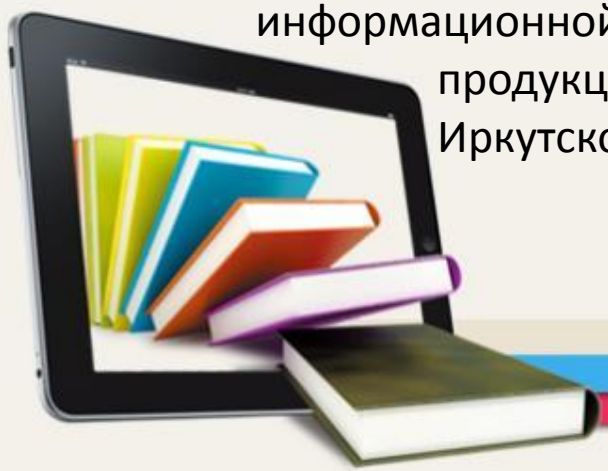
Информационная безопасность детей в сети Интернет

Нормативные акты в сфере информационной безопасности детей

- Конвенция ООН о правах ребенка;
- Федеральный закон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон Российской Федерации от 29 декабря 2012г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Указ Президента РФ от 01.06.2012 г. №761 «О национальной стратегии действий в интересах детей на 2012-2017 годы»;
- Закон Иркутской области «Об утверждении Программы социально-экономического развития Иркутской области на 2011 – 2015 годы» от 31 декабря 2010 года № 143-ОЗ;
- Проект Долгосрочной целевой программы Иркутской области «Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции в Иркутской области на 2013-2015 годы»



Основные Интернет-риски

Контентные риски

Потребитель-ские риски

Коммуника-ционные риски

Электронные риски

КОНТЕНТНЫЕ РИСКИ

материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

КОНТЕНТ

ПРОТИВОЗАКОННЫЙ

НЕЭТИЧНЫЙ

ВРЕДОНОСНЫЙ

КАК ПРЕДУПРЕДИТЬ КОНТЕНТНЫЕ РИСКИ

1. Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой.
2. Создайте на компьютере несколько учетных записей, когда каждый пользователь сможет входить в систему независимо и иметь собственный уникальный профиль. Регулярно следите за активностью вашего ребенка в сети.
3. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе с какой информацией он сталкивается в сети.
4. Объясните детям, что далеко не все, что они могут прочесть или увидеть в интернете – правда.
5. Помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать.

КОММУНИКАЦИОННЫЕ РИСКИ

связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других.

Кибер-преследование (кибербуллинг)

Незаконный контакт

- Домогательство
- Груминг
- Знакомства в сети и встречи с интернет-знакомыми

КИБЕРБУЛЛИНГ (КИБЕРПРЕСЛЕДОВАНИЕ)

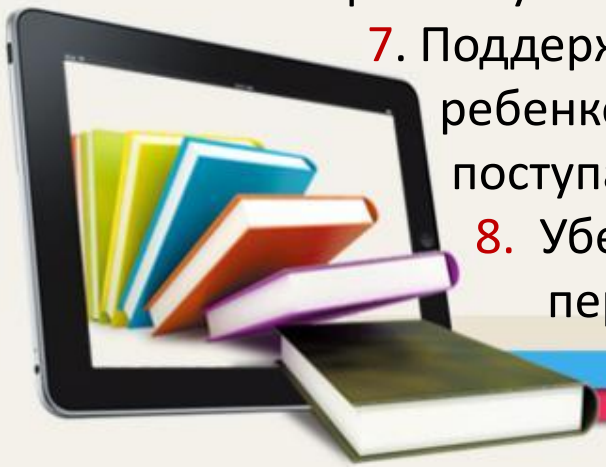
Буллинг – (англ. bullying, от bully – драчун, задира, грубиян, насильник) запугивание, унижение, травля, физический или психологический террор, направленные на то, чтобы вызвать у другого пользователя страх и тем самым подчинить его себе.

Кибербуллинг - буллинг, осуществляемый в виртуальной среде с помощью интернета и мобильного телефона.

Основная площадка для кибербуллинга - **социальные сети**

КАК ПРЕДОТВРАТИТЬ КИБЕРБУЛЛИНГ

1. Объясните детям, что при общении в интернете они должны быть дружелюбными с другими пользователями.
2. Научите детей правильно реагировать на обидные слова или действия других пользователей.
3. Обратите внимание на психологические особенности вашего ребенка.
4. Если кто-то из друзей или знакомых вашего ребенка подвергается буллингу или кибербуллингу – сообщите об этом классному руководителю или школьному психологу.
5. Объясните детям, что личная информация, которую они выкладывают в интернете может быть использована агрессорами против них.
6. Помогите ребенку найти выход из ситуации.
7. Поддерживайте доверительные отношения с вашим ребенком, чтобы вовремя заметить, если в его адрес начнет поступать агрессия или угрозы.
8. Убедитесь, что оскорбления (буллинг) из сети не перешли в реальную жизнь.



НЕЗАКОННЫЙ КОНТАКТ

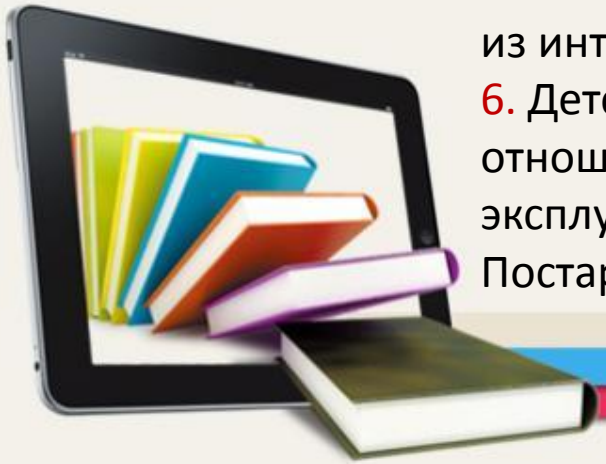
общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для разглашения ребенком личной информации о себе и своей семье, с целью оскорбления, запугивания и домогательства, сексуальной эксплуатации ребенка.

ГРУМИНГ

- установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации.

КАК ПРЕДОТВРАТИТЬ ВСТРЕЧИ С НЕЗНАКОМЦАМИ И ГРУМИНГ

1. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе, с кем ребенок общается в сети.
2. Объясните ребенку, что нельзя разглашать в интернете информацию личного характера, а также пересылать виртуальным знакомым свои фотографии или видео.
3. Объясните ребенку, что нельзя ставить на аватарку или размещать в сети фотографии, по которым можно судить о материальном благополучии семьи, а также нехорошо ставить на аватарку фотографии других людей без их разрешения.
4. Объясните ребенку, что при общении на ресурсах, требующих регистрации лучше не использовать реальное имя.



5. Объясните ребенку опасность встречи с незнакомыми людьми из интернета.
6. Детский познавательный интерес к теме сексуальных отношений между мужчиной и женщиной может активно эксплуатироваться злоумышленниками в интернете. Постарайтесь сами поговорить с ребенком на эту тему.

КАК СПРАВЛЯТЬСЯ С КОММУНИКАЦИОННЫМИ РИСКАМИ

Проговорите с ребенком ситуацию и внимательно его выслушайте.

Сохраните все возможные свидетель-ства происходя-щего.

Сохраняйте спокойствие — вы можете еще больше напугать ребенка своей бурной реакцией на то, что он вам рассказал и показал.

Повторите ребенку простейшие правила безопасности при пользовании интернетом.

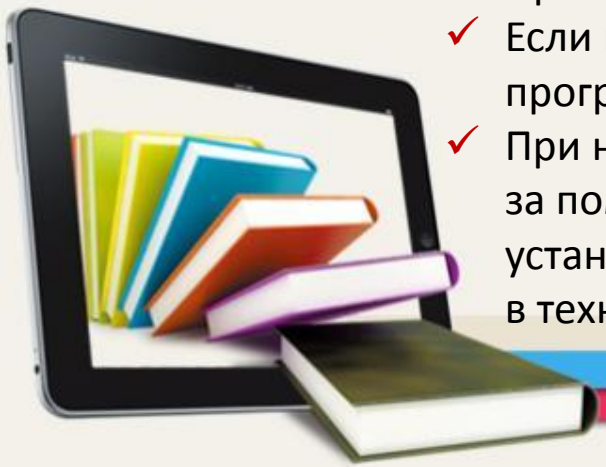
ЭЛЕКТРОННЫЕ (КИБЕР-) РИСКИ

возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д.

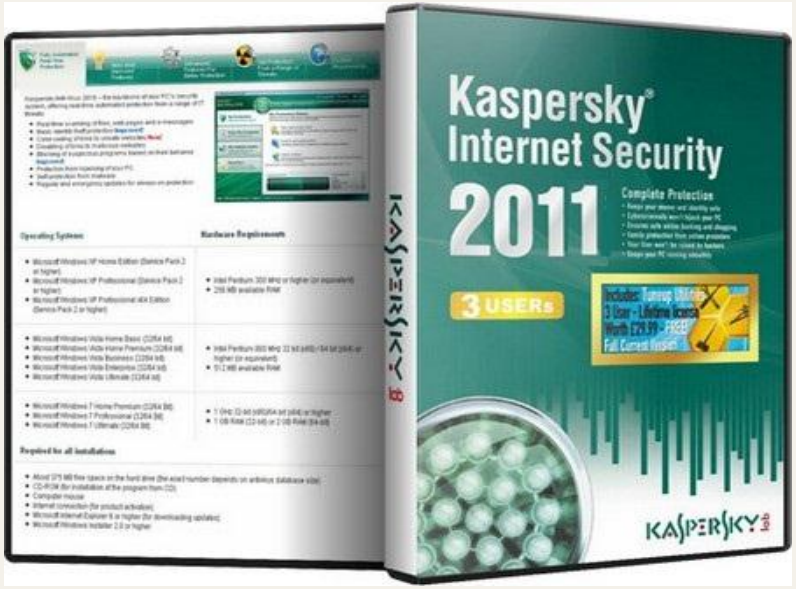
Вредоносные программы - вирусы, черви и «троянские кони», которые могут нанести вред вашему семейному компьютеру и хранящимся на нем данным.

КАК ИЗБАВИТЬСЯ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

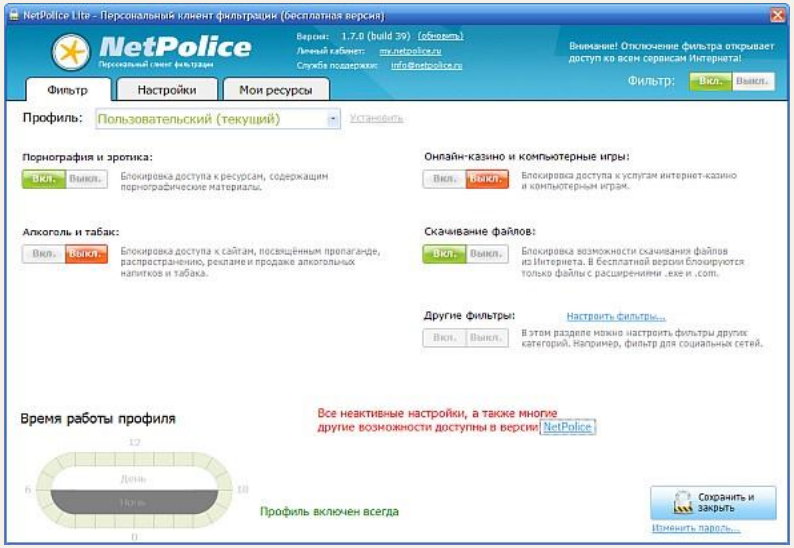
- ✓ Загрузите компьютер в безопасном режиме (включите компьютер, нажмите и, удерживая клавишу F8, выберите Безопасный режим (Safe Mode) в открывшемся меню).
- ✓ Проведите полную антивирусную проверку компьютера.
- ✓ Если в результате проверки обнаружен вирус, червь или троянская программа, следуйте указаниям производителя антивирусного ПО.
- ✓ При невозможности самостоятельно решить проблему обратитесь за помощью в службу технической поддержки производителя установленного на вашем компьютере антивирусного ПО или в технический сервис.



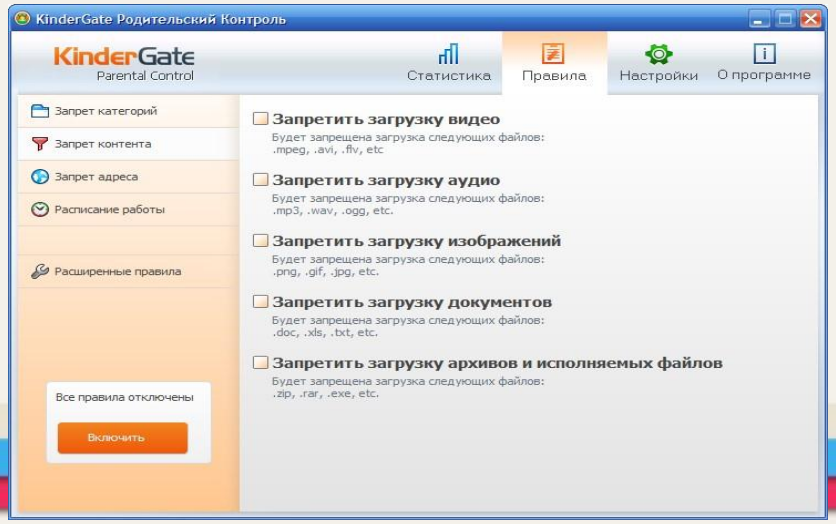
ПРИЛОЖЕНИЯ для РОДИТЕЛЬСКОГО КОНТРОЛЯ



www.kaspersky.ru , 105 Мбайт, 1600 рублей



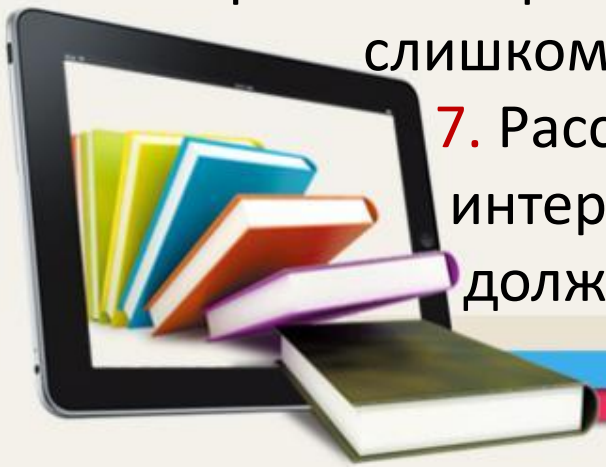
www.netpolice.ru , 32,7 Мбайт, 480 рублей



www.usergate.ru , 17,8 Мбайт, 490 руб/1год

КАК ПРЕДОТВРАТИТЬ ЗАРАЖЕНИЕ ПК ВРЕДОНОСНЫМИ ПРОГРАММАМИ

1. Установите на все домашние компьютеры антивирусные программы и специальные почтовые фильтры.
2. Используйте только лицензионные программы и данные, полученные из надежных источников.
3. Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.
4. Следите за тем, чтобы ваш антивирус регулярно обновлялся.
5. Регулярно делайте резервную копию важных данных.
6. Старайтесь периодически менять пароли, не используйте слишком простые пароли, которые легко взломать.
7. Расскажите ребенку, что если он пользуется интернетом с помощью чужого устройства, он должен не забывать выходить из своего аккаунта.

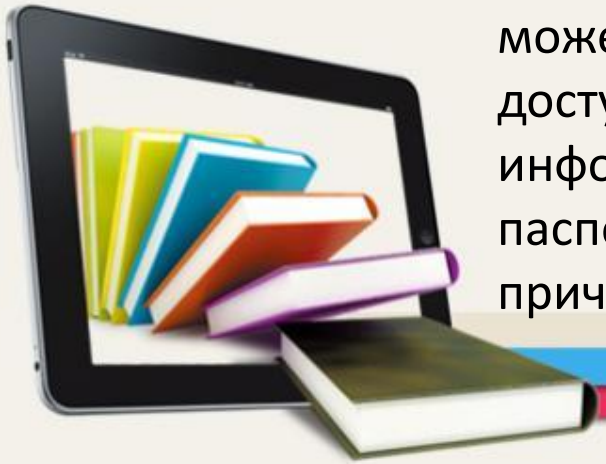


ПОТРЕБИТЕЛЬСКИЕ РИСКИ

злоупотребление в интернете правами потребителя.

Включают в себя:

- риск приобретения товара низкого качества,
- различные подделки,
- контрафактную и фальсифицированную продукцию,
- потерю денежных средств без приобретения товара или услуги,
- хищение персональной информации с целью кибермошенничества и др.



Кибермошенничество — 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 (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный и финансовый ущерб.

КАК ПРЕДОТВРАТИТЬ КИБЕРМОШЕННИЧЕСТВО

1. Проинформируйте ребенка о самых распространенных методах мошенничества в сети.
2. Не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать покупки.
3. Не отправляйте о себе слишком много информации при совершении интернет-покупок: данные счетов, пароли, домашние адреса и телефоны.
4. Установите на свои компьютеры антивирусное ПО.

КАК ПРЕДОТВРАТИТЬ КИБЕРМОШЕННИЧЕСТВО

5. Убедитесь в безопасности сайта, на котором Вы или Ваш ребенок планируете совершить покупку:

- ✓ Ознакомьтесь с отзывами покупателей.
- ✓ Избегайте предоплаты.
- ✓ Проверьте реквизиты и название юридического лица – владельца магазина.
- ✓ Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис Whois).
- ✓ Поинтересуйтесь возможностью получения кассового чека и других документов за покупку.
- ✓ Сравните цены в различных интернет-магазинах.
- ✓ Позвоните в справочную магазина.
- ✓ Обратите внимание на правила интернет-магазина.
- ✓ Выясните, сколько точно вам придется заплатить.

Как помочь ребенку, если он уже столкнулся с какой-либо Интернет-угрозой

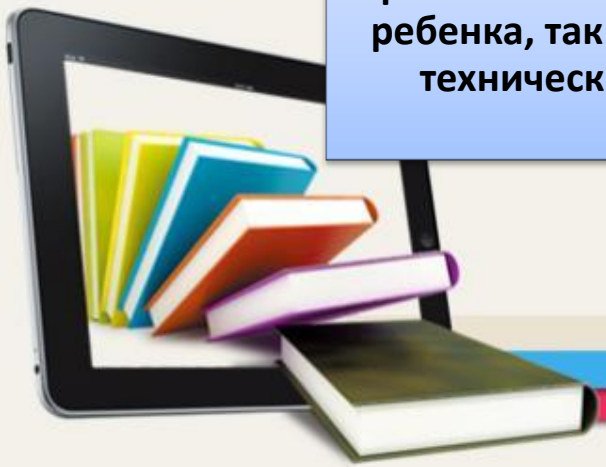
Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло.

Если ребенок расстроен чем-то увиденным или он попал в неприятную ситуацию, постарайтесь его успокоить и вместе разберитесь в ситуации.

Если ситуация связана с насилием в интернете в отношении ребенка, то необходимо узнать информацию об обидчике, историю их взаимоотношений, узнать о том, что известно обидчику о ребенке.

Соберите наиболее полную информацию о происшествии – как со слов ребенка, так и с помощью технических средств.

В случае, если вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, или ребенок недостаточно откровенен с вами и не готов идти на контакт, обратитесь к специалисту.



ТЕЛЕФОНЫ ДОВЕРИЯ, ГОРЯЧИЕ ЛИНИИ

- ✓ Линия помощи «**Дети Онлайн» - тел. 8 800 25 000 15** helpline@detionline.com
- ✓ Всероссийский детский телефон доверия: **8-800-2000-122**. *Звонок с любого телефонного номера, в том числе мобильного — бесплатный*
- ✓ Детский телефон Доверия (круглосуточно) **(8 495) 624-60-01**

- ✓ Уполномоченный по правам ребенка в Иркутской области: *Семенова Светлана Николаевна,* тел:**(3952) 34-19-17,** сайт:http://irkutsk.rfdeti.ru, e-mail:irkutsk@rfdeti.ru

Адрес: 664011, г. Иркутск, ул. Горького, д. 31, каб. 105