

УДК 364.12

ОПАСНОСТИ «ЦИФРОВЫХ СЛЕДОВ» ДЛЯ ЧЕЛОВЕКА

Хаданова К.В., студент гр. ПИМ-191, I курс
Научный руководитель: Баумгартэн М.И., к.ф.-м.н., доцент
Кузбасский государственный технический университет
имени Т.Ф. Горбачева,
г. Кемерово

В настоящее время сложно представить свою жизнь без пользования различными сервисами сети Интернет. Мы ищем нужную информацию, отправляем сообщения, оставляем комментарии и совершаем интернет-покупки. У большинства людей есть страницы в соцсетях, куда они загружают фотографии и данные о себе. Огромное количество информации хранится в цифровом виде. С одной стороны, такая доступность позволяет быстро найти нужные данные, а с другой – ставит под угрозу безопасность пользователей.

Всё дело в существовании так называемого «цифрового следа», который оставляет каждый пользователь сети. Цифровой след – это любая информация, переданная человеком (электронные письма, фотографии, документы), информация от просмотра веб-страниц и любые другие данные, остающиеся в виде записей в базах данных в Интернете [1].

Цифровые следы могут быть активными или пассивными [2]. К активным относят всё то, что пользователь осознанно публикует в Интернете. Это личные данные в социальных сетях, фотографии и видео, отзывы на специальных платформах, отметки «нравится», геолокации, регистрация на сайтах и тому подобное – всё, что создано непосредственно пользователем. Эту информацию легче всего найти в сети, имея лишь первоначальные данные о конкретном человеке, например имя и фамилию.

Создавая же пассивный след, пользователь не всегда отдаёт себе в этом отчет. Даже будучи неавторизованным, он может просто посещать различные сайты или искать нужную информацию в электронных системах поиска. При этом могут сохраняться данные о его IP-адресе и дате посещения веб-страниц, действия, совершенные на сайтах (например, список просмотренных разделов сайта или товаров интернет-магазина). Чаще всего этими данными интересуются маркетологи и IT-компании, целью которых является продажа товаров или услуг в сети Интернет, поскольку этот процесс значительно упрощается при соответствии предложения интересам пользователя. Так появляются персонализированные новости и реклама.

Может показаться, что не оставлять цифровые следы не так уж сложно, если не пользоваться соцсетями и не выкладывать свою информацию, но это не так. Существует такое понятие, как «цифровая тень». Человек создает ее,

сам того не подозревая, даже если не пользуется Интернетом вообще. Можно случайно попасть в объектив чужого фотоаппарата или на записи камер видеонаблюдения, которые позже окажутся в Интернете в облачных хранилищах данных или новостных блогах. Таким образом, цифровая тень – это информация о человеке, загруженная в сеть кем-то другим. И если контролировать свой цифровой след не так уж сложно, то в случае с цифровой тенью нельзя быть ни в чем уверенным. В любом случае объем генерируемой о человеке информации постоянно только увеличивается.

Из чего же состоит цифровой след человека? Принято считать, что наибольшую долю новой информации составляют видеоматериалы (фотографии, видеоролики, записи камер наблюдения), на втором месте текстовые данные (электронные сообщения, документы). Менее популярный тип данных – голосовые записи, в числе которых переданные через Интернет и сотовую связь. Также существуют логи – записи о действиях пользователей на веб-сайтах. К счастью для беспокоящихся о своем цифровом следе пользователей, из-за большого объема этих данных они хранятся всего несколько дней, а затем удаляются.

Если кто-то выкладывает в сеть фотографию, на которой изображено много людей, то для пользователя, который ее опубликовал, это будет являться цифровым следом. Для тех же, кто изображен на фотографии, но не был в курсе такой публикации, это начало цифровой тени. Даже если после этого удалить фотографию из общего доступа, информация о ней скорее всего останется навсегда в базах данных и виртуальных хранилищах. Многие облачные ресурсы считают своим преимуществом и всячески рекламируют пожизненное хранение файлов. Они вообще не удаляют их, а лишь архивируют.

Частью цифрового следа будут текстовые сообщения, передаваемые через соцсети и электронную почту, электронные документы. Даже никнеймы, используемые на различных сайтах и форумах, могут дать некоторую информацию о человеке.

Что касается голосовых данных, записи разговоров могут быть сделаны телефонными операторами для проверки качества связи или настройки алгоритмов передачи. Разговор может записать и собеседник с целью использования полученных данных. Хотя в сравнении с объемами информации остальных типов в наше время это, пожалуй, наименее распространенный.

Даже просто выйдя из дома, человек оказывается под прицелом камер видеонаблюдения. Они стоят в подъездах, в крупных магазинах и возле них, в офисах и других общественных местах. Камеры на дорогах фиксируют нарушения транспортных средств, записывая при этом их номера, местонахождение, время, направление и скорость передвижения. При этом данные с любых камер всё чаще записываются не на пульта операторов, а напрямую на сервера, находящиеся во Всемирной паутине. Эту информацию собирают в основном в целях охраны порядка, но это не значит, что доступ к ней не подлежит взлому, и не гарантирует никакой конфиденциальности.

Чем же опасны цифровые следы и цифровые тени? Для тех, кому нечего скрывать, основной опасностью является раскрытие личных данных мошенникам, которые могут воспользоваться ими для своей выгоды, попытаются обмануть человека или, например, снять средства с его банковских карт. Если же есть какие-то сведения, которые должны остаться в тайне, цифровые следы и тени ставят под угрозу конфиденциальность и безопасность. Кроме того, злоумышленники могут шантажировать людей, угрожая придать огласке какие-либо важные факты или данные.

Цифровая тень в настоящее время мало структурирована, и для того, чтобы найти информацию о человеке, требуются большие вычислительные мощности, специальные программы и много времени [3]. Но уже сейчас развиваются технологии для распознавания лиц и автоматической сортировки больших объемов данных. Возможно, в скором времени достаточно будет одной фотографии для поиска всей доступной информации о человеке.

Цифровая тень существовала и раньше, однако с каждым годом масштабы этого явления всё увеличиваются. Сейчас практически у каждого есть телефон с камерой, способный в любой момент сделать фото, записать аудиофайл или видео и тут же выложить всё в Интернет. Мобильные приложения используют геолокацию и могут отследить текущее местоположение человека, соцсети начинают использовать системы распознавания лиц. В некоторых странах, например в Китае, такие системы уже используются повсеместно и позволяют собирать данные о людях, попадающих в поле зрения камер видеонаблюдения. Но чаще всего люди сами публикуют информацию о себе, оставляют контактные данные и сотни личных фотографий в соцсетях. При этом даже факт того, что страница закрыта от посторонних, не гарантирует безопасности. Доступ к любым материалам всегда имеют администраторы сайтов и правоохранительные органы. Кроме того, известны случаи крупных взломов и утечки информации из баз данных.

В безопасность цифровой тени можно верить лишь до тех пор, пока не получится представить, какие огромные объемы информации каждый день попадают в Интернет и какое количество людей имеет к ним доступ. Цифровой след могут изучать работодатели перед приемом на работу или молодые люди перед началом отношений [4]. В любом случае его влияние на жизнь человека весьма велико.

Цифровой след и цифровая тень – очень важные явления несмотря на то, что не многие это осознают. Они оказывают на всех нас большое влияние, которое со временем и с развитием технологий только увеличивается. Нужно понимать их значимость, быть осторожными, публикуя где-либо свои данные, и осознавать, что контролировать свою цифровую тень в общественных местах практически невозможно.

Главная же их опасность состоит в том, что их трудно контролировать. Технологии движутся к тому, чтобы структурировать цифровые тени и превращать их в цифровые следы. Здесь возникает конфликт доступности и конфиденциальности, и неизвестно, к чему это приведет в итоге. Сейчас стоит

просто быть внимательными к своим действиям в Интернете и не совершать того, о чем пришлось бы жалеть. Ведь облик интернет-пользователя неразрывно связан с обликом реального человека.

Список литературы:

1. Воротилин, Б.Б. Цифровая тень и цифровой след / Б. Б. Воротилин // ИнтернетБезопасность.РФ : Информационно-аналитический проект : сайт. – URL: <https://inetsafety.ru/cifrovaja-ten-i-cifrovoj-sled/> (дата обращения: 07.03.2020). – Текст : электронный
2. Ёлкина, С. Цифровой след – что это? / С. Ёлкина // Журнал Тайны 20-го века №34, сент. 2019 г. – URL: <https://www.bagira.guru/internet/tsifrovoj-sled-chto-eto.html> (дата обращения: 07.03.2020). – Текст : электронный
3. Дегтярев, М. Цифровая тень и цифровой след – новая угроза для человечества! / М. Дегтярев // НWP.ru : сайт. – URL: https://www.hwp.ru/articles/TSifrovaya_ten_i_tsifrovoy_sled___novaya_ugroza_dlya_chelovechestva_21/?PAGEN_1=3 (дата обращения: 07.03.2020). – Текст : электронный
4. Лесных, А. Поймали в Сети: куда ведет «цифровой след» / А. Лесных // Известия : информационный портал : сайт. – URL: <https://iz.ru/976205/aleksandr-lesnykh/poimali-v-seti-kuda-vedet-tcifrovoi-sled> (дата обращения: 07.03.2020). – Текст : электронный