УДК 004

А. С. Мойсевич
преподаватель кафедры оперативно-розыскной деятельности
факультета милиции
Могилевского института МВД
(Беларусь)

КОНФИДЕНЦИАЛЬНОСТЬ КАК МЕРА ЗАЩИТЫ ЦИФРОВОГО СЛЕДА

Есть много различных определений понятия «конфиденциальность». С этимологической точки зрения слово «конфиденциальный» происходит от латинского confidentia — «доверие». В современном русском языке это слово означает: доверительный, не подлежащий огласке, секретный, откровенный [1].

В юриспруденции конфиденциальность понимается как обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [2].

Специалисты в сфере информационной безопасности и защиты информации придерживаются следующего определения: конфиденциальность — свойство безопасности информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право [3].

В настоящей научной статье мы сосредоточимся на конфиденциальности личных данных пользователей сети Интернет, которые могут собирать другие субъекты.

Современный цифровой мир поражает тем, что разные организации не только собирают информацию о пользователях, но и на законных основаниях делятся или продают эту информацию другим. К примеру, каждый раз после просмотра или покупки чего-либо в Интернете, просмотра потокового видео, поиска чего-либо, использования приложения на смартфоне информация об этом и о пользователе собирается и анализируется. В последующем эта информация может быть использована для рекламы, продажи товаров или услуг, определения интересов пользователя [4].

Целью сохранения личной конфиденциальности является управление цифровым следом — попытка защитить и ограничить собираемую информацию о пользователе.

В современном цифровом мире пользователю невозможно полностью устранить или уничтожить свой «цифровой след», однако его можно уменьшить. В связи с этим консультантом и советником по кибербезопасности Кентоном Смитом (Канада) были разработаны и предложены некоторые меры,

предпринимая которые, рядовые пользователи сети Интернет могут частично защитить свою конфиденциальность [4].

Во-первых, по мнению специалиста, пользователям рекомендуется ограничивать те сведения, которые публикуются ими в Интернете, в частности ту информацию, которой пользователь делится, например, на публичных форумах или в социальных сетях. Это рекомендация включает в себя осторожность с размещением фотографий, информации, иных сведений, доступных иным пользователям Сети. Существует большая вероятность того, что все публикуемые пользователем сведения (комментарии, фото- и видеоизображения) на закрытых форумах, в сетях (даже при включении надежных параметров конфиденциальности) в какой-то момент станут общедоступными [4].

Во-вторых, при создании учетных записей в Интернете пользователям необходимо проверять, какую информацию о них собирают сайты, предварительно проверив их политику конфиденциальности [4].

В-третьих, пользователям Интернета необходимо иметь в виду, что независимо от того, какие параметры конфиденциальности установлены ими самими, информация о них все равно собирается, особенно бесплатными сервисами, например, такими как Facebook или WhatsApp [4].

Четвертой рекомендацией является обязательное ознакомление с приложениями перед их загрузкой и установкой. В частности, необходимо изучить: действительно ли интересующие ресурсы поступают от проверенного поставщика; давно ли они доступны к загрузке, установке; много ли у них положительных отзывов. Сюда же следует отнести проверку требований к разрешениям приложения: действительно ли мобильному (иному другому) приложению нужен доступ к местоположению пользователя, контактам из его телефонной книги, камере и микрофону его смартфона [4].

Пятой рекомендацией эксперта является использование возможностей виртуальной частной сети (VPN) для подключений к Интернету, особенно если используется общедоступная сеть, например, бесплатный Wi-Fi. При использовании браузера рекомендуется установить для параметров конфиденциальности значение «конфиденциально» или «инкогнито», чтобы ограничить доступ к информации, способы использования и хранения файлов cookie и защитить историю просмотров. При поиске информации рекомендуется использовать возможности анонимных поисковых систем, предназначенных для обеспечения конфиденциальности, к примеру, DuckDuckGo, StartPage [4].

В заключение отметим, что пользователю сети Интернет достаточно сложно защитить свою конфиденциальность, поскольку во многом она зависит от требований о конфиденциальности каждого отдельного ресурса, сайта, приложения, этических норм компаний, которые выступают поставщиком услуг,

однако рассмотренные выше меры, разработанные специалистами по безопасности, помогут ограничить объем собираемой информации о пользователе.

1. Карта слов и выражений русского языка [Электронный ресурс] // Картаслов.ру. URL: https://kartaslov.ru/значение-слова/конфиденциальность (дата обращения: 30.09.2021). Перейти к источнику Вернуться к статье

2. Большой юридический словарь / под ред. проф. А. Я. Сухарева. 3-е изд., доп. и перераб. М. : ИНФРА-М, 2007. 858 с. Вернуться к статье

3. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. INSIDE. 2015. № 1. С. 14–17. Вернуться к статье

4. Kenton Smith. Privacy — Protecting Your Digital Footprint [Electronic resourse] // SANS. URL: https://www.sans.org/newsletters/ouch/privacy/ (date of access: 30.09.2021). Перейти к источнику Вернуться к статье