Оцінювання захищеності інформації в комп'ютерних системах за соціоінженерним підходом

© Мохор В.В. © Цуркан О.В.
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова
Національної академії наук України,
Київ, Україна
v.mokhor@gmail.com otsurkan24@gmail.com
© Цуркан В.В.
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського",
Київ, Україна
v.v.tsurkan@gmail.com
© Герасимов Р.П.
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова
Національної академії наук України,
Київ, Україна
gerasimov.rostislav@gmail.com

Анотація

Захист інформації в комп'ютерних системах орієнтований на збереження її властивостей конфіденціності, цілісності та доступності від різноманітних за своєю сутністю несприятливих впливів. Потенційно можливий несприятливий вплив тлумачиться загрозою. Для запобігання або ускладнення можливості реалізацій загроз, зменшення потенційних збитків створюється та підтримується у дієздатному стані система заходів захисту інформації в комп'ютерних системах. Така система включає обчислювальну систему, фізичне середовище, персонал та інформацію. На збереження її властивостей у комп'ютерних системах суттєво впливає врахування нетехнічного аспекту, зокрема, персоналу (наприклад, керівника, адміністратора, користувача). З огляду на це, для оцінювання технічної захищеності інформації пропонується соціоінженерний підхід. У рамках такого підходу вразливості персоналу тлумачяться як його слабкості, потреби, манії (пристрасті), захоплення. Маніпулювання ними дозволяє отримати несанкціонований доступ до інформації без руйнування та перекручування головних для нього системоутворюючих якостей (цілісність, розвиток). Як наслідок, це призводить до нової моделі поведінки персоналу, створення сприятливих умов реалізації загроз безпеці інформації і, як наслідок, зменшенню здатності системи захисту інформації протидіяти їх впливові. Це відображається в таких формах як шахрайство, обман, афера, інтрига, містифікація, провокація. Використанню кожної з означених форм маніпулювання передує визначення її змісту шляхом ретельного планування, організування та контролювання. Означені дії є основою методів соціальної інженерії. З одного боку, вони реалізуються засобами сучасних телекомунікацій. Тоді як з іншого, передбачається встановлення особистого контакту з персоналом. Таким чином, шляхом використання методів соціальної інженерії можливе виявлення, нейтралізування, запобігання появі уразливостей інформації в комп'ютерних системах. Цим підвищується її захищеність з урахуванням нетехнічного аспекту.

Ключові слова: комп'ютерна система, захист інформації, оцінювання захищеності інформації, персонал, соціоінженерний підхід, соціальна інженерія, методи соціальної інженерії.

1 Постановка проблеми

Інформаційні ресурси окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю несприятливих впливів. Потенційно можливий несприятливий вплив тлумачиться загрозою. Тому захист інформації в комп'ютерних системах полягає в створенні та підтриманні в дієздатному стані системи заходів для запобігання або ускладнення можливості реалізацій загроз, а також зменшення потенційних збитків. Оскільки комп'ютерна система включає обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію, то на оцінювання технічної захищеності інформації суттєво впливає врахування нетехнічного аспекту, зокрема, персоналу (наприклад, див. рис. 1, керівництва, адміністратора операційної системи, користувачів). Тому для цього пропонується соціоінженерний підхід [1-8].

2 Сутність соціоінжереного підходу

У рамках соціоінженерного підходу вразливості персоналу тлумачяться як його слабкості, потреби, манії (пристрасті), захоплення. Маніпулювання ними дозволяє отримати несанкціонований доступ до інформації без руйнування та перекручування головних для нього системоутворюючих якостей (цілісність, розвиток). Як наслідок, це призводить до нової моделі поведінки персоналу, створення сприятливих умов реалізації загроз безпеці інформації і, як наслідок, зменшенню здатності системи захисту інформації протидіяти їх впливові (див. рис. 2). Це відображається в таких формах як, наприклад [9-13], шахрайство, обман, афера, інтрига, містифікація, провокація. Використанню кожної з означених форм маніпулювання передує визначення її змісту шляхом ретельного планування, організування та контролювання.

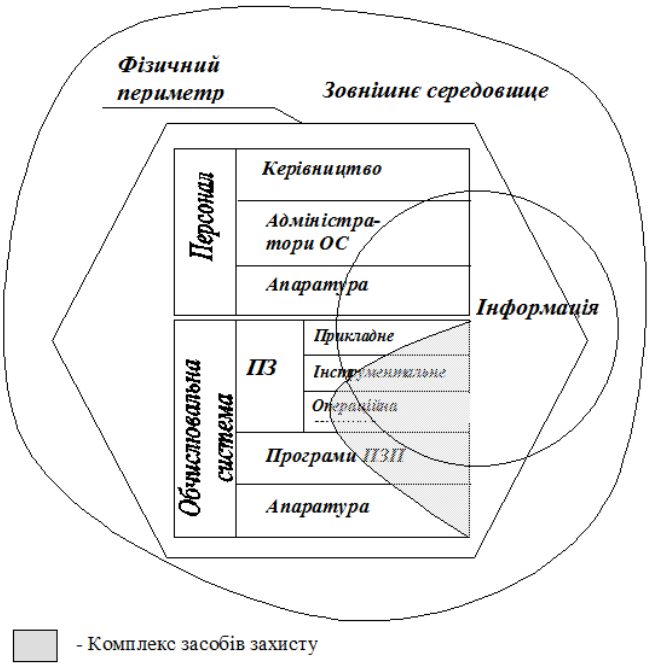

Рис. 1. Елементи комп'ютерної системи [3].

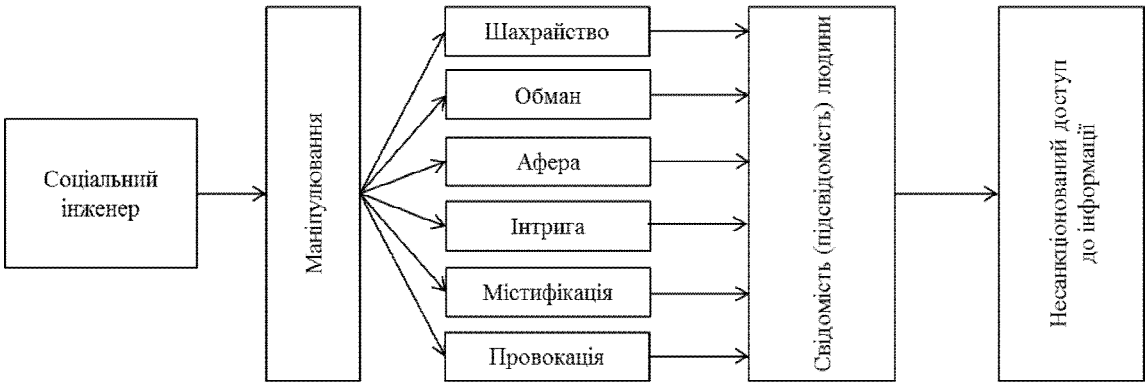

Рис. 2. Використання соціоінженерного підходу

З огляду на рис. 2, використання соціоінженерного підходу до оцінювання захищеності інформації в комп'ютерних системах передбачає цілеспрямований вплив на свідомість (підсвідомість) персоналу проти волі, але за його згодою. Такий вплив дозволяє управляти поведінкою керівництва, адміністратора, користувачів через слабкості, інтереси, потреби, схильності, переконання, звички, психічний та емоційний стан. Тому маніпулювання цими уразливостями і виражається в таких формах як шахрайство, обман, афера, інтрига, містифікація, провокація. Разом з тим, використанню кожної з означених форм маніпулювання передує визначення їх сутності шляхом ретельних планування, організації та контролювання.

У рамках соціоінженерного підходу використання атак соціальної інженерії орієнтоване на отримання "несанкціонового" доступу до інформації при оцінюванні її захищеності шляхом "негативного" інформаційно-психологічного впливу на свідомість або підсвідомість персоналу (див., наприклад [14], рис. 3).

3 Форми маніпулювання персоналом

Форми маніпулювання персоналом при оцінюванні захищеності інформації в комп'ютерних системах змінюються залежно від різновиду атак соціальної інженерії, а саме [15-20]:

1. ***Фішінг (Phishing)*** – масове розсилання електронної пошти великій групі адресатів. Ознайомлення з електронними листами спонукає їх до, наприклад, відкриття вкладення до листа, переходу за посиланням на веб-сторінку. Його метою є виманювання у довірливого або неуважного персоналу комп'ютерної системи персональних даних.
2. ***Фармінг (Pharming)*** – перенаправлення користувачів на шахрайські сайти для отримання їх логіну та паролю. Це досягається завдяки розповсюдженню електронної пошти серед користувачів, наприклад, соціальних мереж, онлайн-банкінгу, поштових веб-сервісів.
3. ***Прітекстінг (Pretextй)*** – отримання інформації або спонукання до вчинення певних дій обманом на основі заздалегідь складеного сценарію або створення фіктивної ситуації. Застосовується через телефон та потребує проведення попередніх досліджень для входження в довіру.
4. ***Смішінг (Smishing)*** – отримання інформації шляхом масового розсилання SMS повідомлень з посиланням на веб-ресурси або з реквізитами організацій (наприклад, фінансових). Внаслідок цього здійснюються відповідні дії, наприклад, дзвінок до банку для перевірки стану рахунку з зазначенням конфіденційних даних: номеру картки, терміну дії.
5. ***Вішінг (Vishing)*** – отримання інформації шляхом входження в довіру під час розмови через ip-телефон. При цьому в порушення конфіденційності здійснюється завдяки викладенню прохання у повідомленні зателефонувати на певний міський номер. Наприклад, вести номер карти, паролі, PIN-коди, коди доступу або іншу інформацію.
6. ***Спір фішінг (Spear Phishing)*** – надсилання листа електронної пошти конкретному адресату (наприклад, керівнику, адміністраторові, користувачеві), що спонукає його до обов'язкового перегляду та відповіді на отриманий лист.
7. ***Вейлінг (Whaling)*** – надсилання листа електронної пошти представнику керівництва організації, що спонукає його до обов'язкового перегляду та відповіді на отриманий лист.

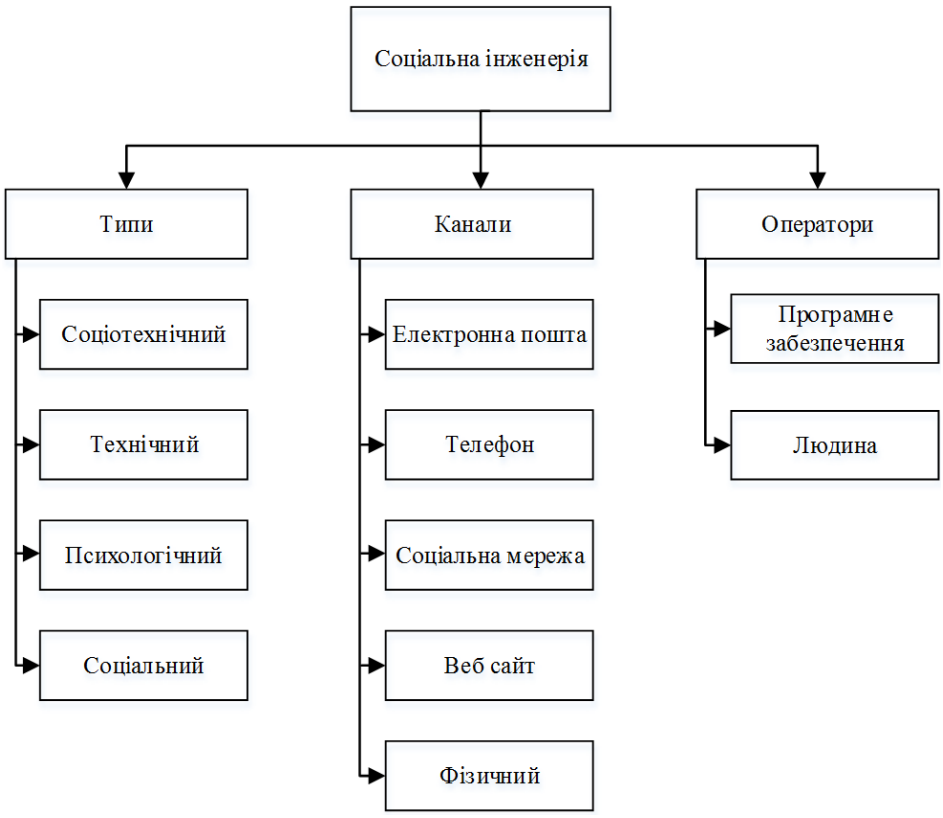

Рис. 3. Класифікування ознак реалізування атак соціальної інженерії [14].

Так (див. табл. 1), отримання несанкціонованого доступу до інформації за допомогою фішингу, фармінгу, смішінгу, вішінгу, спір фішінгу, вейлінгу здійснюється шляхом використання таких форм маніпулятивного впливу як шахрайство та обман. Тоді як основою для створення фіктивних ситуацій при прітекстінгу є афера, інтрига, містифікація та провокація.

Таблиця 1. Форми маніпулятивного впливу при соціоінженерних атаках

№ п/п	Різновид соціоінженерної атаки	Форми маніпулятивного впливу					
		Шахрайство	Обман	Афера	Інтрига	Містифікація	Провокація
1.	Фішінг	+	+	–	–	–	–
2.	Фармінг	+	+	–	–	–	–
3.	Прітекстінг	+	+	+	+	+	+
4.	Смішінг	+	+	–	–	–	–
5.	Вішінг	+	+	–	–	–	–
6.	Спір фішінг	+	+	–	–	–	–
7.	Вейлінг	+	+	–	–	–	–

Тому при оцінюванні захищеності інформації в комп'ютерних системах за соціоінженерним підходом доцільно враховувати форми маніпулятивного впливу.

4 Методи соціальної інженерії

Оцінювання захищеності інформації орієнтоване на отримання відомостей про комп'ютерні системи – етап соціальної інженерії. Цей етап включено в аудит отримання і аналізування інформації зі зовнішнього середовища. Враховуючи високу ймовірність впливу людського фактору на захищеність інформації, на даному етапі вдало використовуються методи соціальної інженерії. Для успішного виконання запланованих дій соціальний інженер проводить роботу узгоджено з мережевим адміністратором. У його конструктивні дії входять: вивчення і аналізування змістовного боку комп'ютерної системи, пошук уразливостей, систематизування отриманих відомостей, розроблення схеми дій.

Використання методів соціальної інженерії для імітування дій порушника, що направлені на користувачів комп'ютерних систем організації, дозволяє оцінити рівень кваліфікації користувачів в області забезпечення безпеки інформації і ймовірність реалізування атак соціальної інженерії.

Вхідною інформацією для соціального інженера при спробі отримання інформації про комп'ютерні системи може бути контактна інформація, що отримується з публічних джерел. Наприклад: прізвища, імена, посади користувачів. За отриманою вхідною інформацію вибираються, виокремлюються вірогідні уразливості в комп'ютерних системах, через які можливе реалізування загроз соціальної інженерії.

Основою використання методів соціальної інженерії є [9-11]:

− особливості, що керують людською свідомістю;

− аудиторія або поле діяльності;

− некомпетентність аудиторії у визначених термінах і предметних областях у сфері інформаційної безпеки;

− нестійкість психологічних властивостей особистості, що характеризуються поведінковими стереотипами. Їх можна використовувати для маніпулювання через основні потреби, слабкості, бажання, ідеали.

Більшість соціальних інженерів діє за ідентичними або близькими шаблонами. Тому вивчення прийомів їх «роботи» дозволяє виокремити такі рівні взаємодії з об'єктом впливу як домінування, маніпулювання, суперництво, партнерство.

Всі методи соціальної інженерії можна поділити на дві групи [9-11, 14-20]:

1. Віддалена соціальна інженерія реалізується засобами сучасних телекомунікацій шляхом використання:

1.1. «Телефону»

Завдяки телефонії, соціальний інженер може залишатися анонімним і в той же час мати прямий зв'язок з об'єктом впливу. Останнє важливо тому, що безпосередній контакт не дає співрозмовнику часу обміркувати поведінку у вірогідних ситуаціях, зважати на всі за та проти. Вирішувати необхідно швидко, до того ж під тиском соціального інженера. Оскільки під час телефонної розмови відбувається обмін тільки звуковою інформацією, то велику роль у прийнятті рішень відіграє анотація і голос співрозмовника. Дані характеристики підбираються у відповідності з моделлю поведінки соціального інженера для отримання інформації про об'єкт впливу, наприклад:

а) **начальник** – людина, яка звикла віддавати команди, цінує свій час, досягає поставленої мети. Манера розмови жорстка, нетерпляча. Повна впевненість у собі і легка (або повна) зверхність до рядового

персоналу. Своїм тоном показує, що проблема, з якою звернувся – дрібниця, яку необхідно вирішити якомога швидше. Ніяких прохань – тільки вимоги і вказівки. У відповідь на недовірливі або перевіряючі репліки – допустиме незадоволення і залякування співрозмовника;

b) **секретар** – дівчина (здебільшого) з приємним голосом. Завдання – виконати конкретне доручення начальника, не відволікаючись на умовності. Вона володіє інформацією про начальника, його справи, у своїй мові користується достовірними або недостовірними фактами, які складно перевірити. Характер розмови – м'який, з легким фліртуванням (якщо співрозмовник – чоловік). Реакція на небажання співпрацювати – бурхливе розчарування, скарга, що скаже начальство;

c) **технічний співробітник** – працівник організації, який характеризується поблажливим, але дружелюбним відношенням до клієнтів. Мета – усунути несправність. Супроводжується використанням специфічних термінів для відображення своєї компетентності. На відмову співпрацювати – реакція здивування, оскільки співпраця у першу чергу вигідна для клієнта. Жодних вмовлять –йому дається зрозуміти, що без його участі проблема тільки ускладнюється. Допустиме залякування тяжкими наслідками.

d) **користувач** – працівник, що виконує свої обов'язки і наляканий виникненням неочікуваної проблеми. Чітко виражений мотив швидкого вирішення усіх проблем і повернення до своєї рутинної роботи. Відсутність уявлення про характер проблеми, зацікавленість тільки в її вирішенні. Характер спілкування – показати безнадійність свого положення і готовність віддатися у руки спеціалісту.

1.2. Глобальної мережі Інтернет

Найбільш розповсюдженими способами реалізації методів соціальної інженерії за допомогою глобальної мережі Інтернет є:

a) проведення соціальної інженерії шляхом електронного листування;
b) проведення соціальної інженерії через системи обміну повідомленнями (Skype, Viber);
c) соціальна інженерія на форумах, чатах, блогах.

У даних випадках вдале реалізування соціальної інженерії обумовлене правильністю розроблення сценарію спілкування.

2. Особистий контакт. Найбільш складний і небезпечний метод соціальної інженерії. Крім перерахованих вимог до сценарію спілкування і моделі поведінки, соціальний інженер повинен приділяти увагу своїй зовнішності і манерам «живого» спілкування. Для правильного візуального сприйняття, необхідно правильно підібрати:

a) колір одягу та взуття;
b) манери та жести при спілкуванні;
c) положення в просторі відносно співрозмовника.

Також при використанні методів соціальної інженерії необхідно характеризувати співрозмовника. За голосом або за зовнішністю, доцільно визначити яку його слабкість доцільно використовувати для досягнення поставленої мети. До основних слабкостей людини, використання яких разом з правильно підібраною поведінкою і сценарієм розмови дозволяє досягнути очікуваного результату, належать, наприклад:

a) довірливість;
b) страх;
c) жадібність;
d) відкритість;
e) зверхність;
f) милосердя.

Основними причинами впливу на об'єкт соціальної інженерії є, наприклад:

a) відчуття достоїнства;
b) прагнення до успіху;
c) матеріальна вигода.

Використання прийомів прихованого і прямого маніпулювання персоналом дають можливість соціальному інженеру дізнаватися і в подальшому використовувати інформацію для оцінювання її захищеності в комп'ютерній системі.

5 Висновок

Таким чином, оцінювання захищеності інформації в комп'ютерних системах за соціоінженерних підходом дозволяє запобігти, виявити, врахувати або усунути уразливості, що пов'язані або обумовлені діяльністю персоналу. У рамках соціоінженерного підходу його вразливості тлумачяться як слабкості, потреби, манії, захоплення. Маніпулювання ними призводить до нової моделі поведінки персоналу. Це відображається в таких формах як, наприклад, шахрайство, обман, афера, інтрига, містифікація, провокація. Використанню кожної з означених форм маніпулювання передує визначення її змісту шляхом ретельного планування, організування та контролювання. При цьому форми маніпулювання персоналом при оцінюванні захищеності інформації в комп'ютерних системах змінюються залежно від різновиду атак соціальної інженерії. Так, отримання несанкціонованого доступу до інформації за допомогою фішингу, фармінгу, смішінгу, вішінгу, спір фішінгу,

вейлінгу здійснюється шляхом використання таких форм маніпулятивного впливу як шахрайство та обман. Тоді як основою для створення фіктивних ситуацій при прітекстінгу є афера, інтрига, містифікація та провокація.

Література

1. Мохор В. В. Наставления по кибербезопасности (ISO/IEC 27032:2013) / В. В. Мохор, А. М. Богданов, А. С. Килевой. К. : ООО "Три-К", 2013. – 129 с.
2. Information technology. Security techniques. Information security management systems. Requirements : ISO/IEC 27001:2013. – Second edition 2013-10-01. – Geneva, 2013. – P. 23.
3. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-002-99. – Чинний від 1999-04-28. – К. : ДСТСЗІ СБ України, 1999. – 15 с. – (Нормативний документ системи технічного захисту інформації).
4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР [Електронний ресурс] / Закони // Верховна Рада України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80. – Дата доступу : верес. 2017. – Назва з екрану.
5. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. – Чинний від 1997-01-01. – К. : ДСТСЗІ СБ України, 1996. – 11 с. – (Нормативний документ системи технічного захисту інформації).
6. Захист інформації. Технічний захист інформації. Порядок проведення робіт : ДСТУ 3396.1-96. – Чинний від 1997-01-01. – К. : ДСТСЗІ СБ України, 1996. – 15 с. – (Нормативний документ системи технічного захисту інформації).
7. Захист інформації. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2-96. – Чинний від 1997-04-11. – К. : ДСТСЗІ СБ України, 1996. – 19 с. – (Нормативний документ системи технічного захисту інформації).
8. Про затвердження Концепції технічного захисту інформації в Україні : Постанова Кабінету міністрів України від 08.10.1997 № 1126 [Електронний ресурс] / Постанови // Кабінет міністрів України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/1126-97-%D0%BF. – Дата доступу : верес. 2012. – Назва з екрану.
9. Цуркан О.В. Використання соціальної інженерії для негативного інформаційно-психологічного впливу на людину в кібернетичному просторі / О.В. Цуркан, В.В. Мохор, В.В. Цуркан // Актуальні проблеми управління інформаційною безпекою держави : збірник матеріалів науково-практичної конференції, 20 березня 2014 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2014. – Ч. 1. – С. 214-215.
10. Цуркан О.В. Соціоінженерний аспект негативного інформаційно-психологічного впливу на людину в кіберпросторі / О.В. Цуркан, В.В. Мохор // ITSEC: IV міжн. наук.-практ. конф., 20 – 23 травня 2014 р. : тези доп. – К. : НАУ, 2014. – С. 46.
11. Цуркан О.В, Маніпулятивна форма соціоінженерного впливу на особистість в кіберпросторі / В.В. Мохор, О.В. Цуркан, Р.П. Герасимов // Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф. (Київ, 19 березня 2015 року). – К. : Центр навч., наук. та період. видань НА СБ України, 2015. – С. 303-304.
12. Остроухов В. В. Інформаційно-психологічна безпека особи: соціально-правові аспекти / В. В. Остроухов // Інформаційна безпека людини, суспільства, держави. – 2010. – № 1(3). – С. 38-41.
13. Жарков Я. М. Інформаційно-психологічне протиборство (еволюція та сучасність): Монографія / Я. М. Жарков, В. М. Петрик, М. М. Присяжнюк та ін. – К.: ПАТ "Віпол", 2013. – 248 с.
14. Krombholz K. Advanced social engineering attacks / K. Krombholz, H. Hobel, M. Huber, E. Weippl // Journal of information security and applications, (2014), pp. 1-10, http://dx.doi.org/10.1016/j.jisa.2014.09.005.
15. Цуркан О.В. Класифікація атак соціального інжинірингу / О.В. Цуркан, А.В. Жилін // Моделювання (Київ, 15-16 січ. 2009 р.) : XXVIII наук.-техн. конф.: тези доп. – К. : ПП "Системи, технології, інформаційні послуги", 2009. – С. 36 – 37.
16. Цуркан О.В. Аналіз соціоінженерних атак на людину в кіберпросторі / В.В. Мохор, О.В. Цуркан // Інформаційні технології та безпека: засади забезпечення інформаційної безпеки, 28 травня 2014 р.: матеріали міжнародної конференції ІТБ-2014. – К. : ІПРІ НАН України, 2014. – С. 100-102.
17. Winterfeld S. The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice / S. Winterfeld, J. Andress. – Waltham : Elsevier, 2013. – 152 p.
18. Mouton F. Necessity for ethics in social engineering research / Francois Mouton, Mercia M. Malan c, Kai K. Kimppa d, H.S. Venter // ScienceDirect (2015), http://dx.doi.org/10.1016/j.cose.2015.09.001.
19. Mouton F. Social engineering attack examples, templates and scenarios / F. Mouton, L. Leenen, H. Venter // Computers & Security (2016), http://dx.doi.org/doi: 10.1016/j.cose.2016.03.004.
20. Junger M. Priming and warnings are not effective to prevent social engineering attacks / M. Junger, L. Montoya, F.-J. Overink // Computers in Human Behavior (2017), http://dx.doi.org/10.1016/j.chb.2016.09.012.

Information Security Assessment of Computer Systems by Socio-engineering Approach

© Volodymyr V. Mokhor © Oksana V. Tsurkan
Pukhov Institute for Modelling in Energy Engineering of National academy of sciences of Ukraine, Kiev, Ukraine
v.mokhor@gmail.com otsurkan24@gmail.com
© Vasyl V. Tsurkan
Institute of Special Communication and Information Protection of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",
Kiev, Ukraine
v.v.tsurkan@gmail.com
© Rostyslav P. Herasymov
Pukhov Institute for Modelling in Energy Engineering of National academy of sciences of Ukraine, Kiev, Ukraine
gerasimov.rostislav@gmail.com

Abstract

Information security of the computer systems is focused on securing its characteristics like confidentiality, integrity and accessibility from different by themselves unfavourable effects. A potentially possible unfavourable effect is construed as threat. To prevent or complicate realization of threats and reduce possible damage, they create and maintain in active capacity an actions system of securing information in computer systems. The system includes computer system, physical environment, personnel and information. To secure its characteristics in the computer systems it is very important to consider a non-technical aspect, in particular a personnel aspect (for example, boss, administrator and user). Due to that, social engineering techniques are proposed to assess the information security. Within the techniques, personnel sensitiveness is taken as its weakness, demands, mania (addiction) and interests. Their manipulation allows get unauthorized access to information without destroying and distortion of the main for him system creating features (integrity, development). It results in the new model of personnel behavior, creation of favourable conditions to realize information threat and, consequently, reduction of the information security capability of the system to prevent the effects. It is reflected in the forms of fraud, cheating, deception, intrigue, hoax and provocation. The use of each form is preceded by defining its content via a thorough planning, organization and control. These actions make the basis of the social engineering techniques. On one side, they can be realized via modern telecommunication techniques. On the other side, it involves establishing direct contact with personnel. Thus, it is possible to disclose, neutralize and prevent information vulnerability in computer systems using social engineering techniques. It raises its security in view of a non-technical aspect.

Keywords: computer system, information security, information security assessment, personnel, socioengineering approach, social engineering, methods of social engineering.