УДК 004.056.53

студентка Е.И. Кузнецова
ГВУЗ «Национальный горный университет»

ЧЕЛОВЕК НА ЛАДОНИ: ВОЗМОЖНОСТИ GOOGLE И DLP-СИСТЕМ

В данной статье рассмотрены проблемы защиты персональных данных в сети. Проведён анализ новой политики конфиденциальности корпорации Google и легитимности внедрения DLP-решений.

Анонимность уходит в прошлое, и новые технологии всё быстрее помогают разрушать тот слабый барьер между личным и общим. Виной этому зачастую становится сам пользователь, выкладывая сознательно либо несознательно информацию о себе в «мировой клубок» сплетен и данных – Интернет, в котором потянув за одну нить, можно распутать целую жизнь человека. Начав с любой отправной точки, составляются полные досье на кого-либо. Не важно, что будет первым в расследовании – номер социального страхования, MAC-адрес, адрес электронной почты, автомобильный номер. Из этой информации можно получить практически все об интересующем субъекте. А сделать это в современном мире помогают социальные сети, блоги, специальные DLP-решения и поисковые системы.

Проблема защиты персональных данных стала ещё актуальней при смене политики конфиденциальности корпорации Google. Согласно даному документу, начинается отслеживание поведения пользователя на всех сайтах Google (Gmail, Google Calendar, YouTube, Google Voice, Picasa Web Albums, Google Books, Google Chrome и другие), и к тому же все данные, вводимые пользователем на таких сайтах, теперь являются собственностью компании. Сбор информации о посещенных сайтах и просмотренных видео осуществлялся и раньше, но впервые компания заявила о том, что информация будет объединяться. В итоге будет составлено полноценное досье на каждого пользователя системы. Google объясняет это благими соображениями: так человеку вовремя напомнят о важной встрече (считав данные календаря и данные о местоположении пользователя), «зная языковые предпочтения пользователей, будут предлагаться им использовать

службы именно на этих языках», говорится в заявлении о конфиденциальности. [1]

Как сообщает компания Google, информацию она берёт из двух источников – информация от пользователей при создании аккаунта Google (имя, адрес электронной почты, номер телефона и другие) и данные из служб, с которыми работает пользователь (сведения об устройстве и о местоположении, сведения журналов, уникальные номера приложений, локальное хранилище, файлы cookie и анонимные идентификаторы). Что касается предоставления персональных данных третьим лицам, то в политике конфиденциальности выделены следующие случаи:

1) пользователь сам дал на это своё согласие;
2) администратор домена дал своё согласие;
3) по требованию законодательства.[2]

Главным достоинством данной политики является возможность управления определенными типами сведений в аккаунте Google с помощью Личного кабинета, где хранится «досье» на каждого пользователя. В нем можно изменить свои настройки конфиденциальности для различных продуктов, например для Android Маркет, Gmail, Контакты, Календарь и других. Кроме того, пользователь может полностью запретить в браузере прием всех файлов cookie, в том числе и от Google, или выбрать, чтобы ему сообщали о последних.

К ещё одной проблеме конфиденциальности персональных данных можно отнести использование DLP-систем для защиты корпоративных секретов фирмы. Это IT-решение, которое предотвращает потери/утечку данных; построено по принципу фильтрации по ключевым словам циркулирующей в компании информации на предмет ее конфиденциальности. Но вопрос легитимности DLP-решений остаётся открытым так, как в поисках злостных разгласителей тайн и секретов прежде всего следует напомнить о разделе II статьи 31 Конституции Украины, декларирующей следующее: «Каждому гарантируется тайна переписки,

телефонных переговоров и иной корреспонденции. Исключения могут быть установлены только судом в случаях, предусмотренных законом».[3]

Касательно DLP-систем, противозаконным является такое их использование, которое нарушает право на тайну связи, то есть предусматривает ознакомление с сообщением кого-либо кроме отправителя, получателя и уполномоченных ими лиц или разглашение сообщения. Если вышеперечисленные действия не были выявлены, то закон не нарушен. А как же быть в том случае, когда в ходе работы DLP-системы человек с сообщениями не был ознакомлен? Если весь анализ происходит автоматически, и подозрительные сообщения просто не пересылаются? Ответ прост: нарушениями не являются любой программный анализ, блокирование или уничтожение сообщения, архивирование и хранение сообщения без ознакомления с ним.

Перед внедрением DLP-решения всех работников официально предупреждают об изменениях в политике безопасности предприятия и о том, что все их сообщения могут просматриваться. Но заблуждением считается тот факт, что это снимает проблему законности. Предварительное уведомление не превращает незаконное деяние в законное.

Создание, внедрение и использование DLP-систем несёт риски, связанные с нарушением закона. Избежать этих рисков не так просто. При проектировании и при внедрении обязательно следует привлекать юриста, квалифицированного в области информационных технологий.[4]

Спастись от слежения в сети можно такими основными способами: думать, что выкладывать в Интернет, особенно в социальные сети, и не хранить по-настоящему конфиденциальную информацию на серверах Google, как и на любых других публичных сервисах.

Перечень литературы:

1. http://www.pravmir.ru;
2. http://www.google.com/intl/ru/policies/privacy;
3. Конституция Украины;

4. http://dlp-expert.ru/dlp-teoriya-i-praktika/faq.