

БЕЗПЕКА ЛЮДИНИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Овсієнко В.С.

Науковий керівник – ст. викл. Хондак І.І.

Харківський національний університет радіоелектроніки

Nowadays, social networks are among the most visited resources in the global Internet. We live in them and rarely think about the dangers that may overtake us. Blackmail, provocation, robbery, manipulation are all consequences of careless use of social networks. Therefore, we need to know and understand how to protect ourselves while being on the Internet.

Поява соціальних мереж здійснилась завдяки класичному веб-сайту Classmates.com, який був створений Ренді Конрадом у 1995 році. Соціальні мережі, безумовно, є одним із найбільших досягнень людства. Вони є ефективним засобом комунікації та самоутвердження. Проте більшість людей досі не мають розуміння того, до яких наслідків може призвести їх необдумані дії і байдужість стосовно наведення інформації[1].

Поряд з великою кількістю переваг у використанні соціальних мереж також існують і небезпеки. Саме про них нам необхідно знати елементарні відомості, адже від них залежить інформаційна безпека, психологічний стан та здоров'я користувачів. При користуванні інтернетом люди добровільно позбавляють себе хоч би частини необхідної конфіденційності (заповнюють профіль правдивими даними, завантажують свої фото, вказують місце свого перебування), не тільки про себе, але й про друзів, родину та інших. Іноді така інформація може суперечити основним положенням закону України «Про захист персональних даних»[1].

Збитки, які завдані розкриттям інформації чи зломом сторінки, можуть носити як моральний (розголошення конфіденційної інформації, шантаж, провокування), так і матеріальний (затрати на відновлення працездатності інформаційно-комунікаційної системи, втрата грошей) характер[2].

Людина, яка має певні навички, вміє “прочитати нас” завдяки нашій поведінці чи персональній інформації в соціальних мережах. В деяких випадках це приводить до маніпулювання свідомістю і поведінкою жертви. Найгіршим наслідком, який ми спостерігали в останній час, є самогубство, також ним може бути шантаж, моральне насилля, емоційне напруження та інше[3].

У колах фахівців із захисту інформації існує думка, що на сьогоднішній день є велика група спеціально підготовлених співробітників, яка розміщує в соціальних мережах ігри, створює групи і приваблює людей до спілкування на певні теми, щоб, створивши психологічний портрет і вивчивши спроможність до певного гіпнотичного

впливу кожної особи-користувача, вмiло манiпулювати свiдомiстю мас, зареєстрованих на сайтах соціальних мереж. Пізніше, в соціальних мережах з'явилася величезна кількість тестів, на перший погляд, для розваги. Потрібно розуміти, що ці тести допомагають зловмисникам дають змогу провести наш психологічний аналіз і створити психологічний портрет, дізнатися про дослідження наших можливостей та здібностей на рівні впливу на нашу свiдомiсть[2].

Щоб захиститися від злочинців і маніпуляторів треба дотримуватися певних запобіжних заходів: слідкувати за конфіденційністю власної інформації (встановлювати стійкі паролі і різні для кожної мережі, обмежувати доступність інформації, часто змінювати паролі і т.д.), не переходити за підозрілими посиланнями, не брати участі у жодних тестах і опитуваннях, якими рясніють соціальні мережі[3]. Деякими додатковими порадами є:

- не піддаватися на маніпуляції, відчувши “моральний напад” в соціальних мережах не тримати все в собі і розповісти близьким людям. Якщо це є погрозами чи шантажом – повідомити до правоохоронних органів;

- приймайте пропозиції про дружбу тільки від тих людей, яких знаєте особисто і безпосередньо;

- не повідомляти на сторінках в мережі про свою сім'ю, друзів, місце проживання і перебування (якщо можливо прізвище і дату народження) [3];

В підсумку можна сказати, що наявність небезпеки в соціальних мережах зовсім не означає, що треба від них відмовитися або боятися. Але все ж таки для безпечного користування слід думати яку інформацію про себе розміщати в соціальних мережах і не вказувати свої персональні дані, інформацію, що стосується близьких людей. Просто не говорити зайвого, адже зазвичай найслабшим механізмом в мережі є людина, а не програмний код.

Список використаних джерел

1. Карманний Є.В. Підходи до захисту інформації при користуванні соціальними мережами / Є.В. Карманний, С.О. Ковжого – Харків, 2015. – С. 4–5.

2. Деркаченко А. Я. Соціальні мережі, як середовище для технологій маніпулятивного впливу [Електронний ресурс] / А. Я. Деркаченко. – 2016. Ре-
жим доступу до ресурсу: <http://journals.dut.edu.ua/index.php/dataprotect/article/view/531/493>.

3. Голубенко О. Л. Соціальні мережі як загроза безпеки [Електронний ресурс] / О. Л. Голубенко, А. С. Петров, А. О. Петров. – 2011. – Режим доступу до ресурсу: http://www.nbu.gov.ua/old_jrn/Soc_Gum/VSunU/2011_7/title/1.pdf.