КОНФИДЕНЦИАЛЬНОСТЬ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Иван БАБЕНКО,
выпускник CSIE, ASEM

This article describes the characteristics of privacy in modern society and the evolution of the privacy perception. The reasons for increasing the risks are described, related to the drain of confidential information, and types of information subject to risk are listed.

Конфиденциальность, как понятие, впервые было озвучено ещё в 1890 году. С тех пор, в его толковании мало что изменилось, но эволюция общества внесла свои коррективы в отношение общества к конфиденциальности.

По принадлежности конфиденциальную информацию можно разделить на 3 группы

- личностная (приватность) – это способность конкретного индивидуума свободно распоряжаться и контролировать персональную информацию;
- коммерческая – регламентируется обязательством о неразглашении информации принадлежащей компании, организации либо группе компаний;
- государственная/международная (секретность) – ограничение государством или международными политическими формированиями распространения данных, которые могут нанести ущерб безопасности государства.

Конфиденциальность регламентируется международными соглашениями, государственными законами, внутренними соглашениями в компаниях и сообществах, а также морально-этическими нормами общества.

Информационные технологии оказали огромное влияние на восприятие конфиденциальности обществом. Сегодня большое количество конфиденциальной информации располагается на цифровых носителях в зашифрованном, либо открытом виде, но при этом у заинтересованных лиц намного больше возможности получить к ней физический доступ, незаметно скопировать или скомпрометировать, а у обладателя секретов всегда есть риск случайно потерять устройство с конфиденциальными данными. Наши тайны транспортируются при помощи сетей передачи данных, а получить доступ к трафику сети теоретически может не только обладатель или получатель этой информации, но и третьи лица, используя методики перехвата данных.

Наибольшую угрозу конфиденциальности представляют: социальные/коллективные сети и сообщества, блоги, почтовые сервисы, cloud-computing сервисы, мобильные и планшетные устройства с выходом в Internet, онлайн-мессенжеры, новостные и медийные ресурсы и т.п.

Эти ресурсы содержат огромные объёмы конфиденциальной информации, осознано или бессознательно доверенной пользователями. Риски, связанные со взломом или утечкой информации от этих сервисов, достаточно велики. Приватностью

пользователя нередко пренебрегают и может произойти, что данные, которые сейчас видите только Вы – завтра станут доступны всем.

По персональным страничкам в социальных сетях, именам, логинам, никам, адресам электронной почты, чаще всего можно составить полный портрет о каждом человеке, использующем Internet если правильно построить механизм агрегации этих данных. Приватности в сети Internet становится всё меньше.

Если просто говорить о том, какую персональную информацию мы передаём на хранение Internet-сервисам и компаниям, то можно перечислить очень много: логины, пароли, даты рождения, идентификационные номера наших документов, календари и расписания, реквизиты банковских счетов, номера телефонов, список родственных и дружественных связей, информация о предпочтениях и увлечениях, биографические данные, истории поиска, фотографии, список посещённых ресурсов, данные о местонахождении, беседы и корреспонденция со знакомыми друзьями, близкими и партнёрами, пробы голоса, данные о биометрических характеристиках, места работы и досуга, комментарии и статьи по поводу основных событий в мире, блогах, людях, компаниях и государствах, политические и религиозные предпочтения, мнения других людей о них и многое другое. Такую информацию можно найти в сети Internet (в большем или меньшем количестве) о каждом человеке не зависимо от того является ли он пользователем глобальной сети.

Субъекты конфиденциальности часто ошибочно считают, что всю эту информацию невозможно собрать объединить и использовать. Существуют мифы о том, что личность в любой момент может быть отчищена от нежелательных конфиденциальных фактов, чаще всего – это заблуждение. Люди склонны доверять сервисам, которыми пользуются, при этом лишь единицы бегло просматривают соглашения о конфиденциальности с которыми соглашаются. Те же пользователи часто считают, что они могут обратиться к «хакерам» и взломать любой аккаунт, пробить любую защиту другого пользователя, причём на том же сервисе, где присутствуют сами.

Сеть Internet даёт каждому заинтересованному инструментарий «для работы с конфиденциальной информацией»: публикации, «вирусного» распространения, искажения, компрометации, поиска, автоматического сбора и многое другое.

Конечно есть и положительные аспекты этого феномена. Нередко человек оставляет в сети следы своей преступной деятельности, заказывая преступления, совершая нарушения авторских прав, высказывая преступные по своей сути мысли, получая несанкционированный доступ к защищённому контенту и т.д. На основе данных сети Internet и других информационных систем, которые имеются в доступе у исследователя, конфиденциальная информация даёт возможность:

- расследовать и раскрывать преступления;
- создавать морально-этический образ этого человека и анализировать его устойчивость или компетентность в той или иной сфере;
- делать мониторинг конкуренции на рынке;
- получать информацию об общественном мнении и социальных трендах;
- быстро создавать информационный повод и распространять информацию.

На сегодняшний день этим уже пользуются спецслужбы и органы охраны правопорядка, посольства таможенные структуры, крупные компании (делая рыночные исследования, участвуя в информационной войне с конкурентами и оценивая кандидатуры работников при приёме на работу) и обычные граждане желающие узнать больше о других и использовать эту информацию либо в своих целях. Информация, которую можно получить таким способом, бывает порой более содержательной и полезной чем данные, содержащиеся в государственных базах данных.

Проблема конфиденциальности продолжает существовать, так как с эволюцией средств хранения и передачи данных, носителей масс-медиа, с зарождением сети Интернет правоприменительная практика в области конфиденциальности информации отступает перед стремительным ростом технологий. Правоохранительные органы на сегодняшний день не располагают достаточной подготовкой кадров, для расследования компьютерных преступлений в области нарушения конфиденциальности, а население делает всё меньше различий между конфиденциальной и общедоступной информацией, что делает эти преступления невидимыми. Необходимо повышать квалификацию для правоприменения существующих законов и соглашений, и информировать население об опасности разглашения конфиденциальной информации.

КЛАССИФИКАЦИЯ СПОСОБОВ НАНЕСЕНИЯ АТАК ДЛЯ ВЫБОРА СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Лидия СИВКО, Александр ДОРОХОВ
Харьковский Национальный Экономический Университет (Украина)

Currently there are many methods of application attacks at the systems technical data protection in modern society. This led to the need for research to the classification of these methods. The obtained results of the work listed below.

Развитие и внедрения в Украине европейских и международных стандартов информационной безопасности, актуализация проблем противодействия компьютерной преступности создали благоприятные условия для стремительного развития средств зхащиты от угроз нарушения режима безопасности.

Выбор средств защиты зависит от того, какими возможными способами злоумышленник будет пытаться совершить информационную атаку. Атака на информацию – это преднамеренное нарушение набора правил, установленных собственниками информационного объекта или уполномоченного им лица при хранении, поддержке или предоставлении доступа к данному информационному объекту.