

Примерный перечень терминов и вопросов по персональным данным

- что такое 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.

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

- что такое 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. Например, человек может сказать: я демократ или я христианин. По таким данным можно сформировать представление о человеке.

- что такое 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. К таким данным относятся:

отпечаток пальца, рисунок радужной оболочки глаза, код ДНК, слепок голоса и пр.

- может ли набор цифр являться персональными данными?

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.

- что такое большие персональные 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 защитить гаджеты от вредоносных программ?

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

- как общаться в Сети?

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.
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.
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. 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.
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.
6. Если решить проблему мирным путем не удалось, напишите жалобу администратору сайта, потребуйте заблокировать обидчика.
7. Если администратор сайта отказался вам помочь, прекратите пользоваться таким ресурсом и удалите оттуда свои данные.
8. Не используйте Сеть для распространения сплетен, угроз или хулиганства.
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.

- 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).

- что такое кибербуллинг (киберзапугивание)?

Доступ к размещаемой вами информации может быть ограничен только кругом вашего общения или быть доступным неограниченному кругу лиц. Однако 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.

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

Как и их коллег – хулиганов в физическом мире, кибер-хулиганов пытаются убедить перестать нарушать права других людей. Разница в том, что кибер-хулиганы в состоянии скрыть свою личность в Интернете, что затрудняет 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, что принадлежащая им информация является конфиденциальной, но как только информация попадает в Сеть, контролировать ее дальнейшее использование уже практически невозможно. Кто, когда и в каких целях может воспользоваться такими данными, прогнозировать невозможно.

- чем занимается Роскомнадзор?

Рассматривает жалобы и обращения, ходит на проверки, ведет реестр операторов, осуществляющих обработку персональных данных.

- куда следует обращаться за защитой персональных данных?

В Роскомнадзор.

С уважением,

Управление Роскомнадзора по Республике Северная Осетия – Алания
362027, г. Владикавказ, ул. Маркуса, 22

Приемная: (8672) 33-30-08

Факс: (8672) 33-30-08

Е-mail: rsockanc15@rkn.gov.ru

Интернет сайт: www.15.rkn.gov.ru

Интернет портал – персональныеданные.дети