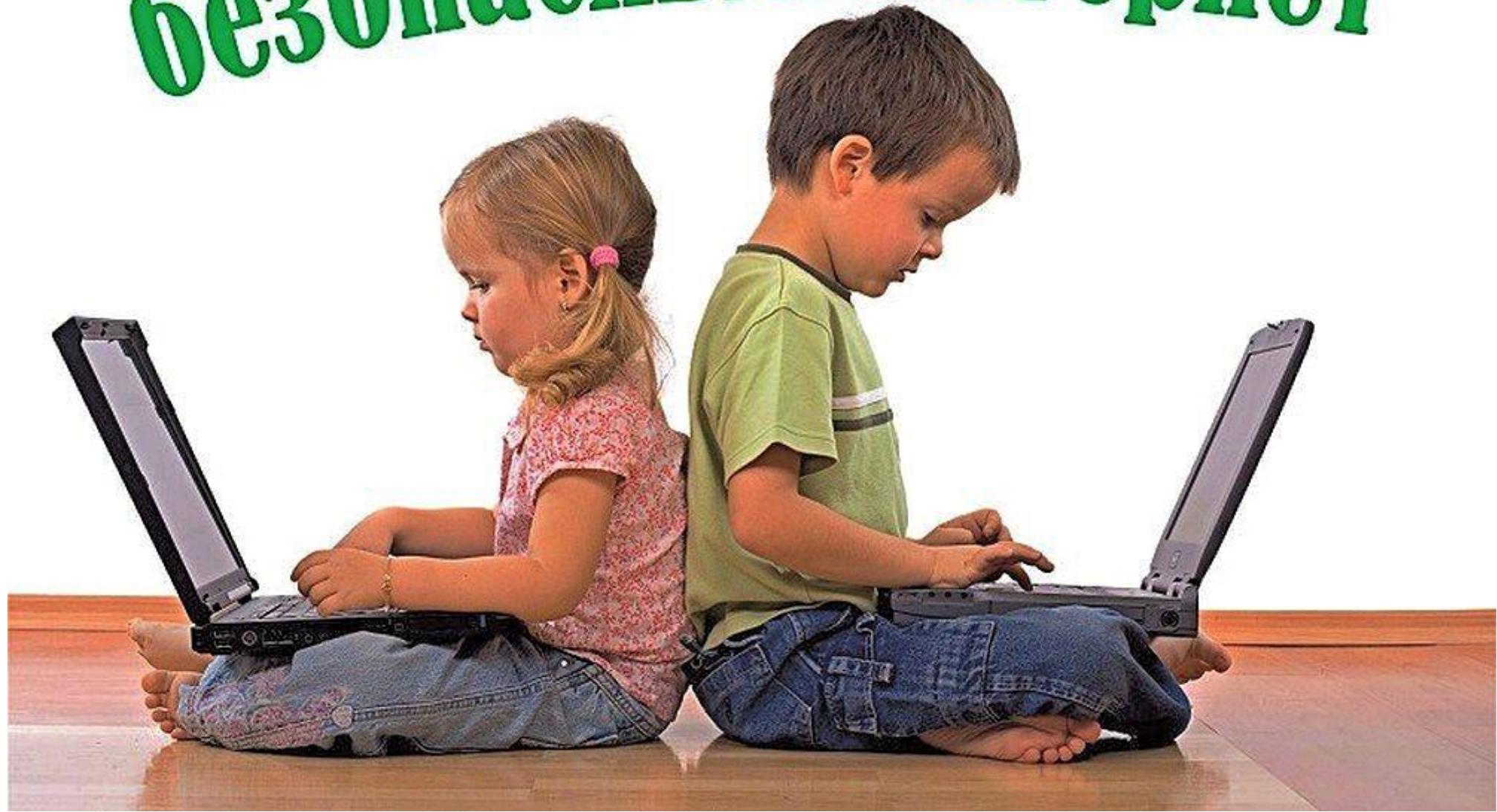


*нужен детям с ранних лет*  
**безопасный интернет**



Start

# Безопасный Интернет

	<p>С осторожностью добавляйте незнакомцев в «друзья» и отказывайтесь от личных встреч с людьми, с которыми вы познакомились в Интернете. Обязательно расскажите взрослым и своим друзьям о запросе на такую встречу. Виртуальные друзья могут на самом деле быть не теми, за кого они себя выдают.</p>		<p>Клевета, оскорбление, незаконное копирование продуктов труда других людей и другие противоправные действия, совершенные в виртуальном мире, влекут за собой реальное привлечение к административной, гражданской правовой или даже уголовной ответственности.</p>
	<p>Заведите отдельный почтовый адрес для регистрации в социальных сетях, форумах и прочих сервисах - придумайте к нему сложный пароль.</p>		<p>Относитесь с подозрением к сайтам, где запрашивают пароль, адрес, данные паспорта и т.д., просят прислать sms, фотографию, ввести номер телефона.</p>
	<p>Незнакомые сайты и письма от неизвестных адресатов могут содержать вредоносные программы.</p>		<p>Всё, что вы сообщите о себе в социальных сетях, чатах или форумах, может быть использовано с мошенническими намерениями.</p>
	<p>Оставляйте в сети минимум информации о себе и своих близких, используйте логины и сложные пароли - новые для каждого сайта - чаще их меняйте!</p>		<p>Помните, что в безопасных играх и квестах никогда не предлагается выполнять задания в реальной жизни или в ночное время. Избегайте таких игр.</p>
			<p>Подумайте прежде, чем разместить фотографии или рассказать о чем-нибудь в онлайн-среде. Фотография, размещенная несколько лет назад, может стать причиной отказа принять вас на работу в будущем.</p>
			<p>Если у вас есть вопросы по безопасности в сети Интернет, позвоните на телефон «горячей линии» 8 800 25 000 15</p>
			<p>Если у вас есть вопросы по безопасности в сети Интернет, зайдите на сайт «Дети России онлайн» <a href="http://www.detionline.com">www.detionline.com</a></p>

# ДЛЯ РОДИТЕЛЕЙ

Интернет это прекрасное место для общения, обучения и отдыха. Но стоит помнить, что как и наш реальный мир, всемирная паутина может быть весьма и весьма опасна. Приведем несколько рекомендаций, с помощью которых посещение Интернет может стать менее опасным для ваших детей:

## СТАНЬТЕ ПРОВОДНИКОМ РЕБЕНКА В ИНТЕРНЕТ

ТО, ЧЕМУ НЕ НАУЧИТЕ РЕБЕНКА ВЫ, НАУЧАТ ДРУГИЕ ИЛИ РЕБЕНОК САМ НАУЧИТСЯ, НЕ ПОДЗРЕВАЯ ОБ УГРОЗАХ. ПОТОМ ВАМ СЛЕДУЕТ Хорошо разобраться в интернете и помочь ребенку ЕГО ОСВАИВАТЬ.

### СПЕЦИАЛЬНЫЕ ПРОГРАММЫ И БРАУЗЕРЫ

Для предотвращения нежелательного контента и вирусов необходимо установить антивирус, настроить антиспам фильтры и почту помощью средств Родительского контроля или блокировщика. Установите ограничения времени, чтобы можно было создавать «тайм-апы» Интернет-сайтов, ограничить время пребывания ребенка в Интернете, настроить возрастной фильтр.

### КОНТРОЛЬ ВЗРОСЛЫХ

Говорите с ребенком об Интернете, спрашивайте, что он сегодня делал, с кем познакомился, с кем интересно учатся. Стремитесь регулярно проверять результаты, отображаемые в социальных сетях, учите ребенка, а проверяйте список его контактов, чтобы убедиться, что он знает, с кем общается.

### ПРАВИЛО: 13-6-9-12

3 – нечестного компьютера  
6 – игральных автоматов  
9 – нечестного Интернета до 9 лет  
12 – Интернета только с родителями

Такая простая инструкция, созданная психологами в стиле курса «Psychologs» (2011), учитывает возраст и особенности физического и психо-личностного развития ребенка.

### ПРЕДУПРЕЖДЕНИЕ – ЗНАЧИТ ВООРУЖЕН

Расскажите ребенку, что в Интернете встречаются и хорошие, и плохие люди. Объясните, почему не стоит добавлять в друзьях незнакомых людей – они могут быть не теми, за кого себя выдают. Предупредите ребенка, что он ни в коем случае не оставляется на «хвосте» встречи с Интернет-незнакомцем, прежде чем не поставит в курс ваших родственных связей. Предупреждите о склонности подростков к информации, обобщенной через веб. Объясните почему не стоит обращать внимание на края баннеров с сообщениями о выигрышах или призах.

# БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

РОССИЯ 12 млн.  
несовершеннолетних пользователей Интернета

1/3  
детей  
посещают  
Интернет  
вместе  
С РОДИТЕЛЯМИ

80%  
заявили, что знают,  
чем занимаются их  
РОДИТЕЛИ

31%  
уверены,  
что родители  
ДЕТЕЙ  
об этом ничего не знают

ДЕТИ  
7-14 часов  
ОНЛАЙН

14-12 часов  
21-18 часов

21-18 часов  
20%

80%  
имеют  
аккаунты  
детей

в социальных сетях

46%  
почти половина  
несовершеннолетних  
россиян старше 5 лет  
часто и портят  
пользуются Интернетом

По данным Фонда «Духовственный Рунет», 2011

10  
ЛЕТ  
средний возраст, с которого  
начинается самостоятельное  
использование социальных сетей

30%  
РОДИТЕЛЕЙ  
устанавливают  
специальные детские  
Интернет-фильтры

Где юные пользователи  
получают доступ  
в Интернет?

По данным Фонда «Духовственный Рунет», 2011

Количество пользователей  
Интернета детского возраста  
растет с каждым годом

Российские эксперты провели масштабное исследование под  
названием «Дети онлайн», в ходе которого выяснили некоторые  
интересные цифры и факты.

# ДЛЯ ДЕТЕЙ

Ни в коем случае не указывай  
свой номер телефона или  
электронный адрес, не  
отправляй с него смс на  
незнакомые номера в  
Интернете.

Если тебе пришло  
сообщение с  
незнакомого адреса,  
его лучше не  
открывать.

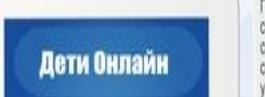
Не используй веб-камеру  
при общении с  
незнакомыми людьми.

Не вступай в незнакомые  
сообщества и не распространяй  
по чай-либо просьбе  
информационные,  
провокационные и  
агрессивно-настроенные  
материалы и сообщения.

Уважай собеседников в  
Интернете. Никогда и ни  
при каких обстоятельствах  
не угрожай другим, не  
размещай агрессивный и  
провокационный  
материал. Будь  
дружелюбен. Не губи.



Никому и никогда не разглашай свои  
пароли. Они – твой главный секрет.  
Придумай свой уникальный пароль, о  
котором никто не сможет догадаться. Не  
записывай пароли на бумажках, не храни  
их в открытом доступе. Не отправляй  
свои пароли по электронной почте.



Дети Онлайн

Линия помощи «Дети онлайн» –  
бесплатная всероссийская  
служба телефонного и онлайн  
консультирования для детей и  
взрослых по проблемам  
безопасного использования  
интернета и мобильной связи.



Интернет-ресурсы для школьника  
window.edu.ru  
Единое окно  
доступа к  
образовательным  
ресурсам  
school-collection.edu.ru  
Единая коллекция  
цифровых  
образовательных  
ресурсов

Автор плаката - Ольга Карленко

### Что включают в себя персональные данные?

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

фамилия, имя и отчество, дата и место рождения, адрес, семейное положение, паспортные данные, профессия, доходы и другая информация.

### Нормативно-правовая база по защите персональных данных:

#### ЗАКОНЫ

Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»

#### Постановления Правительства

№781 от 17.11.2007

№687 от 15.09.2008

Приказы и иные документы

«Приказ трех» от 13.02.2008

Методические материалы ФСТЭК

Приказ ФСТЭК №17



### Где существует наибольший риск потери персональных данных?

Цифровая кража смартфона

Социальные сети и мессенджеры



Электронная почта



Банковские данные



Аккаунты в игровых сервисах



Незащищённая

Мобильные приложения и игры

### ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ОБНАРУЖИЛИ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ИНТЕРНЕТЕ?



Написать жалобу



Владелец аккаунта  
Тех.поддержка сайта  
Администрация сайта



Когда невозможно установить источник распространения персональных данных или связаться с ним напрямую

Нужно обратится в прокуратуру или Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций

Подкрепите требования ссылками на нормы закона № 152 «О персональных данных», который запрещает использовать информацию без разрешения субъекта данных. Предупредите, что в случае отказа вы вправе обратиться в суд согласно статье 24 закона (ответственность за нарушение требований ФЗ № 152).

### ТОП-4 ОСНОВНЫХ СПОСОБОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1

Пароль

\* \* \* \* \*



Используйте двухфакторную аутентификацию

2



Контролируйте доступ приложений  
к вашим данным



3

Пользуйтесь менеджерами паролей

https://

4

Используйте только защищённое соединение

# Полистайте с пользой!



© Министерство образования и науки Алтайского края, 2017 г.  
© КГБУ «Алтайский краевой центр ППМС-помощи», 2017 г.