

Автор(ы) (ФИО, учреждение):	Галина Солдатова, доктор психологических наук, профессор, член-корреспондент РАО Антонина Приезжева, заместитель руководителя Роскомнадзора Владимир Шляпников, кандидат психологических наук, Директор по социальным проектам Фонда Развития Интернет Оксана Олькина, сотрудник Института Психологии Российской Академии Наук
Название модуля и тема внутри модуля (ненужное удалить):	Модуль 2. Информация в Интернете
Форма (ненужное удалить):	урок
Класс:	7-11
Тема урока (собрания, выступления и т.д.):	Как персональные данные попадают в сеть
Цель:	знакомство с понятием «персональные данные»
Основные вопросы	<ul style="list-style-type: none"> • какими способами в браузере появляются цифровые следы; • как персональные данные позволяют идентифицировать пользователей Сети.
Необходимые материалы:	набор из 9 карточек со скриншотами, содержащими «цифровые следы» (Приложение 3.1); ключи с правильными ответами и пояснениями для ведущего (Приложение 3.2); памятки с информацией о средствах защиты персональных данных (Приложение 3.3).
Дополнительные материалы по теме:	

Разминка «Великий идентификатор»

Задача:	помочь учащимся осознать, как по «цифровым следам» можно идентифицировать пользователей Сети
Необходимые материалы:	-
Время проведения:	10 мин

Процедура проведения:

Даже небольшие фрагменты личной информации, которые на первый взгляд могут показаться совершенно безобидными, при обобщении позволяют довольно точно идентифицировать их владельца. Для того чтобы убедиться в этом, классу предлагается следующая игра. Ведущий обращается к группе: «Сейчас я загадаю какое-нибудь существо, например, человека. Это может быть как реально существующий или живший раньше, так и вымышленный человек. Ваша задача – по очереди задавать мне вопросы, на которые можно дать ответ «да» или «нет», чтобы как можно быстрее угадать человека, которого я задумал. Давайте посмотрим, сколько вам потребуется вопросов, чтобы дать правильный ответ». После того как ведущий убеждается в том, что все участники правильно поняли инструкцию, игру можно начинать. Как правило, чтобы угадать одного человека, нужно задать не более 20 вопросов. Участник группы, первым давший правильный ответ, загадывает свое «существо». Если игра понравилась участникам, ее можно повторить несколько раз.

Обсуждение:

Кого угадать было проще, а кого сложнее? Почему?

Какая информация лучше всего помогает нам установить личность человека, т.е. идентифицировать его? Почему?

Как вы думаете, легко ли установить личность человека в реальной жизни? Почему?

Упражнение «Цифровой след»

Задача:	показать, какие «цифровые следы» могут храниться на компьютере и других устройствах, в браузере и приложениях, а также познакомить учащихся с тем, какими путями персональные данные попадают в Интернет.
Необходимые материалы:	набор из 9 карточек со скриншотами, содержащими «цифровые следы» (Приложение 3.1); ключи с правильными ответами и пояснениями для ведущего (Приложение 3.2).
Время проведения:	15 мин

Процедура проведения:

Персональные данные могут попадать в Интернет разными путями. Для того чтобы разобраться в этом вопросе, ведущий предлагает группе следующее задание.

На первом этапе класс делится на 9 групп. В зависимости от размера класса в подгруппе может быть от трех и более человек. Если класс небольшой, то можно работать в парах и даже по одному. Каждая группа получает карточку с изображением скриншота, содержащего «цифровой след» пользователя (Приложение 3.1). Задача – определить, какая информация, представленная на скриншоте, относится к персональным данным, и как она могла туда попасть. На выполнение задания отводится 5 минут. Затем каждая подгруппа по очереди озвучивает свой ответ. Ведущий сверяет ответы с ключами и в случае необходимости задает участникам наводящие вопросы (Приложение 3.2).

На втором этапе задания все карточки выкладываются на один стол или доску. Ведущий обращает внимание группы, что карточки имеют разную маркировку (белый, серый или черный квадрат в верхнем левом углу). Он предлагает участникам определить, по какому принципу маркированы карточки. Если группа не может дать правильный ответ, его дает ведущий. Если группа дает правильный ответ, ведущий его резюмирует.

Обсуждение:

О каких способах попадания информации в Интернет вы узнали впервые, а о каких уже знали?

Как вы думаете, каким способом информация чаще всего попадает в Сеть? Почему?

Как вам кажется, каким способом персональная информация о вас чаще всего попадает в Сеть? Почему?

В помощь ведущему:

Карточки разделены на три группы в соответствии с тем способом, которым они попадают в Сеть:

1 группа (белый квадрат): пользователь выкладывает в Интернет информацию о себе сам;

2 группа (серый квадрат): информацию об активности пользователя в Сети собирают приложения и онлайн-ресурсы;

3 группа (черный квадрат): информацию о пользователе в Сеть выкладывают третьи лица.

Упражнение «Заметаем следы»

Задача:	познакомить учащихся с основными средствами и функциями защиты персональных данных на компьютере и других устройствах
Необходимые материалы:	набор из 9 карточек со скриншотами, содержащими «цифровые следы» (Приложение 3.1); ключи с правильными ответами и пояснениями для ведущего (Приложение 3.2); памятки с информацией о средствах защиты персональных данных (Приложение 3.3).
Время проведения:	20 минут

Процедура проведения:

Подводя итоги предыдущего упражнения, ведущий подчеркивает, что сегодня персональные данные пользователей с легкостью проникают в Интернет, и довольно часто это происходит без нашего ведома. Тем не менее, есть много способов контролировать персональные данные в Сети и даже удалять их оттуда. Задача группы – познакомиться с такими способами.

Ведущий делит группу на три подгруппы. Каждая из них получает памятку с информацией о средствах защиты персональных данных. На ее изучение дается 5 минут (Приложение 3.3).

Затем ведущий предлагает проверить, насколько хорошо ребята усвоили материал и закрепить его на практике. Он дает каждой группе по три карточки со скриншотами (Приложение 3.1).

Задача – проанализировать каждый «цифровой след» и предложить наиболее адекватное средство защиты персональных данных в каждом случае.

На выполнение этого задания отводится 5 минут. Затем каждая группа представляет свое решение, а ученики из других групп могут задать вопросы и высказать свои комментарии. В конце ведущий сверяет ответы с ключами и поправляет участников в случае, если была допущена ошибка.

Обсуждение:

О каких средствах защиты персональных данных вы уже знали и имеете опыт их использования, а о каких услышали впервые?

Какие способы попадания персональных данных в Интернет, по-вашему мнению, контролировать сложнее всего? Почему?

Какие средства защиты персональных данных вы бы стали использовать, а какие нет? Почему?

Итоги занятия:

Существует много каналов, по которым наши персональные данные попадают в Интернет. Что-то выкладываем мы сами, что-то пишут о нас наши друзья и знакомые, определенную информацию о нас собирают приложения и онлайн-ресурсы. Все наши «цифровые

следы» хранятся на наших компьютерах и смартфонах. Если мы хотим сохранить определенный уровень конфиденциальности и хорошую репутацию в Сети, эти «следы» необходимо контролировать.

Важно знать, что «цифровые следы» также хранятся на серверах разработчиков приложений и онлайн-ресурсов, удалить их оттуда практически невозможно. Поэтому всегда нужно крайне внимательно относиться к той информации, которую мы выкладываем в Сеть, а также к тому, что мы делаем в Интернете: какие ресурсы посещаем, какие файлы скачиваем, какие делаем поисковые запросы и т. д.

На первый взгляд может показаться, что отдельные «цифровые следы» не представляют угрозы для нашей конфиденциальности. Например, многое ли можно узнать о человеке по его хобби или гастрономическим предпочтениям? Тем не менее важно понимать, что в Интернете потоки персональных данных объединяются друг с другом, как ручьи сливаются в реки, а реки в моря и океаны. Существуют сайты, которые специально собирают информацию о пользователях в коммерческих целях, например, для рекламы или маркетинговых исследований. Современные технические средства легко позволяют объединить «цифровые следы» одного пользователя в единый портрет или профайл и идентифицировать его.

Сбор персональных данных приложениями и онлайн-ресурсами – условие бесплатного и даже платного использования этих ресурсов, поэтому оградить себя полностью от этого невозможно. Всегда нужно помнить о том, что практически любое наше действие в Интернете оставляет после себя неизгладимый «цифровой след» и по возможности стремиться контролировать свои персональные данные, попадающие в Сеть.