



**РОСКОМНАДЗОР**

**Виртуальная реальность.  
Основы безопасности детей в сети  
«ИНТЕРНЕТ» с использованием персональных  
данных**

Начальник отдела по защите прав субъектов персональных данных и надзора в сфере информационных технологий  
Управления Роскомнадзора по Дальневосточному  
федеральному округу - Ляшенко Олеся Викторовна

## **Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» определяет понятие «персональные данные»**

**Персональные данные** – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Специальные категории персональных данных:** расовая, национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимная жизнь.

**Биометрические персональные данные** - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

# ВИРТУАЛЬНЫЕ РИСКИ С ИСПОЛЬЗОВАНИЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

## Коммуникационные риски:

- Он-лайн знакомства (виртуальные знакомства на различных интернет-сервисах, предоставляющих пользователям услуги по виртуальному общению с другими пользователями, вторжение в частную жизнь).
- Киберпреследование (Киберсталкинг), троллинг — это использование Интернета для преследования или домогательств человека, группы людей или организации, провокации или издевательства в сетевом общении.

## Риски, связанные с нарушением безопасности

- Он-лайн мошенничество (фишинг (фарминг), вишинг, мошеннические интернет-магазины).
- Вирусы, программы – трояны и программы – шпионы, нежелательная почта (спам)

# ОН-ЛАЙН ЗНАКОМСТВА

**«груминг»** - установление дружеских отношений с ребенком с целью вступления в сексуальный контакт

В России проблема встречи с онлайн-незнакомцами остается одной из самых важных среди коммуникационных интернет-рисков. Половина российских детей постоянно знакомится в интернете с новыми людьми, а 40% детей признаются, что встречались с интернет - знакомыми в реальной жизни.

**ХИЩНИКИ** – это люди используют Интернет, чтобы заманить детей на личную встречу



## Правило № 1

Рассказывайте детям, что никогда не стоит встречаться с друзьями из Интернета, которых они не знают в реальной жизни. Ведь люди могут оказаться совсем не теми, за кого себя выдают.

# Киберпреследование (Киберсталкинг), троллинг

- **Киберсталкинг** — это использование Интернета для преследования или домогательств человека, группы людей или организации. Под него могут попасть ложные обвинения, сплетни и клевета. К киберсталкингу также можно отнести мониторинг, похищение личности, угрозы, вандализм, вымогательство секса или соби́рание информации, которая может быть использована для запугивания или домогательств. Киберсталкером может быть как человек незнако́мый, так и человек, знако́мый жертве. Он может анонимно вовлекать незнакомых людей онлайн.
- **Тро́ллинг** — форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации. Ближайшие понятия — это искушение, провокация и подстрекательство — то есть сознательный обман, клевета, возбуждение ссор и раздоров, призыв к неблагоприятным действиям.
- **Киберхулиганы** — и дети и взрослые могут использовать Интернет, чтобы изводить или запугивать других людей.

## Правило № 2

Объясняйте детям, что в он-лай среде встречаются такие же хулиганы, как и в реальной жизни. В случае проявления подобных действий необходимо сообщить взрослым или обратиться в правоохранительные органы. Вышеуказанные действия уголовно наказуемы.



## МОШЕННИЧЕСТВО В ОН - ЛАЙН СРЕДЕ

**Фишинг (Фарминг)** - это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям, доступ к аккаунтам и банковским счетам.

**Вишинг** - это один из методов мошенничества, целью которого является стимулирование к совершению определенных действий со своим карточным счетом / платежной картой.

**Мошеннические интернет-магазины** - сайт, торгующий товарами посредством сети Интернет. Как правило никакого товара после оплаты пользователь не получает, а сайт не существует.

### Правило № 3

Доводите до детей информацию об использовании и регулярном обновлении антивирусных программ.

Использование защиты электронного почтового ящика (отключить предварительный просмотр). Не открывать и не загружать вложения электронных писем от незнакомых и сомнительных адресатов.

Несанкционированный обмен музыкой, видео и другими файлами может повлечь загрузку вредоносных программ



# Вирусы, программы – трояны и программы - шпионы

- Вирусы и программы - черви – это программы, проникающие в компьютер для копирования, повреждения или уничтожения данных.
- Программы - трояны – это вирусы, имитирующие полезные программы для уничтожения данных, повреждения компьютера и похищение личных сведений.
- Программы – шпионы – это программы, отслеживающие ваши действия в интернете или отображающие навязчивую рекламу.



**Правило № 4** Установите на свои ПК защитное ПО (антивирус) и следите за регулярностью обновления антивирусных баз.

Нельзя запускать подозрительные приложения, присланные по электронной почте и через интернет-мессенжеры. Проверяйте адреса при переходе на сайты.



## Вторжение в частную жизнь

Заполняя различные формы в Интернете можно оставить конфиденциальные сведения о себе или своей семье → шантаж, вымогательство, запугивание



### Правило № 5

- Никогда не разглашайте в Интернете личную информацию, за исключением людей, которым вы доверяете. При запросе предоставления личной информации на веб-сайте всегда просматривайте разделы «Условия использования» или «Политика защиты конфиденциальной информации», убедитесь о целях использования ваших персональных данных.
- Не разрешайте ребенку предоставлять личную информацию через Интернет. В Интернете не вся информация надежна и не все пользователи откровенны.
- Ребенку нужно знать, что нельзя через Интернет давать сведения о своем имени, возрасте, номере телефона, школе или домашнем адресе. Научите ребенка использовать прозвища (ники) при общении через Интернет: анонимность – отличный способ защиты.
- Не выкладывайте фото ребенка на веб-страницах или публичных форумах.



**Риски, связанные с содержанием информации (контентные риски):  
нецензурные тексты, запрещенная информация, пропаганда экстремизма,  
нарушение авторских прав, пропаганда наркотиков .**

## **Защита детей от негативной и опасной информации в сети Интернет**

Безопасность в интернете и, в первую очередь, безопасность детей – это не только антивирусы, фильтры и профессиональная информационная безопасность. Наибольшую угрозу для детей представляет:

### **«негативный» контент**

Особенностью детского восприятия является абсолютное доверие детей к приходящей из интернета информации, контактам, коммуникациям. Россия, по сравнению со странами Евросоюза, входит в зону повышенного риска, определяемую остро стоящими вопросами обеспечения безопасности детей и подростков в глобальной сети. Больше 40% детей в России сталкиваются с изображениями сексуального характера в интернете или других источниках. И каждый шестой ребенок из них видит сексуальные изображения каждый день или почти каждый день, каждый пятый — систематически 1–2 раза в неделю.

# **Федеральный закон российской Федерации от 29 декабря 2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»**

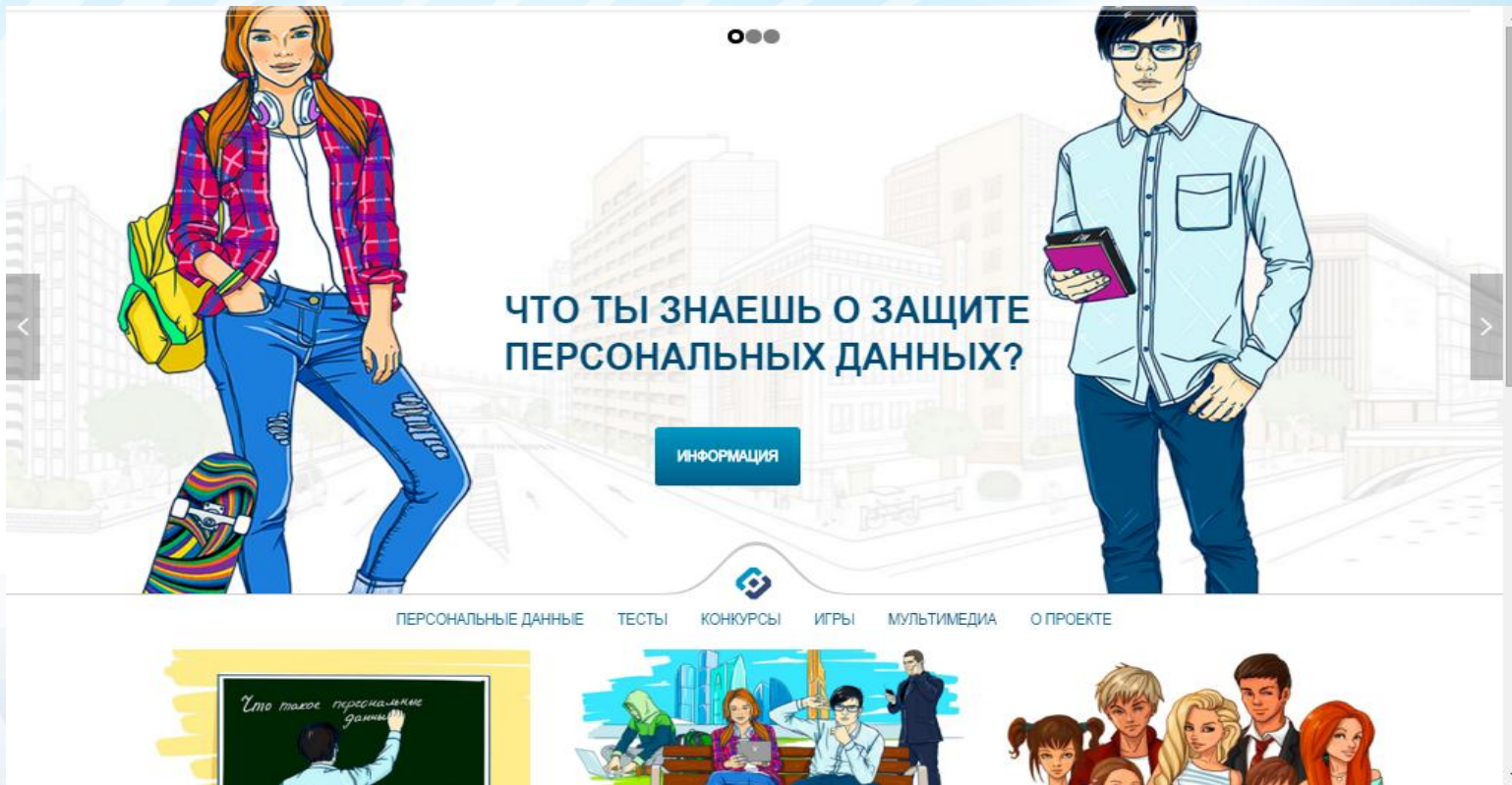
## **Информация, запрещенная для распространения среди детей**

- 1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- 2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- 3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
- 4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- 5) оправдывающая противоправное поведение;
- 6) содержащая нецензурную брань;
- 7) содержащая информацию порнографического характера.

**О нарушениях данного Федерального закона Вы можете сообщить следующим способом:**

На сайте **<http://eais.rkn.gov.ru>** Роскомнадзор принимает сообщения от граждан, юридических лиц, индивидуальных предпринимателей, органов государственной власти, органов местного самоуправления о наличии на страницах сайтов в сети Интернет противоправной информации  
**(вкладка «Прием сообщений»)**

# Портал «ПЕРСОНАЛЬНЫЕ ДАННЫЕ. ДЕТИ»



О

ЧТО ТЫ ЗНАЕШЬ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ?

ИНФОРМАЦИЯ

ПЕРСОНАЛЬНЫЕ ДАННЫЕ ТЕСТЫ КОНКУРСЫ ИГРЫ МУЛЬТИМЕДИЯ О ПРОЕКТЕ

Что такое персональные данные

Illustration of a girl with a yellow backpack and a boy with glasses holding a tablet, standing in a city street.

**СПАСИБО ЗА ВНИМАНИЕ!**

**Управление Роскомнадзора по  
Дальневосточному Федеральному округу**

**сайт: [27.rkn.gov.ru](http://27.rkn.gov.ru)**

**Контактная информация**

**Управление Роскомнадзора по Дальневосточному  
федеральному округу,**

**680000, г. Хабаровск , ул. Ленина, д. 4,**

**email: [rsockanc27@rkn.gov.ru](mailto:rsockanc27@rkn.gov.ru)**

**приемная: (4212) 35-82-70**

**Отдел по защите прав субъектов персональных данных и  
надзора в сфере информационных технологий  
35-82-78 (доб. 602, 603, 604)**