

II Міжнародна науково-практична інтернет-конференція (25-26 квітня 2018 р., м. Бердянськ)

постіндустріалізму насправді реальну загрозу становлять саме наукові відкриття у сфері технічних і природничих дисциплін, які без відповідного гуманітарного супроводу здатні за хвилини знищити людство.

Погоджуючись у значній мірі з міркуваннями філософа, зауважимо, що існують більш фундаментальні причини деградації гуманітарної сфери у загальноцивілізаційному контексті. Будь-які гуманітарні соціальні інновації можуть дати результат лише у перспективі. Відтак, безпідставними є надії на розвиток цього сектору через приватний капітал, зорієнтований на отримання швидкого прибутку. Натомість джерелом і рушійною силою розвитку гуманітарної складової освіти і науки має бути громадянське суспільство, яке має спонукати державу і наддержавні загальноцивілізаційні інституції до тяглої цілеспрямованої гуманітарної політики. Слід враховувати й те, держава нерідко постає як сила, яка нівелює і спотворює розвиток гуманітарної сфери.

Такі тенденції властиві переважно для авторитарних і тоталітарних режимів, зорієнтованих на продукування і поширення у гуманітарній сфері зразків пропаганди. Однак, навіть демократичні режими у країнах зі слабким громадянським суспільством нерідко зовсім не зацікавлені у розвитку гуманітарної сфери, адже малоосвічене населення з більшою ефективністю піддається соціальному контролю та маніпуляціям. Представники владних еліт у таких країнах добре усвідомлюють, що зростання рівня гуманітарної освіти населення з необхідністю підвищує й рівень вимогливості громадянського суспільства щодо якості й ефективності діяльності державних інституцій, що неодноразово засвідчили соціальні виступи в Грузії (2003 р.), в Україні (2004-2005 рр., 2013-2014 рр.), у Румунії (2017 р.) та феномен «арабської весни» (2011 р.).

Список літератури

1. Ковтун Н. М. Криза світоглядно-ціннісних орієнтацій в ситуації транзитивності постіндустріального суспільства // Вісник Житомирського державного університету імені Івана Франка. - Житомир: Видавництво Житомирського державного університету імені Івана Франка, 2017. - Випуск № 1 (87). - С. 32 - 36.
2. Дацюк С. Проблемні ситуації людського розвитку. - Електронний ресурс. Режим доступу: <http://uamfo.org/blognews/1485860321-datsyuk-problem-situatsiyi-lyudskogo-rozvitku.html>

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ В АСПЕКТІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Малихін В.А. асистент
Бердянський державний педагогічний університет
м. Бердянськ, Україна

На сучасному етапі розвитку суспільства важливу роль відіграють інформаційні системи, які все більше входять у всі сфери життя людини. Вони дозволяють нам працювати, навчатись та розважатись. Але в той же час вони працюють і з конфіденційною інформацією. На сьогоднішній день дослідження в

Наука III тисячоліття: пошуки, проблеми, перспективи розвитку

області захисту інформації розглядали лише удосконалення програмно-технічного забезпечення як складової безпеки. В цьому напрямку питання інформаційної безпеки вивчені досить добре, розроблена велика кількість засобів, що дозволяють звести до мінімуму ймовірність успіху програмно-технічних атак зловмисників. У той же час людський фактор в інформаційній безпеці відіграє набагато важливішу роль. Інформація захищається людьми, і основними носіями інформації є також люди зі своїми комплексами та слабкостями на яких можна гарно зіграти.

Останнім часом з'являється багато публікацій як зарубіжних так і вітчизняних авторів (В. Домарева, Дж. Козіола, М. Кузнєцова, Кр. Касперськи, К. Митника, І. Симдянова, В. Саймон та ін.) в яких зазначається, що людина є найменш надійною ланкою в системі захисту інформації.

Соціальна інженерія як сфера науково-практичної діяльності в різні роки розглядалася в працях Г. Антонюка, А. Зайцева, А. Кравченко, І. Попової, А. Пригожина, Ю. Резника Л. Сисоевої, Ж. Тощенко, В. Щербини, С. Ягодзинського та ін.).

Метою нашого дослідження стало теоретичне вивчення питання безпеки інформаційних систем в аспекті соціальної інженерії.

Що таке соціальна інженерія в контексті інформаційної безпеки? Соціальна інженерія у галузі інформаційної безпеки - це метод несанкціонованого доступу до захищених інформаційних ресурсів, який використовує засоби впливу на людську психологію [3].

Наукове обґрунтування соціальної інженерії вперше дав австрійський вчений К. Поппер[2], який визначив даний напрямок, як сукупність підходів прикладної соціології, спрямованих на раціональні зміни соціальних систем на основі фундаментальних знань про суспільство та передбачення можливих наслідків перетворень.

Метою соціальної інженерії є спонукання людей вчиняти певні дії, які при звичайних умовах вони б ніколи не зробили, наприклад, розголошення своєї конфіденційної інформації, перехід на невідомі сайти по сумнівними посиланнями. Вся система соціальної інженерії базується на тому факті, що саме людина є найслабшою ланкою будь-якої системи інформаційної безпеки. Саме тому, коли зловмисникам важко технічно отримати конфіденційну інформацію, вони впливають на найслабше місце в системі інформаційної безпеки - на користувача.

Ламініна О.[1] вважає, що методи соціальної інженерії здатні обійти найпотужніші системи інформаційної безпеки. До того ж використання соціальної інженерії, на думку автора, для несанкціонованого отримання інформації дуже вигідно, тому що: це простіше, ніж зламати систему інформаційної безпеки; атаки не можна обчислити за допомогою технічних засобів захисту інформації; це не вимагає великих вкладень; являє собою мінімальний ризик; працює для будь-якої обчислювальної платформи; має стовідсотковий ефект.

Одна з важливих причин поширення соціальної інженерії як методу атаки - це дуже дешевий вид нападу, атакуючий може навіть не бути фахівцем в сфері інформаційних технологій. Та й при використанні методів соціальної інженерії результат як правило досягається набагато швидше, ніж, якби був використаний

II Міжнародна науково-практична інтернет-конференція (25-26 квітня 2018 р., м. Бердянськ)

інший метод атаки. Користувачі часто недооцінюють важливість інформації, якою володіють, і легко діляться нею з кожним, хто про це попросить, не усвідомлюючи згубні наслідки своїх дій. Але навіть самі пильні користувачі не завжди можуть розпізнати, що піддалися впливу методам соціальної інженерії, тобто піддалися атаці. Нажаль типових протидій методам соціальної інженерії не існує і не може існувати оскільки кожен інцидент вимагає індивідуального підходу і всебічного розгляду.

Потенційними можливостями по частковому вирішенню цієї проблеми має система освіти. Враховуючи здатність особистості до саморозвитку, самоактуалізації, самоосвіти, зміст таких дисциплін, як психологія, педагогіка, соціологія, філософія та дисципліни комп'ютерного циклу мають носити інтегруючий характер, що висвітлюють проблему забезпечення безпеки, як на рівні особистості, так і на рівні використання нею комп'ютера при різних соціальних і професійних взаємодіях.

Ми вважаємо за потрібне озброїти майбутніх спеціалістів засобами протидії методам соціальної інженерії. Для цього майбутній фахівець комп'ютерного профілю повинен володіти низкою професійно важливих якостей, на що і будуть спрямовані наші подальші зусилля.

Література

1. Ламинина О. Возможности социальной инженерии в информационных технологиях / Ольга Ламинина // Гуманитарные, социально-экономические и общественные науки 2017 - № 2 .- С. 21-23 <http://online-science.ru/..science/gid4024/pg2/>
2. Поппер К. Відкрите суспільство та його вороги. / Карл Поппер Том 1 / К.: Основа, 1994. - 444 с
3. Social Engineering Fundamentals [Електронний ресурс] // scribd.com. - 2009. - Режим доступу до ресурсу: <http://ru.scribd.com/doc/19676093/SocialEngineering-Fundamentals>.

МЕТОДОЛОГИЯ ПЛАНИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ИЕРАРХИЧЕСКИХ ОРГАНИЗАЦИЙ ПРИ АВТОМАТИЗИРОВАННОМ УПРАВЛЕНИИ

Автор

(Никифоров А.В., канд. тех. н., с. н. с.)

Национальный университет Воздушных Сил, Харьков, Украина

Организованная человеческая деятельность носит иерархический характер. Причины этого кроются в особенностях обработки информации человеком. Во-первых, человеческое сознание весьма ограничено применительно к размерности информации, обрабатываемой одновременно. Поэтому руководитель не в состоянии следить за всем и управлять всем лично, он вынужден делегировать свои полномочия заместителям, каждый из которых компетентен в определённой области деятельности. Во-вторых, сама методология организационного управления имеет иерархическую природу. Для самодостаточной организации имеют место 5 иерархических уровней управления: целеполагание;