

Береги свои персональные данные!

 РОСКОМНАДЗОР

<http://персональныеданные.дети/>

 РОСКОМНАДЗОР

-  Фамилия, Имя, Отчество
-  Дата рождения
-  Место жительства
-  Номер телефона
-  Фотография
-  Электронная почта



ОБЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

 РОСКОМНАДЗОР

2

Категории персональных данных :

- Общие
- Специальные
- Биометрические
- Набор цифр

<http://персональныеданные.дети/>

Специальные категории персональных данных

К специальным категориям персональных данных относятся:

- *расовая или национальная принадлежность,*
- *политические взгляды,*
- *религиозные и философские убеждения,*
- *состояние здоровья и пр.*

Специальные категории персональных данных характеризуют наши взгляды, убеждения, мировоззрение, они определяют нашу принадлежность к определенным социальным группам, состояние здоровья. Данная категория персональных данных обрабатывается с письменного согласия, если иное не определено другими законами.

Биометрические персональные данные

Биометрические персональные данные представляют собой сведения о наших биологических особенностях. Эти данные уникальны, принадлежат только одному человеку и никогда не повторяются.

Биометрические данные заложены в нас от рождения самой природой, они никем не присваиваются, это просто закодированная информация о человеке, которую люди научились считывать.

<http://персональныеданные.дети/>

К биометрическим персональным данным относятся:

РОСКОМНАДЗОР

- Отпечатки папиллярных узоров пальцев
- Рисунок радужной оболочки глаз
- Термограмма лица
- ДНК
- Слепок голоса



БИОМЕТРИЧЕСКИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

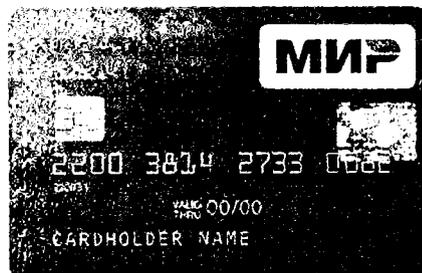
РОСКОМНАДЗОР

7

<http://персональныеданные.дети/>

Набор цифр как персональные данные:

- номер и серия паспорта,
- страховой номер индивидуального лицевого счета (СНИЛС),
- индивидуальный номер налогоплательщика (ИНН),
- номер банковского счета,
- номер банковской карты.



РОСКОМНАДЗОР

8

<http://персональныеданные.рф/>

Big Data или Большие данные

Каждое наше действие, совершаемое в сети Интернет, оставляет определенный цифровой след:

- фотографии в социальных сетях;
- высказывания на форумах;
- «лайки» новостей;
- информация о посещенных сайтах, о совершенных покупках, о географическом месторасположении и пр.

Большие данные используются для:

- направления адресной рекламы;
- при приеме на работу...



Как защитить электронные устройства от вредоносных программ?



- Установите специальные почтовые фильтры и антивирусные программы. Они могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
- Систематически проверяйте свои домашние компьютеры на наличие вирусов.

Как защитить электронные устройства от вредоносных программ?

- Используйте только лицензионные программы. Чаще всего вирусами бывают заражены пиратские копии программ.
- Используйте проверенные сайты.
- Делайте резервную копию важных данных.
- Периодически меняйте пароли от электронной почты, социальных сетей, форумов и пр.



<http://персональныеданные.дети/>

Как защитить электронные устройства от вредоносных программ?



- Используйте только сложные пароли, разные для разных учетных записей и сервисов.
- Периодически меняйте пароли от электронной почты, социальных сетей, форумов и пр.
- Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее).

Правила составления надежных паролей

- Надежный пароль должен:
 - состоять из 8–16 символов;
 - включать в себя буквы, цифры и специальные символы;
 - включать в себя символы в верхнем и нижнем регистре.
- Не следует использовать слова, словосочетания, а также комбинации, которые можно легко угадать.
- Целесообразно использовать двухэтапную аутентификацию с помощью мобильного телефона.
- Для каждого аккаунта необходимо иметь свой пароль.
- Необходимо менять пароли ко всем аккаунтам раз в 3–6 месяцев.
- При столкновении с попыткой взлома одного из аккаунтов необходимо поменять пароли на всех аккаунтах.

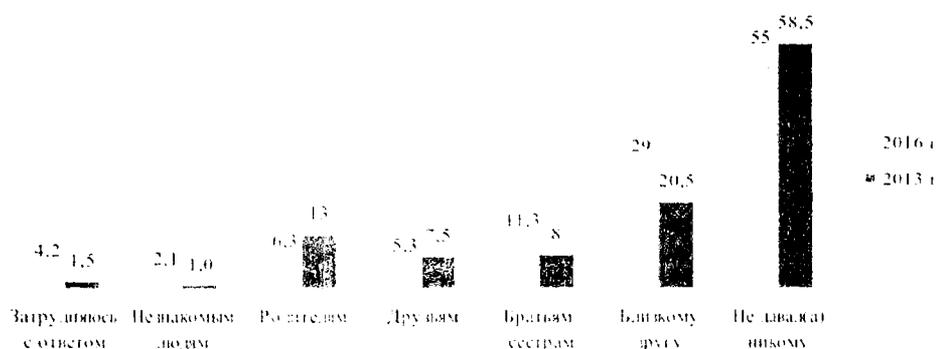
Способы составления надежного пароля

- Для получения сложного, но легко запоминающегося пароля можно использовать любое слово, зашифровав его с помощью одного из следующих методов:
- •• *Транслитерация*. Если взять любое слово русского языка и набрать его на клавиатуре с латинской раскладкой, то получится бессмысленное сочетание символов. Например, RYUHTUFWBZ — это слово «конгрегация». К сожалению, этот метод плохо подходит для устройств с виртуальной клавиатурой, где отсутствует двойная подпись клавиш.
- •• *Смещение по клавиатуре*. Если при написании слова каждый раз смещаться по клавиатуре на одну клавишу влево, мы используем *простое смещение*, например, ВПЬЦЩ — это слово «арбуз». Если менять направление смещения по или против часовой стрелки, мы используем *сложное смещение*, например ЛПТВЛПР — это слово «барабан».
- •• *Акроним*. Если взять первые буквы слов из известной фразы, то мы получаем акроним, который можно использовать в качестве пароля. Например, МДСЧПКНВШЗ — это первые две строки из романа А.С. Пушкина «Евгений Онегин».
- •• *Известные последовательности*. Также для составления пароля можно использовать первые буквы известных последовательностей слов. Например, ЯФМАМИИАСОНД — это двенадцать месяцев. Всегда можно усложнить последовательность, например изменив направление и величину шага. ДОАИАФНСИММЯ — это последовательность месяцев наоборот и через один.

Способы составления надежного пароля

- **Чередования символов.** Любой пароль можно усложнить, добавив последовательность цифр или знаков, которые можно чередовать с зашифрованным словом. Например, П1А2Р3О4Л5Ь6.
- **Псевдографика.** Достаточно сложный, но хорошо запоминающийся пароль можно создать с помощью псевдографики — использования символов шрифта для создания графических изображений. Например набор символов `_>(0:0:0)<_` похож на кошачью мордочку.
- Чтобы сделать надежный пароль, необходимо использовать несколько различных видов шифрования. Возьмем слово ПАРОЛЬ, транслитерируем — GFHJKM, добавим через одну букву шесть цифр, но в обратном порядке — G6F5H4J3K2M1, а теперь поменяем цифры через одну на соответствующие им символы — G6F%N4J#K2M!
- Одну и ту же систему шифрования можно использовать для разных паролей, добавив систему индексов, например: ПАРОЛЬMAIL.RU, ПАРОЛЬGMAIL.COM, ПАРОЛЬVK.COM.
- Это существенно упростит процедуру запоминания паролей и сделает их достаточно надежными и безопасными.

Сохрани пароль в тайне



Ответы подростков на вопрос: «Давал ли ты когда-нибудь пароль от своего аккаунта в социальной сети или электронной почты?», %
(выборка — подростки, пользующиеся интернетом)

Как общаться в Сети?	
<p>1. Старайтесь не выкладывать в Интернет личную информацию (фотографии, видео, ФИО, дату рождения, адрес дома, номер школы, телефоны и иные данные) или существенно сократите объем данных, которые публикуете в Интернете.</p>	
	<p>2. Не выкладывайте личную информацию (совместные фотографии, видео, иные данные) о ваших друзьях в Интернет без их разрешения. Прежде чем разместить информацию о друзьях в Сети, узнайте, не возражают ли они, чтобы вы выложили данные.</p>
<p>3. Не отправляйте свои персональные данные, а также свои видео и фото людям, с которыми вы познакомились в Интернете, тем более если вы не знаете их в реальной жизни.</p>	
	<p>4. При общении с другими пользователями старайтесь быть вежливыми, деликатными, тактичными и дружелюбными. Не пишите грубостей, оскорблений, матерных слов – читать такие высказывания так же неприятно, как и слышать.</p>

<p>5. Старайтесь не реагировать на обидные комментарии, хамство и грубость других пользователей. Всегда пытайтесь уладить конфликты с пользователями мирным путем, переведите все в шутку или прекратите общение с агрессивными пользователями. Ни в коем случае не отвечайте на агрессию тем же способом.</p>	
	<p>6. Если решить проблему мирным путем не удалось, напишите жалобу администратору сайта, потребуйте заблокировать обидчика.</p>
<p>7. Если администратор сайта отказался вам помочь, прекратите пользоваться таким ресурсом и удалите оттуда свои данные.</p>	
	<p>8. Не используйте Сеть для распространения сплетен, угроз или хулиганства.</p>
<p>9. Не встречайтесь в реальной жизни с онлайн-знакомыми без разрешения родителей или в отсутствие взрослого человека. Если вы хотите встретиться с новым интернет-другом, постарайтесь пойти на встречу в сопровождении взрослого, которому вы доверяете.</p>	

- <http://персональныеданные.дети/>

Как защитить персональные данные в Сети?

1. Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.
2. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.
3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает.
4. Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, класса иные данные, посоветуйтесь с родителями или взрослым человеком, которому вы доверяете.
5. Используйте только сложные пароли, разные для разных учетных записей и сервисов.
6. Старайтесь периодически менять пароли.
7. Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее).

Кибербуллинг или Интернет-травля



- намеренные оскорбления, угрозы, сообщения другим людям компрометирующих данных о Вас с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени.

Травля осуществляется путем распространения (угрозы в распространении) компрометирующих материалов в информационном пространстве через информационно-коммуникационные каналы и средства, в том числе в Интернете, посредством электронной почты, программ для мгновенного обмена сообщениями, в социальных сетях, а также через размещение на видеопорталах либо посредством мобильного телефона (СМС – сообщения или надоедливые звонки).

Если Вы, пользуясь Интернетом, оказались в непростой ситуации, Вы можете обратиться на Линию помощи «Дети Онлайн» по телефону: 8 (800) 25-000-15 (звонок по России бесплатный)

<http://detionline.com>

Также можете воспользоваться горячей линией по приему сообщений о противоправном контенте в Интернете на сайте Фонда содействия развитию сети Интернет – «Дружественный Рунет»: www.friendlyrunet.ru

<http://персональныеданные.дети/>

- информационно-развлекательный сайт о персональных данных и их защите



<http://персональныеданные.дети/>

Хакер



Неплохо разбирается в построении компьютерных сетей и способах передачи информации. Может взломать аккаунт, чтобы использовать информацию в своих целях или продать ее.

<http://персональныеданные.дети/>

Агент



Занимается промышленным шпионажем. Собирает информацию о нужных людях через интернет, иногда покупая ее у хакеров.

СПАСИБО ЗА ВНИМАНИЕ!

 **РОСКОМНАДЗОР**