**Персональные данные и их защита в сети Интернет**

учитель информатики МБОУ «СОШ№45 г.Челябинска»

**Жадько Н.П.**

**Слайд 1**

Одно из неотъемлемых прав каждого интернет-пользователя — **право на защиту персональных данных**.

 По данным ряда опросов, больше половины россиян не знают о своих правах в Интернете. Нет среди пользователей и точного понимания того, **что такое «персональные данные».**

Так, в нашей стране в течение 2015 г. Роскомнадзором зарегистрировано приблизительно 33 тыс. обращений от граждан с жалобами на нарушения, связанные с публикацией их личных данных в интернете.

С развитием Интернета вопросы защиты персональных данных попали в число самых актуальных вопросов безопасности не только взрослых, но и детей.

Именно поэтому важно привлечь внимание обучающихся к проблемам и последствиям ненадлежащей обработки персональных данных и широкого распространения личной информации в информационной среде.

Одним из ключевых направлений работы по защите прав субъектов персональных данных становится информационно - просветительская деятельность, в рамках которой особое внимание уделяется несовершеннолетним пользователям интернета как одной из наиболее уязвимых категорий пользователей. Главная задача — донести до российских учителей и их учеников необходимость защиты личной информации и объяснить правила безопасного управления персональными данными в Интернете.

 **Слайд 2**

В целях осуществления профилактических мер, направленных на популяризацию правил защиты персональных данных несовершеннолетних лиц Роскомнадзор в 2014 г. провел первый Всероссийский День защиты персональных данных детей, а также

**Слайд 3**, разработал информационно-развлекательный портал для педагогов, родителей и детей  [http://персональныеданные.дети/](http://xn--80aalcbc2bocdadlpp9nfk.xn--d1acj3b/)

направленный на изучение вопросов, связанных с защитой персональных данных при использовании цифровых технологий.

На сайте размещены информационные материалы для детей, которые могут быть использованы как в рамках школьных уроков по теме персональных данных, так и просто в виде интересной и познавательной информации. Все материалы разрабатывались с учетом ошибок детей в онлайн среде.

**Что такое персональные данные?**

 **Слайд 4**

Персональные данные — это любая информация, которая имеет отношение к конкретному человеку.

**Персональные данные – это совокупность данных, которые необходимы и достаточны для идентификации какого-то человека.**

**Идентифицирующие данные:**

***фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр*.**

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

 **Слайд 5**

**Виды персональных данных:**

**• Регистрационные идентификационные данные (паспортные данные, пароли, пин-коды, СНИЛС, индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты).**

**• Физические характеристики (внешние данные, биометрические данные, состояние здоровья и др.).**

**• Пространственная локализация (фиксация местоположения и перемещения).**

**• Материально-экономическое положение (движимое, недвижимое имущество, зарплата, накопления и др.).**

**• Официальные статусы (семейное положение, достижения, награды, наличие судимостей и т.д.).**

**• Профессиональная занятость (включая образование).**

**• Социальные связи (информация о родственниках, друзьях, знакомых, принадлежность к различным формальным и неформальным группам).**

**• Образ жизни и поведенческие установки (мировоззрение, ценности, интересы и хобби, социальные привычки и действия, настроения, вкусы, особенности).**

**• Психологические особенности (черты характера, способности, знания, умения, навыки, личностные черты).**

**• Хроника личных событий (личный блог, сайт и т.д.).**

 **Слайд 6**

**Основные понятия в рамках безопасного обращения с персональными данными в сети Интернет :**

*Акка́унт,* учетная запись (англ. account) – хранимая в компьютерной системе совокупность данных о пользователе, необходимых для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

*Кибербу́ллинг*(англ. сyberbulling) – намеренное и регулярное причинение вреда (запугивание, унижение, травля, физический или психологический террор) одним человеком или группой людей другому человеку с использованием электронных форм контакта.

*Конфиденциа́льность*(англ. сonfidence – «доверие») –

1. Необходимость предотвращения утечки (разглашения) какой-либо информации.

2. Обязательное для выполнения лицом, получившим доступ к определенным сведениям (сообщениям, данным) требование не передавать их третьим лицам без согласия лица, самостоятельно создавшего информацию либо получившего право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

*Фи́шинг* (англ. phishing, от fishing – «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, социальных сетей.

Вывод очень простой — чем больше мы выкладываем о себе, тем больше о нас информации узнают другие пользователи.

Стоит отметить, что о некоторых видах данных мы не задумываемся, когда выкладываем их в сеть Интернета. Утечка важной и значимой информации может негативно отразиться на нашей жизни, поэтому необходимо обратить внимание на то, что вы размещаете.

 **Слайд 7**

**МЕХАНИЗМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Существуют «Три кита» защиты персональных данных:

• **Надежный пароль**. Надежные пароли позволят защитить от третьих лиц ваши аккаунты на онлайн-ресурсах и в приложениях.

• **Управление уровнями доступа к персональным данным (настройки приватности).** Настройки приватности дадут вам возможность определить уровень доступа других пользователей к вашим персональным данным, размещенным на различных онлайн-ресурсах.

 • **Сознательное отношение к информации, размещаемой в интернете**. Правила управления персональными данными помогут вам понять, как персональные данные, размещенные в интернете, влияют на вашу репутацию в сети.

 **Слайд 8**

**Правила защиты персональных данных 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).

Прежде чем вводить свои персональные данные в интернете, необходимо убедиться, что вы находитесь именно на том ресурсе, на который хотели попасть, а не на поддельной (фишинговой) странице, созданной мошенниками. Существует несколько простых способов убедиться в подлинности ресурса:

• Всегда обращайте внимание на адресную строку браузера. Адрес поддельной странички может отличаться всего на одну букву, которую легко не заметить.

• Не стоит переходить на ресурсы по ссылкам, которые вы получили по электронной почте или в личной переписке и которые требуют ввода персональных данных — многие из них ведут на поддельные сайты. Забейте адрес в адресную строку самостоятельно, а еще лучше — используйте для поиска нужных ресурсов надежные поисковые системы, например, Яндекс.

 • Прежде чем вводить персональные данные в интернете, убедитесь, что ресурс, на котором вы находитесь, использует защищенное соединение. Если в адресной строке браузера присутствует иконка замка, а сам адрес начинается с аббревиатуры https:// вместо привычной http://, то такое соединение использует шифрование при передаче ваших персональных данных. В этом случае злоумышленникам будет гораздо сложнее перехватить ваши персональные данные и воспользоваться ими.

• Комплексные антивирусные программы также могут помочь защититься от мошенников

 **Слайд 9**

**Защита персональных данных на своем устройстве**

 • Для удаления «цифровых следов» с компьютера после работы в интернете очистите журнал посещений (в браузере) и историю поисковых запросов.

• В настройках программ сетевой защиты также можно установить запрет на загрузку временных файлов и cookies с незнакомых сайтов, ограничившись лишь проверенными и надежными ресурсами.

• Будьте внимательны с настройками мобильных приложений: отключите опцию «автосинхронизации» данных, автоматического проставления «геометок» и т.д., если хотите избежать случайного попадания персональных данных в сеть.

**Слайд 10**

**Защита персональных данных на чужом устройстве**

• При входе в свой аккаунт с чужого устройства всегда выбирайте опцию «чужой компьютер», «не сохранять пароль», «безопасный ввод» и т.д. (на странице онлайн-ресурса). В этом случае вы можете быть уверены, что никто не войдет в ваш аккаунт после вас.

• Чтобы не оставить цифровых следов на чужом устройстве, используйте режим инкогнито (в браузере). Благодаря ему история поисковых запросов и посещенных страниц не сохраняется в браузере, а сайты не загружают cookies на устройство.

 **Слайд 11**

**Защита персональных данных от третьих лиц**

• Используя вкладку «настройки приватности» (на странице онлайн-ресурса), запретите другим пользователям отмечать вас на фотографиях и упоминать в постах. Ограничьте круг лиц, которые могут комментировать ваши записи. Как правило, добавление пользователя в «черный список» автоматически лишает его возможности просматривать и комментировать ваши посты, а также упоминать вас в своих постах.

 • Если другой пользователь использует ваши персональные данные, например фотографии, без вашего согласия, вы можете пожаловаться в службу поддержки ресурса (на странице онлайн-ресурса), приложив доказательства нарушения. Если другой пользователь, разместив недостоверную или устаревшую информацию, нанес существенный урон вашим чести и достоинству, вы можете обратиться в суд.

 **Заключение**

С развитием Интернета, уже в недалеком будущем частная жизнь станет прозрачной и публичной «по умолчанию» –персональную информацию будет невозможно не открыть государству и различным организациям, а справляться с вопросами ее безопасности будет все сложнее.

 **Роскомнадзором разработаны материалы для проведения обучающих мероприятий с детьми и подростками по безопасному поведению в Интернете для двух возрастных групп детей 9-11 лет и 12-14 лет и могут быть использованы дистанционно в рамках классных часов и обучающих мероприятий со школьниками (https://pd.rkn.gov.ru/multimedia/video114.htm)**