



НАЦИОНАЛЬНЫЙ УЗЕЛ  
ИНТЕРНЕТ - БЕЗОПАСНОСТИ  
В РОССИИ

# Как защититься от интернет-угроз



ПАМЯТКА  
для школьников, учителей, родителей



Региональный общественный  
Центр интернет-технологий  
[www.rocit.ru](http://www.rocit.ru)



ОБЩЕСТВЕННАЯ ПАЛАТА  
РОССИЙСКОЙ ФЕДЕРАЦИИ



**СОПРОТИВЛЕНИЕ**  
правозащитное движение

## Как защититься от...



## ...фальшивых интернет-магазинов

### 1. Проверьте «черные списки» недобросовестных магазинов.

Такие списки легко доступны в Интернете и существуют для того, чтобы предостеречь других пользователей. Посмотрите несколько списков – ведь один автор может быть субъективен.

### 2. Ознакомьтесь с отзывами покупателей.

Стоит поискать в Интернете отзывы о магазине, в котором собираетесь сделать покупку. Если сайт обманул кого-то, об этом обязательно напишут на каком-нибудь форуме или блоге.

### 3. Избегайте предоплаты.

Если это возможно, закажите товар с оплатой по факту получения. Например, доставку курьером или оплату на почте при получении посылки.

### 4. Проверьте реквизиты и название юридического лица – владельца магазина.

Магазины-«однодневки», скрываясь от контролирующих органов, часто не указывают свои реквизиты либо вовсе не их имеют.

### 5. Уточните, как долго существует магазин.

Даже если на сайте утверждается, что магазин работает несколько лет, это может быть обманом. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs).

### 6. Поинтересуйтесь выдачей чека.

Если магазин не выдает кассовых или товарных чеков, значит, с ним что-то не так. Если же при доставке товара обнаружите, что на чеке указана другая организация, от покупки надежнее будет отказаться.

### 7. Сравните цены в разных интернет-магазинах.

Вас должно насторожить, если магазин предлагает товар по слишком низким ценам, объясняя это тем, что продает товар с оптового склада или конфискат.

### 8. Позвоните в справочную магазина.

Каждый уважающий себя интернет-магазин отвечает на вопросы по телефону. Позвонив, вы сможете составить представление о качестве обслуживания и убедиться лишний раз в правильности своего выбора.

### 9. Обратите внимание на правила интернет-магазина.

Практически на всех сайтах присутствует текст соглашения между магазином и заказчиком, с которым пользователь автоматически соглашается, оформляя заказ. Крайне важно ознакомиться с этим соглашением заранее, чтобы, например, не узнать в момент получения товара, что бесплатная доставка полагается только постоянным клиентам.

### 10. Уточните, сколько точно вам придется заплатить.

Недобросовестные магазины могут указывать на сайте оптовую цену или стоимость без комплектации, а в реальности за доставленный товар придется заплатить намного больше.

## Как защититься от...



Родители вполне в состоянии избавить своего ребенка от возникновения интернет-зависимости – причем задолго до того, как это придется делать психологу или психиатру. Специалистами разных стран и разного профиля установлено, что для этого необходимо.

### 1. Как можно больше общаться с ребенком.

Дети, не обделенные родительским вниманием, не станут искать утешения в уничтожении монстров, поскольку не будут чувствовать себя одинокими.

### 2. Приобщать ребенка к культуре и спорту, чтобы он не стремился заполнить свободное время компьютерными играми.

Если у ребенка не останется времени на компьютерные игры, то и зависимости взяться будет неоткуда. К тому же заниматься спортом куда полезнее, нежели горбиться перед монитором. Интересно, что 90% детей, занимающихся спортом или искусством, не увлекаются компьютерными играми.

### 3. Не сердиться на ребенка за увлечение играми и ни в коем случае не запрещать их. Исключение составляют игры с насилием и жестокостью.

Детская психология такова – чем больше нельзя, тем больше хочется. Поэтому заострять внимание на том, что «компьютерные игры – зло», излишне, вы лишь сделаете малыша одержимым мыслями о запретном плоде со всеми вытекающими последствиями.

## ...интернет-зависимости

(советы родителям)

### 4. Объяснять ребенку разницу между игрой и реальностью.

Реалистичная компьютерная графика стирает в мозгу ребенка разницу между виртуальным и реальным мирами. Важно дать понять, что «в реале» гибель – это навсегда.

### 5. Не давать ребенку забыть, что существуют настоящие друзья, родители и учеба.

Если верить статистике, 80% детей начинают увлекаться компьютерными играми из-за недостатка общения в реальной жизни. Помогите своему ребенку найти общий язык со сверстниками и он предпочтет поиграть во дворе, нежели играть в одиночестве.

### 6. Занимать его чем-то еще, кроме компьютера.

Найдите своему ребенку замену компьютерной игре исходя из его личных талантов и предпочтений. Не существует детей, которых бы не интересовало ничего, кроме компьютера.

### 7. Ребенку обязательно нужно чувствовать вашу любовь и заботу, быть уверенным, что его обязательно поймут и поддержат.

Тогда у него будет меньше поводов отдалиться от вас, «зависнув» в виртуальной реальности. Больше половины юных пользователей Интернета ищут в нем игры и развлечения, которых им не хватает в реальной жизни. Они стремятся заполнить этот пробел виртуальными радостями. Если же у ребенка будет достаточно увлечений и друзей в реальной жизни, ему просто не захочется проводить долгие часы за компьютером.

## Как защититься от...



Стопроцентно защититься от спама невозможно. Но можно свести к минимуму вероятность его попадания в вашу деловую или личную почту следующими простыми мерами.

- 1. Не сообщайте свой электронный адрес никому, кроме людей, которым доверяете.**
- 2. Не указывайте ваш e-mail в формах опросов и гостевых книгах.**
- 3. При работе с интернет-магазинами и прочими сервисами используйте отдельный e-mail, который вы не используете для важных дел.**
- 4. Ни в коем случае не публикуйте свой электронный адрес в открытом доступе.**  
В icq, на форумах, сайтах знакомств и вообще везде, где его могут увидеть посторонние.
- 5. При выборе названия почтового ящика не используйте простые названия, которые спамеры могут подобрать «в уме».**
- 6. При работе в icq скрывайте информацию о себе.**  
Запретите писать неавторизованным пользователям и пользуйтесь анти-спам защитой.
- 7. В социальных сетях установите настройки приватности на максимальный уровень.**

## ...спама

Если это возможно, запретите всем, кроме друзей, писать на вашей «стене» (если она есть в соцсети). То же самое касается личных сообщений.

### **8. Держите включенными все возможные анти-спам системы.**

Таковые имеются в почтовых клиентах, службах мгновенной доставки сообщений, антивирусах (например, Kaspersky Anti-Spam) и фаерволах.

### **9. Запретите всплывающие окна в своем браузере, это спасет вас от переходов на ненужные страницы.**

В Интернете существует множество сайтов, борющихся со спамом. Например, проект «Антиспам.РУ» (antispam.ru).

Также в Сети можно найти немало фильтров для контроля действий спамеров, как платных, так и бесплатных (например, spamfighter.com). Настройка фильтра приема почты позволяет распознать нежелательные письма и заранее поместить в корзину или специально отведенную папку.

Бесплатным фильтром является «черный список» на большинстве почтовых серверов, который запоминает адреса, с которых приходит спам и блокирует их. Минусом сервиса является то, что в «черный список» попадают почтовые ящики обычных пользователей, что приводит к потере писем. Фильтр по теме письма работает эффективнее, но и его многие спамеры научились обходить.

## Как защититься от...



**1. По возможности используйте псевдонимы.**

**2. Указывайте лишь электронные способы связи, причем созданные специально для таких контактов.**

Например, специально выделенный для подобного общения e-mail или номер icq. Если собеседник окажется интересным и безопасным, ничто не мешает поделиться с ним потом «более реальными» электронными координатами, а то и телефоном или адресом.

**3. Тщательно обдумайте, какую информацию о себе загружать в Интернет.**

В Интернете действует принцип «все, что вы выложили, может быть использовано против вас». Даже если вы удалите фото, его уже могли скопировать – а значит, оно по-прежнему ходит по Интернету. Например, фото разгульной вечеринки может вызвать разрыв с близким человеком, видеоролик драки – стать доказательством для суда, демонстрация богатства наведет на вас грабителей, а подробные данные о себе подскажут им, где и как вас лучше ограбить.

## ...негативного использования персональной информации в социальных сетях

**4. Осторожно подходите к выбору друзей, не принимайте все заявки подряд для количества.**

Радость от большого числа «друзей» быстро омрачится неприятностями. Другом в соцсети может быть только тот, кто хорошо известен – желательно в реальной жизни.

**5. Не открывайте доступ к своим личным страничкам незнакомым людям.**

Есть те, кто специально ходит по социальным сетям с целью сбора информации. Затем ее используют для киберпреследования или подготовки серьезных преступлений. Чем меньше вы им дадите информации о себе – тем безопаснее.

## Как защититься от...



### 1. Игнорируйте оскорбителя

Самый простой и действенный способ. Просто представить, что данного пользователя не существует. Добавить его в игнор-лист («черный список») и мысленно удалить его из Интернета. Не отвечать ему и не поддаваться на провокации. Продолжать общаться на этом же ресурсе с людьми, приятными и близкими вам по духу.

### 2. Сообщите модератору

Это можно сделать с помощью специальной формы на форуме (она обычно выглядит как кнопка «пожаловаться на сообщение») или личным письмом. Если это популярный и уважаемый ресурс или если модераторская служба на нем поставлена на высоком уровне, его хозяева обязательно примут меры и воздействуют на сетевого агрессора (предупредят или вообще заблокируют ему доступ). В случае, если агрессором является сам модератор – воспользуйтесь третьим советом.

### 3. Найдите другой ресурс

Ничего не мешает вам покинуть сайт, на котором процветают хамство и оскорбления, и найти аналогичный, где можно спокойно общаться. Сделать это особенно просто, если вы не успели освоиться на сайте и привыкнуть к нему. Однако никто не гарантирует, что на новом месте не найдется своих местных хамов.

## ...хамства и оскорблений

### 4. «Задавите интеллектом»

Можно попытаться задавить сетевого хама интеллектом, показать, что с вами шутки плохи и, дескать, шел бы он оттачивать свои способности на ком-нибудь другом. Делается это лаконичными негрубыми ответами, высмеивающими грубияна и его действия.

*Что НЕ нужно делать:*

#### 1. Грубить в ответ.

Если вы опуститесь до уровня не очень умного человека, то будете выглядеть ничуть не лучше его.

#### 2. Угрожать хаму противозаконными последствиями в реальной жизни.

Подобные вещи чреваты наказанием согласно Уголовному кодексу. Хамы обычно люди весьма подлые и могут такую угрозу повернуть против вас. А получить судимость из-за сетевого хама – дело совсем не перспективное.

#### 3. Создавать темы на форуме с жалобами.

Если вас обидели – свяжитесь с администрацией сайта. Ни к чему засорять ресурс пустыми темами. Не теряйте уважения к себе и окружающим вас людям. Ведите себя в Интернете так, как хотите, чтобы вели себя с вами. Тогда вы обязательно найдете интересных собеседников и существование различных агрессивных личностей перестанет вас беспокоить.



## Как защититься от...

*В зависимости от типа ресурса, на котором вы столкнулись с киберхамом, подходящими могут быть различные действия.*

### 1. Чат.

Если при общении в тематическом чате к вам пристаёт пользователь с оскорблениями, злыми шутками или издевательствами, отправьте его в игнор-лист (персональный «черный список») или сообщите администратору чата о его неприемлемом поведении. Скорее всего, грубиян будет забанен, то есть исключен из числа пользователей. Грубить хаму в ответ чревато получением такого же бана.

### 2. Icq и прочие онлайн-мессенджеры.

Отвязаться от нежелательного собеседника в аське проще всего. Добавив разбушевавшегося грубияна в «черный список», вы больше никогда не увидите и не услышите его. Чтобы предотвратить дальнейшие беседы с «клонами» хама (то есть его «реинкарнациями» под другими номерами icq), необходимо поставить в настройках клиента запрет на получение сообщений от неавторизованных пользователей. Тогда вы будете получать сообщения только от тех контактов, которые одобрите сами.

### 3. Социальные сети.

Решить проблему хамства в социальных сетях обычно помогают модераторы ресурса, которые обязаны внимательно следить за публичными сообщениями пользователей. В случае добросовестной работы модераторов вы даже не успеете прочесть оскорбительное послание. Если же сетевой грубиян донимает вас по личной почте, вы всегда можете пожаловаться тому же модератору в индивидуальном порядке.

### 4. Сайты знакомств.

К сожалению, заметная часть посетителей сайтов знакомств приходят туда вовсе не для того, чтобы найти себе друзей и любимых. Сайты знакомств являются излюбленным местом обитания сетевых хамов, любителей онлайн-издевательства и розыгрышей. Поэтому, пользуясь подобными ресурсами, нужно быть предельно внимательным и быть морально готовым к неадекватным сообщениям. Отвечать на провокации и грубости вовсе не обязательно, а кнопка для отправки жалобы администрации всегда под рукой.

## ...хамства и оскорблений

### 5. Форумы.

Пытаться доказать что-то таким людям совершенно бесполезно, так как они преследуют единственную цель – позлить вас. Лучше представьте, что этого пользователя вовсе не существует на форуме и его сообщений тоже. Продолжайте беседу в привычной манере, не реагируя на попытки «тролля» вывести вас из себя. Вероятно, вскоре ему надоест тратить время зря и он оставит вас в покое.

Если же вы сами не прочь сорвать злость и плохое настроение в Интернете, можете рискнуть пообщаться с сетевым хамом на его языке. В конце концов, он первый начал и вы не обязаны быть вежливым. Однако опускание до уровня банального грубияна – занятие не делающее чести никому, поэтому куда лучше будет не обращать на него внимания.

Если вы оставались в таком общении относительно корректны, ваша моральная правота позволяет вам прибегнуть к методам «сетевого саморегулирования» – написать модераторам форума. «Стукачеством» подобные действия называют теперь только сами «тролли», ибо на практике большая часть форумистов заинтересована в нормальной и спокойной атмосфере для общения и молчаливо поддержит забанивание тролля. Если же на этом форуме «троллинг» возведен в культ, то лучше оттуда уйти – немного потянете.



## Как защититься от...



### 1. Контролируйте время, которое ребенок проводит в Интернете.

Длительное времяпровождение в Сети может быть связано с «заигрываниями» со стороны педофилов, особенно в блогах и социальных сетях.

### 2. Периодически читайте электронную почту ребенка.

Несмотря на моральный аспект, это вполне эффективный способ узнать, с кем ваш ребенок контактирует в Интернете и что за этим может последовать. Другое дело, что это можно делать, только если у вас есть достаточные основания полагать, что ребенку кто-то наносит вред через электронную переписку – ребенок после прочтения электронной почты регулярно растерян, испуган, расстроен.

### 3. Будьте в курсе, с кем контактирует в Интернете ваш ребенок.

Помогайте ему увидеть тех, кто явно выдает себя в Сети не за того, кто он есть.

### 4. Если ребенок интересуется контактами с людьми намного старше его, следует провести мягкий обучающий разговор.

В ходе него следует разъяснить ребенку возможные опасности такого контакта, его последствия в дальнейшей жизни, потенциальные цели педофилов.

## ...онлайн-педофилов

(советы родителям)

### 5. Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Если он желает познакомиться со взрослым интернет-другом, следует настоять на сопровождении ребенка на эту встречу.

### 6. При обнаружении признаков совращения следует немедленно сообщить об этом в правоохранительные органы.

Милиция в любом случае обязана принять заявление о преступлении и при необходимости перенаправить его в профильное ведомство (например, Следственный комитет при прокуратуре).

### 7. Если Вы увидели в Сети детскую порнографию – сообщите об этом на «Горячую линию» по борьбе с противоправным контентом в Интернете.

В отличие от милиции (включая веб-формы правоохранительных сайтов), здесь это можно сделать полностью анонимно. «Горячая линия» приложит все усилия для того, чтобы противоправный контент был удален или закрыт.





## Общие «аксиомы безопасности» при работе в Интернете

Соблюдая эти простые правила безопасной работы в Интернете, вы избавите себя от множества серьезных проблем и опасностей, существующих в Сети.

### 1. Поступайте и пишите в Сети так, как поступили бы в реальной жизни и как хотели бы, чтобы поступали с вами.

Помните – все, что вы сделаете в Интернете, будет иметь последствия в реальной жизни. Анонимность в Интернете не гарантирует, что любые поступки сойдут с рук. Стоит вспомнить хотя бы то, сколько хакеров и интернет-мошенников уже оказались за решеткой. Вычислить человека по его виртуальным следам (IP, cookies, мак-адрес) не так уж сложно.

### 2. Уважайте своих собеседников и чужую собственность в Интернете, за ними скрываются настоящие люди и реальный труд.

Вы общаетесь не с абстрактным псевдонимом, а с человеком – даже за ботом стоит человек. Кстати, у всех материалов, находящихся в Сети есть авторы и хозяева.

### 3. Не сохраняйте на своем компьютере неизвестные файлы, не переходите по ссылкам от незнакомцев, какими бы заманчивыми они не были.

Такая ссылка может оказаться вирусом, трояном или, если «повезет», рекламой порносайта. 80% ссылок, присылаемых незнакомцами, являются рекламой, а 20% – вредоносными объектами.

### 4. Обязательно установите антивирус и фаервол и регулярно обновляйте их базы.

Необновленные и устаревшие базы не смогут гарантировать вам стопроцентную защиту от вредоносных объектов. Дело в том, что ежедневно в мире появляется несколько новых вирусов, поэтому антивирусу необходимо как можно чаще получать информацию о методах борьбы с ними.

### 5. Не запускайте неизвестные файлы, особенно с расширением \*.exe

Старый совет, но по-прежнему актуальный. Файл с таким разрешением не может являться картинкой или фильмом. Это всегда программа, в крайнем случае флеш-анимация. Поэтому велика вероятность, что такой файл является вирусом или трояном.

### 6. Старайтесь давать как можно меньше информации о себе в Интернете.

«Что написано пером – не вырубить топором» – эта мудрость актуальна и для Интернета. Например, 90% мошенничеств происходит из-за утечки информации по вине пользователя.

### 7. Будьте осторожны при общении с незнакомыми людьми.

Ничто не мешает сорокалетнему извращенцу прикидываться в чатах пятнадцатилетней школьницей и заводить знакомства со «сверстницами». Опросы показывают, что каждый пятый пользователь Сети выдавал себя за другого человека (реально существующего или придуманного).

### Национальный Узел создан для того, чтобы:

- дать пользователям понятную, качественную и доступную информацию о вредных проявлениях Интернета;
- помочь им уберечь себя, свой компьютер и своих близких от воздействия интернет-угроз;
- формировать культуру пользования Интернетом у детей и взрослых;
- помочь обществу и государству бороться с преступлениями, совершаемыми с помощью Интернета;
- помочь пользователям и жертвам интернет-преступлений советом и профессиональной консультацией.

### Национальный Узел включает следующие разделы.

#### Информационно-аналитическая часть:

- статьи об интернет-угрозах и способах защиты;
- аналитика;
- памятки по борьбе с конкретными интернет-угрозами;
- статистика;
- наглядные ролики о вреде интернет-угроз и защите от них;
- безопасные ресурсы.

#### «Горячая линия» по противоправному контенту:

- прием сообщений о противоправном контенте;
- содействие в прекращении его оборота в Сети.

#### «Линия помощи»:

- консультации по защите от интернет-угроз;
- помощь жертвам интернет-преступлений.

### Специальные проекты Национального Узла:

**Социальный проект «НеДопусти»** призван помочь в борьбе с таким злом как сексуальная эксплуатация и похищения детей ([www.detivrunete.ru](http://www.detivrunete.ru), [www.nedopusti.ru](http://www.nedopusti.ru)).

**Хулиганам.Нет** – против киберунижений и психологического насилия в Сети ([www.huliganam.net](http://www.huliganam.net))

**СтопКонтрафакт** – помощь авторам и владельцам интеллектуальной собственности в Интернете ([www.storcontrafact.ru](http://www.storcontrafact.ru))

**Национальный Узел** является первым членом Международной Сети «горячих линий» по противоправному контенту INHOPE из Российской Федерации.

**Национальный Узел** – соорганизатор ведущей российской конференции по контентной безопасности в Сети i-SAFETY.

**Национальный Узел** – участник проекта Европейской комиссии Safer Internet Day.

**Национальный Узел** – участник Года безопасного Интернета в России.

**Национальный Узел** – партнер главного российского проекта по этике в Интернете «Этика.Ру».

Организаторы Национального Узла: РОЦИТ и правозащитное движение «Сопrotивление».

Под патронатом Общественной Палаты Российской Федерации.



### «Горячая линия» по противоправному контенту

Нашли в Интернете противоправный контент?  
Сообщите об этом в «Горячую линию»  
Национального Узла Интернет-безопасности  
в России!

#### «Горячая линия» – это:

- простота сообщения о противоправном контенте;
- анонимность;
- независимость экспертизы;
- общественный характер механизма;
- прием сообщений из любой точки мира;
- быстрое закрытие противоправного контента;
- передача информации о зарубежных сайтах в нужную страну.

«Горячая линия» Национального Узла входит в Международную сеть «горячих линий» INHOPE и является ее официальной частью на территории Российской Федерации.



[www.saferunet.ru](http://www.saferunet.ru)  
Национальный Узел Интернет-безопасности в России  
Общественная Палата РФ  
125993 Москва, Миусская пл., 7  
[info@saferunet.ru](mailto:info@saferunet.ru)