



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

Здесь Вы найдете различные материалы, которые были разработаны специалистами Роскомнадзора, не только для педагогов и родителей, которые хотят помочь детям понять важность конфиденциальности личной жизни при использовании цифровых технологий, но также для молодых людей, которые с легкостью и энтузиазмом используют среду Интернет.

Мы хотим помочь детям понимать последствия, которые информационные технологии могут оказать на личную жизнь, и предоставить вам инструменты и информацию, необходимые для принятия решений в вопросах виртуальной жизни.



ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Сегодня реальность во многом заменяется виртуальным миром. Мы наводимся, общаемся и играем в Интернете; у нас есть друзья, с которыми в настоящей жизни мы никогда не встречались, но доверяемся таким людям больше, чем близким. Мы создаем своего виртуального (информационного) прототипа на страничках в социальных сетях, выкладывая информацию о себе.

Используя электронное пространство, мы полагаем, что это безопасно, потому что мы делимся всего лишь информацией о себе и к нашей обычной жизни вроде бы это не относится.

Но на самом деле границы между абстрактной категорией «информация» и реальным человеком носителем этой информации стираются.

Информация о человеке, его персональные данные сегодня превратились в дорогой товар, который используется по-разному:

- кто-то использует эти данные для того, чтобы при помощи рекламы продать вам какую-то вещь;
- кому-то вы просто не нравитесь, и в Интернете вас могут пытаться оскорбить, очернить, выставить вас в дурном свете, создать плохую репутацию и сделать изгоем в обществе;
- с помощью ваших персональных данных мошенники, воры, могут красть ваши деньги, шантажировать вас и заставлять совершать какие-то действия;
- и многое другое.

ЧТО ТАКОЕ ПДн?

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.*

Так, если мы кому-то скажем, свои фамилию, имя, отчество и адрес эта жительства, то нас вполне можно будет опознать как конкретное цо. Но если мы исключим из этого набора данных фамилию или адрес эта жительства, то понять, о каком человеке идет речь будет возможно.

Получается, что персональные данные -это не просто ваши фамилия или имя, персональные данные - это набор данных, их совокупность, которые озволяют идентифицировать вас.

В целом можно сказать, что персональные данные – это совокупность анных, которые необходимы и достаточны для идентификации какого-то ловека.

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, беждения, мировоззрение, они определяют нашу социальную ринадлежность к определенным группам. Например, человек может сказать: демократ или я христианин. По таким данным можно сформировать редставление о человеке.

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 никому 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.

Следует заметить, что приведенный перечень персональных данных не является исчерпывающим и может включать в себя еще множество иных идентификационных данных.

Поэтому защита личной информации может приравниваться к защите реальной личности. И важно в первую очередь научиться правильно, безопасно обращаться со своими персональными данными.

Кибербуллинг или киберзапугивание

Развитие коммуникационных технологий изменило нашу жизнь. Обычные процессы отношений между людьми с помощью Интернета, приобретают в ифровом мире новые особенности.

Скорость распространения информации в сети Интернет уже через гновение позволяет делиться своими жизненными новостями, фотографиями общаться с множеством людей.

Доступ к размещаемой вами информации может быть ограничен только углом вашего общения или быть доступным неограниченному кругу лиц. днако оборот личной информации в сети может приводить к проблемам, гда незнакомцы, прохожие или даже друзья используют информацию эответственно и без учёта права на неприкосновенность частной жизни. Так явился кибербуллинг и возможность при помощи технологий проявлять егативные качества, делать это анонимно, не опасаясь ответной реакции.

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

Независимо от формы проявления кибербуллинг может причинить ачительный вред жертве, а в крайних случаях привести к самым агическим последствиям.

Как и их коллег – хулиганов в физическом мире, кибер-хулиганов ытаются убедить перестать нарушать права других людей. Разница в том, го кибер-хулиганы в состоянии скрыть свою личность в Интернете, что итрудняет возможность оперативного пресечения такой деятельности.

Риски, которые влечёт обмен информацией в Интернете

К сожалению, реальность такова, что люди выдают слишком много информации о себе в Интернете, испытывая при этом ошибочное убеждение, го принадлежащая им информация является конфиденциальной, но как ьлько информация попадает в Сеть, контролировать ее дальнейшее спользование уже практически невозможно. Кто, когда и в каких целях ожет воспользоваться такими данными, прогнозировать невозможно.

- В Интернете нет кнопки «Удалить», чтобы удалить информацию, размещённую в Интернете. Вы можете пожалеть о создании, например, комментария в виде замечания по отношению к любому человеку, потом, давлив его в течение часа, крайне удивиться, что этот комментарий уже прочитан десятками или сотнями людей и столько же людей перенаправили его по разным адресам.

Пример 1:

Именинник после празднования дня рождения выложил в сеть тридцателетний комментарий по поводу подарка одного из своих гостей, после чего он подвергся резкой критике со стороны других пользователей, которые в диалоге раскрывали место проведения праздника и свое отношение к нему, на именинника было оказано огромное давление, что привело его к необходимости принести публичные извинения.

- Возможно, вы осторожный и аккуратный человек, и, прежде чем, выложить фотографию или информацию в сеть воспользовались настройками приватности. Соответственно, к информации, которую размещаете Вы, имеет доступ ограниченный круг лиц, определённый Вами. Однако следует всегда помнить и понимать, что вы не будете иметь никакого контроля в случае, когда ваши друзья скопировали информацию и распространили ее в дальнейшем, при этом, не спросив вашего мнения или разрешения.

Пример 2:

Девушка разместила в сети сообщение для своих онлайн друзей, где пожаловалась, что её бросил парень. Она обвинила своего бывшего парня в том, что он применил к ней физическую силу, толкнул ее на лестнице, после чего она упала и ударилась. Её друзья по сети высказали ей слова поддержки, используя ненормативную лексику по отношению к парню. В таком контексте они обсуждали его личные данные, в том числе имя, фото, адрес проживания, при этом приводили подробности его личной жизни, не имея на это никаких оснований и подтверждений тем фактам, которые были изложены. А другие пользователи сети встали на сторону бывшего парня и решили отомстить за него, после чего разместили в сети личные данные девушки с фотографиями и опутствующими обидными комментариями.

- Смартфоны с подключением к Интернету и высоким качеством камер стали доступными и недорогими для среднего потребителя. Пользователи

мартфонов часто становятся свидетелями различных инцидентов, которые происходят в общественной жизни и моментально публикуют снятое на фото или видео в Интернете. Некоторые Интернет-форумы пользуются популярностью среди своих пользователей благодаря так называемому мастерству раскрытия личности лиц, размещенных в онлайн-видеороликах». аже если вы или ваши друзья оставляют в сети неструктурированную и взрозненную информацию о вас на разных сайтах, есть те кто может аходить способы собирать всю имеющуюся о вас информацию без вашего эдома.

Пример 3:

Два пассажира в метро поссорились из-за одного свободного места. Спор ыл заснят на видео другим пассажиром посредством использования мартфона, видео было размещено им в Интернете и разошлось по сети. нтернет-пользователи раскрыли имена и номера телефонов главных героев. результате в Интернете, после раскрытия личности героев, пассажиры голкнулись с огромным давлением, кроме того резкой критикой поведения вух пассажиров теперь завалено большинство Интернет-форумов.

- То, что вы говорите или то чем вы делитесь в Интернете может повлечь и собой критику. Информация, которой вы поделились с другими может гать мишенью для кибер-хулиганов. Они выставят вас на всеобщее бозрение, подвергнут вас «суду» за ваши он-лайн слова или действия и знесут вам свой «вердикт».

Пример 4:

Пациент оказался недоволен услугами врача, к которому обратился за омощью и разместил видео, где грубо назвал врача непрофессионалом и явил, что клиника не соответствует заявленному уровню. Свой гнев он зразил неприятными словами. К его удивлению, пользователи сети нашли то поступок необоснованным и он сам стал объектом нападения. Его фото, омашний и рабочий адреса были опубликованы в Интернете. Была создана аже группа в социальной сети, призывающая его извиниться.

- Кибербуллинг также может произойти, когда злоумышленник создает зжную учетную запись жертвы и использует ее для отправления жкорбительных, агрессивных или неуместных сообщений на почту друзей и

емьи, а также на их аккаунты в социальных сетях, включая друзей, таким образом, создавая впечатление, что сообщения были отправлены жертвой.

Пример 5:

Девочка поделилась со своей подругой паролем от своего аккаунта в социальной сети. Подруга периодически использовала этот пароль для входа в аккаунт и просматривала личные сообщения и однажды, в своем разочаровании увидела в личных сообщениях отрицательный комментарий по отношению к себе. Тогда девушка под видом своей подруги послала неприятные сообщения многим из ее друзей.

- Кибер-хулиганы могут специально создавать поводы заставляя сердиться всю жертву до такой степени, что они рано или поздно отвечают изгнанным или оскорбительным замечанием. После такой реакции кибер-хулиган может уведомить администратора ресурса о недопустимом поведении и нарушении правил пользования услугами сети, после чего ваш аккаунт может быть заблокирован.

Пример 6:

Подруги сильно поссорились. Обе выплёскивали свой гнев друг на друга на Интернет-форуме. У обеих были свои сторонники, которые довели их оскорбительные комментарии до сведения администраторов ресурса, что привело к блокировке аккаунтов обеих девушек.

- Вы можете быть уверенными, что находитесь в безопасности от кибер-издевательств, если вы никогда не раскрывали ваших личных данных в Интернете. Тем не менее, поскольку Интернет настолько проник в нашу обычную жизнь, любое лицо, Интернет-пользователь или нет, являетсяязвимым к безответственному онлайн – поведению.

В законодательстве отсутствует конкретное положение, предусматривающее ответственность за кибер-издевательства, это вызвано тем, что такая деятельность довольно широка и охватывает собой начительный перечень уже имеющихся составов преступлений и правонарушений, это в первую очередь нарушение права на неприкосновенность частной жизни, выражающееся в незаконном сборе или распространении сведений о частной жизни лица, составляющих его личную или семейную тайну. Также в соответствии с Конституцией Российской Федерации достоинство личности охраняется государством и ничто не может

ыть основанием для его умаления, никто не должен подвергаться
нижающему человеческое достоинство обращению или наказанию.
сновным законом, определяющим порядок оборота персональных данных,
зляется Федеральный закон «О персональных данных» № 152-ФЗ, который
держит ряд принципов, помнить и знать которые необходимо. Например,
бор личных данных для преступных целей недопустим, потому что сама цель
законна. Даже если данные предоставлены субъектом самостоятельно, это
е даёт права третьим лицам использовать такие данные по своему
смотрению.

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.

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.

Сегодня информационные технологии позволяют обрабатывать и анализировать огромные объемы данных для выявления новой информации, представляющей ценность для принятия различных решений.

Представьте себе данные о следах всех пользователей сети Интернет России или другой страны, которые они оставили за последние 10 лет.

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

При этом Большие данные получают не только благодаря Вашим цифровым следам, их добывают из иных источников, например, с помощью датчиков погоды или геолокационных систем.

Как общаться в Сети «Интернет»

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 убликуете в Интернете.

2. Не выкладывайте личную информацию (совместные фотографии, видео, ные данные) о ваших друзьях в Интернет без их разрешения. Прежде чем зместить информацию о друзьях в Сети, узнайте, не возражают ли они, гобы вы выложили данные.

3. Не отправляйте свои персональные данные, а также свои видео и фото одиям, с которыми вы познакомились в Интернете, тем более если вы не аете их в реальной жизни.

4. При общении с другими пользователями старайтесь быть вежливыми, эликатными, тактичными и дружелюбными. Не пишите грубостей, скорблений, матерных слов – читать такие высказывания так же неприятно, ак и слышать.

5. Старайтесь не реагировать на обидные комментарии, хамство и грубость ругих пользователей. Всегда пытайтесь уладить конфликты с ользователями мирным путем, переведите все в шутку или прекратите бщение с агрессивными пользователями. Ни в коем случае не отвечайте на рессию тем же способом.

6. Если решить проблему мирным путем не удалось, напишите жалобу министратору сайта, потребуйте заблокировать обидчика.

7. Если администратор сайта отказался вам помочь, прекратите ользоваться таким ресурсом и удалите оттуда свои данные.

8. Не используйте Сеть для распространения сплетен, угроз или улиганства.

9. Не встречайтесь в реальной жизни с онлайн-знакомыми без разрешения оидателей или в отсутствие взрослого человека. Если вы хотите встретиться с овым интернет-другом, постарайтесь пойти на встречу в сопровождении рзрослого, которому вы доверяете.

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. 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 и другие 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).

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.

Развитие информационных технологий изменило модель сбора, копирования, использования и передачи данных, существенно упростило нашу жизнь и сделало ее мобильнее. Однако за удобством, простотой, скоростью и легкостью использования информационных технологий скрывается обратная сторона медали. Таким образом, соблюдая элементарные правила поведения в сети «Интернет» Вы сможете защитить свои персональные данные.

Берегите свои персональные данные!!!

ИНТЕРНЕТ - ПОРТАЛ



«ПЕРСОНАЛЬНЫЕ
ДАнные. ДЕТИ»

