществе.

Мария Викторовна Бердник

Юрисконсульт ООО «Дельта Форензикс»
юрист, специалист в области правового обеспечения информационной безопасности

center_ib@kubstu.ru

В игре с неполной информацией преимущество получает тот, кто знает или может получить дополнительную информацию.

Максим Гострый

Ведущий специалист ООО «АТЭК-С»

center_ib@kubstu.ru

Если Вы хотите вырастить хороших детей, тратьте на них в два раза меньше денег и в два раза больше времени.

Даниил Погорелов

Руководитель отдела информационной безопасности компании Delta Forensics

root@delta-forensics.ru

Информационная безопасность как личная гигиена. Если не соблюдать элементарных правил, то со временем проблемы обязательно дадут о себе знать.

С КАКИМИ ОПАСНОСТЯМИ В ИНТЕРНЕТЕ МОЖЕТ СТОЛКНУТЬСЯ РЕБЕНОК?

1. Травля (буллинг).

Интернет-среда является очень агрессивной. Связано это с фактом наличия возможности остаться неизвестным, что дает отдельным пользователям ощущение вседозволенности. О причинах и последствиях кибертравли подробнее в разделе «Как недопустить или отреагировать на травлю в Интернете».

2. Мошенничество.

В связи с легкой возможностью обеспечения анонимности Интернет является пристанищем огромного количества различного рода мошенников. Современные технологии позволяют злоумышленникам атаковать одновременно огромное количество потенциальных жертв. В числе которых запросто может оказаться и Ваш ребенок. Какие меры стоит предпринять для защиты своей семьи в цифровом пространстве – читайте в разделе «Как не стать жертвой мошенников».

3. Вовлечение в незаконную деятельность.

«Дурное дело не хитрое» - говорит народная мудрость. Вовлечению в незаконную деятельность подвержены в большей степени дети подросткового возраста. Чаще всего это обусловлено первыми проявлениями самостоятельности – желанием заработать первые деньги, найти компанию по интересам или объяснение происходящим в окружающем мире событиям. Как выявить и пресечь попытки вовлечения ребенка в незаконную деятельность читайте в разделе «Вовлечение подростков в незаконную деятельность»

4. Информация, наносящая потенциальный вред психическому здоровью ребенка.

Интернет уже давно не является местом исключительно «молодежной тусовки». На сегодняшний день глобальная паутина позволяет удовлетворить запрос на любую информацию, в числе которой присутствует и информация, которая может оказать существенное негативное влияние на полноценное и всестороннее

развитие ребенка (просто в силу возрастных особенностей). Не говоря уже о контенте, имеющем деструктивную направленность, одинаково шокирующую как детей, так и взрослых. Как, зачем и с помощью чего можно исключить потребление деструктивного и ограничить потребление возрастного контента в разделе «Информация, наносящая потенциальный вред психическому здоровью ребенка ».

5. Склонение к действиям сексуального характера.

Уровень интереса ребенка к разным жизненным сферам может проявляться очень по-разному в зависимости от темперамента – от последовательного и аккуратного изучения, до взрывного всепоглощающего интереса. Любопытство, характерное для подросткового возраста, а также естественные физиологические процессы, происходящие в организме ребенка постепенно подводят его к познанию принципов и механизмов отношений. К тому же, общепринятые ритуалы ухаживания тоже претерпели некоторые изменения в угоду времени. Как правильно направить подростка, о чем с ним нужно поговорить, с какими опасностями он может столкнуться – в разделе «Склонение к действиям сексуального характера».

6. Игромания

И речь сейчас идет не только об известной проблеме пристрастия детей и подростков к компьютерным играм, но и о более «классической» игровой зависимости – пристрастию к азартным играм. У самих детей к традиционным казино интереса мало, однако в Сети присутствует огромное количество сервисов, на которых за реальные деньги разыгрываются столь вожделенные для подростков реальные и виртуальные предметы. Как это устроено и как отреагировать на интерес ребенка к таким вещам – читайте в разделе «Лудомания и зависимость от видеоигр»

КАК ПОДГОТОВИТЬ РЕБЕНКА К ВЗАИМОДЕЙСТВИЮ С ИНТЕРНЕТ-СРЕДОЙ.

Коммуникации с использованием Сети стали важной частью нашей жизни на всех социальных уровнях: начиная от бытового (семейного), заканчивая практически полностью произошедшей миграцией рабочей переписки в социальные сети и мессенджеры.

Расхожее мнение о том, что Интернет ограничивает пространство вокруг человека до размера площади монитора верно лишь отчасти. Использование телекоммуникаций не только стирает географические границы, но и позволяет более грамотно распоряжаться своим временем. Это могут подтвердить те, кто уже не стоит в очередях и оплачивает счета за коммунальные услуги, связь и иные услуги с использованием банк-клиента через Интернет.

Великая сила и, одновременно, опасность Интернета кроется в том, что он позволяет любому пользователю генерировать и потреблять именно тот контент, который ему интересен. То есть настраивать свое информационное окружение в соответствии со своими индивидуальными вкусовыми предпочтениями.Вековую мудрость «Скажи мне, кто твой друг, и я скажу тебе кто ты» впору переформулировать в «Скажи мне, на кого ты подписан, и я скажу тебе, чем ты живешь». Возможность самостоятельно формировать свою информационную повестку позволяет с одинаковым успехом как утолять жажду знаний об окружающем мире, так и окружить себя деструктивным контентом.

Сегодня ни одно публичное явление не может существовать в отрыве от контекста социального восприятия. Связано это с тем, что Интернет позволяет комментировать и транслировать частное мнение о любом событии в любой точке планеты на неограниченную аудиторию. В последнее время нередки случаи, когда шумиха вокруг какого-либо события вызывает в Интернете гораздо больше резонанса, чем само событие. Единственным эффективным регулятором градуса адекватности этих мнений и комментариев являются общепринятые социальные нормы, которые в силу разных причин, в том числе территориальных и социальных особенностей, могут давать сбой и приводить к распространению недостоверной информации.

Всего на свете знать невозможно. Ребенок, не имеющий возможности получить удовлетворение своего интереса по поводу какого-либо события, факта или явления от родителей, родственников или старших товарищей, может искать способ удовлетворить свое любопытство с использованием доступных источников информации. Неразвитое критическое мышление, характерное для юного возраста в силу естественных причин в купе с юношеским максимализмом могут приводить к неконтролируемому потреблению контента, в числе которого может присутствовать и деструктивный.

Однако, не только любопытство может стать причиной учащенного посещения глобальной паутины. Давайте рассмотрим более подробно, почему детей и подростков так тянет в виртуальный мир.

Евгения Глебова

Когнитивный психолог. Клинический психолог. Преподаватель Института развития образования Краснодарского края. Врач высшей категории.

@evgeniya.psychologist

Поведение подростка отражает стремление к приключениям, завоеванию признания, испытанию границ дозволенного. Его поисковая деятельность служит расширению этих границ и индивидуального опыта. Суть такого поведения заключается в том, что стремясь уйти от реальности пытаются создать иллюзию успешности, равновесия, безопасности.

«Подобное поведение может быть способом попытки решения конфликта с окружающими или с самим собой»

Причинами могут быть пробелы или дефекты в знаниях правовых и моральных норм, несформированные нормативные потребности и ценности, особенности характера и эмоционально-волевой сферы, отрицательное влияние семьи или окружения, влияние контекстной информации социальных сетей (групп, на которые подписан ребенок и его сетевого окружения).

К основным причинам, предрасполагающим к уходу от реальности в виртуальный мир или организованные группы относятся:

- Стремление получить сильные впечатления
- Заболевания, ограничивающие деятельность ребенка
- Повышенная возбудимость, неумение себя контролировать
- Неблагополучная ситуация в семье
- Стремление к самостоятельности и независимости
- Отставание в учебе
- Плохие отношения со сверстниками
- Нарушенные детско-родительские отношения (отсутствие взаимопонимания)
- Неуверенность в себе
- Отсутствие или неоформленность смысла жизни
- Негативные формулировки будущего
- Отрицательная оценка взрослыми способностей ребенка
- Частые стрессовые ситуации
- Напряженная экономическая ситуация в семье (или частые разговоры взрослых на эту тему)
- Чрезмерная отдаленность родителей от ребенка (в том числе эмоциональная)
- Конфликты между родителями и ребенка с родителями
- Большое количество запретов со стороны родителей
- Неразвитость ребенка
- Повышенная коммуникативность (общительность), доверчивость ребенка
- Низкий уровень самоконтроля и знаний о нем
- Подверженность ребенка принимать чужую оценку своих действий, как единственно верную
- Одиночество
- Излишний родительский контроль и авторитарность позиции родителей
- Отсутствие навыков социальной адаптации (незнание норм и правил поведения в обществе)
- Отсутствие занятости ребенка
- Желание завоевать внимание любым путем
- Влияние близкого окружения
- Постановка перед ребенком слишком сложных для него задач

Чаще всего в виртуальной группе:

- происходит получение психологической поддержки и поощрения виртуального увлечения;
- увеличивается привлекательность виртуального увлечения за счет отсутствия контроля
- получая одобрение виртуальных действий растет потребность в их совершении
- Создается иллюзия освобождения от травмирующих обстоятельств
- Появляется ощущение повышения самооценки и оценки виртуальной группой

О наличии проблем могут говорить следующие особенности поведения ребенка:

- Негативная направленность
- Повышенная тревожность
- Нежелание искренних доверительных разговоров
- Готовность к риску
- Эмоциональная неустойчивость настроения
- Непредсказуемость реакции
- Высокая агрессивность

---

1. Как бы мы не относились к этому явлению, общение в Сети – важная часть социальной жизни. Большая часть информации в Интернете генерируется людьми и для людей. Фактически Интернет представляет собой отражение общества в цифровом виде.

2. Интернет может удовлетворить запрос на абсолютно любую информацию: вне зависимости от времени события, географии происхождения и вкусовых предпочтений.

3. При наличии ряда психологических проблем, корни которых могут находиться, в том числе, внутри семьи, дети могут искать их решения в кругу виртуальных друзей, истинная мотивация которых может существенно отличаться от общепринятых норм и правил.

Поэтому, так важно направить ребенка в этом информационном океане и научить его правильно распоряжаться получаемой им информацией. Согласитесь, что с учетом озвученных в предисловии опасностей ребенок нуждается в вашей помощи по этому вопросу. Для этого нужно:

Первое и самое важное – нужно объяснять ребенку и показывать собственным примером, что Вы обеспокоены безопасностью себя и своей семьи в цифровом пространстве, а также ответственно подходите к потреблению информации.

Второе (если необходимо) – предпринимать меры технического характера для исключения доступа к информации и ресурсам, которые так или иначе могут нанести вред ребенку или подтолкнуть его к нежелательным действиям.

УГРОЗА № 1.КАК НЕДОПУСТИТЬ ИЛИ ОТРЕАГИРОВАТЬ НА ТРАВЛЮ В ИНТЕРНЕТЕ?

Травля – агрессивное преследование одного из членов коллектива другими членами коллектива. Травля от обычного межличностного конфликта отличается четким распределением ролей. Всегда есть явно выраженная «жертва» и явно выраженный «агрессор». К тому же для травли характерна продолжительность во времени и неоднократные повторения действий со стороны агрессора.

Главная опасность травли состоит в доведении жертвы до психически нестабильного состояния, что несомненно может «аукнуться» на процессе дальнейшей социализации и становления ребенка как полноценного члена общества.

В случае любой замкнутой социальной группы (класса или группы) при выявлении травли окружающие детский коллектив взрослые могут вмешаться и принять адресные меры против этого негативного явления. Эти меры могут включать в себя как физическое отстранение агрессора от коллектива, так и профилактическую работу по локальному искоренению травли и созданию благоприятной атмосферы в коллективе.

Однако, в случае травли в Интернете все немного иначе. Большинство ресурсов в Интернете являются общедоступными и охватывают на несколько порядков большую аудиторию и географию, чем привычные нам социальные группы. Кибертравля может сопровождаться:

- Распространением слухов и сплетен в отношении конкретного лица (явление, известное как «моббинг»);
- распространением грубых и непристойных шуток, обзывательств и высмеивания;
- навязчивым вниманием со стороны «агрессора», помешательством и постоянным преследованием (явление, известное как «сталкинг»)
- распространение личных фотографий и персональной информации «жертвы», в том числе с нелицеприятными и грубыми подписями;

- разглашением компрометирующей жертву информацией об обстоятельствах личной и общественной жизни, которая может стать дополнительным поводом для травли. Такая информация может стать известна агрессору в результате непреднамеренного разглашения информации самой жертвой, взломов страниц и неправомерного доступа к социальным сетям, облачным хранилищам и резервным копиям данных (подробнее о том, как этого не допустить читайте в разделе про то, как не стать жертвой мошенников).

Евгения Глебова

Когнитивный психолог. Клинический психолог. Преподаватель Института развития образования Краснодарского края. Врач высшей категории.

@evgeniya.psychologist

Этим вопросом задаются многие родители и дети, столкнувшиеся с таким видом проявления агрессии, как попытка унижения чести и достоинства другим лицом (собеседником, знакомым, незнакомцем). В первую очередь в такой ситуации необходимо оценить ситуацию «без эмоций»:

1. Совершал ли объект «травли» действия, которые спровоцировали «травлю»? Если да, то необходимо оценить вред, которые нанесли эти действия нападающему, хотя в данном случае «нападающий» на самом деле переходит в роль жертвы, которая защищает свою честь и достоинство. В данном случае – необходимо принести извинения жертве и гарантировать их искренность и полное раскаяние, без дальнейшего ведения диалога или дискуссий.

2. Если провоцирующих действий не выявлено, то просто игнорировать такие информационные нападки. Если в виртуальной группе происходит развитие событий с вовлечением все большей аудитории в разбор ситуации – необходимо оценить значимость такого окружения. Если членство в такой группе не является значимым для реальной жизни, то решением вопроса будет выход из такого сообщества. Никогда не пытайтесь перевоспитывать социально-агрессивных людей! Это бесполезно! Возможно ваш ребенок стал участником группы, в которой присутствуют подростки с психопатологией.

3. Если ваш ребенок регулярно сталкивается с элементами «травли» при общении со своими сверстниками, это может говорить о его низкой самооценке и поведенческой стратегии «жертвы». Скорее всего ваш ребенок в поведении и своих высказываниях представляется своему окружению как слабая, неуверенная в себе, психо-эмоционально зависимая личность. В таком случае необходима помощь психолога по повышению самооценки и воспитанию самостоятельности.

Если же Вы столкнулись с обратной ситуацией и увидели, что Ваш ребенок осуществляет травлю в чей-то адрес: нецензурно выражается, хамит, оскорбляет всех родственников и домашних животных оппонента до третьего колена, то примите меры по пресечению такого рода активности. У такого поведения тоже имеются свои причины, и обнаружить их возможно, к сожалению, только в результате совместной работы с психологом.

Николай Дорин

Руководитель компании по расследованию киберпреступлений «Delta Forensics»

@nikolay.dorin

В крайнем случае, если Интернет-оппонент, что называется, «не унимается», настойчиво прерывает тишину в адрес Вашего ребенка и продолжает свое «черное дело», то на этого пользователя всегда можно пожаловаться. На сообщение, комментарий или пост при наличии прямых оскорблений, унижения чести и достоинства (в том числе и по национальным и внешним признакам) можно обратить внимание модераторов/администраторов используемого Интернет-ресурса.Сделать это можно в меню

сообщения/поста/комментария . Практика показывает, что администрация сервисов реагирует на такие вещи практически незамедлительно, а ответственность для учетной записи нарушителя спокойствия может быть фатальной. К тому же, практически все мессенджеры и социальные сети имеют функцию «черный список», помещение в который практически всегда приводит к тишине в радиоэфире.

Кроме того, если Вы видите, что в публичных комментариях или чатах незаслуженно принижают честь и достоинство другого человека или позволяют себе нелицеприятные комментарии – не проходите мимо.

В случае, если кибертравля уже привела к неприятным последствиям, а обидчик находит все новые и новые способы выхода на контакт, то самым правильным решением будет привлечь его к установленной Законом ответственности. Для этого необходимо обратиться с заявлением в правоохранительные органы. К заявлению необходимо приложить:

1. Если угрозы поступают по электронной почте:

- сохраните оригинал электронного письма. Сделать это можно в меню открытого сообщения. «Письмо – сохранить оригинал письма» или «… - свойства письма».
- сделайте снимки экрана (скриншоты) на которых видно сам текст письма, адрес электронной почты Вашего ребенка, дату и время. Если письмо содержит какие – либо материалы или ссылки на них, то необходимо сохранить ссылки на этим материалы в текстовом файле. Если в письме содержатся фотографии или документы, то также сохраните их отдельно. Осуществлять эти действия необходимо в присутствии нескольких свидетелей. Еще лучше – у нотариуса.
- Не удаляйте оригинал электронного сообщения до момента привлечения агрессора к ответственности.

2. Если угрозы поступают в социальных сетях или мессенджерах:

В присутствии свидетелей сделайте снимок экрана (скриншот), на котором видны:

- Полный текст сообщения.
- какой-либо указатель на учетную запись отправителя: имя учетной записи и пиктограмму фотографии
- отдельным снимком экрана сделайте снимок страницы возмутителя спокойствия (содержащую сетевые адреса на страничку, идентификаторы, номера телефонов и адреса электронной почты).
- Если речь идет о мессенджерах, то воспользуйтесь функцией экспорта чата.
- Не удаляйте поступившие сообщения до момента привлечения агрессора к установленной ответственности.

УГРОЗА № 2. КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ?

Как уже было отмечено в предисловии, Интернет является естественной средой обитания огромного количества мошенников. Причин этому несколько:

- Место совершения преступления уже не является местом реального местонахождения злоумышленника. Это значит, что кто угодно, находящийся где угодно может обмануть кого угодно, находящегося где угодно;
- Возможность легкого обеспечения анонимности (сокрытия реальной личности) с использованием технических средств позволяет злоумышленнику «менять личину» по несколько раз в минуту;
- Использование технических и автоматических средств дает злоумышленнику возможность осуществлять одновременные атаки против неограниченного количества пользователей.

Николай Дорин

Руководитель компании по расследованию киберпреступлений
«Delta Forensics»

@nikolay.dorin

Основной целью злоумышленников являются:

- Логины и пароли от учетных записей: платежных систем, личных кабинетов банков, страниц в социальных сетях, адресов электронной почты, игровых сервисов.
- Реквизиты банковских карт и других платежных систем;
- Введение детей в заблуждение с целью выманивания денежных средств под различными предлогами.
- Несанкционированный доступ к вашему компьютеру и хранящемуся на нем данных;
- Получение доступа к Вашим устройствам в целях последующего осуществления атак с него на другие сетевые ресурсы.

Помните, что злоумышленник атакуя вашего ребенка стремится завладеть в том числе и Вашими данными, которые случайно могут оказаться на его устройстве. Поэтому объясните ребенку эти простые правила как не попасться на удочку мошенников:

1. Бесплатный сыр бывает только в мышеловке.

Розыгрыш больших призов и подарков не происходит путем рассылок в мессенджерах или по электронной почте, а, как правило, связан с совершением определенных действий с рекламируемыми товарами и услугами. Деньги в Интернете зарабатываются точно таким же трудом, как и в обычной повседневной жизни. Помните об этом.

2. Не стоит регистрироваться на сомнительных ресурсах или осуществлять вход с помощью социальных сетей на них.

К таким ресурсам относятся: сайты с розыгрышами ценных призов и подарков, сайты с игровыми дополнениями или бесплатными предметами для компьютерных игр; сайты, предлагающие легкий заработок; сайты, использующие «желтые» заголовки; сайты и приложения для накрутки «лайков» и осуществления репостов.

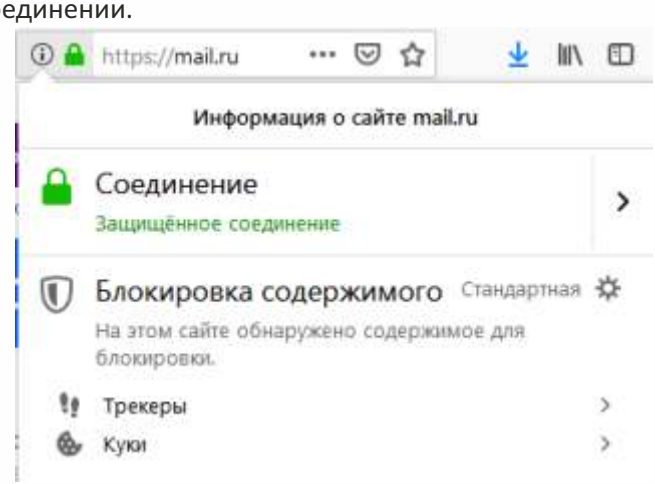
Почему так? Во-первых имеется вполне очевидная опасность похищения логинов и паролей от учетных записей.

Во-вторых, основная опасность кроется здесь не столько в недостоверности размещенной на псевдоновостных сайтах информации, сколько в том, что большая часть таких ресурсов живет за счет показов рекламы. Чем больше рекламы – тем больший уровень дохода имеет владелец ресурса. Это может приводить к тому, что среди огромного количества рекламных баннеров могут оказаться ссылки на зараженные ресурсы, поскольку, как правило, администрация таких ресурсов не проверяет своих рекламодателей.

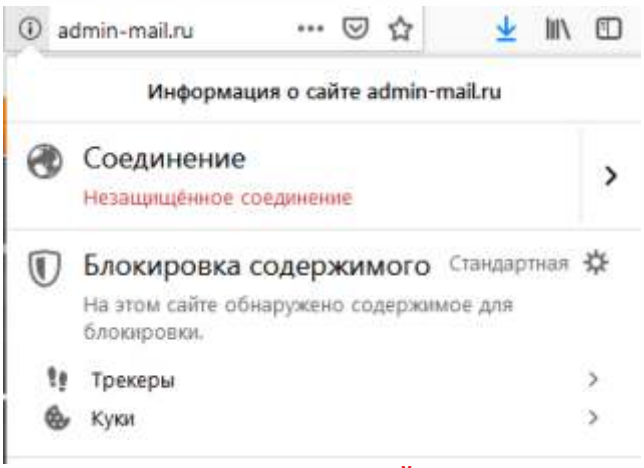
3. При регистрации или подтверждении учетных данных проверяйте, чтобы в адресной строке была иконка замка (это значит, что соединение является защищенным), а адрес, указанный в адресной строке содержал действительный адрес ресурса.

Например, при обращении к ресурсу «mail.ru» в адресной строке должно быть именно «mail.ru», а не «mai1.ru» или «pochta-mail.ru».

Проверить название организации, для которой был выпущен или подтвержден сертификат, используемый при соединении между вашим устройством и сервером можно просто щелчком на иконке замка в адресной строке. Большинство браузеров предупреждают пользователя о незащищенном соединении.



ОРИГИНАЛЬНЫЙ РЕСУРС



МОШЕННИЧЕСКИЙ РЕСУРС

4. Привяжите учетную запись к номеру телефона или своему устройству.

Большинство современных сервисов имеют такую возможность. В случае, если злоумышленник скомпрометирует логин и пароль, то ему этого будет недостаточно для того, чтобы осуществить вход в вашу учетную запись. Для входа потребуется дополнительное действие – либо ввести одноразовый код из СМС или push-уведомления в приложении на Вашем устройстве.

5. Используйте разные сложные пароли для всех учетных записей. Для простоты следования этому правилу можно использовать парольные менеджеры.

В некоторых операционных системах (например MacOS и iOS) хранение паролей в парольном менеджере является предустановленной производителем функцией. И этот способ уже годами доказывает свою эффективность в предотвращении такого рода атак.

Если вы пользуетесь ОС Windows или любым Linux'ом, то добавить функцию хранения паролей можно установив бесплатное приложение «keepass». Вы запоминаете только один сложный пароль от контейнера, где надежно сохраняются ваши логины и пароли, а затем просто осуществляете копирование пароля из защищенной области. К тому же в парольные менеджеры обычно встроены генераторы надежных паролей, которые невозможно «подобрать».

Если вы не хотите доверять самую ценную информацию сторонней бесплатной программе: парольные менеджеры есть и в составе большинства современных антивирусных продуктов. Существуют и отдельные решения для хранения паролей от производителей антивирусов.

6. Не переходите по ссылкам из электронных писем, мессенджеров, сообщений, полученных от неизвестных адресатов.

Скорее всего, за этой ссылкой прячется установщик вредоносного программного обеспечения: банковского троянца или кейлоггера, которые в момент похитят деньги с банковских счетов или украдут пароли; либо шифровальщика, который зашифрует все ваши документы и фотографии и потребует выкуп за вашу же информацию.

7. Используйте средства антивирусной защиты с функциями сетевого анализа.

В таком случае Вы, как минимум, создадите еще один уровень родительского контроля, а как максимум – не дадите ребенку посетить мошеннический сайт или подвергнуться атаке с помощью вирусов.

8. Пользуйтесь лицензионным программным обеспечением, его бесплатными ограниченными версиями или аналогами от известных производителей.

Из личного опыта могу сказать, что этого вполне достаточно для бытового использования. Поверьте опыту экспертов нашей компании – дешевле купить антивирус, чем пытаться восстанавливать уничтоженные файлы и доказывать несанкционированные платежные операции с банковской карты. Кроме того, большая часть заражений происходит по причине поиска заведомо пиратского программного обеспечения или «программ для лечения от жадности» (как называют их некоторые пользователи).

К слову, рынок программного обеспечения в нашей стране является достаточно демократичным. Например, крупные производители средств антивирусной защиты предлагают семейные тарифы на 3-5 устройств по весьма приемлемой цене.

9. Не пренебрегайте обновлениями программ и операционной системы.

Этот совет является последним по списку, но не по значению. Своевременное обновление операционной системы значительно снижает вероятность пострадать при массовых атаках и глобальных вирусных эпидемиях.

УГРОЗА № 3. ВОВЛЕЧЕНИЕ ПОДРОСТКОВ В НЕЗАКОННУЮ ДЕЯТЕЛЬНОСТЬ

Предложение легкого заработка в Интернете в настоящий момент значительно превышает спрос. Связано это с тем, что киберкриминал, неотделимо сросшийся с традиционным криминалом, постоянно находится в поисках исполнителей. Злоумышленники предлагают подросткам попробовать себя в качестве:

«обнальщиков» - лиц, осуществляющих обналичивание через свои банковские счета денежных средств, добытых преступным путем,

«курьеров» - лиц, осуществляющих распространение наркотических средств или иных запрещенных в гражданском обороте предметов;

«мулов» - лиц, осуществляющих простые технические действия, обеспечивающие проникновение злоумышленника в техническую систему или осуществляющих доставку денежных средств по результатам произведенной кибератаки.

Источниками информации о наличии «вакантных мест» являются:

- Комментарии к постам в популярных сообществах, социальных сетях, открытых чатах с недостаточно качественной модерацией;
- Открытые и закрытые форумы тематической направленности;
- Объявления в социальных сетях или на иных сетевых ресурсах (веб-сайтах, в поисковой выдаче).

Фактически данные «подработки», если их можно так назвать, требуют наличия минимальных технических знаний и оборудования, что существенно снижает порог вхождения в криминальную деятельность. Чаще всего, вовлекаемые в приведенные занятия подростки не осознают до конца возможную правовую ответственность, а также тот факт, что люди, привлекающие их к этим занятиям, остаются за ширмой анонимности.

Признаками наличия такой «подработки» являются:

- Наличие у ребенка неоправданно большого количества банковских карт или счетов в платежных системах (QIWI, Яндекс. Деньги, PerfectMoney и иные платежные системы);
- Появление денег и предметов, происхождение которых ребенок не может объяснить;
- Наличие СИМ-карт операторов сотовой связи с неустановленным происхождением;
- Наличие дополнительных средств связи (телефонов, смартфонов, планшетов, компьютеров) неустановленного происхождения;
- Регулярное исчезновение ребенка из дома в темное время суток;

Кроме того, как уже было отмечено ранее, для подростков характерен поиск цельной картины мира, которая в полной мере может дать однозначную оценку происходящим вокруг событиям. Часто этим пользуются представители террористических, экстремистских и религиозных организаций, деятельность которых запрещена на территории Российской Федерации. Вы удивитесь, насколько на первый взгляд стройными бывают теории экстремистского, националистического или криминального толка.

Как правило, первый контакт вербовщиком осуществляется с использованием популярных социальных сетей или мессенджеров. Для выявления заинтересованности вербовщик, как правило, анализирует активность жертвы в Интернете: посты на личных страницах, комментарии под новостями, подписки на сообщества и публичные чаты соответствующих тематик. При этом злоумышленник максимально быстро старается перевести контакт в мессенджеры или СМС, чтобы переписка носила скрытый характер.

Деньги в Интернете, как и в реальной жизни, можно заработать лишь применив свой труд, способности и таланты.

Как понять, что компьютер или телефон используются не только для учебы?

Николай Дорин

Руководитель компании по расследованию киберпреступлений «Delta Forensics»

@nikolay.dorin

1. Наличие программ для обхода блокировок и доступа к теневым и заблокированным ресурсам:

Возможно, что указанные программы используются ребенком для доступа к нелицензионному контенту (заблокированным на территории Российской Федерации торрент-трекерам, сайтам для просмотра и загрузки фильмов и сериалов, программам и играм). Но точно также возможно, что эти программы используются для доступа к теневым (скрытым) частям интернета: интернет-площадкам по продаже запрещенных в гражданском обороте предметов и веществ, запрещенным форумам, группам и сетевым ресурсам.

К таким программам относятся:

TOR-Browser.

Это браузер, предназначенный для анонимного посещения Интернет-страниц. Он не нуждается в установке, а его использование мало чем отличается от обычного браузера.

Вообще обращайте внимание на любые программы, имеющие в своей иконке луковицу – как правило эти программы так или иначе предназначены для обхода блокировок и/или посещения ресурсов в теневой части Интернета.

OpenVPN

Данная программа предназначена, помимо основного своего функционала, для сокрытия реального местоположения пользователя. Эта программа не является единственной, поэтому стоит обращать внимание на любые приложения, содержащие в названии слово «VPN».

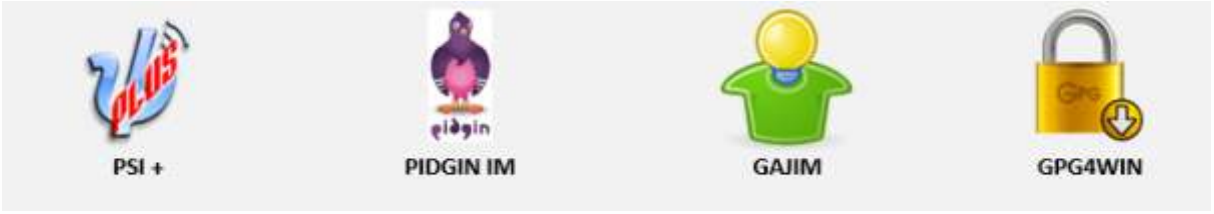
Как правило, эти программы запускаются вместе с запуском компьютера и имеют пользовательский интерфейс.

2. Наличие нестандартных интернет-мессенджеров: PSI+, Miranda и им подобных.

Представленные ниже программы (PSI+, PIDGIN IM, GAJIM) – представители множества мессенджеров, работающих по протоколу XMPP (Jabber). В народе более известны как «жаба».

Пик популярности Jabber уже давно позади. Однако списывать эти мессенджеры со счетов рано. Благодаря своей способности работать на множестве различных платформ, а также совместимостью с огромным количеством других приложений они до сих пор пользуются популярностью в узких кругах. К тому же на сегодняшний день доступно достаточно большое количество полностью анонимных серверов.

Одним из дополнений к «жабе» является возможность внедрения шифрования сообщений, например, с использованием программы GPG4WIN. Этим, в купе с учетными записями на анонимных серверах, активно пользуются злоумышленники, поскольку ключевая информация хранится только на конечных устройствах.



3. Появление второй операционной системы на компьютере

По аналогии с предыдущим пунктом это не является прямым свидетельством – это может произойти просто из технического интереса ребенка.

В качестве примера приведу весьма популярную операционную систему «Kali linux». Эта операционная система предназначена для исследования состояния безопасности компьютерных систем и широко используется профильными специалистами. Она бесплатна для загрузки и использования.

Но она может быть использована и в качестве средства совершения атак. Неконтролируемое использование программ, входящих в ее состав может приводить к тому, что подросток из интереса может пробовать атаковать различные ресурсы, в том числе нести возмездие своим Интернет-обидчикам. Эти действия могут в свою очередь приводить к очень серьезным правовым последствиям как для ребенка, так и для Вас, как его законных представителей.

Однако, мы еще раз скажем о том, что если ребенок проявляет интерес к тому как устроена техника – создайте возможность для безопасного удовлетворения его интереса. Вполне возможно, что эти навыки сильно пригодятся ему в последующем или сыграют важную роль в его профессиональной ориентации.

УГРОЗА № 4. ИНФОРМАЦИЯ, НАНОСЯЩАЯ ПОТЕНЦИАЛЬНЫЙ ВРЕД ПСИХИЧЕСКОМУ ЗДОРОВЬЮ РЕБЕНКА.

Как мы уже отметили в предисловии, и рассказали ранее – Интернет делают люди. И, как известно, люди бывают разные. Всех нас с детства учили - не общаться с плохими ребятами и незнакомцами. И если угроза прямого физического контакта добавляет убедительности этим советам, то с Интернет-общением дела обстоят немного иначе.

Интернет развивается и растет очень быстрыми темпами. Настолько быстрыми, что ни один из существующих технических механизмов не позволяет осуществлять контроль за доступностью контента в режиме реального времени для каждого пользователя в глобальных масштабах. Поэтому, ситуация аналогична ситуации в известной притче: «не нужно устилать ковром весь мир, если можно обуть сандалии».

Несмотря на то, что государством принимаются активные действия по ограничению детей и подростков от информации, которая может принести вред их здоровью и развитию, отличным подспорьем в этом плане станут средства родительского контроля, имеющиеся в практически любой цифровой технике. Как правило, средства родительского контроля по умолчанию настроены в соответствии с принятыми в государстве законодательными ограничениями. В Российской Федерации такие ограничения изложены в Федеральном Законе № 436-ФЗ от 29.12.2010 г. «О защите детей от информации, причиняющей вред их здоровью и развитию»

Рада Сахаренкова

Заведующая сектором по продвижению библиотечно-информационных технологий МУК ЦБС города Краснодара

@glambookworm

Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» четко определяет, какая информация может быть предоставлена ребенку. Запрещена к распространению среди детей любого возраста информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- обосновывающая или оправдывающая допустимость насилия и жестокости, либо побуждающая осуществлять насильственные действия по отношению к людям или животным;
- отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и другим членам семьи;
- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера.
- позволяющую прямо или косвенно установить личность несовершеннолетнего, пострадавшего в результате противоправных действий (бездействия).

Закон определяет информацию, доступ к которой среди детей разных возрастов, ограничен, это:

1. Изображения или описание жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия.
2. Информация, вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, авария или катастрофы и (или) их последствий.
3. Изображение или описание половых отношений между мужчиной и женщиной.
4. Бранные слова и выражения, не относящиеся к нецензурной брани.

Ограничения на предоставление информации по возрастам выглядит следующим образом:

	Разрешено:	Запрещено:
0-6	Эпизодическое ненатуралистическое изображение или описание физического и психического насилия при условии торжества добра над злом и выражения сострадания к жертве и осуждения насилия	Изображение или описание сексуального насилия
6-12*	Кратковременное и ненатуралистическое изображение или описание заболеваний человека и их последствий в форме, не унижающей человеческого достоинства Ненатуралистическое изображение или описание несчастного случая, аварии, катастрофы, ненасильственной смерти Эпизодическое изображение или описание антиобщественных действий и преступлений при условии, что не обосновывается и не оправдывается их допустимость и выражается отрицательное, осуждающее отношение к лицам, их совершающим	Изображение тяжелых заболеваний Демонстрация последствий несчастного случая, аварии, катастрофы, ненасильственной смерти Информация, побуждающая к совершению антиобщественных действий и преступлений
12-16*	Эпизодическое изображение или описание жестокости и насилия без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и отрицательное, осуждающее отношение к жестокости, насилию Эпизодическое упоминание (без демонстрации) наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий при условии, что не обосновывается и не оправдывается допустимость антиобщественных действий, выражается отрицательное, осуждающее отношение к ним и содержится указание на опасность потребления указанных продукции, средств, веществ, изделий Не эксплуатирующие интереса к сексу и не носящие возбуждающего или оскорбительного характера эпизодические ненатуралистические изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.	Изображение тяжелых заболеваний Демонстрация последствий несчастного случая, аварии, катастрофы, ненасильственной смерти Информация, побуждающая к совершению антиобщественных действий и преступлений
16*	Изображение или описание несчастного случая, аварии, катастрофы, заболевания, смерти без натуралистического показа их последствий	Изображение или описание сексуального насилия

Разрешено:	Запрещено:
Изображение или описание жестокости и насилия без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства)	
Информация о наркотических средствах или о психотропных и одурманивающих веществах (без их демонстрации), об опасных последствиях их потребления с демонстрацией таких случаев при условии, что выражается отрицательное или осуждающее отношение к потреблению таких средств или веществ и содержится указание на опасность их потребления	
Отдельные бранные слова и выражения, не относящиеся к нецензурной брани	
Не эксплуатирующие интереса к сексу и не носящие оскорбительного характера изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера	

*Для возрастной категории разрешена/запрещена информация из предыдущего пункта.

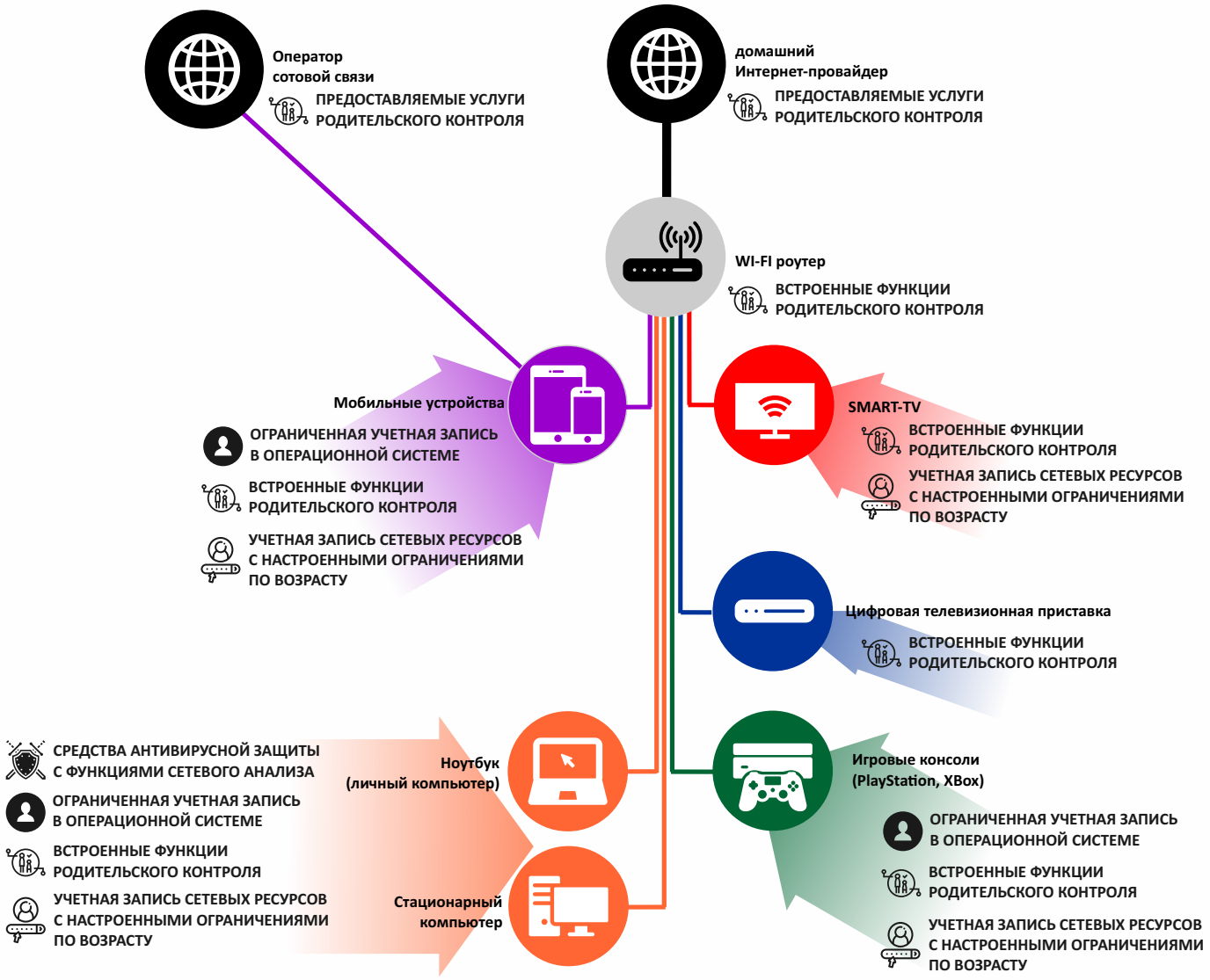
Ниже приведены основные меры для обеспечения функций родительского контроля на домашних устройствах. Все они по своей сути являются схожими. Инструкция по настройке каждого из средств сильно разнится от марки и модели устройства, версии операционной системы и оборудования. Инструкцию для Вашего устройства Вы можете найти:

- в технической документации к Вашему устройству;
- в электронном виде на сайте производителя устройства;
- в инструкциях от энтузиастов на форумах и других сайтах;
- в пошаговых инструкциях на YouTube.

Внедрение любого средства родительского контроля всегда проходит в два этапа:

1. Настройка ограничений.
2. Защита настроенных ограничений от изменения и обхода с помощью пароля.

Это значит, что вам придется запомнить еще несколько паролей. Как их не забыть и не потерять смотрите в пункте про парольные менеджеры.



Предоставляемые провайдером (оператором) функций родительского контроля.

Предоставление услуги родительского контроля заключается в ограничении доступа к сетевым ресурсам на стороне провайдера. Это значит, что заданные ресурсы будут недоступны с любого устройства, подключенного к Интернету с использованием данного канала связи. Некоторые провайдеры предлагают не прямое ограничение доступа к ресурсам, а подписку с ежемесячной оплатой на антивирус с функциями родительского контроля. Уточнить о наличии этой опции можно в офисе Интернет-провайдера или по телефонам горячей линии.

Операторы сотовой связи гораздо чаще имеют отдельную тарифную опцию «родительский контроль» и позволяют заблокировать доступ к сайтам с нежелательной информацией на уровне провайдера. Это значит, что провайдер не будет показывать информацию, не предназначенную для детей. Более того, у большинства операторов сотовой связи при оказании услуги родительского контроля имеется возможность определять местоположение ребенка в любое время. Подключить тарифную опцию «родительский контроль» можно через мобильное приложение вашего оператора (через которое, к слову, очень удобно контролировать расходы вашего ребенка на связь и Интернет), в офисе или по телефону горячей линии.

Встроенные функции родительского контроля.

Встроенные функции родительского контроля на сегодняшний день имеются практически во всех устройствах, которыми потенциально могут пользоваться дети. Использование встроенных средств (при их наличии) практически полностью решает проблему ограничения доступа к нежелательной информации.

Учетная запись сетевых ресурсов с настроенными ограничениями по возрасту.

Под учетной записью с ограничениями по возрасту мы подразумеваем включение функций родительского контроля на используемых Интернет-сервисах. Эта функция также может называться «Функция безопасного просмотра», «Фильтрация нежелательного контента», «Сокрытие нежелательных материалов». Эти функции целесообразно включать на следующих ресурсах:

· Онлайн видеохостинги и стриминговые сервисы (YouTube, RuTube, Vimeo, Twitch)
· Социальные сети (Вконтакте, Одноклассники, Facebook, Instagram)
· Онлайн-кинотеатры и фильмотеки
· Игровые сервисы (Steam, Origin, PlayStation Network, Xbox Live, облачные игровые сервисы).

Ограниченная учетная запись в операционной системе.

Под ограниченной учетной записью мы подразумеваем учетную запись, лишенную прав администратора. Практически в любой операционной системе учетная запись без прав администратора означает, что присутствуют ограничения:

· на установку программ и приложений;

· на изменение системных настроек: подключения к беспроводным сетям, создании других пользователей с административными правами

· на изменение параметров родительского контроля: изменения расписания использования устройств, отключения средств антивирусной и сетевой защиты.

· на приобретение с использованием привязанных к устройству платежных систем (GooglePay, ApplePay, Qiwi и др.) программ, дополнительного контента или платных подписок.

Найти инструкцию о том, как сделать ограниченную учетную запись в любой операционной системе не составляет труда с помощью вашей любимой поисковой системы.

Средства антивирусной защиты с функциями сетевого анализа.

Как уже ранее было отмечено, в большинстве современных антивирусов существуют встроенные функции родительского контроля. Как правило, этот пункт настроек имеет именно такое название.

Антивирус осуществляет анализ посещаемой страницы и, если обнаруживаются признаки запрещенной информации, то просто выдает в браузере сообщение о том, что посещение данной страницы запрещено средствами родительского контроля. Можно запретить посещение следующих категорий интернет-ресурсов:

- Игровые сервисы и сайты игровой тематики
- Видеосервисы и видеохостинги
- Сайты, содержащие информацию эротического и порнографического содержания.
- Сайты и веб-страницы, содержащие нецензурную брань и оскорбительные высказывания.
- Сайты и веб-страницы, содержащие информацию экстремистского характера.

Дополнительное программное обеспечение для обеспечения функций родительского контроля

К такому программному обеспечению относятся как дополнительные программы, устанавливаемые на используемые ребенком устройства, так и настройки функций родительского контроля в отдельных приложениях. Например, такие функции присутствуют в браузерах (для ПК и мобильных устройств).

Функционал таких программ является достаточно разнообразным и позволяет вести мониторинг в любом режиме – от, что называется, «параноидального» при котором фиксируются абсолютно все действия пользователя, до «легкого» режима, при котором фиксируется общая статистика использования устройства без детального анализа информации.

Как правило, такие программы состоят из двух частей. Одна часть ставится на персональное устройство ребенка (телефон, планшет или компьютер), а вторая на персональное устройство родителя. Часть программы, которая ставится на устройство ребенка осуществляет блокировку сетевых соединений, использования программ и некоторых компонентов операционной системы (например, приложений для осуществления настроек), а другая часть предоставляет доступ к статистике использования устройства. Как правило, такие программы позволяют:

- Получать снимки экрана в момент использования устройства
- Контроль за временем использования отдельных приложений и устройства в целом
- Перечень посещенных интернет-страниц с указанием категорий

- Доступ к личным сообщениям в мессенджерах и социальных сетях

Преимущества	***Недостатки***
· *Возможность детальной настройки перечня контролируемых событий.* · *Низкая вероятность обхода ребенком при наличии технических навыков на уровне «выше среднего»* · *Возможность наглядно видеть историю использования устройства (на что кон кретно тратится время за компьютером)* · *Автоматическое обновление средств контроля вслед за обновлением операционной системы, программ и сетевых сервисов.*	· *Большинство таких программ работает по подписке (с ежемесячными платежами);* · *Большой объем собираемых да нных может приводить к невозможности их анализа;* · *Утеря пароля доступа к сервису может привести к невозможности дальнейшего использования устройства* · *Сложность первоначальной установки и настройки*

1. Wi-Fi роутер.

Обязательный атрибут современного жилища. Устройство, находящееся на рубеже Вашего дома и Интернета. Родительский контроль на современных маршрутизаторах позволяет достаточно гибко настраивать правила доступа определенных устройств к сети. Например, в зависимости от устройства:

- Можно полностью выключить Интернет для определенного компьютера или устройства: как на постоянной основе, так и по расписанию.
- Можно заблокировать отдельный сетевой ресурс: сайт, сервис или страничку.
- Можно разрешить посещение сайтов из только разрешенного списка

Если на Вашем маршрутизаторе данная функция отсутствует, попробуйте обновить прошивку устройства. Инструкции и актуальные файлы прошивки находятся на сайте производителя устройства.

2. Smart-TV или обычный телевизор + цифровая телеприставка

Цифровые приставки бывают двух видов:

1. Приставки, поставляемые интернет-провайдером в рамках оказания услуги «Цифровое телевидение».

В этом случае для ограничения доступа ребенка к потенциально неприемлемому видеоконтенту достаточно установить встроенные настройки родительского контроля. Цифровое телевидение при передаче видеконтента имеет встроенную цифровую маркировку. Это значит, что если ограничения установлены на рейтинге «16+», то приставка автоматически скроет изображение и попросит пароль, если в трансляции появится передача, помеченная рейтингом выше установленного.

2. Приставки, расширяющие функционал обычного телевизора до «умного».

С этими устройствами все несколько сложнее. По своей сути данные устройства ничем не отличаются от обычных устройств на Android, а значит, что для работы ограничений на них необходимо настраивать все функции родительского контроля точно так же, как это делается на мобильном устройстве. Как настроить функции родительского контроля на таких устройствах смотрите подробнее в пункте «Мобильные устройства».

Тем не менее при использовании SMART-TV и приставок, расширяющих функционал обычного телевизора до умного можно воспользоваться:

- Встроенными функциями родительского контроля.
- В результате настройки ограничений на используемых учетных записях.

3. Мобильные устройства (телефоны, планшеты и другая носимая электроника)

Настройка функций родительского контроля на мобильном устройстве зависит от марки и модели самого устройства. Для устройств под управлением операционной системы «Android» характерно изобилие различных версий, что делает эту рекомендацию строго индивидуальной.

С помощью средств родительского контроля на мобильном устройстве можно осуществлять:

- Запрет на открытие других программ и приложений. В этом случае будет зафиксировано только то приложение, которое зафиксировано родителем.
- Запрет на покупки и скачивание приложений, помеченных возрастными ограничениями.
- Ограничение использования голосовых помощников – запрет на поиск информации в Интернете и запрет на отображение ненормативной лексики.
- Блокировка нежелательного содержимого на Интернет-страницах.
- Ограничение использования устройства по времени
- Запрет на изменение системных настроек, в том числе изменение паролей пользователей мобильного устройства

4. Игровые консоли (PlayStation, XBOX, Wii)

Из наших наблюдений – самое «темное» (неизвестное) устройство для большинства родителей.

Фактически, на сегодняшний день большинство консолей предназначены не только для игр, но и являются универсальными мультимедийными центрами. С помощью игровых консолей можно слушать музыку, просматривать фильмы, пользоваться видеосервисами (YouTube, например), использовать социальные сети и иные интернет-ресурсы. Поэтому для наиболее полного ограничения функционала рекомендуем использовать не только встроенные в игровые консоли функции родительского контроля, но и использовать возрастные ограничения в учетных записях сетевых ресурсов.

УГРОЗА № 5. СКЛОНЕНИЕ К ДЕЙСТВИЯМ СЕКСУАЛЬНОГО ХАРАКТЕРА.

Сайты знакомств разделяют пальму первенства по количеству среднего времени удержания пользователя с социальными сетями. Причин этому множество:

Во-первых сайты знакомств имеют основным своим предназначением дать пользователю возможность выйти за рамки своего привычного социального круга. И ситуация осложняется тем, что на сайтах знакомств большинство пользователей заведомо настроены на контакт с незнакомцами. В отличии от большинства пользователей социальных сетей, использующих их для общения внутри своего социального окружения.

Во-вторых, как уже было отмечено в предисловии, дети и подростки могут пользоваться сайтами и приложениями для знакомств в силу естественного любопытства. Зачастую это, а также наличие ограничений на сайтах знакомств приводит к тому, что дети сознательно завышают свой возраст в анкетах;

В-третьих для некоторых подростков факт наличия «амурных» отношений является косвенным свидетельством «взрослости», поэтому добывать эти отношения они могут «любой ценой».

Что может пойти не так?

Как правило сайты и приложения для знакомств являются лишь «точкой входа». Практически всегда, для удобства переписка перемещается в мессенджеры и социальные сети. Говоря иначе – приобретает большую приватность. Большая приватность, в свою очередь, может оказывать непосредственное влияние на характер и градус отправляемых сообщений. И, как у любого явления, у такого приватного общения тоже имеются крайние формы.

Секстинг – обмен текстами и фотографиями интимного характера.

Название этого явления в русском языке еще не является общеупотребительным. Свою этимологию слово «секстинг» берет от смешения двух английских слов («sex» и «texting»).

Некоторые подростки отмечают, что откровенную переписку они осуществляли не только с теми, с кем они знакомы, но и с теми, с кем они хотели бы встречаться. Самым пугающим является также тот факт, что подростки допускают «секстинг» с людьми, с которыми они знакомы только через Интернет.

Чем так опасен секстинг?

1. Человек, получивший тексты и фотографии интимного характера может использовать их для осуществления травли, преследования и шантажа. Причем, не только преднамеренно. Если для одного из адресатов переписка не является столь интимной, то он вполне может показать ее своим друзьям и знакомым, в том числе и в Интернете;

•

2. Даже если обе стороны общения сохраняют интимную переписку в тайне, это абсолютно не значит, что доступ к ней или ее отдельным материалам (фото или видео) не могут получить злоумышленники. Например, получив доступ к облачным хранилищам, практически всегда находящихся во включенном состоянии на смартфонах и планшетах; или к страницам в социальных сетях, на которых содержатся отправленные медиафайлы.

3. Утеря не защищенного паролем и шифрованием устройства в общественном месте также может сыграть злую шутку с его обладателем;

4. Не стоит забывать и о том, что ни одна техническая система может дать 100% гарантию приватности. Особенно, если вы пользуетесь публичными точками доступа в торговых центрах, кафе, барах и ресторанах.

В некоторых случаях о фактах утечки таких фотографий и видео узнается спустя годы. Интимные фотографии, кочующие по Сети могут стать серьезной проблемой уже во взрослой жизни: в общении со студенческим коллективом, с коллегами и руководством. Уже известны случаи, когда результаты «подростковых забав» становились причиной разрывов отношений и разводов в молодых семьях спустя годы.

Более того, помимо добровольного обмена таким контентом нашими специалистами неоднократно выявлялись случаи обмена интимных фотографий и видео, снятых несовершеннолетними за небольшое денежное вознаграждение. На контакт с несовершеннолетними «покупатели» выходят через сайты и сервисы знакомств, а также тематические группы в мессенджерах и социальных сетях. Как правило, дети не являются инициаторами знакомства в таком контексте, а просто ищут новых друзей и знакомств.

Что делать, чтобы не попасть в неприятную ситуацию из-за утечки данных?

1. Перво-наперво, не стоит делать и, тем более, хранить фотографий, публикация которых может нанести ущерб репутации. Совсем.

2. Расскажите ребенку, что не стоит отправлять свои фотографии и видео даже в ответ на долгие уговоры со стороны незнакомца, а также в качестве ответа на фото или видео с аналогичным содержимым;

3. Расскажите также, что недопустимо привлечение внимания парня или девушки за счет интимных фотографий. Если избранник негативно реагирует на отказ, то это повод задуматься о его истинных мотивах.

4. Расскажите подростку, что публикация откровенных фото и видео ради завоевания популярности – дешевый трюк. В конечном итоге все может привести к ранее озвученным последствиям (травле, моббингу, шантажу и т.д.).

Что делать, если фотографии или переписка уже опубликованы?

Николай Дорин

Руководитель компании по расследованию киберпреступлений «Delta Forensics»

@nikolay.dorin

Практика показывает, что с такими ситуациями сталкиваются не только дети и подростки. Одной из распространенных причин публикации порочащих честь и достоинство фото и видео являются «вечные» мотивы: ревность, зависть, нечестная конкуренция.

1. Публикация Ваших фото – не конец света. Важно это понимать, особенно если пострадавшим лицом является ребенок или подросток. Здесь нет Вашей или его вины. Даже взрослым людям в таких ситуациях требуется помощь и поддержка.

2. Не так уж и важно где были опубликованы фотографии, видео или переписка – в социальных сетях или на тематических ресурсах интимной направленности. При своевременном и грамотном обращении администрация ресурсов моментально реагирует удалением информации. Особенно, если на изображениях или видео запечатлен несовершеннолетний. Наказание за тиражирование и распространение изображений несовершеннолетних без их ведома сурова во всех юрисдикциях.

3. «Не тушите пожар бензином». Если фотографии распространяются в социальных сетях, не стоит писать с пострадавшей странички в комментариях и отзывах. Не давайте агрессорам шансов устроить охоту.

Для того, чтобы подготовить обращение на ресурс (самостоятельно или с помощью юриста), либо подать заявление в правоохранительные органы в случае отказа администрации от удаления информации необходимо зафиксировать наличие нежелательных материалов на странице способом, аналогичным закреплению доказательств при травле и буллинге: сделать снимок страницы, содержащий нежелательные материалы в присутствии свидетелей, лучше – нотариуса. Снимок должен содержать: полный сетевой адрес страницы, информацию о пользователе, разместившем фотографию (если такая информация имеется).

Евгения Глебова

Когнитивный психолог. Клинический психолог. Преподаватель Института развития образования Краснодарского края. Врач высшей категории.

@evgeniya.psychologist

1. Если вы боитесь столкнуться с такой проблемой, но фактов, подтверждающих такие случаи нет, то вам необходимо провести анализ собственных мыслей по поводу вашего ребенка – почему вы ему не доверяете?

2. Для профилактики таких случаев необходимо давать информацию о сексуальной жизни человека дозированно, в зависимости от возраста ребенка. Ребенок должен знать откуда берутся дети и как именно человек размножается. Какое поведение является интимным, а какое поведение является вызывающим и недопустимым. Вы должны своевременно информировать ребенка о норме сексуального поведения и патологии.

3. Вызвать интерес ребенка к информации о сексуальной жизни могут возрастные изменения. Поэтому родитель должен быть открыт к беседам на эти темы. Если вы сами не готовы к таким беседам, необходимо обратиться к психологу за консультацией о рамках таких бесед в зависимости от возраста ребенка.

4. Если у вас есть веские основания считать, что ваш ребенок состоит в группе или контакте с человеком (или группой лиц) склоняющих его к таким действиям, вы должны срочно обратится за психологической помощью к психологу (и ребенку и родителям!) и сообщить в инспекцию по делам несовершеннолетних о таком факте для проведения защиты ребенка.

УГРОЗА № 6. ЛУДОМАНИЯ И ЗАВИСИМОСТЬ ОТ ВИДЕОИГР

Священный Грааль для споров экспертов и представителей общественности. На сегодняшний день однозначной оценки специалистами по поводу пользы или вреда, наносимого видеоиграми не существует. Справедливости ради, стоит заметить что она и невозможна, поскольку если

Однако, это не отменяет того факта, что видеоигры уже давно органично вписались с современную социокультурную картину. Ряд компьютерных игр уже несколько лет как являются полноценными соревновательными дисциплинами (в классическом понимании понятия «соревновательная дисциплина»), по которым проводятся локальные и международные соревнования.

Игровая зависимость является всего лишь частным случаем зависимости. Под зависимостью понимается навязчивая потребность, подвигающая человека к определенной деятельности.

Евгения Глебова

Когнитивный психолог. Клинический психолог. Преподаватель Института развития образования Краснодарского края. Врач высшей категории.

@evgeniya.psychologist

Формирование зависимости у ребенка может протекать достаточно долго. Зависимое поведение может начать проявляться с «безобидных» на взгляд родителя вещей:

1. Страсть к просмотру определенных мультфильмов и неадекватное поведение, при невозможности его посмотреть.

2. Пристрастие к некоторым продуктам (сладостям и прочее) с формированием неадекватного пищевого поведения при отсутствии этого продукта в доме – отказ от еды, агрессивное поведение, плаксивость.

3. Слишком выраженная привязанность к определенным игрушкам или предметам.

Если вы заметили такое поведение ребенка, то в будущем есть вероятность формирования зависимости от более серьезных вещей, которые могут угрожать благополучию ребенка. Чаще всего причинами формирования зависимости ребенка являются:

· Недостаточная или неправильно проявляемая забота о ребенке.
· Непринятие его как личности.
· Негативная оценка результатов поведения ребенка и его личностных качеств.
· Косвенное отвержение ребенка.
· Эмоциональное отвержение ребенка
· Недоверие к способностям и действиям ребенка.
· Обесценивание ребенка, как личности.
· Негативная обстановка в семье, конфликты между членами семьи.
· Большая занятость родителей

Для избежания формирования зависимости у ребенка, необходимо поддерживать с ним добрые, искренние взаимоотношения. Принимать его характер и темперамент «таким какой есть». Знакомить с законами взаимодействия с обществом в позитивном ключе. Знакомить ребенка с моральными и социальными нормами поведения. Научить ребенка правильно ставить цели и перспективы своей деятельности, научить его развивать творческие способности, формировать свой рабочий день и досуг.

Еще одним видом зависимости является классическая зависимость от азартных игр (лудомания). Несмотря на то, что игровые автоматы и вывески игорных заведений давно покинули улицы населенных пунктов, идея «сорвать джек-пот» за минимальную ставку до сих пор является актуальной.

И связано это вот с чем: мы помним что Интернет делают люди. Желание обозначить свою индивидуальность в реальном мире испокон веков считается естественным. Так почему же тогда в мире «виртуальном», являющимся мультимедийным отображением нашей повседневной жизни что-то должно быть иначе?

Обозначить свою индивидуальность в социальных сетях и сетевых играх позволяет дополнительный контент, приобретаемый пользователем отдельно. Если акцентировать внимание на детях и подростках, то в качестве примера целесообразно привести самый распространенный способ виртуальной индивидуализации – с помощью внутриигровых предметов.

Под фразой «внутриигровой предмет» понимается цифровой объект, предназначенный для использования внутри какой-либо компьютерной игры. К таким предметам относятся:

· Внутриигровые валюты;
· Виртуальные ресурсы;
· визуальные оболочки для внутриигровых предметов (скины) – виртуального оружия, техники или персонажей;

Максим Гострый

Ведущий специалист ООО «АТЭК-С»

center_ib@kubstu.ru

Как уже было отмечено ранее, ребята подросткового возраста в своей массе не играют в традиционных онлайн-казино (несмотря на огромное количество Интернет-рекламы). В настоящее время гораздо более популярны сервисы по розыгрышу внутриигровых предметов. Данные сервисы эксплуатируют тягу подростка к обладанию дорогими и редкими экземплярами. Ценник на некоторые предметы доходит до сотни тысяч (!) рублей, поэтому возможность выиграть такие вещи за небольшую (по сравнению с призом) ставку выглядит весьма заманчиво.

Это работает так: пользователь вносит на свой счет реальные деньги, открывает за фиксированную стоимость кейс (коробку с внутриигровыми предметами), из которого ему случайным выпадает один или несколько предметов, который может стоить как больше суммы «ставки», так и меньше. Ничего не напоминает? Фактически данный аттракцион представляет собой разновидность беспроигрышной «рулетки», а значит де-факто подразумевает появление азарта. Однако в отличии от реального казино в данной рулетке призом является внутриигровой объект, а не деньги.

1. Объясните ребенку что такое азартные игры. Расскажите также, что казино всегда находится в выигрыше, поскольку вероятность выигрыша составляет десятые доли процента и на тысячу человек может быть всего несколько счастливчиков;

2. Расскажите также, что все это может быть простым обманом. Механизм определения победителя неизвестен никому кроме создателей сервиса. Более того, самого желанного «дорогого» предмета может вообще не существовать, как и алгоритма его выпадения;

3. Пойдите ребенку на уступки. Попробуйте вместе с ним «сыграть» на небольшую сумму на таком сервисе. С высокой долей вероятности к концу игровой сессии Ваш денежный счёт будет опустошен, а коллекция игровых предметов пополнится не самыми ценными экземплярами (сильно дешевле суммы итоговой ставки).

Не мне рассуждать на тему того, насколько полезны или вредны для детей и подростков компьютерные игры. Скажу лишь, что согласно международному и отечественному законодательству любой цифровой контент, в том числе и игры имеют определяемый специальными комиссиями возрастные рейтинги.

Steam (1) 

Origin (2) 

Делается это потому, что некоторые игры могут содержать контент для взрослых: сцены физического насилия, кровавые сцены, сцены сексуального характера и т.д.

Некоторые из онлайн-игр бесплатны для загрузки, некоторые необходимо приобретать. Приобретаются эти игры, как правило с помощью сервисов цифровой дистрибьюции.

Самые популярные из этих сервисов: Steam (1) и Origin (2). При покупке с использованием этих сервисов пользователь, как правило, предупреждается о возрастном рейтинге приобретаемого контента.

Для того чтобы контролировать, как и во что играют Ваши дети:

1.Создайте для ребенка на устройстве отдельную учетную запись в операционной системе с ограниченными правами. Так вы будете полностью контролировать какие программы устанавливает ребенок.

2.Если ребенок просит приобрести игру с помощью сервиса цифровой дистрибуции, то создайте учетную запись для себя и приобретайте игру именно на нее. При этом ребенок должен создать или уже иметь свою учетную запись. Согласно правилам сервисов Вы сами сможете настраивать функции семейного просмотра – ограничивать доступ к определенным играм, в том числе по расписанию или по времени использования. Инструкции по настройке семейных ограничений можно найти на сайтах этих сервисов и на популярных видеохостингах.

Кроме того, в указанных сервисах отображается общее время, проведенное в игре и дата приобретения. Путем несложных арифметических вычислений можно выяснить сколько времени ежедневно в игре проводит ребенок. И сделать выводы.

В настоящий момент некоторой популярностью пользуются также облачные игровые сервисы. Суть их работы заключается в следующем: пользователь приобретает возможность играть на оборудовании, установленном у провайдера посредством удаленного доступа. Оплата услуги осуществляется согласно установленному тарифному плану – в виде абонентского платежа или по поминутной тарификации. В этом случае на компьютере ребенка вы не увидите ни иконок популярных игр, ни установленных приложений сервисов цифровой дистрибуции.

Большинство таких сервисов на основании размещенных ими публичных правил использования сервиса не несут никакой ответственности за нарушение установленных возрастных ограничений и перекладывают её на пользователя или его законных представителей (родителей или опекунов).

ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ В ИНТЕРНЕТЕ

Мария Викторовна Бердник

Юрисконсульт ООО «Дельта Форензикс»
юрист, специалист в области правового обеспечения информационной безопасности

center_ib@kubstu.ru

У большинства людей понятия «преступление», «преступник» ассоциируются, в первую очередь, с хищением имущества либо незаконными действиями с наркотиками, а также с насилием. Однако Уголовный кодекс содержит гораздо больший перечень деяний, которые признаются преступлениями и влекут ответственность. Для того чтобы совершить некоторые из них, вовсе не обязательно иметь изначально криминальные наклонности, и более того, их можно совершить путем использования Интернета.

В качестве примеров таких преступлений можно привести:

ст. 128.1 УК РФ	клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию
ст. 146 УК РФ	Нарушение авторских и смежных прав
Ст 159 УК РФ	Мошенничество
ст. 171.2 УК РФ	незаконные организация и проведение азартных игр, в том числе с использованием сети «Интернет»
ст. 187 УК РФ	изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов
ст. 205.2 УК РФ	публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма (публичное заявление о признании идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании)
Ст. 228.1 УК РФ	сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации либо электронных или информационно -телекоммуникационных сетей
ст. 242 УК РФ	незаконное изготовление и оборот (в том числе распространение, публичная демонстрация или рекламирование) порнографических материалов
ст. 242.1 УК РФ	изготовление и оборот материалов или предметов с порнографическ ими изображениями несовершеннолетних
ст. 272 УК РФ	неправомерный доступ к компьютерной информации
ст. 273 УК РФ	создание, использование и распространение вредоносных компьютерных программ
ст. 280 УК РФ	публичные призывы к осуществлению экстремистской д еятельности
ст. 280.1 УК РФ	публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации
ст. 282 УК РФ	возбуждение ненависти или вражды, а равно унижение достоинства человека либо группы лиц по пр изнакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой -либо социальной группе, совершенные публично или с использованием средств массовой информации
ст. 354 УК РФ	публичные призывы к развязыванию агре ссивной войны
ст. 354.1 УК РФ	реабилитация нацизма, то есть отрицание фактов, установленных приговором Международного военного трибунала для суда и наказания главных военных преступников европейских стран оси, одобрение преступлений, установленных указанным приговором, а равно распространение заведомо ложных сведений о деятельности СССР в годы Второй мировой войны, совершенные публично

Таким образом, даже высказывание на форуме или в социальной сети, обращенное к неопределенному кругу лиц, может быть расценено как преступление, если содержит в себе запрещенные законом призывы либо суждения.

Более того, некоторые статьи уголовного закона предусматривают более суровую ответственность именно за те преступления, которые совершены при помощи информационно-телекоммуникационных сетей, поскольку в Интернете круг лиц, которые могут прочитать либо посмотреть то или иное информационное сообщение, гораздо шире, чем мог быть при простом публичном выступлении, а, следовательно, общественная опасность таких действий более серьезная.

Административная ответственность:

п. 1 ст. 6.13 КоАП РФ	пропаганда либо незаконная реклама наркотических средств, психотропных веществ
ст. 7.12 КоАП РФ	Нарушение авторских и смежных прав
ст. 13.11. КоАП РФ	Нарушение законодательства Российской Федерации в области персональных данных
ст. 13.35 КоАП РФ	Распространение владельцем аудиовизуального сервиса незарегистри рованных средств массовой информации
ст. 13.36. КоАП РФ	Нарушение владельцем аудиовизуального сервиса установленного порядка распространения среди детей информации, причиняющей вред их здоровью и (или) развитию
ст. 13.14. КоАП РФ	Разглашение информации с ограниченным доступом
ст. 13.37 КоАП РФ	Распространение владельцем аудиовизуального сервиса информации, содержащей публичные призывы к осуществлению террористической деятельности, материалов, публично оправдывающих терроризм, или других материалов, призывающих к осуществлению экстремис тской деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности

Гражданско-правовая ответственность

ст. 151 п. 1 ст. 152 ГК РФ	Распространение сведений, порочащих честь, достоинство или деловую репутацию
ст. 1082 , 1302ГК РФ	Нарушение авторских и смежных прав
ст. 1252 ГК РФ	Нарушение исключительных прав на произведение

А ЧТО ЕСЛИ?

«Я слишком стар для этих новомодных штучек».

Что ж, как бы это страшно не звучало, но в этом случае Интернет-пространство все сделает за Вас.

«Я умею пользоваться техникой на уровне пользователя, но не смогу это сам настроить».

Во-первых, в Интернете достаточное количество пошаговых статей и справочных материалов по настройке родительского контроля для любых версий устройств, операционных систем и сервисов.

Во-вторых, на сегодняшний день имеется достаточно широкий выбор стороннего программного обеспечения, позволяющего настроить все в два щелчка мыши. Мы советуем использовать программы от производителей антивирусных продуктов, поскольку именно эти решения соответствуют требованиям Законодательства. К тому же, производители антивирусов всегда держат руку на пульсе и регулярно обновляют базы мошеннических и запрещенных ресурсов. В противном случае Вы можете натолкнуться на других мошенников, поделки которых ничем не отличаются от обычных троянских программ.

В-третьих на рынке представлено множество сервисных компаний, которые помогут Вам в этом деле. При этом, это не стоит сумасшедших денег. Для того, чтобы создать разумных пределов «песочницу» не нужно даже покупать какое-либо программное обеспечение: достаточно использовать встроенные в уже имеющееся программное обеспечение механизмы. Просто посмотрите на список подстерегающих Вашего ребенка опасностей и сравните его со стоимостью предлагаемых услуг. Не так уже и дорого, правда?

«А что если ребенок воспримет это как акт тотального недоверия?»

Если не объяснить ребенку что это делается в целях его и Вашей безопасности, то это и будет так воспринято. Будьте уверены.

Основным возражением может стать тот факт, что у других детей подобного рода ограничения отсутствуют. Расскажите, что это не значит, что Вы не доверяете своему ребенку. Апеллируйте к тому, что прекрасно понимаете, как работает Интернет и стараетесь обеспечить его и Вашу безопасность. Пообещайте ребёнку, что как только вы увидите, что он готов к выходу «в открытое плавание», Вы тут же отключите все средства родительского контроля. Пусть ребенок докажет делом, что научился использовать Интернет для творчества и учебы, а не только для развлечений.

«Можно ли следить абсолютно за всем, что делает ребенок в сети?»

Можно, но...

Чисто технически это не составляет абсолютно никакого труда. Более того, как законный представитель ребенка Вы имеете на это полное право. Однако, как Вы думаете, сможет ли ребенок комфортно чувствовать себя в Сети, если он знает, что «большой брат» следит за каждым его действием? Согласитесь, что неприятно когда кто-то или что-то постоянно стоит над душой. Скорее всего в этому случае ребенок просто найдет способы воспользоваться другим устройством и другими учетными записями, о которых вы просто не будете знать.

«ОК. А если оставить механизмы контроля в тайне?»

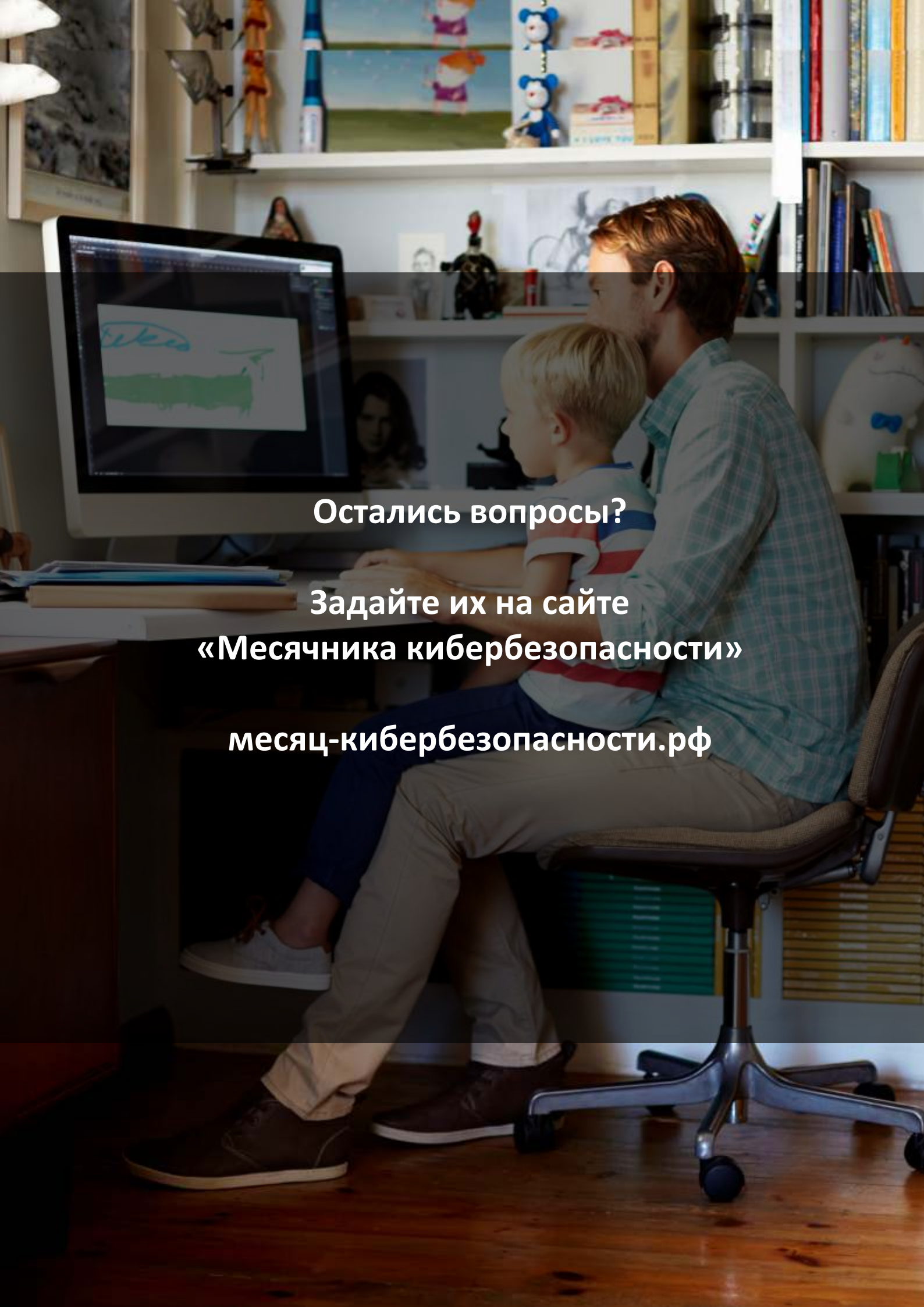
Поверьте нашему опыту, в таких ситуациях всё тайное рано или поздно становится явным. Например, если ребенок достаточно подкован технически или Вы попробуете предотвратить ситуацию, о которой кроме ребенка неизвестно никому. И в этой ситуации это может привести к еще более серьезному конфликту.

«Какие мероприятия мы можем посетить вместе с ребенком, чтобы узнать больше об информационной бнзопасности?»

Библиотеки готовы помочь. У нас вы найдете:

- книги и журналы, бесплатно и без регистрации;
- школы компьютерной грамотности для детей;
- мастер-классы от психологов и экспертов по информационной безопасности;
- детские летние площадки для чтения, игр и творчества.

Все еще думаете, что библиотеки - пыльные книгохранилища? Самое время проверить!



Остались вопросы?

Задайте их на сайте
«Месячника кибербезопасности»

месяц-кибербезопасности.рф