ВОСПИТАНИЕ ЦИФРОВОЙ БЕЗОПАСНОСТИ.

ЦИФРОВОЙ СЛЕД РЕБЁНКА – БЕЗОПАСНЫЙ ЦИФРОВОЙ СЛЕД СЕМЬИ.

Бажуткина Екатерина Евгеньевна, методист СП ДОД «Детско-юношеский центр «Открытие»» ГБОУ СОШ с. Красный Яр, м.р. Красноярский, самарская область.

В современном мире всё большее внимание уделяется цифровой безопасности и цифровой гигиене. Педагог должен постоянно знакомить детей с правилами пользования сети Интернет, с особенностями использования компьютерного программного обеспечения и мобильных приложений. Все эти меры необходимы для того, чтобы уже с юношества оставлять в сети корректный цифровой след.

Цифрово́й след (англ. digital footprint; интернет-след, электронный след, цифровая тень), сведения о человеке, его поведении и предпочтениях, остающиеся в Интернете после его посещения.

Каждый человек в сети оставляет два вида цифрового следа: активный и пассивный.

Активный цифровой след — это информация, которую пользователь самостоятельно размещает в интернете. К такому следу относятся регистрация и публикация постов в социальных сетях, видеохостингах и интернет-блогах. Активный цифровой след человека постоянно растёт, и, чем больше пользователь делится постами и фотографиями, тем больше о нём можно узнать из открытых источников.

Пассивный цифровой след — это информация, которая сохраняется и попадает в интернет без ведома пользователя.

Пассивный цифровой след формируется множеством различных способов. Но у такого следа есть несколько основных понятий:

1. Куки (cookies) — это хранящиеся на компьютерах и гаджетах небольшие файлы, с помощью которых сайт запоминает информацию о посещениях пользователя. В таких файлах может храниться следующая информация: время и устройство с какого человек заходил на страницу; предпочтения пользователя (например, язык, валюта или размер шрифта); товары, которые просматривались или добавлялись в корзину, даже если пользователь временно вышел из интернет-магазина; текст, который ранее вводился на сайте; IP-адрес и местоположение пользователя; дата и время посещения сайта; версия операционной системы и браузера; клики и переходы.
2. IP-адрес — это уникальный номер вашего компьютера в интернете, который формируется в момент его подключения к Сети. Он позволяет идентифицировать устройство.
3. Данные из мобильных приложений. Мобильные приложения способны собирать следующие данные: название сотового оператора; контактная информация пользователя (телефон, электронные адрес); данные об устройстве (идентификатор, ОС и т.д.); посещенные веб-сайты (история браузера); геолокация пользователя (его маршруты); перечень установленных программ на устройстве.
4. Фингерпринт — это уникальная совокупность характеристик устройства: модели гаджета, его месторасположения, настроек браузера, времени посещения сайтов, разрешения экрана и других параметров. Все вместе они могут указывать на конкретного пользователя, как отпечаток пальцев. Благодаря этому фингерпринт позволяет идентифицировать человека, даже если он использует инструменты для повышения анонимности в интернете.

Все данные, собранные о пользователе в Интернете, составляют часть его цифрового портрета и могут использоваться организациями и корпорациями для удобства пользования сайтом или приложением. Но информация об активности человека в интернете может попасть и к мошенникам. Часто для получения данных о пользователе злоумышленники используют схемы фишинга.

Фи́шинг - вид компьютерного мошенничества, целью которого является получение доступа к конфиденциальным данным (логинам и паролям) пользователей онлайновых служб.

Например, одна из распространённых схем фишинга — прислать пользователю письмо со ссылкой на сайт, имитирующий интернет-магазин, на котором он только что смотрел товары. Человек может подумать, что просто продолжает покупки. Если ввести данные банковской карты на таком сайте, то можно потерять деньги.

Поэтому важно помнить про цифровой след и стараться его минимизировать, используя разные подходы и инструменты. Цифровой след способен влиять не только на виртуальную жизнь пользователя, но и на реальный мир, так как он может стать частью репутации человека. Если пользователь выкладывает пост в социальных сетях, то он теряет контроль над этой информацией. Любой пользователь может сделать скриншот или сохранить файл к себе на компьютер. А ещё удалённую информацию можно найти в веб-архиве. Виртуальные атаки мошенников способны лишить пользователя реальных денежных средств.

Для защиты своего цифрового следа можно использовать несколько подходов. Важно сообщать о способах защиты информации детям при любом удобном случае на занятиях, которые предполагают выход в сеть Интернет или работу с программным обеспечением.

Советы для пользователей:

Желательно закрывать профили в соцсетях. Так можно ограничить круг людей, которые следят за жизнью пользователя в интернете.

Осознанно выбирать браузеры, которые отклоняют сторонние cookie-файлы или же блокируют трекеры, чтобы никто не мог собирать данные без согласия пользователя.

Добавлять в браузер блокировщик трекеров. Трекер — это специальная программа, которая собирает информацию о том, какие страницы вы просматриваете, чтобы потом показывать вам персонализированную рекламу.

Запретить сайтам и приложениям собирать необязательные данные. При установке приложения не следует разрешать ему доступ к данным, без которых оно сможет обойтись.

Не использовать общественный Wi-Fi. В таких сетях часто не используются пароли или протоколы шифрования WPA/WPA2. Злоумышленник может узнать информацию о подключённых устройствах или даже личные данные участников сети. Чаще всего крадут пароли и информацию о банковских картах.

Не авторизовываться на сайтах через соцсети и «Госуслуги». Это может быть удобно, но при такой авторизации вы передаёте сайту большое количество дополнительной информации о себе. Например, сервис сохранит не только вашу почту, но может

При поиске своего цифрового следа можно воспользоваться социальными сетями, так как цифровой портрет формирует сам пользователь и его друзья и родственники. Следующим шагом будет ввод своих данных в поисковую строку браузера. Так можно найти достаточное количество информации и по возможности удалить ненужную. Избавиться от цифрового следа полностью невозможно, но можно принять меры для уменьшения его размера и ограничения доступа

к личной информации. Для этого пользователь очищает историю браузера и cookie-файлы, удаляются неиспользуемые аккаунты в онлайн-сервисах, так как чем меньше данных хранится в Сети, тем меньше риск их кражи.

Цифровой след — это любая информация о человеке, которая попадает в интернет. Его нельзя удалить, но можно минимизировать риски, связанные с кражей данных о пользователе. Советы по цифровой гигиене необходимо постоянно давать обучающимся на занятиях.

Литература:

1. Габдрахманов, Н.К. Цифровой след в прогнозировании образовательной стратегии выпускников школ / Н.К. Габдрахманов, В.В. Орлова, Ю.К. Александрова // Университетское управление: практика и анализ. — 2021.

2. SkillboxMedia: https://skillbox.ru/media/code/chto-takoe-tsifrovoy-sled-i-kak-on-vliyaet-na-vashu-zhizn/?ysclid=m2a3l721vp340415455;

3. Большая Российская энциклопедия: https://bigenc.ru;

4. Словарь Картаслов.ру: https://kartaslov.ru/значение-слова/фишинг;

5. Энциклопедия «Секрет фирмы» https://secretmag.ru/enciklopediya/chto-takoe-kuki-cookies-obyasnyaem-prostymi-slovami.htm;