1403031/2018-47962(2)

ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА

КОМИТЕТ ПО ОБРАЗОВАНИЮ

пер. Антоненко, д.8, Санкт-Петербург, 190000
Тел. (812) 570-3179 Факс (812) 570-3829
E-mail: kobr@gov.spb.ru
http://www.k-obr.spb.ru

ОКПО 00086993 ОКОГУ 2300223 ОГРН 1027810356485
ИНН/КПП 7830002053/783801001

27.11.2018 № 03-16-405/18-1-1

На № _____ от _____

Начальникам отделов образования администраций районов Санкт-Петербурга

Руководителям общеобразовательных организаций, находящихся в ведении Комитета по образованию

Об информационно-профилактической работе в сфере защиты персональных данных несовершеннолетних

Уважаемые руководители!

С целью максимального охвата детской и подростковой аудитории при проведении профилактических мероприятий в сфере защиты персональных данных направляем методические материалы по проведению внеклассных уроков по тематике защиты персональных данных, разработанные Управлением Федеральной службы по надзору в сфере информационных технологий и массовых коммуникаций по Северо-Западному Федеральному округу (далее – методические материалы).

Методические материалы предназначены для возрастных категорий обучающихся: 9-11 и 12-14 лет.

Дополнительно просим использовать материалы, размещенные на сайте http:/персональныеданные.дети/, а также информационный ресурс с адресом ссылки https://pd.rkn.gov.ru/multimedia/video114.htm, на котором представлены презентации на тему «Защита персональных данных», ориентированные также на две целевые возрастные группы несовершеннолетних: от 9 до 11 лет и от 12 до 14 лет. Ранее информация об этом направлялась письмом Комитета по образованию № 03-16-405/18-0-1 от 08.10.2018.

Просим Вас поручить руководителям общеобразовательных учреждений разместить методические материалы и ссылки на информационные ресурсы на официальных сайтах образовательных учреждений, а также использовать указанные рекомендации на внеклассных мероприятиях по теме защиты персональных данных в течение учебного года.

Приложения: 1. Типовая программа для 9-11 лет - на 1 л. в 1 экз.
2. Презентация для 9-11 лет в 1 экз.
3. Типовая программа для 12-14 лет - на 1 л. в 1 экз.
4. Презентация для 12-14 лет в 1 экз.
5. Буклеты для детей – 2 в 1 экз.

С уважением,
временно исполняющий обязанности
заместителя председателя Комитета **Е.Б. Спасская**

Горина М.А., (812) 576-18-27

Комитет по образованию
№ 03-16-405/18-1-1
от 27.11.2018

Типовая программа проведения внеклассных уроков для учащихся образовательные учреждений общего и среднего образования, детских учреждений дополнительного образования (детских обучающих центров, санаторно-оздоровительных лагерей круглогодичного действия) (9-11 лет)

Исследование проблемы медиабезопасности детей и подростков в последние годы является особенно актуальным в связи с бурным развитием IT-технологий и информационно-коммуникативных сетей.

В настоящий момент увеличивается количество детей и подростков, использующих для общения сеть Интернет (в том числе социальные сети и т.п), играющих в компьютерные игры. Правильное использование персональных данных в сети Интернет – это часть медиабезопасности ребенка.

Поэтому данная программа элективного курса нацелена на решение следующих проблем:

- Просвещение школьников по вопросам безопасного поведения с персональными данными, в том числе в сети Интернет;
- Формирование у учащихся навыков поведения с персональными данными, в том числе в информационно-телекоммуникационной сети Интернет

Цели обучения: формирование у учащихся навыков поведения с персональными данными, в том числе правильного использования персональных данных в медиапространстве.

Задачи: помочь детям понять важность правильного использования персональных данных, конфиденциальности личной жизни, в том числе в сети Интернет, при использовании цифровых технологий, научиться понимать последствия неправильного обращения с персональными данными.

1. Образовательная задача:

Знания (раскрыть понятия персональных данных, субъекта персональных данных; обработки персональных данных; рассказать о последствиях распространения в сети Интернет своих и чужих персональных данных; рассказать об органе, который защищает права субъектов персональных данных)

Умения и навыки: специальные (как защитить свои персональные данные в Сети? Как не навредить иным лицам при обработке их персональных данных), дети должны овладеть навыками как ограничить свои персональные данные в Сети; как общаться в Сети, чтобы не нарушить права других субъектов персональных данных; дети должны знать к кому и куда обратиться в случае нарушения их прав в сети Интернет.

2. Воспитательная: нравственные и этические представления о частной жизни в Сети, способность следовать нормам поведения, а именно, соблюдать

приватность своих персональных данных и персональных данных других субъектов, исполнять законодательство в области персональных.

Поэтому данная программа элективного курса нацелена на решение следующих проблем:

- Просвещение школьников по вопросам безопасного поведения с персональными данными, в том числе в сети Интернет;
- Формирование у учащихся навыков поведения с персональными данными, в том числе в информационно-телекоммуникационной сети Интернет

Тема внеклассного занятия

Что такое персональные данные и как правильно с ними обращаться. Распространение персональных данных в сети Интернет, в том числе в социальных сетях, блогах и т.д.

План урока:

1. Организационная часть — 2 мин.
2. Сообщение новых знаний с презентацией — 30 мин.
3. Демонстрация видеоматериалов — 10 мин.
4. Раздача буклетов— 2 мин.
5. Завершение урока — 1 мин.

(Демонстрируется анимационный ролик «Береги свои персональные данные!»)

Почему эта история, которая началась так радостно, закончилась так печально?

Мальчик слишком много рассказал о себе и своей семье в Интернете. Этой личной информацией, которую ещё называют персональными данными, воспользовались преступники.

Слайд 2
Что же такое **персональные данные**?

Беседа с учащимися.

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 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 места жительства, то нас вполне можно будет опознать как конкретное лицо. Но если мы исключим из этого набора данных фамилию или адрес места жительства, то понять, о каком человеке идет речь будет невозможно.

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

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

Слайд 3-5

Персональные данные делятся на разные категории:

Есть **специальные категории персональных данных**:

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 принадлежность к определенным социальную группам, состояние здоровья. Данная категория персональных данных обрабатывается с письменного согласия, если иное не определено другими законами. Например, медицинский работник в медицинском кабинете обрабатывает персональные данные учеников о состоянии здоровья на основании законодательства.

Слайд 6-7

Как вы думаете, какие персональные данные относятся к биометрическим? (обсуждение)

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

Биометрические данные – это то, что заложено в нас от рождения самой природой, это просто закодированная информация о человеке, которую люди научились считывать. К таким данным относятся:

отпечатки пальцев,
рисунок радужной оболочки глаза,
код ДНК,
слепок голоса и пр.

Слайд 8

Набор цифр как персональные данные. Существуют персональные данные, которые представляют собой набор цифр. Благодаря такому набору цифр можно установить нашу личность.

Как вы думаете, какие персональные данные представляют собой набор цифр? (обсуждение)

Такими 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. 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.

Слайд 9

Большие данные - что такое?

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.

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

Слайд 10-12

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.
-

Слайд 13-15

Правила создания надежного пароля

Слайд 16

Результаты опроса «Давал ли ты когда-нибудь пароль от своего аккаунта в социальной сети или электронной почты?»

К сожалению, исследования показывают, что подростки легко делятся паролями с друзьями, знакомыми и даже незнакомыми людьми.

Слайд 17-18

Как общаться в Сети и как защитить свои персональные данные 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.

Слайд 19

Итак, какие правила мы должны соблюдать чтобы обезопасить себя и своих близких!

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).

Слайд 20

Ещё одно опасное явление современной жизни – кибербуллинг, или Интернет-травля – намеренные оскорбления, угрозы, сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени.

Травля осуществляется в информационном пространстве через информационно-коммуникационные каналы и средства. В том числе в Интернете посредством электронной почты, программ для мгновенного обмена сообщениями (Instant Messenger, например, ICQ) в социальных сетях, а также через размещения на видеопорталах (YouTube, Vimeo и других) непристойных видеоматериалов, либо посредством мобильного телефона (например, с помощью SMS-сообщений или надоедливых звонков).

Слайд 21

Если Вы оказались в непростой ситуации, обратитесь за помощью к взрослым, родителями, учителям, школьному психологу. Также Вы можете обратиться на Линию помощи «Дети Онлайн» по тел. 8 (800) 25-000-15 (звонок по России бесплатный) http://detionline.com или воспользоваться горячей линией по приему сообщений о противоправном контенте в Интернете на сайте Фонда содействия развитию сети Интернет – «Дружественный Рунет»: www.friendlyrunet.ru.

Слайд 22-24

Роскомнадзор специально для детей и подростков создал информационно-развлекательный сайт http://персональныеданные.дети/, направленный на изучение вопросов, связанных с защитой персональных данных.

На сайте размещены информационные материалы для детей, в виде интересной и познавательной информации. Все материалы на портале разрабатывались с учетом ошибок детей в онлайн среде, о которых становилось известно Роскомнадзору в рамках повседневной работы. На этом портале можно найти различные материалы, которые не только помогут детям понять важность конфиденциальности личной жизни при использовании цифровых технологий, но и смогут помочь детям понимать последствия, которые информационные технологии оказывают на личную жизнь человека, а также на Портале предоставлены инструменты и информация, необходимая детям для принятия решений в вопросах виртуальной жизни.

Вы познакомитесь с персонажами сайта Галей и Васей, Хакером и Агентом, узнаете, что такое персональные данные, какие персональные данные относятся к категории специальных и биометрических, как защитить личные данные в Интернете, каковы правила безопасного общения в Сети.

Анализ полученных в ходе проведения внеклассного урока знаний предлагаем провести отдельным уроком посредством прохождения теста с сайта «http://персональныеданные.дети» Что ты знаешь о персональных данных?

Список медиаисточников:

1. портал http://персональныеданные.дети
2. Портал персональных данных (https://pd.rkn.gov.ru)
3. Видео-материалы для проведения уроков по вопросам защиты персональных данных, размещенные в разделе «Мультимедиа» Портала персональных данных (https://pd.rkn.gov.ru/multimedia/video114.htm)

Типовая программа проведения внеклассных уроков для учащихся образовательные учреждений общего и среднего образования, детских учреждений дополнительного образования (детских обучающих центров, санаторно-оздоровительных лагерей круглогодичного действия) (12-14 лет)

Исследование проблемы медиабезопасности детей и подростков в последние годы является особенно актуальным в связи с бурным развитием IT-технологий и информационно-коммуникативных сетей.

В настоящий момент увеличивается количество детей и подростков, использующих для общения сеть Интернет (в том числе социальные сети и т.п), играющих в компьютерные игры. Правильное использование персональных данных в сети Интернет – это часть медиабезопасности ребенка.

Поэтому данная программа элективного курса нацелена на решение следующих проблем:

- Просвещение школьников по вопросам безопасного поведения с персональными данными, в том числе в сети Интернет;
- Формирование у учащихся навыков поведения с персональными данными, в том числе в информационно-телекоммуникационной сети Интернет

Цели обучения: формирование у учащихся навыков поведения с персональными данными, в том числе правильного использования персональных данных в медиапространстве.

Задачи: помочь детям понять важность правильного использования персональных данных, конфиденциальности личной жизни, в том числе в сети Интернет, при использовании цифровых технологий, научиться понимать последствия неправильного обращения с персональными данными.

1. Образовательная задача:

Знания (раскрыть понятия персональных данных, субъекта персональных данных; обработки персональных данных; рассказать о последствиях распространения в сети Интернет своих и чужих персональных данных; рассказать об органе, который защищает права субъектов персональных данных)

Умения и навыки: специальные (как защитить свои персональные данные в Сети? Как не навредить иным лицам при обработке их персональных данных), дети должны овладеть навыками как ограничить свои персональные данные в Сети; как общаться в Сети, чтобы не нарушить права других субъектов персональных данных; дети должны знать к кому и куда обратиться в случае нарушения их прав в сети Интернет.

2. Воспитательная: нравственные и этические представления о частной жизни в Сети, способность следовать нормам поведения, а именно, соблюдать

приватность своих персональных данных и персональных данных других субъектов, исполнять законодательство в области персональных.

Поэтому данная программа элективного курса нацелена на решение следующих проблем:

- Просвещение школьников по вопросам безопасного поведения с персональными данными, в том числе в сети Интернет;
- Формирование у учащихся навыков поведения с персональными данными, в том числе в информационно-телекоммуникационной сети Интернет

Тема внеклассного занятия

Что такое персональные данные и как правильно с ними обращаться. Распространение персональных данных в сети Интернет, в том числе в социальных сетях, блогах и т.д.

План урока:

1. Организационная часть — 2 мин.
2. Сообщение новых знаний с презентацией — 30 мин.
3. Демонстрация видеоматериалов — 10 мин.
4. Раздача буклетов— 2 мин.
5. Завершение урока — 1 мин.

Ход урока сопровождается демонстрацией презентации (приложение 1)

СЛАЙД 1

Сеть Интернет в настоящее время представляет собой мировой информационный и коммуникационный ресурс, доступ к которому имеет значительная часть населения планеты и стал неотъемлемой частью нашей жизни. С его помощью мы получаем информацию, общаемся, обмениваемся данными, оплачиваем товары и услуги, отправляем документы для поступления в вузы и делаем многое другое. Вместе с тем интернет таит в себе опасности. В ходе урока мы поговорим о них и научимся их избегать.

Наедине с компьютером или смартфоном легко забыть, что в Сети миллиарды людей и до любого человека всего пара кликов, чтобы связаться с ним. Но не надо забывать, что в Сети кроме доброжелательных собеседников нами могут заинтересоваться мошенники разного рода, а также тролли разной степени небезобидности. Чтобы максимально обезопаситься от подобных угроз, нужно научиться правилам сетевой безопасности, которые столь же важны, как правила дорожного движения. Правила просты, вот основные: во-первых, не стоит никому сообщать о себе излишнюю информацию, например, свои место учебы и проживания, обстоятельства своей жизни (о том, что едем в отпуск, о дорогостоящих приобретениях и т.п.), даже иногда имеет смысл воспользоваться

псевдонимом и не раскрывать свое настоящее имя; во-вторых, необходимо сообщать родителям или другим взрослым, которым мы доверяем, о любых разговорах на тревожные темы, которые с нами заводят незнакомцы, в-третьих, обязательно анализировать публикуемый в Сети контент, то есть мы должны осознавать насколько могут быть опасные последствия от публикации, например, фотографий и видео, поскольку по изображениям можно понять, где происходит дело, тем более смартфоны еще и заботливо снабжают фотографии геометками.

Самый большой объем данных о себе, пожалуй, мы распространяем в социальных сетях.

СЛАЙД 2

Какие социальные сети вы знаете? В каких социальных сетях зарегистрированы? Какие данные сообщали, когда регистрировались?

Социальные сети — большое технологическое достижение, которое сулит много возможностей, но вместе с этими возможностями приходят и неприятности. Нельзя сказать, что социальные сети это один сплошной вред. Во всем должен быть разумный подход, нам необходимо соизмерять вред и пользу нашего нахождения в социальной сети. Польза очевидна - например, можно познакомиться с новыми людьми, которые находятся очень далеко, можно общаться с друзьями, с которыми давно не виделись или они находятся вне зоны непосредственной досягаемости, можно очень оперативно получить новую информацию о чем-либо или о ком-либо. Но стоит отметить и о вреде социальных сетей. Чрезмерное увлечение социальными сетями, таит в себе опасность, может негативно отразиться на нашем:

- физическом здоровье, например, известный факт, что страдает зрение, падает иммунитет, может даже испортиться осанка, так как долго находимся без движения в одной позе,

- психологическом здоровье. Погружение в виртуальный мир, например, увлечение он-лайн играми, может вызвать болезненное привыкание у ребят с возбудимой и только формирующейся психикой. По результатам проведенных исследований, в значительном количестве случаев у игроков отмечается подъем психотических проявлений, таких как бред, беспокойство, спутанность сознания, формируется ощущение безнаказанности, так как правила виртуальной игры часто ребята переносят в реальный мир, развивается синдром гиперактивности.

- также мы утрачиваем навыки межличностного общения. Очень часто бывает, что виртуальное общение иногда заменяет собой детям реальные взаимоотношения с людьми, оно способно погрузить ребенка в ирреальный мир, вытеснив желание жить обычной жизнью, не связанной с компьютером. Что не позволяет вам ребята социализироваться в обществе, то есть живое человеческое общение сводится к нулю.

Отдельного внимания заслуживает вопрос нарушения нашей личной безопасности (нарушение приватности) - информация, которую дети публикуют на своих страницах, может сделать их уязвимыми для, например,

фишинговых сообщений, это когда сообщения электронной почты, отправляются злоумышленником, чтобы обманом вынудить вас посетить поддельные веб-узлы и предоставить личные данные;

в отношении вас могут совершаться действия, так называемой мистификации, это сообщения электронной почты, чтобы обманом вынудить пользователя отдать деньги.

и многое другое.

Более подробно о рисках мы поговорим чуть позже (слайд 5)

СЛАЙД 3

Регистрация в любой социальной сети всегда должна начинаться с прочтения Пользовательского соглашения и Политики конфиденциальности, которые, как правило, размещены в доступном месте на главной странице в любой социальной сети. Но, к сожалению, которые мы никогда не читаем. Повторюсь, что когда мы указываем максимальный набор данных о себе, то такими своими действиями мы сами создаем опасности, угрожающие нашей приватности в сети Интернет. Прежде чем регистрироваться, именно в соответствующих Правилах следует ознакомиться, как можно установить настройки приватности в сети, а также обратить внимание на предупреждения социальной сети о том, что чем больше информации о себе мы размещаем в Интернете, тем проще другим пользователям установить нашу личность. Поэтому, еще раз говорим о том, что при регистрации в социальных сетях по-возможности не указывать набор личной информации о себе, в максимальном объеме. Это же принцип работает и в дальнейшем, когда мы начинаем общение в социальной сети.

СЛАЙД 4

Так что же такое личная информация, из чего она состоит. Личная информация равнозначна по смыслу с понятием **персональные данные.** Важность особенного отношения к личной информации, персональным данным можно подчеркнуть тем, что принят специальный закон по этой теме, закон, определяющий порядок обращения с персональными данными - Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.2006. В этом законе раскрывается и персональных данных - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту).

Чтобы вам было понятно, приведу примеры персональных данных. К персональным данным можно отнести: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, а также к персональным данным могут быть отнесены файлы **cookie**, являющиеся онлайн-идентификатором, и геолокационные данные и др.

Кстати, отдельно можно поговорить, о пользовании средствами геолокации. Исследования показали, что использование геотегов являются возможными угрозами собственной безопасности и считаются одним из способов распространения личной информации. Нужно понимать, что «чекиниться» (то есть отмечать свое местоположение; от англ. check-in – регистрация) опасно из-за

угрозы собственной жизни или имуществу. Например, если мы оставляем свое имущество без присмотра и при этом оставляем в Сети информацию о своем текущем местоположении (уезжая с родителями в путешествие и размещаем на своей страничке в Интернете фотографию с места отдыха с геометкой), то воры могут использовать эту информацию как сигнал для своих действий.

Еще один минус такого раскрытия информации состоит в том, что она позволяет выявить предпочтения и интересы, что может дать мошенникам возможность использовать различные уловки для привлечения внимания к некачественным услугам (например, на своей страничке вы часто размещаете фотографии с тренировок с геотегами, как следствие, к вам может начать поступать навязчивая реклама товаров, связанных с видом спорта, которым вы занимаетесь). Поэтому пользователям не стоит увлекаться использованием новых возможностей социальных сетей и не забывать о том, что информация об их местоположении может быть крайне важной. Во избежание проблем на смартфоне эту функцию лучше вовсе отключить.

Мы уже много говорили об объеме, персональных данных, который следует указывать при регистрации в социальных сетях, поэтому еще раз, обращаем внимание, что предлагаемые формы регистрации содержат поля, которые вовсе не обязательны для заполнения и не заполняя которые, все равно можно создать свой аккаунт.

СЛАЙД 5.

В виртуальной реальности, существует особенность, которая, состоит из двух частей: «Написать опаснее, чем сказать» и «За каждым словом и действием всегда следят посторонние». Таким, образом, мы опять возвращаемся к негативным последствиям (рискам) размещения в Сети личной информации о себе, либо о друзьях. В качестве примеров можно привести следующие случаи:

Нежелательная информация. Получая информацию в социальной сети, ребята должны понимать, что всегда есть риск натолкнуться на вредную информацию, призывающую к употреблению наркотиков, суициду, информацию о псевдорелигиозных и мистических действах, сектах, мошеннические и порнографические ресурсы. Поэтому важно критически относиться к тому, о чем вы узнали из Сети, не доверять сразу, а разумно и обдуманно относиться к прочитанному.

Угроза мошенничества. В сети можно столкнуться с различными услугами, которые предлагаются после оплаты СМС на короткий номер. Чаще всего это обычное мошенничество, так как, выполнив, просьбу об отправке СМС на короткий номер, Вы не получите обещанное. Например, многие из Вас играют в он-лайн игры, и если отправка СМС необходима для покупки некоторых артефактов для игры, это должно быть всегда согласовано с родителями.

Угрозы существуют и если вы принимаете файлы от незнакомых людей, при этом открывать сомнительные ссылки не следует, потому что в результате этого можно заразить компьютер вирусами.

Опасное общение. Вы уже взрослые, и должны понимать, что нельзя общаться с незнакомыми людьми. Вообще стоит осторожнее знакомиться в

интернете, всегда очень внимательно и критично относиться к явно выраженному желанию встретиться, созвониться, списаться по электронной почте. Потому что, к сожалению, есть в нашей практике факты, когда такие встречи заканчивались совершением в отношении детей различных преступных деяний. Рискованно вступать в группы, которые на первый взгляд не содержат негативных проявлений или негативной информации и кажутся группами для общения, а в последующем вовлекают ребенка в различные деяния, в том числе противоправные.

Тем более не следует моментально встречаться с виртуальными друзьями в реальной жизни, пока вы не узнали его лучше, как бы они этого ни хотели, друг может оказаться не тем, за кого он себя выдает.

Важно также отметить еще один момент, если от знакомого человека приходят странные сообщения, нужно, не отвечая, сообщить родителям. Технические «умельцы» могут взломать любой аккаунт и использовать его для распространения спамерских сообщений и иных сообщений противоправной направленности. Также может быть взломан и ваш аккаунт. И чтобы особо не привлекать к себе внимание и избежать негативных последствий стоит выбрать какой-нибудь ник и нейтральный не вызывающий аватар.

И у же много говорили, что не стоит делать свои личные странички достоянием всего интернета, а ограничиться группой друзей, которых знаешь лично. И уж более того нельзя сообщать информацию о родителях: полное имя, где они работают и свой настоящий адрес.

Информация, содержащая персональные сведения не только о вас, но и о ваших близких — это риск вызвать интерес со стороны граждан, ведущих не совсем законный образ жизни. Например, ребенок, делясь с неограниченным кругом знакомых информацией о том, что ему приобрели дорогостоящей телефон или его семья в ближайшее время планирует продать или купить недвижимость ставит в опасное положение благосостояние своей семьи.

Нарушение чужой приватности. Также дети должны понимать, негативные последствия, которые могут наступить от разглашения, распространения личной информации и о знакомых и друзьях. Можно сказать, что размещать фотографии друзей в Интернете без их разрешения так же нехорошо, как и читать чужие письма.

Мы четко должны понимать, что в Интернете нет кнопки «Удалить», чтобы бесследно удалить информацию, которую вы там вольно или невольно разместили. Нужно помнить о том, что та информация, которую мы выкладываем в Интернет, там и хранится, она никуда не исчезает. Даже если ее удалить в одном месте, она там находится, и уже распространяется, в последующем даже без участия ее создателя. Например, вы можете пожалеть о создании, комментария, например, в виде:

- замечания по отношению к любому человеку;
- размещения своей или чужой фотографии;
- скриншота какого-либо документа, содержащего обстоятельства личной жизни другого человека либо своей жизни,

и после написания удалить этот комментарий в течение короткого времени, НО!!! этот комментарий уже прочитан десятками или сотнями людей и столько же

людей перенаправили его по разным адресам, и личная информация стала общедоступной.

Таким образом, какие-то ваши действия, шутки, комментарии сохранятся и будут отражаться не только на вашей жизни, но и на жизни ваших близких, знакомых и друзей, которых они касаются.

Интегрируясь в мир интернет-технологий, подростки становятся уязвимыми к виртуальной агрессии сверстников, которая может довести до самых печальных результатов. Отдельно стоит остановиться на так называемом троллинге в социальных сетях. **Кибербуллинг (Интернет-троллинг)** провокационные агрессивные сообщения, издевательства, оскорбления, угрозы, сообщение другим лицам компрометирующих данных, с помощью современных средств коммуникации (социальных сетей, почтовых ящиков электронной почты, мессенджеров и т.п.) как правило, в течение продолжительного периода времени. Вот несколько советов, которых стоит придерживаться, чтобы не стать жертвой:

1. Не спеши выбрасывать свой негатив в кибер-пространство. Советуйся со взрослыми, прежде чем отвечать на агрессивные сообщения. Прежде чем писать и отправлять сообщения, следует успокоиться, утолить злость, обиду, гнев.

2. Храни подтверждения фактов нападений. Если ребенка очень расстроило сообщение, картинка, видео и т.д., следует немедленно обратиться к родителям за советом, а старшим детям — сохранить или распечатать страницу самостоятельно, чтобы посоветоваться со взрослыми в удобное время.

3. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать — часто кибер-буллинг вследствие такого поведения останавливается на начальной стадии. Опытные участники интернет-дискуссий придерживаются правила: «Лучший способ борьбы с неадекватами — игнор».

4. Если ты стал очевидцем кибер-буллинга, правильным поведением будет: а) выступить против агрессора, дать ему понять, что его действия оцениваются негативно, б) поддержать жертву — лично или в публичном виртуальном пространстве предоставить ей эмоциональную поддержку, в) сообщить взрослым о факте некорректного поведения в кибер-пространстве.

5. Блокируй агрессоров. В программах обмена мгновенными сообщениями есть возможность блокировки сообщений с определенных адресов. Пауза в общении часто отбивает у агрессора желание продолжать травлю.

Ребята, вы должны понимать, что выражение «Виртуальная реальность», содержит в себе две составляющие, из которых вторая – «реальность» точно отражает суть дела: всё, что происходит в Сети, реально, и опасности там тоже реальны.

СЛАЙД 6, 7. Но, тем не менее, главная ошибка, подстерегающая в Сети детей, — ощущение, что все это игра. Не видя перед собой лицо человека, не получая привычный отклик в виде жестов, интонации и мимики, легко почувствовать, что все это понарошку, и сказать лишнее. Нужно соблюдать нормы корректного общения, чтобы в свою очередь не провоцировать такие действия по отношению к себе. Вы, подростки, должны придерживаться принципа: не пиши в Интернете того, что не сможешь сказать человеку в глаза, стоя перед всем классом

и всеми знакомыми. В Сети каждый человек может придумать себе новую жизнь, новое «амплуа», новое поведение. Ведь крайне маловероятно, что правда рано или поздно выяснится. Таким образом, человек не боится, что когда-то ему придется отвечать за поступки, высказывания, действия, поэтому он ведет себя как угодно, как правило, совсем плохо, некорректно. Чтобы быть цивилизованными людьми необходимо соблюдать элементарные правила общения в Сети при общении с другими пользователями:

- старайтесь быть вежливыми, деликатными, тактичными и дружелюбными;
- старайтесь не реагировать на обидные комментарии, хамство и грубость других пользователей. Если решить проблему мирным путем не удалось, напишите жалобу администратору сайта, потребуйте заблокировать обидчика. Если администратор сайта отказался вам помочь, прекратите пользоваться таким ресурсом и удалите оттуда свои данные;
- не используйте Сеть для распространения сплетен, угроз или хулиганства.

В заключении еще раз обобщим, все то, что мы услышали, для того чтобы соблюдать правила безопасного поведения в сети Интернет:

- отклонять запросы о добавлении в друзья от незнакомцев;
- не стоит переходить по ссылкам, которые поступают от неизвестных адресатов;
- обязательно регулярно проверять все ли настройки безопасности включены и являются рабочими. Ограничивать открытый доступ к персональной страничке, таким образом, чтобы ее не мог видеть любой пользователь, зарегистрированный в социальной сети;
- использовать сложные пароли. Не сообщать пароли от своих аккуантов кому-либо;
-не отправлять свои личные данные незнакомцам;
- по-возможности не указывать набор персональных данных о себе, в максимальном объеме;

СЛАЙД 8.

Рассказать учащимся об информационно-развлекательном сайте для детей и подростков http://персональныеданные.дети/ , созданном Роскомнадзором с демонстрацией его возможностей.

На сайте размещены информационные материалы для детей, в виде интересной и познавательной информации. Все материалы на портале разрабатывались с учетом ошибок детей в онлайн среде, о которых становилось известно Роскомнадзору в рамках повседневной работы. На этом портале можно найти различные материалы, которые не только помогут детям понять важность конфиденциальности личной жизни при использовании цифровых технологий, но и смогут помочь детям понимать последствия, которые информационные технологии оказывают на личную жизнь человека, а также на Портале предоставлены инструменты и информация, необходимая детям для принятия решений в вопросах виртуальной жизни.

В настоящее время на сайте представлены правила «Как защитить гаджеты от вредоносных программ», «Как общаться в Сети», «Как защитить персональные

данные в сети», а также размещены интерактивные материалы (презентации, тесты, игры), объясняющие основы информационной безопасности детям, а также целью, которых является закрепление прочитанного материала.

СЛАЙД. 9

В заключении, провести блиц-опрос:

1. Каких данных достаточно для регистрации в соц.сети.
2. Каким рискам персональные данные подвергаются в сети Интернет.
3. Какие способы защиты можно придумать.

Анализ полученных в ходе проведения внеклассного урока знаний предлагаем провести отдельным уроком посредством прохождения теста с сайта «http://персональныеданные.дети» Что ты знаешь о персональных данных?

Список медиаисточников:

1. портал http://персональныеданные.дети
2. Портал персональных данных (https://pd.rkn.gov.ru)
3. Видео-материалы для проведения уроков по вопросам защиты персональных данных, размещенные в разделе «Мультимедиа» Портала персональных данных (https://pd.rkn.gov.ru/multimedia/video114.htm)

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

РОСКОМНАДЗОР

3

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.*

РОСКОМНАДЗОР

4

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.

РОСКОМНАДЗОР 5

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.

РОСКОМНАДЗОР 6

http://персональныеданные.дети/

К биометрическим персональным данным относятся:

РОСКОМНАДЗОР

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

БИОМЕТРИЧЕСКИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

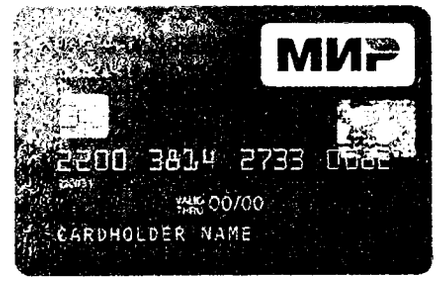
РОСКОМНАДЗОР

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.дети/

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.

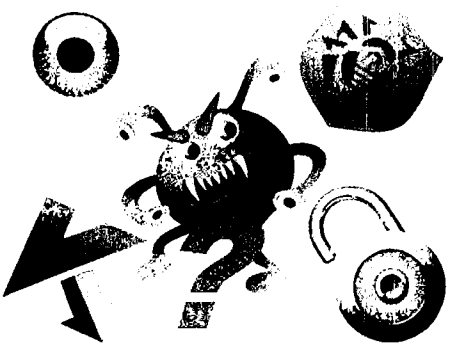
Большие данные используются для:

- направления адресной рекламы;
- при приеме на работу…

РОСКОМНАДЗОР

9

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.

РОСКОМНАДЗОР

10

Как защитить электронные устройства от вредоносных программ?

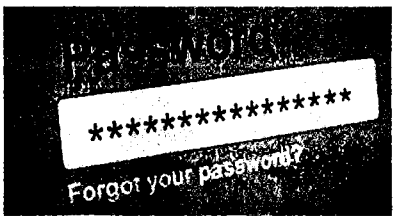
- Используйте только лицензионные программы. Чаще всего вирусами бывают заражены пиратские копии программ.
- Используйте проверенные сайты.
- Делайте резервную копию важных данных.
- Периодически меняйте пароли от электронной почты, социальных сетей, форумов и пр.

РОСКОМНАДЗОР

15

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).

РОСКОМНАДЗОР

16

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.

РОСКОМНАДЗОР

17

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, RJYUHTUFWBZ — 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 с оставления 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.

РОСКОМНАДЗОР

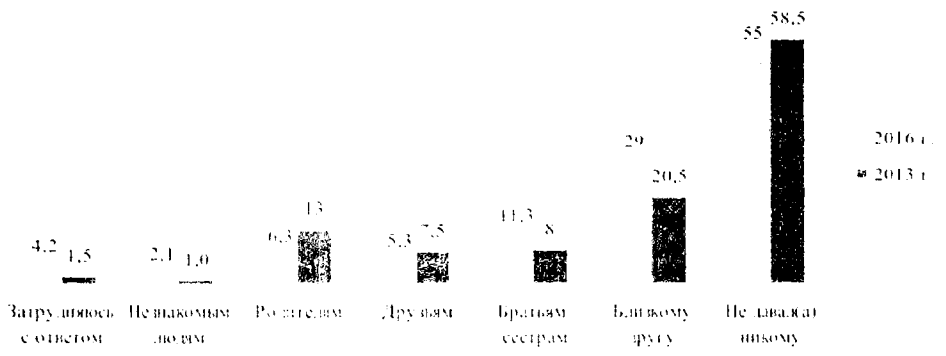
18

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:o: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%H4J#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.

РОСКОМНАДЗОР

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)

РОСКОМНАДЗОР

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.

РОСКОМНАДЗОР

17

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.

РОСКОМНАДЗОР

22

- 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).

РОСКОМНАДЗОР

19

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).

РОСКОМНАДЗОР

20

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

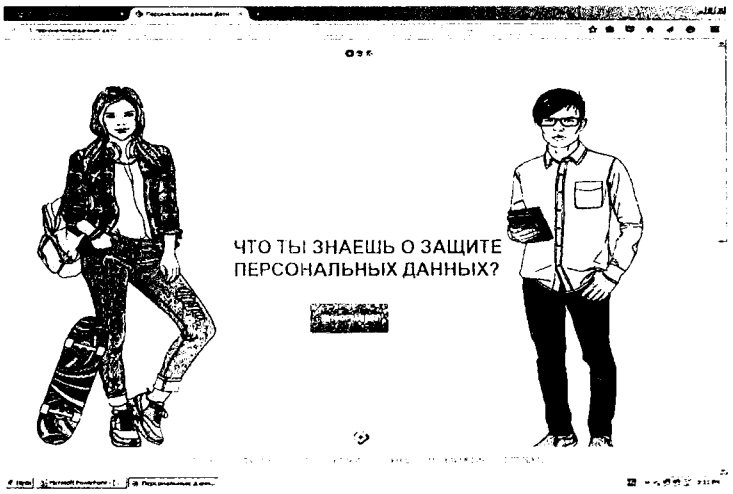
Также можете воспользоваться горячей линией по приему сообщений о противоправном контенте в Интернете на сайте Фонда содействия развитию сети Интернет – «Дружественный Рунет»: www.friendlyrunet.ru

РОСКОМНАДЗОР

21

http://персональныеданные.дети/

- информационно-развлекательный сайт о персональных данных и их защите



РОСКОМНАДЗОР

22

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.

РОСКОМНАДЗОР

23

http://персональныеданные.дети/

Агент

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

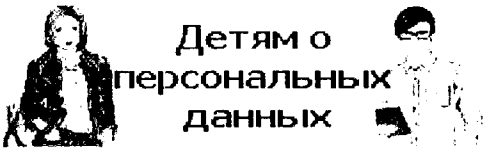
РОСКОМНАДЗОР

24

СПАСИБО ЗА ВНИМАНИЕ!

РОСКОМНАДЗОР

Обеспечение информационной безопасности детства



Социальные сети.
Быть или не быть, вот в чем вопрос....

Польза и вред социальных сетей

проект Роскомнадзора
"Персональныеданные.дети"

Кому доступна, указанная информация

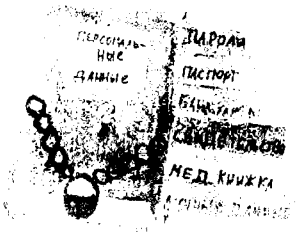
«Размещая информацию на персональной странице, в том числе, свои персональные данные, Пользователь осознает и соглашается с тем, что указанная информация может быть доступна другим пользователям сети Интернет» *

** Выдержка из Правил «ВКонтакте», которые почти никто не читает при регистрации!*

проект Роскомнадзора
"Персональныеданные.дети"

Персональные данные - вся информация, указанная Вами при регистрации и в дальнейшем размещаемая на странице:

- ФИО
- email
- Номер телефона
- Школа, класс...
- Адрес
- Фото
- Сведения о предпочтениях (группы, посты и т.д.)
- Геопозиция
- IP-адрес
- и т.д.



проект Роскомнадзора
"Персональныеданные.дети"

Риски размещения информации в сети:

- Информация может попасть в руки злоумышленникам
- Взросление (размещенный Вами пост сегодня, через несколько лет может вызвать у Вас чувства стыда и неуместности)
- Ответственность (общаясь в соц.сетях можно оскорбить человека, за что предусмотрена ответственность - статья 5.61 КоАП РФ)
- Размещаемая Вами информация, может негативно отразиться на родителях
- Размещаемая Вами информация, может негативно отразиться на Вашем будущем (учеба, работа...). Интернет «помнит всё»!!!!!

«Виртуальная реальность»!!!! Второе слово точно отражает суть дела: **всё, что происходит в Сети, реально, и опасности там тоже реальны**.

проект Роскомнадзора
"Персональныеданные.дети"

Как общаться в Сети

- 1. Не выкладывайте личную информацию (совместные фотографии, видео, иные данные) о ваших друзьях в Интернет без их разрешения.
- 2. 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.
- 3. При общении с другими пользователями старайтесь быть вежливыми, деликатными, тактичными и дружелюбными.
- 4. Старайтесь не реагировать на обидные комментарии, хамство и грубость других пользователей.
- 5. Если решить проблему мирным путем не удалось, напишите жалобу администратору сайта, потребуйте заблокировать обидчика.
- 6. Если администратор сайта отказался вам помочь, прекратите пользоваться таким ресурсом и удалите оттуда свои данные.
- 7. Не используйте Сеть для распространения сплетен, угроз или хулиганства.
- 8. Не встречайтесь в реальной жизни с онлайн-знак разрешения родителей или в отсутствие взрослого ч

проект Роскомнадзора
"Персональныеданные.дети"

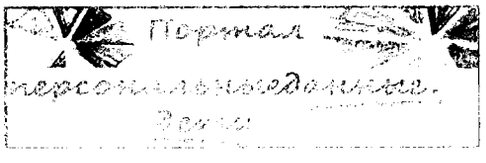
Безопасность Ваших данных

Также как и личный дом с вещами и ценностями, надо держать взаперти свой аккаунт с личной информацией

- **При составлении паролей рекомендуется придерживаться следующих правил:**
- Пароль должен содержать не менее **шести** символов.
- В состав пароля могут входить цифры, латинские буквы, пробелы и специальные символы («.», «,», «?», «!», «<», «>». «"» и др.).
- Рекомендуется составлять пароль из смешанного набора цифровых и буквенных (прописных и строчных) символов.
- **Не используйте в качестве пароля:**
- Общеупотребительные слова и устойчивые словосочетания.
- Наборы символов, представляющие собой комбинации клавиш, расположенных подряд на клавиатуре, такие как: **qwerty, 123456789, qazxsw** и т. п.
- Персональные данные: **имена, фамилии, адреса, номера паспортов, страховых свидетельств и т.д.**

проект Роскомнадзора
"Персональныеданные.дети"

О портале персональныеданные.дети



- 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.
- Портал поможет детям понимать последствия, которые информационные технологии могут оказать на личную жизнь, и предоставить им инструменты и информацию, необходимые для принятия решений в вопросах виртуальной жизни.

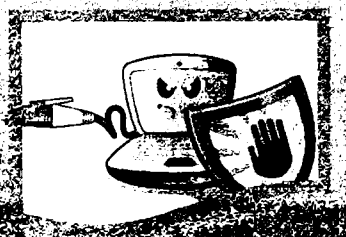
проект Роскомнадзора
"Персональныеданные.дети"


Спасибо за внимание
РОСКОМНАДЗОР
проект Роскомнадзора
"Персональныеданные.дети"

Есть в большой сети злодей
Злой и страшный Бармалей!
Поджидает он детей,
Способом обманным,
Он желает, вход найти
К ПЕРСОНАЛЬНЫИ ДАННЫМ!

Данные свои храни,
Никому не говори,
Бережно к ним относись,
В ИНТЕРНЕТЕ не делись!

Будь на страже своих персональных данных



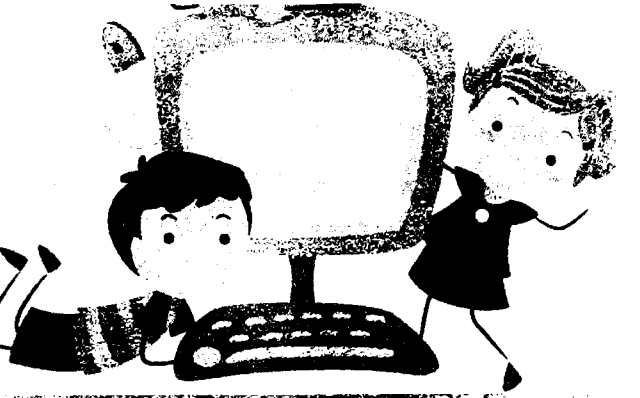
Управление Роскомнадзора по
Северо-Западному федеральному округу
Телефон: [illegible]
[illegible]

РОСКОМНАДЗОР

Береги свои ПЕРСОНАЛЬНЫЕ ДАННЫЕ!

Правила безопасности в сети интернет

для тебя и твоих друзей



Или добрый милый мишка?
Может спорт это и книжка?
На вопрос об Интернет,

Мы откроем Вам секрет.
Это вовсе не злодей,
Собирает сто друзей,
Ищет нужные вещички,
И уроки, и странички,
В Интернете все легко,
Клик и все уже нашлось.

Можно книгу отыскать,
Можно сказку прочитать,
Посмотреть любое диво,
Что красиво и игриво,

А еще там все ответы,
Обо всем на белом свете...
НО!

Нельзя Вам забывать,
Кроме пользы, Важно знать!
Безопасность в Интернете,
Надо детям соблюдать!

далее правила

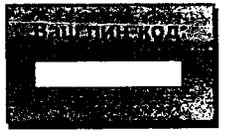
1

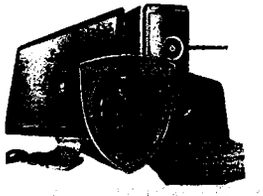
фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.

2

Если Вы нашли страничку,
Где к Вам просится безличка –
это злое приложение,

Хочет вирус навязать,
Просит Вас пин - код отдать?
Или просит Ваше имя, адрес,
карту, телефон,





Никогда нельзя ребята,
Таким сайтам доверять!
Уходи оттуда просто,
Лучше взрослого спроси,
А уж если все несносно,
Антивирус запусти!

3

А еще мы в Интернете,
Можем друга завести,
Незнакомец в Интернете
[illegible]

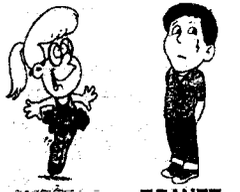
4

[illegible]
кому-нибудь из взрослых людей!

Помни! В мире Интернета,
Виртуального
пространства,
Все реально, как и в жизни
Наполняется коварством.

5

Если ты попал в
беду,
И затеял чехарду,
В Интернете видно
сразу
Кто ты, где ты, слезы
градом,
Троллят, издеваются?
Тебе это не нравится!



Не отчаивайся друг,
Ведь подмога тут как тут,
Сразу взрослым сообщай,
Все странички удаляй,
Никого не обзывай,
И в ответ не отвечай!

Все решится без труда,
Улыбнись, и будь на страже,
Своих данных личных, Важных!
Персональные они,
В твоей жизни так Важны!

Как защитить гаджеты от вредоносных программ

⇒ Установите на гаджеты специальные почтовые фильтры и антивирусные программы. Они могут предотвратить, как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

⇒ Используйте только лицензионные программы. Чаще всего вирусами бывают заражены пиратские копии программ.

⇒ Используйте проверенные сайты.

⇒ Систематически проверяйте свои домашние компьютеры на наличие вирусов.

⇒ Делайте резервную копию важных данных.

⇒ Периодически меняйте пароли от электронной почты, социальных сетей, форумов и пр.

Будьте бдительны

и соблюдайте

основные правила

Интернет-безопасности!

Управление Роскомнадзора по Северо-Западному федеральному округу

Телефон: (812) 678-95-41,

ул. М.Морская

Санкт-Петербург

Роскомнадзор

Управление Роскомнадзора по Северо-Западному федеральному округу

Правила общения в сети Интернет

персональные данные.дети

Правило 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.

Правило 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.

Правило 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. Выходите из своих аккаунтов, если пользуетесь общественными компьютерами в школе, кафе или библиотеке.

Правило 4

При общении с другими пользователями старайтесь быть вежливыми, деликатными, тактичными и дружелюбными. Не допускайте грубостей, оскорблений, матерных слов — читать такие высказывания так же неприятно, как и слышать.

Правило 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.

Правило 6

Не используйте Сеть Интернет для распространения сплетен, угроз или хулиганства. Если решить проблему мирным путем не удалось, напишите жалобу администратору сайта, потребуйте заблокировать обидчика.

Правило 7

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

Правило 8

Если к вам пришло незнакомое приложение, подумайте, стоит ли его открывать? Возможно лучше сразу его удалить.

Правило 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.

Правило 10

Не оставляйте без присмотра компьютер с важными сведениями на экране.