УДК 004
О.М.Бойко
(Тернопільський національний технічний університет ім. І. Пулюя)

РОЗРОБКА МЕТОДОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

UDC 004
O. M Boiko

DEVELOPMENT OF METHODOLOGY FOR INFORMATION PROTECTION AGAINST SOCIAL ENGINEERING ATTACKS

Ключові слова: інформаційна безпека, соціальна інженерія, захист інформації.

"Соціальна інженерія" (social engineering) – це набір різних психологічних методик і шахрайських прийомів, метою яких є отримання конфіденційної інформації про особу обманним шляхом. Конфіденційна інформація – це логіни / паролі, особисті дані, компромат, номери банківських карт і все, що може принести фінансові або репутаційні втрати. Саме поняття прийшло до нас зі сфери хакинга. Хакер – це людина, яка шукає уразливості в комп'ютерних системах, по-іншому говорять – «зламує». Яке відношення, здавалося б, до цього має соціальна інженерія? Все дуже просто. В один момент часу хакери усвідомили, що головна вразливість в будь-якій системі –це людина, а не машина. Людина, точно також, як і комп'ютер, працює за певними законами. Використовуючи накопичений людством досвід в психології, маніпуляціях і механізми впливу, хакери стали «зламувати людей». Я ще це називаю "brain hack". Різниця вразливостей людей та ПК колосальна: комп'ютер може мати декілька основних недоліків в захисті системи DDos атака, відкриті порти, вразливий антивірус, поганий захист мережі до якого можна підключитися через WiFi і т. д., коли ж людину варто зустріти і, навіть, базовими навичками психології віднайти її вразливості, які і надалі можна використовувати в власних цілях. Основною метою задля захищення всієї інформації в межах однієї організації, корпорації чи держави є кваліфіковані працівники, які досконало володіють та використовують методологію захищення знань та вмінь обробки данних. Наскільки б мережа була не захищена та ізольована від зовнішніх та внутрішніх атак ключовою ланкою доступу інформації є та залишається людина.

У магістеріській роботі ми розглядаємо усі види атак соціальної інженерії, та методи боротьби і захисту проти них. Розглянемо актуальну методологію захисту для працівників які володіють будь-якою інформацією якій необхідна захист та конфіденційність.

Корпоративна мережа має вразливості, які призводять до пошкодження цілісності та втрати інформації. Отож ми розглянемо як зберегти інформацію від зловмисників шляхом навчання персоналу боротьби з атаками соціальної інженерії.

Література.

1. Кузнецов М.М., Симдянов И.И. Социальная инженерия и социальные хакеры. Москва, «Вильямс» 2014. – 366 с