

Вологодская областная универсальная научная библиотека им. И.В. Бабушкина

Отдел библиографии и краеведения

Безопасный интернет для детей и взрослых

Методические рекомендации

Вологда
ВОУНБ
2017

УДК004.056
ББК32.971.353
Б40

Б40 Безопасный интернет для детей и взрослых [Электронный ресурс]: методические рекомендации / Вологод. обл. универс. науч. б-ка им. И. В. Бабушкина ; [сост. Д. П. Ятвицкая]. – Вологда : ВОУНБ, 2017. – 45 с.: табл.

УДК004.056

ББК32.971.353

© БУК ВО «Областная универсальная
научная библиотека», 2017

Введение

Почти в каждом руководстве по безопасности в Сети можно прочитать совет для детей – «в любой непонятной ситуации обращайся к взрослому человеку». К сожалению, все мы понимаем, что это не панацея – иногда взрослый человек тоже чувствует свою беспомощность перед новыми информационными технологиями и рисками. Некоторые основные вещи нужно знать самим. Тут не обойтись без затрат времени на изучение азов. Но время это окупится, к тому же, в случае необходимости ваша помощь пригодится как ребёнку, так и близким людям и друзьям.

В качестве мини-курса «Безопасность при работе в сети Интернет» для взрослых мы рекомендуем использовать, к примеру, [руководство](#), подготовленное компанией «Яндекс», выдержки из которого приведены ниже (полную версию можно найти по ссылке выше, для этого надо нажать клавишу **CTRL**, курсор при этом превращается в значок руки, и щёлкнуть по ссылке).

I. Интернет-безопасность для взрослых (руководство от [ЯндексПомощь](#))

1. Как настроить компьютер для безопасной работы в интернете.....	5
2. Как защитить браузер и настройки интернета от действий нежелательных программ.....	7
Какие угрозы несут нежелательные программы?	7
Как удалить нежелательные программы?	7
3. Защита личной информации.....	8
Способы хищения личной информации.	9
Основные рекомендации по защите данных.	10
4. Безопасность при работе в сети.....	11
Используйте последнюю версию вашей операционной системы и настройте автоматическое обновление.	11
Не откладывайте и не отменяйте обновления браузера и его компонентов.....	11
Установите антивирус.	12
Включите и настройте файрволл (брандмауэр).	14
Пользуйтесь учетной записью с ограниченными правами.	14
Используйте легальное ПО	15
Делайте резервные копии ценных данных	15
5. Вирусы.....	15
6. Безопасность электронных платежей.....	16
7. Сетевое мошенничество.....	16
Как защититься от сетевого мошенничества?	19
Что делать, если вы стали жертвой мошенников?	20

1. Как настроить компьютер для безопасной работы в интернете

Безопасность компьютера при работе в интернете зависит от множества факторов, и в первую очередь — от соблюдения пользователем всего комплекса правил и предосторожностей, а также от настроек, как пользовательских, так и по умолчанию, установленных патчей («заплаток») и антивирусов, средств защиты на интернет-шлюзе и многого другого. Но при прочих равных:

1. Браузеры Opera 28 и Firefox 36 безопаснее, чем Opera и Firefox предыдущих версий. Microsoft Internet Explorer 11 существенно безопаснее предыдущих версий Microsoft Internet Explorer.

2. Если в операционной системе установлен и включен антивирус — работать в ней безопаснее, чем без антивируса.

Высокие оценки AV Comparatives в 2014 получили антивирусы Kaspersky, ESET, BitDefender, Avast! Free Antivirus, AVIRA, Panda Cloud Antivirus, F-Secure, G DATA.

Некоторые антивирусы из этого списка являются бесплатными, например: Kaspersky, Avast! Free Antivirus и Panda Cloud Antivirus.

Примечание. Обновление и доступ к интернету являются для большинства современных антивирусов критически важными, без этого эффективность их защиты быстро снижается.

3. Если в операционной системе включен и правильно настроен фаерволл, он безопаснее. Правильная настройка заключается в том, чтобы в брандмауэре была разрешена только та сетевая активность, в которой есть необходимость. Брандмауэр можно включить так:

○ *Microsoft Windows XP: Пуск → Панель управления → Центр обеспечения безопасности → Брандмауэр Windows → Включить → ОК.*

○ *Microsoft Windows 7: Пуск → Панель управления → Система и безопасность → Брандмауэр Windows → Включение и отключение брандмауэра Windows → Включение брандмауэра Windows в доменных, домашних и рабочих, а также в общественных сетях.*

4. Работать под учетной записью с **ограниченными полномочиями** существенно безопаснее, чем под учетной записью с правами локального, а тем более доменного системного администратора. Кроме того, рекомендуется, чтобы:

○ *полномочия учетной записи соответствовали компьютерной грамотности и ответственности тех, кто под ней работает;*

○ вход под учетной записью системного администратора был возможен только после ввода пароля, причем не формального «qwerty» или «111», а полноценного: минимум 11 букв в разных регистрах, цифр и специальных символов.

5. Microsoft Windows 7 безопаснее предыдущих операционных систем компании Microsoft для рабочих станций, в том числе Microsoft Windows XP. UNIX-подобные операционные системы (в том числе Linux, BSD, «промышленные» UNIX) безопаснее остальных распространенных ОС.

6. Если программное обеспечение, в том числе операционная система, обновляются, они безопаснее. Обновление можно включить так:

○ Microsoft Windows XP: Пуск → Панель управления → Центр обеспечения безопасности → Автоматическое обновление → Автоматически → ОК.

○ Microsoft Windows 7: Пуск → Панель управления → Система и безопасность → Центр обновления Windows: Включение и выключение автоматического обновления → Важные обновления: Устанавливать обновления автоматически.

7. Неофициальные сборки, а также образы программных продуктов, распространяемые неофициально (в том числе на контрафактных дисках, с помощью торрентов и «неофициальных» зеркал сайтов) часто менее безопасны, чем официальные.

8. **Делайте резервные копии наиболее ценных для вас данных**, так как вредоносные программы могут блокировать доступ к системе, шифровать данные на дисках, а иногда и безвозвратно их портить. При этом платить деньги злоумышленникам за восстановление доступа к собственным данным означает финансировать разработку и распространение новых, еще более изощренных вредоносных программ.

Удобство почти всегда противоречит безопасности. Система с полностью отключенной безопасностью «не мешает» пользователю ограничениями, вопросами, необходимостью дополнительных подтверждений и действий. Работа антивируса часто снижает быстродействие системы, авторизация и переключение учетных записей — отнимает время. Но потеря данных часто стоит дороже, ведь среди них могут быть результаты работы и хобби, фотографии, архивы, коллекции, данные для авторизации в платежных системах, системах обмена сообщениями, социальных сетях, онлайн-играх. Даже если учитывать только потери времени, то на однократное восстановление данных и работоспособности системы его обычно уходит больше,

чем на соблюдение правил техники безопасности работы с интернетом в течение нескольких лет.

2. Как защитить браузер и настройки интернета от действий нежелательных программ

Нежелательные программы незаметно устанавливаются при скачивании торрент-клиентов, дополнений и других программ с сомнительных сайтов, распространяющих нелегальный контент. Они не являются вирусами, но могут негативно влиять на удобство и безопасность работы в интернете. Например, снизить скорость работы браузера, без согласия пользователя установить дополнительные панели инструментов, перенаправлять на мошеннические, фишинговые или рекламные страницы.

Если вы столкнулись с действиями нежелательных программ, воспользуйтесь утилитой очистки системы. Она проверит компьютер и удалит программы, которые могут вмешиваться в работу браузера.

Утилита предоставляется бесплатно и работает со всеми популярными браузерами на компьютерах с операционной системой Windows.

Какие угрозы несут нежелательные программы?

Модифицированные параметры запуска системы (StartPage)

Драйвер-фильтр, показывающий нежелательный контент (Fake NetFilter)

Подмененный DNS (Infected DNS)

Нежелательные записи в файле hosts (Infected Hosts)

Нежелательные расширения браузера (Unwanted Extensions)

Нежелательное ПО, модифицирующее трафик (PBot)

Модификации ярлыков браузера (Infected LNK)

Как удалить нежелательные программы?

Установите утилиту.

Примечание. Если вы используете Яндекс.Браузер, то скачивать и устанавливать утилиту не нужно. При выявлении угрозы в окне браузера появится предупреждение: Обнаружены вредоносные программы. Чтобы запустить утилиту, нажмите кнопку: Начать проверку и лечение.

1. Чтобы получить утилиту очистки системы, напишите в [службу поддержки](#).
2. В ответном письме придет ссылка для скачивания утилиты. Перейдите по этой ссылке.

3. Откройте сохраненный исполняемый файл `rescue_tool.exe` и нажмите кнопку: Запустить.

Запуская утилиту, вы соглашаетесь с [условиями ее использования](#).

Запустите очистку.

1. В окне Утилита очистки системы нажмите кнопку: Начать проверку.
2. После проверки системы вам будет предложено удалить нежелательные программы.

Вы можете посмотреть список найденных программ — для этого нажмите ссылку Отчёт о проверке.

Чтобы завершить очистку, нажмите кнопку: Удалить. Для окончательного удаления некоторых программ, возможно, понадобится перезагрузить компьютер.

Перезапустите очистку.

Если нежелательные программы не были найдены или не все программы были удалены, проведите очистку еще раз:

1. Для повторной проверки нажмите кнопку: Перезапустить.
2. Разрешите утилите вносить изменения на устройстве.
3. В окне Найденны нежелательные программы нажмите кнопку: Удалить.

Если после повторной очистки удалить программы не получилось или они не были обнаружены, но вы уверены, что компьютер под угрозой, посмотрите, что еще [можно сделать](#), или обратитесь в [службу поддержки](#).

3. Защита личной информации

Личная информация — это ваши имя и фамилия, паспортные данные (номер, серия, копия паспорта), пароли для доступа к различным сервисам и электронным кошелькам. Также личной информацией стоит считать:

- номер вашего телефона,
- номера телефонов ваших родственников,
- ваш домашний адрес,
- ваш возраст и дату рождения,
- ваше место работы — если вы работаете, и номер школы и класса — если вы учитесь,

- любые другие данные, с помощью которых можно разыскать вас или ваших родственников.

Вы сами выбираете, какую информацию о себе сообщить. В интернете никто не может заставить вас предъявить паспорт или назвать настоящую фамилию. Некоторым сайтам (например, интернет-магазинам) необходимо знать о вас правду, но стоит ли раскрывать свои данные — всегда решаете вы. Если вы сомневаетесь в том, что какому-либо сайту можно доверить вашу личную информацию, лучше не доверяйте.

Важно помнить о том, что если сайт недостаточно хорошо защищен, мошенники могут взломать его и получить доступ к информации, которую вы передали сайту.

Способы хищения личной информации

Чтобы получить ваш пароль от какого-либо сайта или другие личные данные, злоумышленники могут прибегать к самым разным обманным тактикам. Вот самые распространенные способы кражи пароля:

- **Фишинговые письма.** Мошенник присылает вам письмо, представляясь администрацией сайта, социальной сети или банка. В письме вас просят перейти по ссылке на поддельный сайт, где запрашивается пароль. Введенный пароль перехватывается и становится известен мошенникам.

- **Телефонные звонки от злоумышленников.** Мошенники выдают себя за операторов, сотрудников банка и т. д. — в ходе телефонного разговора вас могут попросить сообщить свой пароль или другую личную информацию.

- Мошенник может **найти ваши пароли** на выброшенных или оставленных без присмотра компьютерах, телефонах, флеш-картах, записках.

- Пароль можно **подслушать**, если вы диктуете его по телефону.

- Сайт **предлагает вам обмануть** банк или платежную систему, заработать без вложений, получить доступ к чужим SMS-сообщениям и т. д. Чаще всего такие сервисы просто выманивают личную информацию, не оказывая услуг.

- Мошенник **может угадать ваш пароль**, если он слишком простой (например, «qwerty123» или «сергей»), и ответ на секретный вопрос, если его достаточно легко найти (например, в вашем профиле социальной сети).

Основные рекомендации по защите данных

Будьте внимательны при работе в интернете. Помните, что защита ваших личных данных, банковских счетов и других данных на вашем компьютере находится, в первую очередь, под вашей ответственностью.

- **Не запускайте** сомнительные программы, полученные от знакомых и незнакомых людей — особенно если программа была скачана с сайта, распространяющего нелегальный контент (взломанные программы, нелицензионные фильмы или музыку).
- **Не записывайте номера** ваших счетов и другую **личную информацию** в легкодоступных местах.
- **Не диктуйте** секретную информацию по телефону (номер банковской карты, пароль от карт предоплаты и т. д.).
- **Не вводите пароли в необычные формы авторизации** (например, в текстах электронных писем).
- Прежде чем вводить пароль, **убедитесь**, что в адресной строке браузера указан верный адрес сайта. Поддельные формы регистрации часто размещают на веб-страницах с адресами, очень похожими на настоящие (например, yanclex.ru вместо yandex.ru).
- **Не игнорируйте** предупреждения браузера о проблемах с сертификатом или о всплывающих окнах.
- **Будьте осторожны** при работе на чужих компьютерах, например в интернет-кафе. Не ставьте флажок запомнить пароль, если компьютером могут пользоваться другие люди. Всегда выходите с сайтов, на которых вы авторизовались на чужом компьютере: на большинстве сайтов для этого предназначены специальные ссылки — Завершение работы или Выход. После окончания работы закройте браузер.
- Если домашним компьютером пользуются несколько человек, **используйте для них разные профили** операционной системы.
- **Не выкладывайте в открытый доступ и не храните** в электронной почте отсканированные копии документов, например паспорта. Копии документов часто требуют в качестве удостоверения личности в интернете: если вашу почту взломают, мошенники могут воспользоваться этими копиями без вашего ведома. Если письмо с такими данными сохранилось в папке «Отправленные», «Удаленные» или «Черновики», злоумышленники также могут получить к нему доступ.
- **Не отправляйте свои пароли открытым текстом** по электронной почте, через мессенджеры (например, ICQ) или в SMS.

- **Проверяйте** все скачанные файлы антивирусом.
- Регулярно **проверяйте антивирусом съемные диски, флеш-карты** и прочие носители информации, которые вы подключаете к чужим компьютерам.

4. Безопасность при работе в сети

Защитить компьютер от большинства угроз интернета можно, соблюдая простые правила безопасности.

Среди перечисленных ниже советов есть как конкретные рекомендации, так и общие правила. Следовать каждому конкретному совету — ваш выбор, но каждый из них поможет сделать вашу работу в интернете безопаснее.

Используйте последнюю версию вашей операционной системы и настройте автоматическое обновление.

Большинство обновлений операционных систем выпускается, чтобы закрывать уязвимости, которые могут использовать вирусы.

Включить автоматическое обновление в Windows можно следующим образом:

- *Windows XP: Пуск → Панель управления → Центр обеспечения безопасности → Автоматическое обновление → Автоматически.*
- *Windows 7: Пуск → Панель управления (просмотр по категориям) → Система и безопасность → Включение и отключение автоматического обновления → Важные обновления. В выпадающем списке выберите пункт Устанавливать обновления автоматически (рекомендуется).*
- *Windows 8: Нажмите правой кнопкой мыши на кнопку Пуск → Панель управления. Убедитесь, что установлен просмотр по категориям. Система и безопасность → Включение и отключение автоматического обновления → Важные обновления. В выпадающем списке выберите пункт Устанавливать обновления автоматически (рекомендуется).*
- *Windows 10: Пуск → Параметры. На вкладке Центр обновления Windows нажмите ссылку Дополнительные параметры. В выпадающем списке Выберите, как устанавливать обновление выберите пункт Автоматически (рекомендуется).*

Не откладывайте и не отменяйте обновления браузера и его компонентов.

Так же, как и при обновлении операционной системы, при обновлениях браузера часто устраняются уязвимости предыдущих версий.

Установите антивирус

Важно, чтобы антивирусные базы регулярно обновлялись. Без доступа к обновлениям антивирусы гораздо менее эффективны.

- *По возможности настройте антивирус так, чтобы он постоянно следил за поведением программного обеспечения.*
- *Не игнорируйте предупреждения антивируса, операционной системы и браузера, связанные с безопасностью. Ложные срабатывания не должны отвлекать от настоящей угрозы.*

Если компьютер необходимо срочно проверить на вирусы, рекомендуем воспользоваться бесплатными утилитами:

- [Dr.Web CureIt!](#)
- [Kaspersky Virus Removal Tool](#)

Чтобы обеспечить постоянную защиту компьютера, установите антивирус с регулярным обновлением вирусных баз. Желательно настроить антивирус таким образом, чтобы он постоянно следил за поведением работающих на компьютере программ.

Если у вас нет возможности установить платный антивирус, воспользуйтесь **одной из бесплатных программ**, перечисленных ниже. Большинство этих программ — пробные версии платных антивирусов, с урезанной функциональностью. Но даже такой антивирус сделает работу с интернетом безопаснее, чем его отсутствие.

Бесплатные антивирусы:

- [Kaspersky](#)
- [SUPERAntiSpyware](#)
- [Malwarebytes Anti-Malware](#)
- [AVG AntiVirus FREE](#)
- [AVZ](#)
- [Avast! Free Antivirus](#)
- [ClamWin](#)
- [Comodo Antivirus](#)
- [Microsoft Security Essentials](#)
- [NANO Антивирус](#)
- [Panda Cloud Antivirus](#)
- [Zillya! Антивирус](#)

- [360 Total Security](#)

Если вирус полностью блокирует работу операционной системы, можно использовать образ загрузочного диска с антивирусным сканером:

- [Dr.Web LiveDisk](#)
- [Kaspersky Rescue Disk](#)
- [VBA32 Rescue LiveCD](#)

Чтобы проверить компьютер с помощью загрузочного диска:

1. *Скачайте образ диска на другой, не зараженный компьютер.*
2. *Запишите его на нужный носитель (CD/DVD или флеш-накопитель).*
3. *Перезагрузите зараженный компьютер, вставив или подключив подготовленный носитель.*
4. *Войдите в BIOS при загрузке компьютера. Обычно для этого нужно часто нажимать определенную клавишу, как правило F2, Del или Esc. Узнать, какую именно клавишу надо нажать, можно при загрузке компьютера: внизу экрана появится соответствующее указание (например, «Press F2 to run SETUP»).*
5. *Настройте Boot Sequence в BIOS зараженного компьютера так, чтобы компьютер в первую очередь загружался с записанного вами носителя.*
6. *Снова перезагрузите компьютер. В этот раз он должен загрузиться с носителя и запустить антивирус.*
7. *Запустите проверку и дождитесь, пока антивирус полностью проверит систему и удалит найденные вирусы.*
8. *Извлеките загрузочный диск и перезагрузите компьютер. Верните настройки Boot Sequence в исходное состояние, если вы изменяли их.*
9. *Вылечив компьютер, в первую очередь установите на него антивирус.*

Если в браузере показывается навязчивая и шокирующая рекламы, открываются рекламные вкладки, происходит перенаправление на нежелательные сайты, проверьте вашу операционную систему программой против вредоносной рекламы:

Windows	MacO
<u>Chistilka</u>	S
<u>Reason Core</u>	<u>Adwar</u>
<u>Security</u>	<u>eMedic</u>

Включите и настройте файрволл (брандмауэр)

Правильно настроенный файрволл разрешает только те интернет-запросы, которые вы считаете необходимыми, и создает дополнительный уровень защиты операционной системы от вирусов.

Включить файрволл, встроенный в Windows (брандмауэр Windows), можно следующим образом:

- *Windows XP: Пуск → Панель управления → Центр обеспечения безопасности → Брандмауэр Windows → Включить.*
- *Windows 7: Пуск → Панель управления. Убедитесь, что установлен просмотр по категориям. Система и безопасность → Брандмауэр Windows → Включение и отключение брандмауэра Windows (в левом меню страницы). Включите брандмауэр для всех сетей — доменных, частных и общественных.*
- *Windows 8: Нажмите правой кнопкой мыши на кнопку Пуск → Панель управления. Убедитесь, что установлен просмотр по категориям. Система и безопасность → Брандмауэр Windows → Включение и отключение брандмауэра Windows (в левом меню страницы). Включите брандмауэр для всех сетей — доменных, частных и общественных.*
- *Windows 10: Нажмите правой кнопкой мыши на кнопку Пуск → Панель управления. Убедитесь, что установлен просмотр по категориям. Система и безопасность → Брандмауэр Windows → Включение и отключение брандмауэра Windows (в левом меню страницы). Включите брандмауэр для всех сетей — доменных, частных и общественных.*

Пользуйтесь учетной записью с ограниченными правами

Если права пользователя операционной системы ограничены, вирус не сможет внедриться в систему, даже если он проникнет в компьютер. Учетную запись системного администратора при этом нужно защитить достаточно сложным паролем.

Хороший пароль содержит не меньше 8 символов и содержит цифры, буквы и специальные символы: ! # \$ % ^ { } [] () " : \ |. Не используйте простые и легко подбираемые пароли — «123456», «qwerty», «password» и т. д. Посмотрите, нет ли вашего пароля в списках худших паролей в интернете. Мошенники часто взламывают учетные записи, просто перебирая пароли из таких списков.

Рекомендуем менять пароли не реже чем раз в три месяца.

Используйте легальное ПО

Старайтесь избегать неофициальных сборок и взломанных программ, скачивайте программы с официальных сайтов. В установочные файлы, выложенные на других сайтах, могут быть внедрены вирусы. Будьте особенно внимательны, скачивая взломанные программы, — запуская их, вы слепо доверяете взломщикам.

Делайте резервные копии ценных данных

Вирусы могут портить данные на жестких дисках или шифровать их, предлагая разблокировку за деньги. Платить деньги в таком случае — значит финансировать разработку новых, еще более изощренных вирусов. Делайте резервные копии на других носителях (CD, DVD, внешние диски, флеш-накопители, облачные сервисы).

Забота о безопасности часто доставляет неудобства. Но время, потраченное на соблюдение простых правил безопасности, окупается всегда.

5. Вирусы

Вирусы — это программы, которые позволяют мошенникам похищать, изменять или удалять информацию с компьютера. Также с помощью вируса мошенники могут блокировать работу компьютера, чтобы вымогать деньги за разблокировку.

Вирусы могут перехватывать пароли и другую личную информацию, которую вы вводите с клавиатуры, распространять спам от вашего имени, заражать другие компьютеры в сети. Злоумышленники могут даже управлять вирусом, если вирус получает доступ к интернету. Вы можете и не подозревать, что ваш компьютер используется кем-то еще.

Вирусы часто мешают компьютеру нормально работать, замедляя остальные программы и активно используя интернет-соединение. Действия зараженного компьютера могут привлечь внимание интернет-провайдера и правоохранительных органов.

Вы можете заразить компьютер вирусом, когда:

- *скачиваете файлы;*
- *заходите на сайт, который незаметно запускает вирус в вашем браузере (например, с помощью JavaScript, Java или Flash);*
- *используете непроверенные флеш-носители или компакт-диски;*

- *подключаете компьютер к локальной сети (используются провайдерами типа «домашняя сеть», в общежитиях, интернет-кафе, на точках доступа к бесплатному Wi-Fi).*

6. Безопасность электронных платежей

Как правило, системы электронных платежей хорошо защищены. Учетные записи в таких системах обычно взламывают потому, что клиенты сами раскрывают свои секретные данные, по невнимательности или излишней доверчивости, например, записывают пароль на видном месте, по ошибке выкладывают файлы с ключами в открытый доступ, переходят по фишинговой ссылке в письме и т. д.

Все советы по защите личной информации применимы и к электронным платежам, ведь пароли, защищающие ваши деньги, — это тоже личная информация. Кроме того, для безопасного использования платежных систем важно **соблюдать еще несколько правил:**

- *Перед вводом пароля **убедитесь**, что используется защищенное соединение — адрес в строке браузера должен начинаться с *https*.*
- *Дополнительно защищайте свои платежи.*
- *Используйте **одноразовые** пароли (например, усиленную авторизацию на Яндекс.Деньгах).*
- ***Не доверяйте** незнакомым людям, которые обещают крупный подарок, прося небольшую сумму денег за «участие в акции» или «оформление перевода».*
- ***Не покупайте** у частных лиц игровую валюту, голоса в социальных сетях и игровых персонажей. Если такие покупки не одобряются официальными представителями игры или социальной сети, вы рискуете потерять деньги вместе со своими приобретениями.*
- ***Не участвуйте** в финансовых махинациях и пирамидах, обещающих мгновенный доход и требующих вложения средств.*

7. Сетевое мошенничество

Как правило, целью сетевого мошенничества является получение конфиденциальных данных (паролей от учетных записей, номера или PIN-кода кредитной карты и т. д.), заражение компьютера или списание денежных средств пользователя (при отправке SMS на короткий номер и т. п.).

Основные виды сетевого мошенничества:

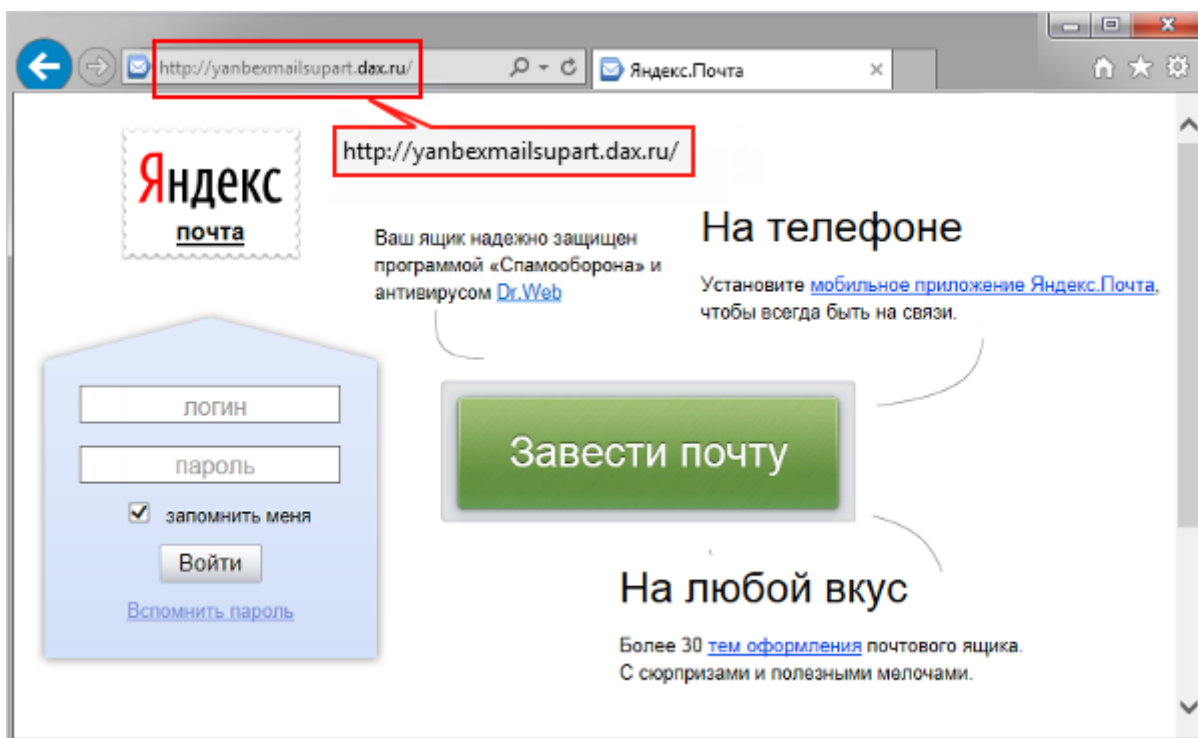
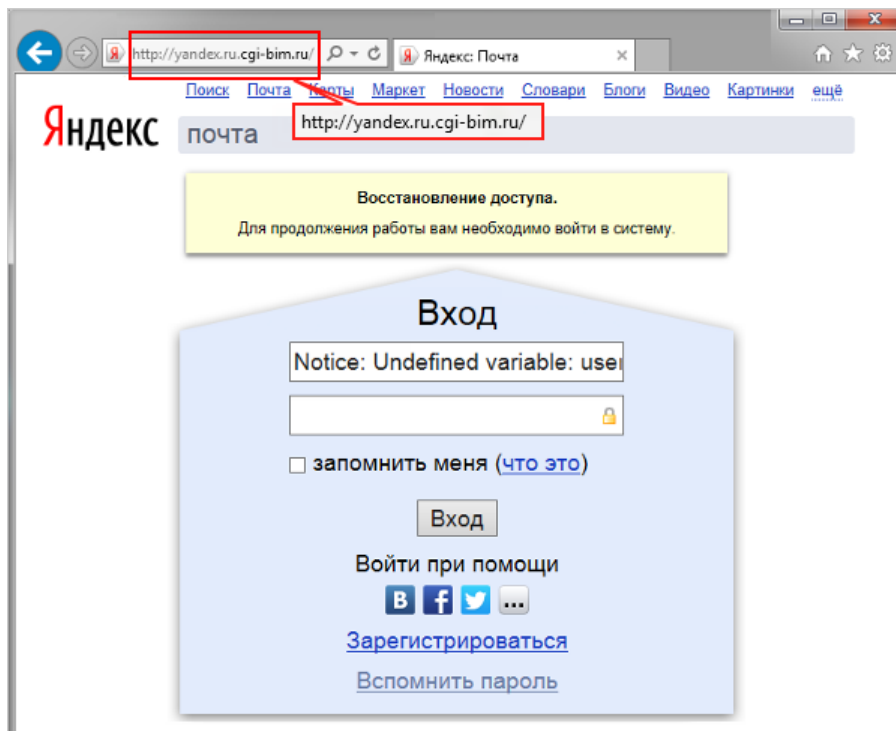
- **Фишинговые письма** — массовые рассылки от имени компаний, сервисов, социальных сетей и т. п. с уведомлениями о событиях, в связи с которыми пользователь должен предоставить, обновить или подтвердить свои конфиденциальные данные.

Например:

- Подтверждение учетных данных, проблемы с доставкой или сбой в системе. В письме вас попросят указать ваш логин и пароль к данному сервису или сайту. Чаще всего в поле От кого у таких писем указывается Служба поддержки, support или admin. Сотрудники Яндекса никогда не попросят вас прислать ваши авторизационные данные.
- Подтверждение личности или активация почтового ящика. Для этого вас попросят отправить SMS на короткий номер. Стоимость отправки SMS на короткий номер обычно выше стоимости SMS по вашему тарифу — но эта информация может быть не указана вообще либо приведена в той части письма, где ее сложнее всего заметить. В результате сразу после отправки сообщения на короткий номер с вашего телефона списывается некоторая сумма, чаще всего 100–200 рублей. В ряде случаев может включиться ежедневное списание денежных средств с вашего телефона. Яндекс никогда не просит отправить SMS — он может прислать его со своей стороны. Отвечать на это SMS не нужно.
- Участие в розыгрыше призов. Для этого вам предложат заполнить анкету, в которой, помимо фамилии, имени, отчества и контактных телефонов, нужно указать паспортные данные и номер кредитной карты. Если вы получили письмо о проведении Яндексом розыгрыша призов, свяжитесь с нами по контактам, указанным на странице <http://company.yandex.ru/contacts> и уточните информацию. Если розыгрыш действительно проводится, убедитесь, что вас не просят заранее оплатить доставку приза или сделать взнос за участие — Яндекс никогда не предлагает оплачивать то, чего вы не заказывали сами.

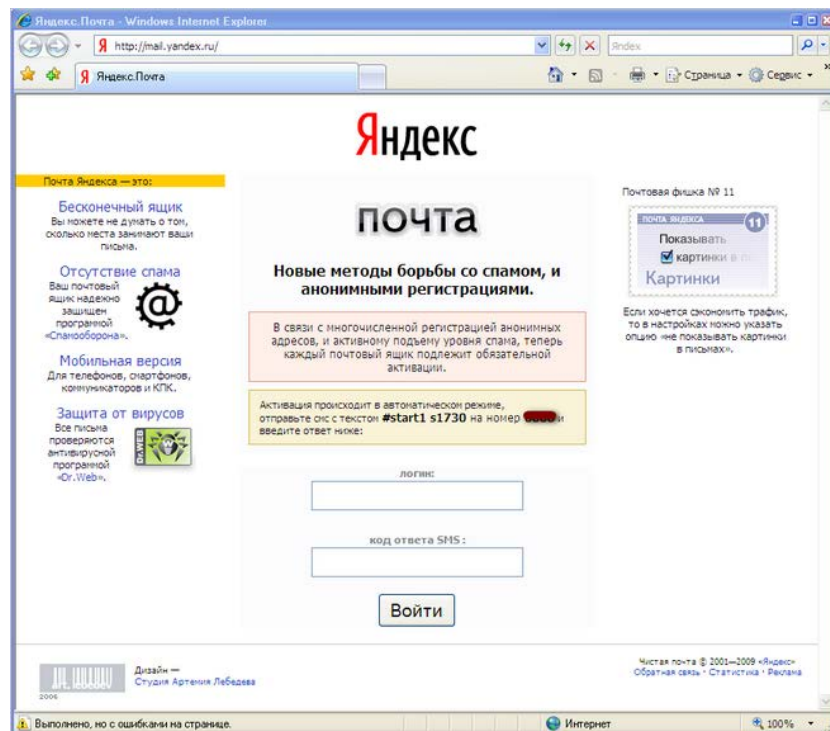
- **Фишинговые ссылки** — ссылки для перехода на поддельную страницу сайта. Если пользователь вводит свои данные на такой странице, мошенники легко получают к ним доступ. При авторизации на Яндексе убедитесь, что адрес сайта имеет вид имя.yandex.ru/раздел. После yandex.ru обязательно должен находиться символ /, а не точка.

Например:



- **Подмена сайта** — механизм скрытого автоматического перенаправления пользователей на поддельные сайты с помощью вредоносных программ. Пытаясь зайти на популярный сайт, пользователь попадает на сайт-подделку, очень похожий на оригинал, и вводит данные своей учетной записи, которые попадают к злоумышленникам. Действие вируса может проявляться другим образом: при регистрации или авторизации на сайте вам предложат подтвердить свои данные с помощью SMS.

Например:



Как бороться с вирусами подмены сайтов ([алгоритм действия на сайте ЯндексПомощь](#)).

- **Мобильное мошенничество** — телефонные звонки или SMS злоумышленников от имени банка или платежной системы с просьбой предоставить конфиденциальную информацию и т. д. Причины для предоставления данных могут называться самые разные: истекший срок действия пароля, блокировка карты, поломка в системе, потеря данных, крупный выигрыш и другое.
- **Неявное разглашение паролей.** Примеры: вы сообщаете пароль во время телефонного разговора, который слышит кто-то еще, или открыто вводите пароль или PIN-код при свидетелях.
- **Предложение участвовать в мошенничестве:** обмануть банк или платежную систему, заработать без вложений, получить доступ к чужим SMS и т. д.

Как защититься от сетевого мошенничества?

1. Используйте и периодически обновляйте лицензионные антивирусные программы.
2. Настройте защиту электронного почтового ящика (отключите предварительный просмотр писем).

3. Не открывайте и не загружайте вложения и не переходите по ссылкам из электронной почты или программ для обмена сообщениями (Skype, ICQ и т. п.) от незнакомых и сомнительных адресатов.

4. Внимательно просматривайте все входящие письма и проверяйте адреса ссылок — фишинговые ссылки зачастую содержат бессмысленный набор символов или опечатки.

5. Не отправляйте SMS на подозрительные незнакомые номера.

6. Никогда не оплачивайте покупки или счета, в которых вы не уверены.

7. Никому не передавайте ваши пароли, PIN-коды и другую конфиденциальную информацию.

8. Избегайте неявного разглашения паролей, например, сообщать пароль во время телефонного разговора, который слышит кто-то еще, или открыто вводить пароль или PIN-код при свидетелях.

9. Не оставляйте без присмотра и не выбрасывайте носители, на которых хранятся пароли: бумаги, компьютеры, телефоны, SIM-карты, flash-карты и т. п.

10. Не используйте простые пароли и контрольные вопросы, ответы на которые легко найти или угадать.

Что делать, если вы стали жертвой мошенников?

- Если с вашего счета незаконно списали денежные средства, позвоните в свой банк, чтобы срочно заблокировать карту, и обратитесь в полицейский участок.

- Если вы отправляли SMS на короткий номер, указанный мошенниками, обратитесь с запросом на возврат денег к своему мобильному оператору или в компанию, обслуживающую данный короткий номер.

- Если вы перешли по фишинговой ссылке, проверьте ваш компьютер на вирусы с помощью бесплатных антивирусных программ.

- Если вы ввели пароль на поддельной странице, обязательно смените его, а также измените секретный вопрос и ответ на него. Эти данные лучше менять после проверки на вирусы.

II. Безопасный Интернет для детей и подростков

Как показывают исследования Фонда Развития Интернет, современные школьники почти в **два раза чаще, чем взрослые**, пользуются Интернетом и быстрее осваивают новые цифровые технологии. От этого часто приходит чувство уверенности и самостоятельности, безусловно, полезное, но в некоторых случаях – опасное. Дети и подростки находятся в группе риска при использовании информационных технологий. Высокий уровень онлайн-активности и чрезмерная самоуверенность в своих силах притягивают проблемы. В Сети ими могут быть онлайн-мошенничество, преследования, унижения, оскорбления, шантаж. Это лишь небольшой список неприятностей, с которыми может столкнуться ребёнок.

Онлайн-активность российских школьников (2016 г.)



Количество детей с высоким уровнем интернет-активности увеличилось в два раза, по сравнению с 2013 г.
Если в 2013 году треть жизни в Сети проводил каждый седьмой подросток, то в 2015-2016 гг. - почти каждый третий (32%).

(Слайды здесь и далее взяты из презентации Солдатовой Галины (член-корр.РАО, д.псих.наук), «Цифровое детство: новые риски и безопасность» (07.02.2017, Digital October)).

К сожалению, большая часть этих проблем пока не имеет эффективных технических решений, а школьники (особенно подростки) предпочитают самостоятельно решать свои проблемы в Интернете и крайне редко обращаются за

советом к взрослым - стремятся сохранить свою независимость в «цифровом мире», боятся быть наказанными и не очень-то верят, что их «предки доцифровой эры» смогут понять их и помочь.

Но они остаются детьми и всё равно нуждаются в помощи и поддержке. В такой ситуации родителям стоит первыми прервать затянувшееся молчание и поговорить с детьми об Интернете. Главная и самая надёжная защита от онлайн-угроз - это доверие между детьми и родителями.



Вызовы родителям: индикаторы низкой цифровой компетентности

90% родителей не знают о средствах технического контроля за безопасностью ребенка

90% родителей не интересуются, что за программное обеспечение стоит на компьютере ребенка

92% родителей не могут помочь детям при решении всех проблем в Сети

46% родителей чувствуют себя неуверенными интернет-пользователями

84% детей не обращаются за помощью к родителям

Каждый третий родитель не знает о проблемах ребенка в Интернете

Каждого пятого родителя пользоваться Интернетом научили дети

Более половины детей не считают полезной помощь родителей

Проблема ещё в том, что родители и учителя часто чувствуют себя «не продвинутыми», не находят времени и слов, чтобы поговорить об Интернете с детьми. Иногда это происходит от занятости, иногда от невысокой цифровой грамотности. Часто это выливается в тотальные запреты, драконовские ограничения и т.д. Но полностью оградить ребенка от Интернета сегодня так же реально, как и от остальной окружающей среды. Проще научить его основам безопасности в Сети - чтобы ребёнок мог спокойно пользоваться теми уникальными возможностями, которые современные технологии представляют для общения, обучения и развития.

Современные школьники воспринимают Интернет не как набор технологий, а как среду обитания



Если родители и дети, а также учителя и ученики доверяют друг другу, действуют вместе в Сети, не боятся проговаривать острые моменты, то это лучшее средство повышения цифровой грамотности и профилактики онлайн-рисков.

Векторы эволюции онлайн-рисков



Риски в Сети

Риски в Сети для детей те же, что и для взрослых (см. часть I. «Интернет-безопасность для взрослых»). Но к ним прибавляется ещё понятная наивность, связанная с возрастом, к тому же, навык самоконтроля в подростковом и детском возрасте развит плохо.

1. Коммуникационные риски. Возникают при общении людей в Интернете. В их числе кибертравля, сексуальные домогательства, нежелательные знакомства в Сети, встречи с интернет-знакомыми в реальной жизни и др. С подобными рисками можно столкнуться при общении в онлайн-мессенджерах, социальных сетях, на сайтах знакомств, форумах, блогах и других ресурсах.

2. Контентные риски или риски получения информации. Возникают при столкновении с противозаконной, неэтичной и вредоносной информацией в сети (тексты, картинки, аудио- и видеофайлы, ссылки на различные ресурсы). К такой информации относятся: агрессия, эротика или порнография, нецензурная лексика, информация, разжигающая расовую ненависть, пропаганда анорексии, булимии, суицида, азартных игр, наркотических веществ. Подобный контент можно встретить на различных сайтах и в социальных сетях.

3. Потребительские риски. Возникают в процессе приобретения товаров и услуг через Интернет. В их числе риск купить товар низкого качества, подделки, контрафактную и фальсифицированную продукцию; потерять денежные средства или стать жертвой мошенников, использующих персональные данные онлайн-покупателей.

4. Технические риски. Опасность повреждения программного обеспечения компьютера, хищения или нарушения конфиденциальности личной информации посредством взлома с использованием вредоносных программ (вирусы, черви, троянские кони, шпионские программы, боты и др.).

5. Появление интернет-зависимости

Как защитить ребёнка от рисков в Сети, общие рекомендации:

1. Вкладывайтесь в доверие между вами и ребенком. Важно, чтобы ребёнок чувствовал: ваша цель **не наказать, а помочь ему**, в этом случае он сможет

вам довериться. Не стоит нагнетать страх перед чем-то непонятным и опасным в Сети – пусть ребёнок чувствует вашу уверенность, что вы можете объяснить ему правила поведения в этом «мире»;

2. **Установите правила пользования Интернетом для всех электронных устройств.** Необходимо прийти к соглашению по следующим вопросам: что разрешено делать в Сети? Где можно пользоваться мобильными устройствами? Когда и сколько времени можно проводить в Интернете?

3. **Регулярно разговаривайте с ним, в том числе об Интернете.** Расскажите ребенку об основных угрозах, с которыми он может столкнуться в Сети. Точная и достоверная информация — лучшее средство от онлайн-рисков.

4. **Будьте в курсе событий ребенка в реальной жизни и виртуальном пространстве.** Искренне интересуйтесь активностью ребенка в Интернете. Попросите его помочь вам завести аккаунт в социальной сети или игре, где он «обитает». Расскажите о нормах онлайн-этикета. Как и в реальной жизни, в Интернете надо вести себя вежливо и дружелюбно. Ребёнок должен понять, что анонимность в Сети — иллюзия, и любое действие навсегда оставляет свой след.

5. **Объясните необходимость защиты личной информации.** Любая личная информация, которую ребенок выкладывает в Сеть, может быть использована против него. Расскажите ему про средства защиты персональных данных, помогите установить настройки приватности на всех посещаемых ресурсах.

6. **Расскажите, где можно получить помощь.** Если ребёнок столкнётся с проблемой в Сети, он может обратиться к вам, к администрации сайта, в службу техподдержки и получить помощь. Важно проговорить это на начальных этапах, чтобы в случае наступления проблем, ребёнок знал, что делать.

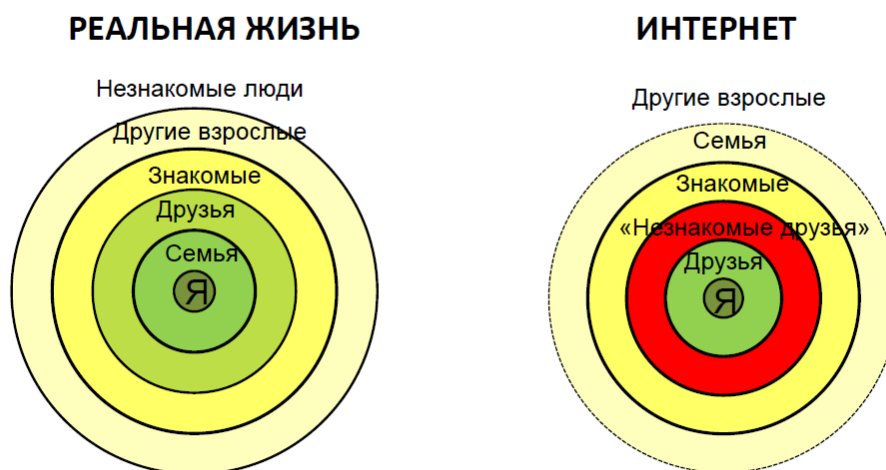
7. **Станьте для ребенка примером онлайн-пользователя.** Повышайте свою цифровую компетентность и старайтесь сами соблюдать правила, которые установили для детей.

1. Коммуникационные риски в Сети

Социологи и психологи сходятся во мнении, что главное нововведение эпохи, изменившее наше поведение, конечно, социальные сети — это **гигантские и глобальные коммуникативные площадки**. Они информируют, объединяют людей по всему миру, стирают культурные барьеры, помогают найти единомышленников, получить поддержку, то есть, делают доступным многое, о чём можно было только мечтать. Но обратная сторона доступности — **уязвимость**. В социальном сетевом взаимодействии рождаются жутковатые на вид, уродливые или просто навязчивые формы поведения, психологического прессинга контроля и вторжения. Коммуникация в интернете может выглядеть неприятно и раздражающе, а может и нести угрозу состоянию психики.

По статистике Фонда Развития Интернет более 80% российских школьников в возрасте от 12 до 17 лет пользуются социальными сетями. По данным исследований Фонда 88% детей в возрасте 11-12 лет уже имеют свой профиль в социальной сети.

Личное онлайн пространство ребенка: семья «за кадром»



В Интернете в зоне личного пространства остаются лишь ДРУЗЬЯ. Знакомые уступают место «виртуальному», «незнакомому другу», а семья (родители) и профессиональная помощь (педагоги) остаются «за кадром».

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. Примерами таких рисков могут быть: незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др. Для подобных целей используются

различные чаты, онлайн-мессенджеры (Google talk, Skype и др.), социальные сети, сайты знакомств, форумы, блоги и т.д. Каждый третий ребенок время от времени ищет новых друзей в Интернете, каждый пятый - отправляет незнакомым людям персональную информацию. Более половины детей добавляют в список друзей людей, которые НИКАК не связаны с их реальной жизнью.

Оказаться жертвой намного проще, чем кажется. Любому участнику социальной сети хотя бы раз приходило непристойное предложение от неизвестного человека. Это беда не только социальных сетей. На любом популярном форуме, в блогговом сообществе и чате есть такие участники, которые хамят и оскорбляют других участников («тролли» и т.д.).

Троллинг

Эта социальная провокация — подцепить, заставить спорить с заведомо абсурдной позицией, пытаться защитить и оправдать здравый смысл — одна из самых знаменитых стратегий психологической атаки в интернете. На первый взгляд, она годится разве что для подростков. Но увлеченность троллингом переживают и люди куда старше, давно преодолевшие школьный возраст. Его стратегии варьируются от изящного до «толстого», в зависимости от задач и умений агрессора.

Незаконный контакт — это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка. Это понятие включает в себя такие интернет-преступления как груминг, секстинг, etc. Например, **груминг** — установление дружеских отношений с ребенком с целью домогательства, **секстинг** – пересылка личных фотографий, сообщений интимного содержания посредством современных средств связи. Злоумышленник нередко общается в интернете с ребенком, выдавая себя за ровесника либо ребенка немного старше. Он знакомится в чате, на форуме или в социальной сети с жертвой, пытается установить с ним дружеские отношения и перейти на личную переписку. Общаюсь лично («в привате», «в личке») он входит в доверие к ребенку, пытается договориться о встрече.

Кибербуллинг (кибертравля) — намеренное и регулярное причинение вреда (запугивание, унижение, травля, физический или психологический террор) одним человеком или группой людей другому человеку с использованием электронных форм контакта. Каждый четвёртый российский школьник ежегодно сталкивается с

унижением, оскорблениями или преследованием в Сети.

Сам феномен **травли**, или **буллинга**, возник задолго до эпохи соцсетей. Его определяют как физический или психический террор со стороны группы, преследование ею одного из участников. Если в мягких случаях буллинг понижает эмоциональный фон жертвы и ее самооценку, то в жестких способен довести до суицидальных действий. При этом травля не всегда представляет собой прямую атаку. Стратегии группы в нападении могут быть разными: от сплетен и оскорблений за спиной до бойкота. Задача — привести жертву к потере уверенности в себе, деморализовать, получить чувство собственного превосходства, отделиться от жертвы, выставив ее неполноценной.

Для насмешки и унижения может быть выбрана практически любая, с точки зрения агрессора, унижительная, не нейтральная особенность жертвы: возраст, рост, внешний вид, национальность, место жительства. Точкой приложения для буллинга может быть что угодно, а может быть и ровное место. Бывает, что атакующие создают поддельные профили жертвы, «позорящие ее», жертве присылают фотографии оскорбительного содержания и так далее: от всего этого нападающие получают эмоциональное удовлетворение. Буллер может также взломать профиль или страницу жертвы и организовать спам-рассылку по всем контактам жертвы.

Также можно упомянуть о такой опасности соцсетей, как ответственность за размещение на своей странице информации. Чаще всего в таких делах идёт речь о призывах к сепаратизму и экстремизму. Законодательство не разделяет ответственность за оригинальную публикацию и репост. Запись появилась в блоге или на странице — и вы уже к ней причастны. Наказанием могут стать как денежные штрафы, так и лишение свободы.

Взрослый человек (и то не всякий) знает, что такая возможность существует. Но ребёнок искренне считает сетевую жизнь игрой, которую можно остановить в любой момент. Между тем, в случаях, когда малолетний совершает то, что закон считает правонарушением, взрослым приходится расплачиваться — в прямом смысле. То есть, выплачивать материальные компенсации. С того момента, как он научился пользоваться компьютерной мышью, ребёнку нужно знать, что он несёт ответственность за семью.

Если же подросток искренне и последовательно проводит в жизнь какую-то политическую позицию, не стоит обесценивать его точку зрения, даже если она кажется плодом юношеского радикализма. В этом случае он скорее найдёт поддержку у людей, которые вам не понравятся. Постарайтесь спокойно разобраться, что именно волнует

вашего ребёнка, и заключите пакт о том, что до совершеннолетия он будет заниматься только теоретическим изучением разных точек зрения, чтобы более взвешенно сформировать свою.

1.1. Кибербуллинг: как помочь ребёнку?

Многие родители опасаются, что в сети на связь с ребенком выйдет опасный взрослый, но такие случаи происходят куда реже, чем издевательства детей и подростков друг над другом. В эмоциональном смысле кибербуллинг ничем не отличается от травли реальной — жертва ощущает себя абсолютно такой же несчастной и подавленной.

К сожалению, кибербуллинг — очень распространенное явление среди российских подростков. Существует много его форм и видов (см. **Приложение «10 форм кибербуллинга»**). Каждый пятый ребенок подвергался буллингу онлайн или в реальной жизни. Нередко кибербуллинг берет начало в отношениях с реальными людьми, и в этом случае, жертва знает своих оскорбителей. Когда же буллинг берет свое в интернете, всегда важно удостовериться, чтобы он не перерос в реальное насилие над ребенком.

Основные исследования буллинга направлены на анализ ситуации в подростковой среде. Считается, что именно подростки (достаточно вспомнить фильм «Чучело») — наиболее уязвимая аудитория. Большая эмоциональная чувствительность и меньшая критичность повышают риски встать в позицию того, кто травит, и не найти выхода из позиции жертвы. Но, по сути, травля не обязательно оказывается проблемой только несовершеннолетних. И подростков, и взрослых стоит учить тому, что в интернете есть несколько возможностей для спасения: во-первых, **постараться дистанцироваться от болезненного треда**, если есть возможность (удалить переписку, выйти из сообщества). Во-вторых, в случае кибербуллинга полезно **делать скриншоты, сохранять переписку, предавать агрессию огласке, жаловаться в техническую поддержку соцсети**. И всегда важно сохранять долю критичности по отношению к происходящему, произносимому атакующими, хотя порой это очень сложно.

Тревожные сигналы:

- **Беспокойное поведение.** Даже самый замкнутый школьник будет переживать из-за происходящего. Депрессия и нежелание идти в школу — часто самые явные признаки того, что ребенок подвергается агрессии.

- **Неприязнь к Интернету.** Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.
- **Нервозность при получении новых сообщений.** Негативная реакция ребенка на звук уведомлений о новых сообщениях должна насторожить родителя.

ЧТО ДЕЛАТЬ, ЕСЛИ РЕБЕНОК СТАЛ ЖЕРТВОЙ КИБЕРБУЛЛИНГА/БУЛЛИНГА?

1. Сохраняйте спокойствие сами и успокойте ребёнка, не добавляйте ему негативных ощущений своей повышенной эмоциональной реакцией. Прежде всего, следует донести, что ребенок вам дорог, что вы его принимаете, каким бы он ни был, и волнуетесь о нем. Сейчас ему особенно важно знать – что бы ни произошло, что бы он ни натворил, вы все равно будете рядом с ним и на его стороне;
2. Избегайте необдуманных действий. Дайте ребёнку понять, что владеете ситуацией, готовы помочь и не станете его ругать или осуждать. Избегайте двойных стандартов: если вы заверили ребенка в том, что вы на его стороне, следуйте этому до конца.
3. Разберитесь в ситуации вместе с ребёнком. Не стоит смягчать инцидент, не надо говорить, что бывают вещи и страшнее, потому что сейчас для ребенка нет ничего хуже того, что произошло. Будучи в стрессе, он не может философски посмотреть на проблему, поэтому дайте ему знать, что вы прекрасно понимаете, насколько серьезна его ситуация, насколько его боль оправдана.
4. Важно найти ответы на вопросы: когда возник конфликт? Что стало причиной? Кто принимает участие в травле? Существует ли угроза здоровью или жизни ребёнка?
5. Соберите доказательства травли.
6. Сохраните все возможные свидетельства происходящего (скриншоты экрана, электронные письма, фотографии и т.п.).

7. Научите правильно реагировать на агрессора. Лучший способ остановить травлю - игнорировать обидчиков, или вытащить их «на свет божий», прямо назвав вещи своими именами (на собрании класса, или ещё на какой-то значимой площадке). Помогите ребенку заблокировать агрессоров или добавить их в «чёрный список». Иногда стоит временно удалить аккаунт на тех ресурсах, где происходит травля (сменить электронные контакты, завести новый email, Skype, учетную запись VK, новый номер мобильного телефона).
8. Обратитесь за помощью, жертве кибербуллинга трудно постоять за себя.

Если травля происходит в открытом сообществе или группе, обратитесь к администраторам ресурса с просьбой **заблокировать аккаунты обидчиков**, прикрепите **скриншоты со свидетельствами кибербуллинга**. Оповестив администрацию ресурса о киберхулигане, можно обезопасить от него и себя, и других пользователей. Если в травле участвуют ученики школы, **расскажите о ситуации классному руководителю, школьному психологу, завучу, директору**.

Если существует угроза здоровью и жизни ребёнка, обратитесь в **правоохранительные органы, приложив к заявлению собранные доказательства**.

Предупреждение кибербуллинга

Важно помнить, что агрессоров всегда больше, чем жертв, и ваш ребенок может оказаться как среди вторых, так и среди первых.

- Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости так же неприятно, как и слышать;
- Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же (см. [Кибербуллинг](#) : (советы для родителей) от Лаборатории Касперского)
- Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз;
- Старайтесь следить за тем, что ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

1.2. Рекомендации по предупреждению встреч с незнакомцами, груминга, секстинга

Познавательный интерес подростков к вопросам секса — возрастная норма. В Интернете этот интерес может эксплуатироваться злоумышленниками.

Меры предосторожности:

1. **Напоминайте о принципе «доверяй, но проверяй».** При общении в Сети никогда нельзя быть уверенным, кем на самом деле является собеседник. По ту сторону монитора может оказаться взрослый человек с преступными намерениями.
2. **Обсудите последствия.** Например, собеседник может разослать друзьям ребенка переписку или откровенные фото, опубликовать их в открытом доступе. Это способно нанести психологическую травму и навредить репутации ребенка.
3. **Расскажите, что не вся информация в Сети об отношениях, в том числе интимных, соответствует действительности.** Гармоничные отношения между людьми связаны с заботой и доверием, но в Сети тема любви часто представлена в искаженной, вульгарной форме. Отнеситесь к вопросам ребенка внимательно: лучше, если он получит эту информацию от вас, чем от незнакомца.
4. **Посещайте социальную сеть, в которой общается ребенок.** Обращайте внимание на тех, кого он добавляет в друзья. Появление взрослых незнакомцев — повод насторожиться.
5. **Не позволяйте ребенку ходить на встречи с незнакомцами одному.** Если виртуальный друг действительно доброжелательный, он с пониманием отнесется к такой предосторожности.
6. **Поощряйте и создавайте условия для позитивного общения в реальной жизни.**

2. Контентные риски

Столкновение с негативной информацией в Интернете может быть опасным для ребенка, в том числе в его образовательной деятельности. Потенциальный вред от встречи с опасным контентом и реакция на него зависят от разных, не всегда предсказуемых факторов - недостоверная информация встречается в любых сферах. Масса ошибок встречается в различных банках рефератов, которыми так любят пользоваться школьники и студенты.

Доверять в сети можно официальным энциклопедиям, словарям. Но, к примеру, в таком популярном ресурсе, как Википедия, доступ к редактированию статей имеет любой желающий – от научного сотрудника до учащегося начальной школы. Информация, опубликованная в ней, вполне может оказаться недостоверной.

2.1. Профилактика контентных рисков

Открытый и доброжелательный диалог – лучшее противоядие от контентных рисков. Помните, что даже постоянный контроль за действиями ребенка в Интернете и применение средств фильтрации никогда не дадут 100% гарантии защиты от негативной информации. Он может столкнуться с ней, выйдя в Сеть в гостях у друга, или найти самостоятельно. Будьте откровенны с ребенком, не бойтесь аккуратно и тактично спрашивать его об увиденном и прочитанном в Интернете, обсуждайте это вместе. Лучше, если ребенок получит грамотные комментарии от вас, нежели от сверстников или случайных знакомых.

Научите критично относиться к информации в Сети, объясните ребенку, что большинство информации, размещенной в Интернете, не может считаться правильной по умолчанию. Зачастую опубликованные материалы требуют проверки.

Обсудите правила, которые помогут школьнику оценить достоверность сведений (**См. также приложение «Достоверность информации в интернете»**):

Как оценить достоверность сведений в Интернете?

- *Если Вы что-то узнали в Интернете, найдите источник информации и её автора.*
 - *Следуйте правилу трех источников: прежде чем поверить в какой-либо факт, проверьте еще, как минимум, два источника информации.*
 - *Красиво сделанный сайт — еще не повод верить всему, что на нём написано. Важно понимать, с какой целью создан этот ресурс.*
-

- Если информацию сложно проверить или не удалось найти первоисточник, можно принять её к сведению, но распространять не стоит.

В учебные планы российских школ **медиаграмотность** пока не проникла. От нашего отношения к проблеме зависит формирование картины мира у наших детей. Важно открыто говорить о том, что информационная среда не всегда отражает реальное положение вещей. Существуют **памятки** для того, кто хочет проверить подлинность новости из интернета (конкретно эта взята из статьи Марии Лазаревой [«Учим детей не верить новостям в интернете: как выявлять фальшивые новости в интернете и почему важно научить этому детей»](#)). Она состоит из вопросов, которые нужно задать самому себе, когда появляются подозрительные новости:

<p>1. Вызывает ли новость сильные эмоции: страх, гнев или надежду, что новость правдива?</p>	<p>Если ответ положительный, то к содержанию новости стоит отнестись настороженно. Авторы фальшивых новостей стремятся играть на чувствах читателей и могут искажать или брать факты из воздуха для привлечения внимания аудитории.</p>
<p>2. Как вы нашли эту новость? Была ли она представлена на новостном портале, официальном сайте информационного агентства, или появилась в ленте социальных сетей?</p>	<p>Новость, появившуюся и размещённую на странице личного профиля или сообщества в социальной сети, необходимо проверить. Попробуйте связаться с автором новости, задать ему уточняющие вопросы в комментарии или личном сообщении. Проверяйте наличие одних и тех же фактов на нескольких порталах сразу. По возможности, проверьте также и зарубежные СМИ.</p>
<p>3. Проанализируйте заголовок</p>	<p>Используется ли эмоциональная пунктуация (!!!)? Используется ли CAPS LOCK при написании заголовка? Разоблачает ли заголовок некую тайну или заговор? Заканчивается ли заголовок «на самом интересном месте»? Прерывается ли фраза, есть ли недосказанность? «СЕНСАЦИЯ!!! ТО, О ЧЕМ МОЛЧАТ СПЕЦСЛУЖБЫ!!! Оказывается, если взять обычный фонарик...» Очевидно, что подобные заголовки — кликбейты. Те, кто действительно обладают секретными данными, вряд ли будут кричать об этом в интернете. Кликбейт (от англ. click — щелчок, bait — приманка) — способ построения заголовка, который допускает искажение смысла текста ради того, чтобы заинтересовать читателя и заставить его перейти по ссылке.</p>
<p>4. Присмотритесь к тексту.</p>	<p>В каком виде подана информация? Если текст написан нелитературным языком, в нём присутствует брань или неуместные шутки, то, скорее всего, в этой новости больше субъективного мнения, нежели фактов.</p>

	<p>Указана ли точная дата публикации новости? Обозначены ли хронологические рамки в тексте новости? В начале или в конце статьи обязательно должна стоять дата (для новостных порталов — и время) публикации статьи. Тело текста должно содержать чёткие хронологические рамки, то есть указывать, когда произошло описываемое событие.</p>
<p>5. Изучите ресурс</p>	<p>Известен ли сайт, где размещена новость? Можно ли положиться на него? Названия новостных порталов с уже сложившейся репутацией давно известны публике (ТАСС, РБК, ВВС, CNN, National Geographic и другие). Новостные порталы, информационные агентства, сайты телекомпаний и прочие источники могут быть достоверными в случае, если содержание статьи подозрения не вызывает.</p>
<p><i>Указан ли автор?</i></p>	<p>Можно ли связаться с автором и задать ему вопросы? Активен ли он в комментариях и ручается ли за предоставленную информацию? Авторы, особенно уже успевшие приобрести репутацию в профессии, не публикуются анонимно и готовы отвечать за информацию, которую они подают читателю. Связаться с автором можно через комментарии, по форме обращения, если такая предусмотрена на сайте, либо по электронной почте, если таковая указана. При первых сомнениях в правдивости новости, попробуйте связаться с автором или очевидцем описываемых событий: так вы точно будете уверены, что вас не пытаются обмануть.</p>
<p><i>Как давно ресурс предоставляет информацию?</i></p>	<p>Хороший сайт — это старый сайт. Имеется в виду не древний дизайн страницы и отсутствие оптимизации для мобильных приложений, а работа ресурса на протяжении долгого времени. Новые сайты-однодневки, которые появляются и исчезают, явно не заслуживают доверия. Дважды стоит подумать, если интернет-страница была заброшена на несколько лет, а потом неожиданно возобновила работу.</p>
<p><i>Как сайт позиционирует себя?</i></p>	<p>Страница информационного агентства явно выигрывает у интернет-журнала, который специализируется на светской хронике. Отраслевые страницы, публикующие новости в своей области, не будут обращать внимания на новости, выходящие за рамки их интересов. Практически у каждой страницы есть своя специализация, и при анализе источника важно понять, что это за сайт — жёлтые СМИ, новостной портал или радикально левая интернет-газета.</p>
<p><i>Есть ли у сайта (или автора) стандарт оформления страницы? Выверена ли</i></p>	<p>На профессионально оформленных сайтах новость подаётся в стандартном формате, который</p>

<p><i>верстка, гармонично ли смотрится текст и иллюстрации?</i></p>	<p>доведен до автоматизма. Следовательно, если на сайте нет ошибок, то портал давно специализируется на подаче подобной информации, и ему есть основания верить. В обратной же ситуации, когда страница выглядит неопрятно, сделана будто впопыхах, то стоит насторожиться: возможно, вас пытаются накормить фейком.</p>
<p>6. Проверяйте источники</p>	<p>Не всегда стоит доверять новостям, которые распространились по множеству ресурсов. Новостной агрегатор Яндекса тоже ошибается.</p>
<p><i>Есть ли ссылки на источники, официальные документы или статистические данные?</i></p>	<p>Когда автор приводит статистические данные с точными цифрами, то на эту информацию должны быть предоставлены ссылки. Мифические «британские ученые» или «эксперты в области...» без указания на конкретные исследования остаются только в анекдотах. Передача информации должна быть конкретной и точной.</p>
<p><i>Есть ли гиперссылки на конкретную информацию? Не вырваны ли данные из контекста?</i></p>	<p>Описание случая, свидетелем которого не был сам автор, также должен опираться на источник, причём информация должна соответствовать тексту статьи. Любимый прием лже-новостников — указать ссылку на стартовую страницу официального сайта уважаемого источника. Так можно ввести в заблуждение. Не давайте себя обмануть, обязательно проверяйте соответствие информации источнику.</p>
<p><i>Присмотритесь к изображениям. Поищите фотошопные «ляпы»</i></p>	<p>Отличить отредактированную картинку от оригинальной не так сложно, если речь идет о горячих новостях: слепленный впопыхах фейк будет содержать ошибки. Найдя их, вы сможете спокойно закрывать страницу — верить тому, что проиллюстрировано фальшивой картинкой, естественно, не стоит.</p>
<p><i>Проверьте, не «гуляет» ли картинка по сети</i></p>	<p>Поиск по Google-картинкам прост и понятен. Научитесь этому сами и объясните ребенку, как это делать. Попробуйте найти изображение из статьи на просторах сети и посмотреть, на каких сайтах оно успело засветиться. Если картинку используют с отличным от статьи контекстом, то это точно не репортаж с места событий.</p>
<p><i>Найдите подтверждение новости в других источниках</i></p>	<p>Новости, особенно о событиях в мире, разлетаются по сети моментально, и если события обсуждаются в нескольких источниках сразу, то им есть основания верить. Главное — определиться с порталами, которым стоит доверять (читаем пункт об анализе ресурса).</p>
<p><i>Проверьте подлинность информации на специальных сервисах</i></p>	<p>Проекты Fake News Watch (дозор фальшивых новостей) отслеживает сайты, на которых появляются фальшивые новости. Американская компания Poynter Institute создала свою сеть по проверке фактов International Fact-Checking</p>

	Network , на которых тоже можно проверить мировые новости в режиме онлайн.
--	--

3. Потребительские риски

По данным Фонда Развития Интернет, каждый десятый российский школьник сталкивался в Интернете с кражей денег, а каждый пятый - персональных данных. Для того чтобы не стать жертвой кибермошенников, следует соблюдать правила:

- **Никогда не отвечайте на сообщения, которые приходят от незнакомых людей.** Особенно осторожно следует относиться к письмам, которые приходят с неизвестных вам почтовых сервисов.

- **Если в письме вам сообщают о крупном выигрыше в лотерею, о том, что ваши близкие попали в беду, или о сборе средств на благотворительность, лучше всего такую информацию проверить с помощью другого канала информации, например, по телефону или через поисковик.**

(См. Приложение «Герои фишинга»)

- **Никогда не проходите по ссылкам, содержащимся в подозрительном сообщении, никогда не заполняйте формы во всплывающих окнах.** Если автор сообщения просит вас сохранить содержания письма в тайне или совершить определенные действия в сжатые сроки, скорее всего, это мошенничество.

- **Даже если в сообщении содержится персональное обращение или оно написано вашим другом или приятелем, это не повод доверять письму.** Личные данные можно украсть или подделать.

- **Если вам кажется, что вы стали жертвой интернет-мошенничества, поменяйте все пароли, свяжитесь с администрацией интернет-ресурса, на котором произошла кража личных данных, а лучше всего обратитесь к родителям, они наверняка помогут вам и подскажут, что нужно сделать.**

- **Никогда не пытайтесь бороться с мошенниками самостоятельно.** Зачастую мошенники - это взрослые опытные люди, они хорошо оценивают риски, на которые идут.

4. Технические риски

Исследования показывают, что практически каждый второй российский школьник сталкивается в Интернете с различными техническими рисками. Простые и эффективные правила интернет-безопасности позволяют избежать многих проблем, но, к сожалению, и дети, и взрослые часто о них забывают.

1) Защитите все устройства

Защитите надёжными паролями вход в компьютер и мобильные устройства. Научите ребёнка пользоваться этой функцией. Объясните ему, что пароль нужно держать в секрете даже от самых близких друзей. Для каждого устройства нужен свой пароль, который стоит регулярно менять.

2) Создайте отдельную учётную запись

Заведите для ребёнка на компьютере отдельную учётную запись без прав администратора. Это значительно снизит риск установки вредоносного программного обеспечения на компьютер и не позволит юному пользователю поменять настройки безопасности в браузере и операционной системе.

3) Антивирусная защита для всех устройств

Обязательно установите программу комплексной защиты компьютера. Не забывайте о том, что в защите нуждается не только компьютер, но и мобильные гаджеты - планшеты и смартфоны.

4) Регулярно обновляйте операционную систему и ПО

Всегда используйте лицензионное программное обеспечение. Регулярно обновляйте операционную систему, браузер и антивирусную программу.

5) Устанавливайте приложения для ПК и мобильного телефона только с надёжных ресурсов (см. приложение «Безопасность смартфонов и опасность бесплатного сыра»).

6) Сами избегайте подозрительных ссылок и баннеров

Объясните ребёнку, что не стоит кликать на незнакомые ссылки и яркие баннеры на сайтах. Гораздо безопаснее вводить адрес сайта самому или находить его через поисковые системы, а любимые сайты ребёнка, которые он посещает чаще всего, лучше добавить в закладки.

7) Используйте защищённые соединения

Подключаясь к Интернету через Wi-Fi, убедитесь, что используете безопасное соединение. Защитите домашнюю сеть надёжным паролем. Объясните ребёнку, что использование незащищённых сетей (в кафе, публичных местах и т.д.) может привести к потере персональных данных (*см. приложение «Безопасность смартфонов и опасность бесплатного сыра»*).

5. Интернет-зависимость

Чем больше у младшего школьника и подростка интересных дел, физической активности «в радость» и дружеских и прочих социальных связей в реальном мире – тем меньше у него шанс попасть как в интернет-зависимость, так и в прочие виды зависимостей. Общение с ровесниками – одна из определяющих форм деятельности в подростковом возрасте, и Интернет может помочь с этим, в таком случае, его роль положительная.

К сожалению, часто реальность поворачивается к детям в виде проблем в семье, огромного количества домашних заданий, неприятностей с учебой и одноклассниками. В таких случаях человек может легко «подсесть» на чувство мимолётного удовлетворения от бесконечного просмотра видео на YouTube, игр, сериалов, фильмов и получить [«лайк-зависимость»](#). То есть, в сумме у него появятся **симптомы Интернет-зависимости**.

В подростковой среде она чаще всего проявляется в форме увлечения компьютерными играми, играми на телефоне, навязчивой потребности к общению в чатах и социальных сетях, круглосуточном просмотре фильмов и сериалов в Сети.

Симптомы интернет-зависимости:

1. Потеря контроля над временем и поведением в Сети (выражается в длительном и бесцельном пребывании в Интернете).
2. Синдром отмены
3. Отсутствие доступа в Интернет вызывает плохое настроение, подавленность, агрессию, а также бессонницу, головные боли, потерю аппетита.
4. Замена реальности.
5. Пренебрежение семьей, учебой, друзьями, сном и питанием, личной гигиеной из-за постоянного пребывания онлайн.

При чрезмерной увлеченности Интернетом наблюдается нарушение биоритмов сна и бодрствования, хронический недосып, усталость; снижение волевого контроля, апатия; ухудшение успеваемости и отношений со сверстниками в реальной жизни, сужение круга общения, изоляция.

Профилактика интернет-зависимости:

1. **Придумайте общее дело в Интернете** - вместе с ребенком заведите блог, создайте веб-сайт, поиграйте в одну игру, поощряйте использование Интернета для творчества и учебы. Цифровые технологии должны объединять, а не разъединять вас.

2. **Приучите делать регулярные перерывы.** Если школьник провел за компьютером больше часа, полезно встать из-за стола, сделать разминку, гимнастику для глаз; также можно выйти на прогулку или устроить совместное чаепитие.

3. **Научите использовать Интернет эффективно.** Задайте ребенку вопрос: «Что ты собираешься сделать сегодня в Сети?» Запишите ответ на яркий листок и разместите его рядом с монитором. Устройство следует выключить, как только цель будет достигнута. Если ребенок теряет счет времени в Сети, предложите ему использовать таймер или будильник. Дети постарше могут подробно записывать, что они делают в Интернете, и сколько времени на это тратится. Это поможет осознать проблему пустой траты времени, избавиться от навязчивых действий (например, бездумное обновление странички или проверка смартфона).

4. **Исключите электронные технологии из системы «поощрение-наказание».** Лишение любимого устройства не снижает интерес к нему, но может вызвать раздражение и злость. Если ребенок провинился, следует объяснить, в чем он неправ, помочь исправить ошибку, привлечь к делам по дому. Это научит

ребенка воспринимать виртуальное пространство нейтрально, как одну из сфер жизни, а не как сверхценный объект, доступ к которому нужно получить любой ценой.

5. Не используйте планшет как «цифровую няню». Научите ребенка простым играм и занятиям, которые помогут ему скоротать время ожидания в перерывах между занятиями, в дороге и очереди без цифровых устройств и Интернета. Это снизит риск чрезмерной увлеченности онлайн-развлечениями в будущем.

6. Помогите ребенку найти себя вне виртуального пространства. Чем больше у ребенка интересных хобби, тем меньше времени на бессмысленное блуждание по Сети. Многие виды онлайн-активности имеют свои аналоги в реальной жизни. Например, если ребенку нравятся игры со сражениями, запишите его в секцию единоборств. Важно поддержать ребенка в его начинаниях, отмечать успехи в деятельности, не связанной с Интернетом.

Дополнительное чтение (приложения):

1. Игровая и/или интернет-зависимость.

[Статья Д. Вонга «Пять гадких способов, при помощи которых игры сажают вас «на иглу»/делают вас зависимыми»](#)

2. Фишинг.

[Статья «Герои фишинга»](#)

3. Достоверность информации в Интернете.

Статья Якушиной Е. В. (к.п.н, старший научный сотрудник лаборатории медиаобразования ИСМО РАО «Медиаобразование») [«Как проверить достоверность информации в Интернете?»](#).

4. Безопасность смартфонов и опасность бесплатного сыра.

[«У вас в смартфоне дыра. Как крадут деньги через смартфоны и что с этим делать»](#)

[«Мой телефон постоянно подключается к чужим вайфаям, это опасно?»](#)

5. Многоликий и мерзкий: буллинг/кибербуллинг.

[«10 форм кибербуллинга»](#)

[«Школа агрессии: исследователь Даниил Александров о подростковом буллинге и способах с ним справиться»](#)

Список использованной литературы и прочих ресурсов:

1. Поговорите с ребенком об Интернете : метод. пособие [Электронный ресурс]. – Режим доступа: <http://detionline.com/assets/files/mts/Pogovorite-s-rebenkom.pdf>
2. Солдатова, Г.У. Цифровое детство: новые риски и безопасность: доклад [Электронный ресурс] / Г. У. Солдатова // Роль библиотек, обслуживающих детей, в создании позитивного Интернета : всерос. видеоконференция, 3 февр. 2017 г. – Режим доступа: <http://psiholog-rmo.ru/wp/wp-content/uploads/2017/02/20170215-cifrovoe-detstvo.pdf>
3. Кибербуллинг : (советы для родителей) [Электронный ресурс] / Лаборатория Касперского. – Режим доступа: <https://www.youtube.com/watch?v=EY75xb2-yQo>
4. Дети в Интернете : образовательно-выставочный проект [Электронный ресурс]. – Режим доступа: <http://detionline.com/mts/about>
5. Безопасность в интернете : руководство Яндекс Помощь [Электронный ресурс]. – Режим доступа: <https://yandex.ru/support/common/security/security-intro.html>
6. Лазарева, М. Учим детей не верить новостям в интернете: как выявлять фальшивые новости в интернете и почему важно научить этому детей [Электронный ресурс] / М. Лазарева. – Режим доступа: <https://newtonew.com/school/detektor-lzhi-dlya-interneta>

Полезные ресурсы:

1. Информационный портал «Дети России Онлайн»

<http://detionline.com/>

2. Всероссийская Линия помощи «Дети Онлайн»

Служба телефонного и онлайн-консультирования, оказывающая психологическую и информационную поддержку детям и подросткам по вопросам безопасного использования Интернета и мобильной связи. Операторы Линии помощи - профессиональные психологи-эксперты Фонда Развития Интернет и факультета психологии МГУ имени М.В. Ломоносова.

Часы работы: с 9 до 18 часов в будние дни (перерыв с 13 до 14), звонок по России бесплатный. Обращения по электронной почте: helpline@detionline.com Онлайн чат: <http://detionline.com/>

3. Журнал «Дети в информационном обществе»

www.detionline.com/journal/

4. Материалы к урокам безопасного интернета с сайта «Лига безопасного интернета».

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

(Для проведения занятия в 1-4 классах мы рекомендуем использовать старую, анимированную версию презентации с сайта [«Лига безопасного интернета»](#) (она более интерактивная и дети её легче воспринимают), плюс к этому 1 серия словенского мультсериала «SheepLive» «Белые овцы»: [«Тайный друг»](#) (про общение с незнакомцами в Сети).

Информационное издание

Безопасный интернет для детей и взрослых

Методические рекомендации

[Электронный ресурс]

Вологодская областная универсальная научная библиотека
160000, г. Вологда, ул. М. Ульяновой, д.1; т/ф.8(8172)21-17-69