Типовая программа проведения внеклассных уроков для учащихся образовательных 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 п**ерсональные 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, https://digital-likbez.datalesson.ru;
2. Портал персональных данных (https://pd.rkn.gov.ru).