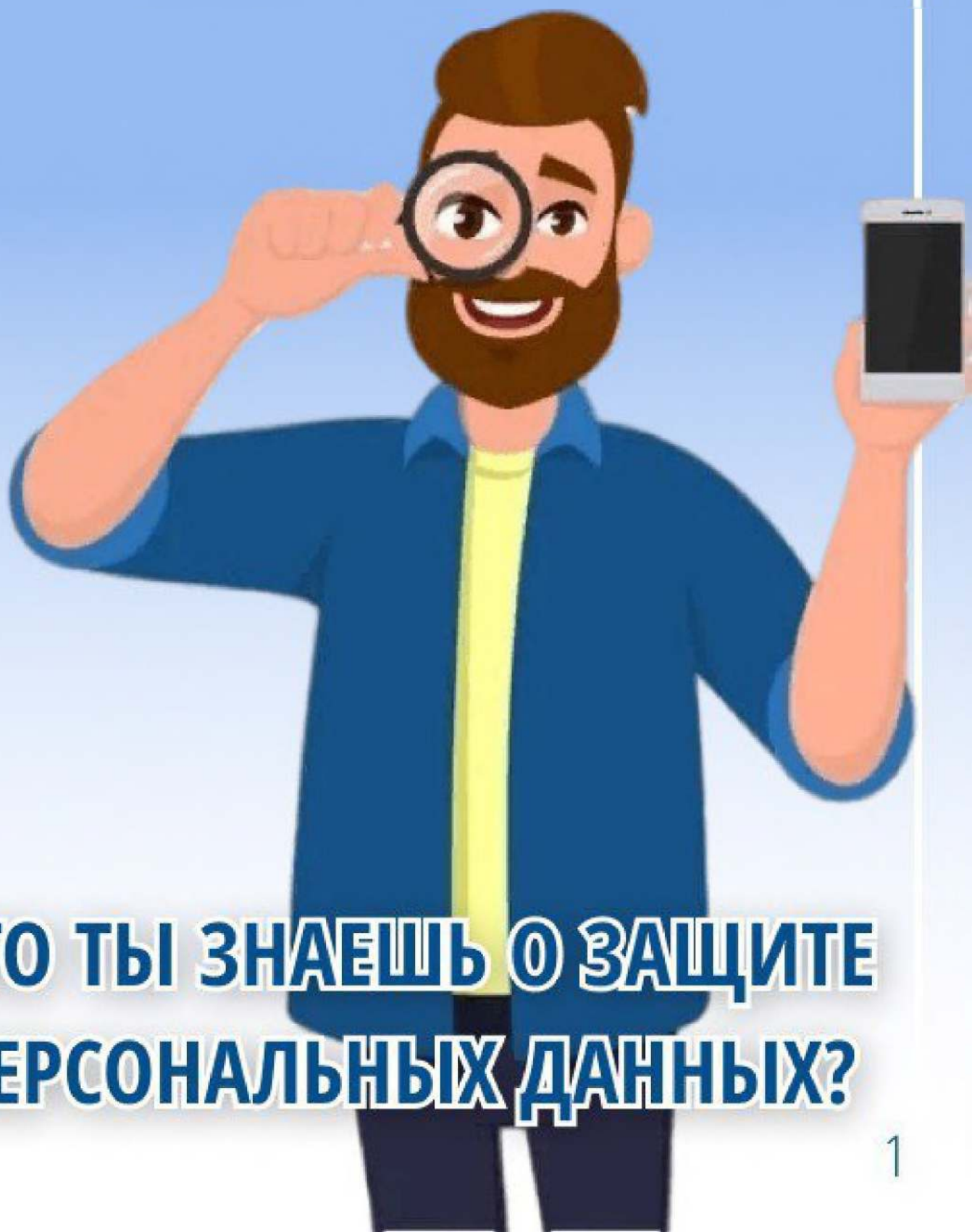




# РОСКОМНАДЗОР

г. Иркутск



**ЧТО ТЫ ЗНАЕШЬ О ЗАЩИТЕ  
ПЕРСОНАЛЬНЫХ ДАННЫХ?**

# ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Персональные данные представляют собой информацию о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность.

Таких идентифицирующих данных огромное множество, к ним относятся: фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.



# СПЕЦИАЛЬНЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

К специальным персональным данным относятся: расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья и пр.

Таким образом, специальные данные характеризуют наши взгляды, убеждения, мировоззрение, они определяют нашу социальную принадлежность к определенным группам.



# БИОМЕТРИЧЕСКИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

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. К таким данным относятся: отпечаток пальца, рисунок радужной оболочки глаза, код ДНК, слепок голоса и пр.



# КИБЕРБУЛЛИНГ ИЛИ КИБЕРЗАПУГИВАНИЕ

Оборот личной информации в сети может приводить к проблемам, когда незнакомцы, прохожие или даже друзья используют информацию безответственно и без учёта права на неприкосновенность частной жизни. Так появился кибербуллинг и возможность при помощи технологий проявлять негативные качества, делать это анонимно, не опасаясь ответной реакции.

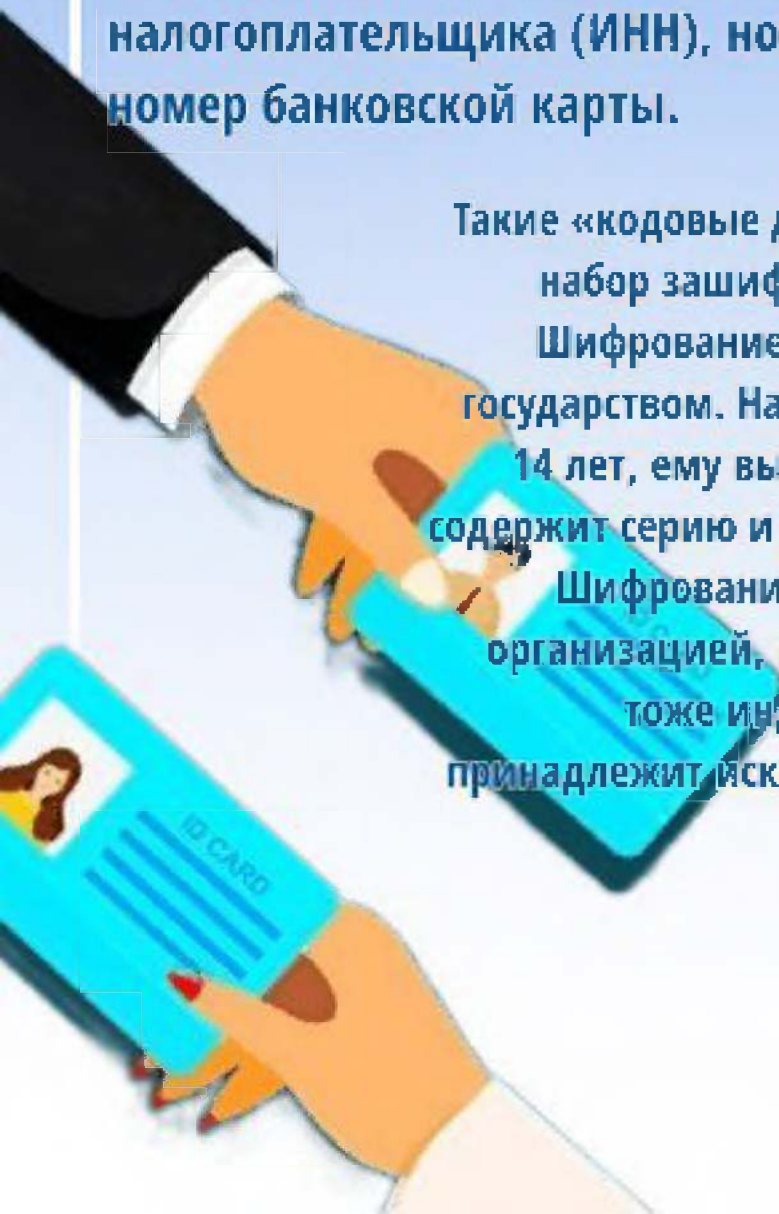
Основной площадкой кибербуллинга стали социальные сети. В них можно не только оскорблять человека в сообщениях, но и взламывать страницу жертвы или создавать поддельные страницы на имя жертвы, где размещается унижительный контент, распространяются обидные и непристойные сообщения



# НАБОР ЦИФР КАК ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Существуют персональные данные, которые представляют собой набор цифр. Благодаря такому набору цифр нас можно определить как конкретного человека, установить нашу личность.

Таковыми персональными данными являются: номер и серия паспорта, страховой номер индивидуального лицевого счета (СНИЛС), индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты.

An illustration showing two hands holding blue ID cards. The top hand is a man's hand in a suit sleeve, holding a card with a photo of a man. The bottom hand is a woman's hand with red nail polish, holding a card with a photo of a woman. The cards are labeled 'ID CARD' and have some illegible text and lines on them.

Такие «кодовые данные» представляют собой некий набор зашифрованной информации о человеке. Шифрование этих данных может производиться государством. Например, когда ребенку исполняется 14 лет, ему выдают паспорт в ФМС. Такой паспорт содержит серию и номер, а также иную информацию. Шифрование может производиться банковской организацией, например, номер банковской карты тоже индивидуальный, он не повторяется и принадлежит исключительно держателю банковской карты.

# БОЛЬШИЕ ДАННЫЕ

Каждое наше действие, совершаемое в сети Интернет, оставляет определенный цифровой след. Такие следы оставляет информация, которую вы добровольно размещаете в сети Интернет, например, фотографии в социальных сетях, высказывания на форумах, «лайки» новостей и многое другое.

Кроме того, цифровые следы оставляет та информация, о наличии которой вы можете и не подозревать, например, информация о посещенных сайтах, о совершенных покупках, о вашем географическом месторасположении и пр.

Если обработать всю эту информацию, то получится очень точный портрет («профайл»), который можно использовать для принятия решений в отношении конкретного человека. Например, направить ему адресную рекламу в соответствии с предпочтениями, «лайками» или отказать в поступлении на работу и пр

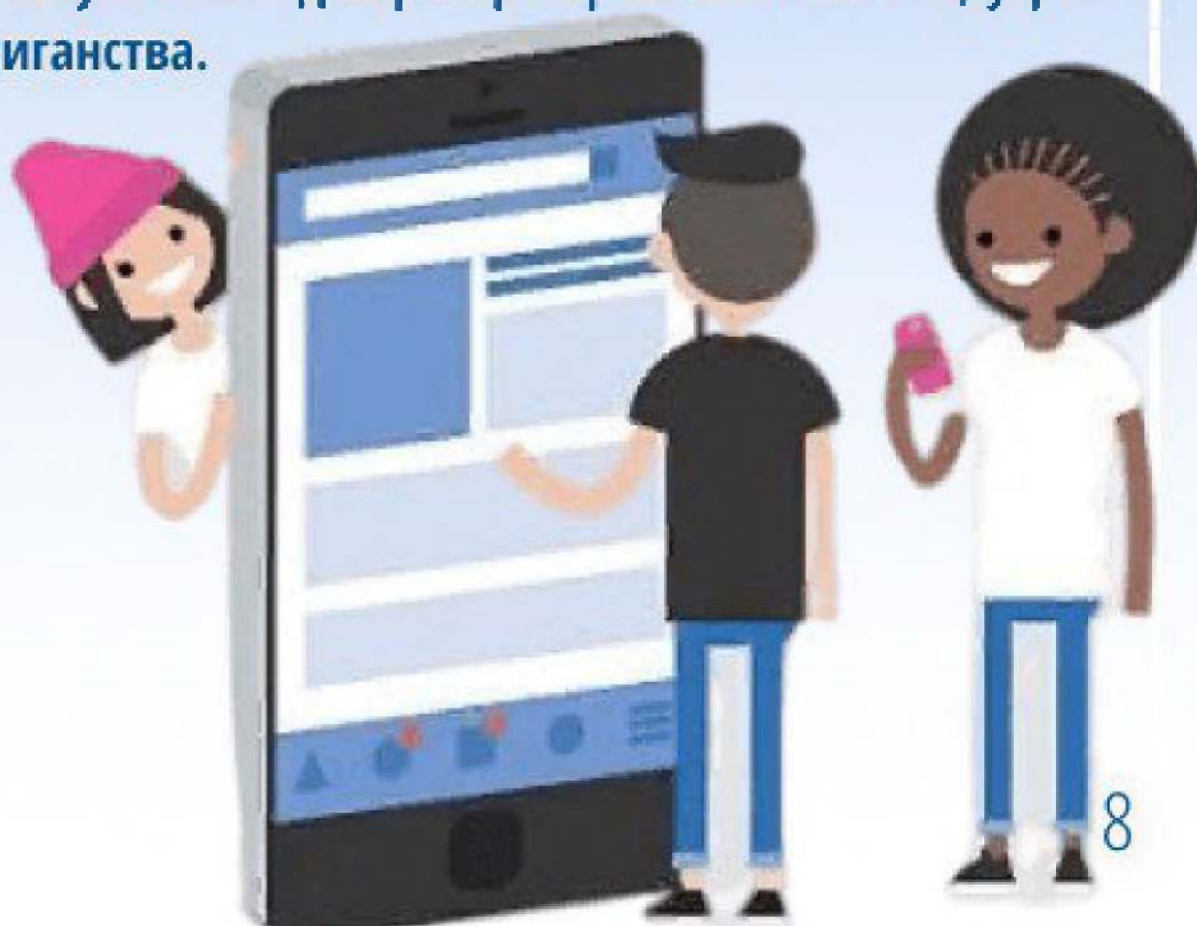
## BIG DATA

Этот колоссальный объем информации, подлежащий обработке и анализу, получил название Big Data или Большие данные.



# КАК ОБЩАТЬСЯ В СЕТИ “ИНТЕРНЕТ”

1. Старайтесь не выкладывать свою личные данные в социальные сети;
2. Не передавайте информацию о себе незнакомым вам людям, не разглашайте информацию о друзьях без их разрешения;
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;
4. Старайтесь не реагировать на обидные комментарии, хамство и грубость других пользователей;
5. Не используйте Сеть для распространения сплетен, угроз или хулиганства.





# КАК ЗАЩИТИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ В СЕТИ “ИНТЕРНЕТ”

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. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает;
3. Используйте только сложные пароли, разные для разных учетных записей и сервисов;
4. Старайтесь периодически менять пароли;
5. 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).



# КАК ЗАЩИТИТЬ ГАДЖЕТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

1. Установите на гаджеты специальные почтовые фильтры и антивирусные программы. Они могут предотвратить, как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения;
2. Используйте только лицензионные программы. Чаще всего вирусами бывают заражены пиратские копии программ;
3. Используйте проверенные сайты;
4. Систематически проверяйте свои домашние компьютеры на наличие вирусов;
5. Делайте резервную копию важных данных;
6. Периодически меняйте пароли от электронной почты, социальных сетей, форумов и пр.





# БЕРЕГИТЕ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

По вопросам защиты прав субъектов персональных данных, Вы можете обратиться непосредственно в отдел по защите прав субъектов персональных данных и надзора в сфере информационных технологий.

