У останній версії ППЗ Gran1 для кожного інтервалу можна вказати кількість підінтервалів (Рис. 7), що призводить до відповідної зміни графіка функції розподілу статистичних ймовірностей (Рис. 8).

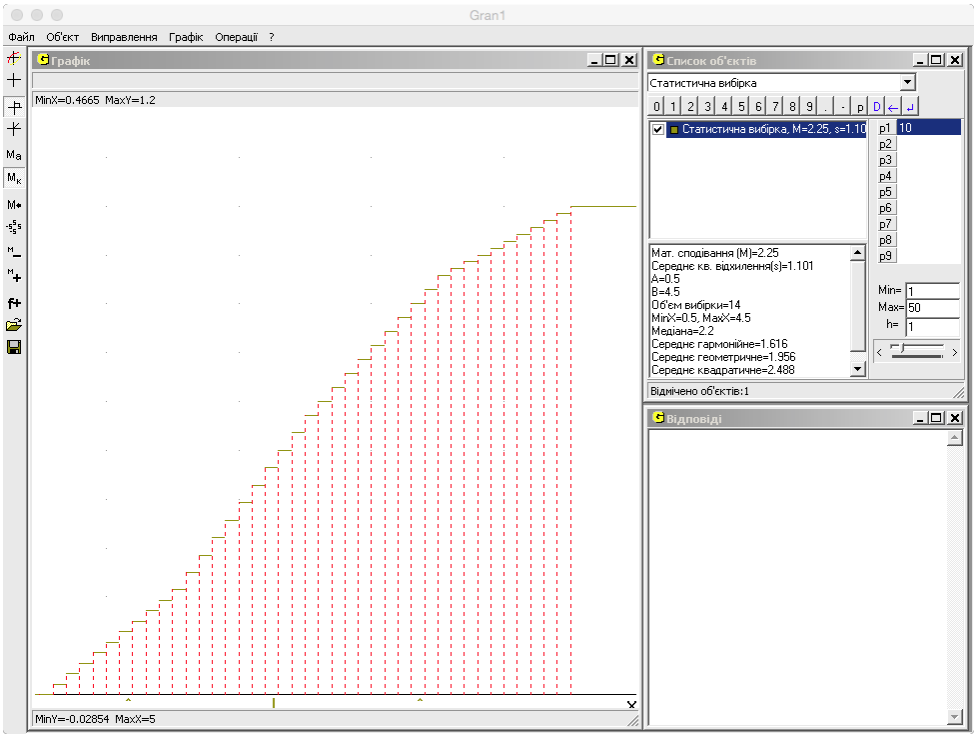

Рис. 8

5. Створення вибірки із псевдовипадкових чисел

Тепер у програмі Gran1 можна створити вибірку, що складається із псевдовипадкових чисел, згенерованих за програмою. Для цього потрібно натиснути кнопку *"Випадкові дані"* у допоміжному вікні *"Дані статистичної вибірки"* (Рис. 7) та вказати відрізок, на якому будуть генеруватися псевдовипадкові числа, а також їх кількість.

Література

1. Жалдак М. І. Математика з комп'ютером : посіб. для вчителів. – 2-ге вид. / М. І. Жалдак, Ю. В. Горошко, Є. Ф. Вінниченко. – К.: вид-во НПУ імені М. П. Драгоманова, 2009. – 274 с.
2. Інформатика: підруч. для 11 кл. загальноосвіт. навч. закл.: академ. рівень, профіл. рівень. / [Й.Я. Ривкінд, Т.І. Лисенко, Л.А. Чернікова, В.В. Шакотько]; за заг. ред. М.З. Згуровського. – К.: Генеза, 2011. – 304 с.: іл.
3. Zadącznik nr 2 do zarządzenia nr 163 Rektora Uniwersytetu Śląskiego w Katowicach z dnia 25 października 2012 r. Literatura i treści programowe studiów podyplomowych kwalifikacyjnych technologia informacyjna i informatyka w szkole. – Mode of access: http://bip.us.edu.pl/sites/bip.us.edu.pl/files/prawo/zal201216302.pdf.
5. Трошин П.И. Моделирование фракталов в среде MAXIMA. – режим доступу http://kpfu.ru/docs/F1526739216/main.pdf.
6. Преобразование равномерно распределенной случайной величины в нормально распределенную. – Режим доступу: http://habrahabr.ru/post/208684/.
7. Моделирование броуновского движения. – режим доступу http://famsl.ru/Broun.aspx.

Франчук В.М.
Національний педагогічний університет імені М.П. Драгоманова

Захист даних. Соціальна інженерія

У сучасному світі дані є найціннішим глобальним ресурсом. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Дані постійно ускладнюються, змінюються якісно, зростає кількість їх джерел і користувачів. Водночас зростає уразливість сучасного інформаційного суспільства від невірогідних (а іноді й шкідливих) даних, їх несвоєчасного надходження, промислового шпигунства, комп'ютерної злочинності і т. ін. Інформаційна безпека – це стан захищеності суспільства, держави,

особистості, стан захищеності інформаційних ресурсів, на основі яких забезпечується прогресивний розвиток життєво важливих сфер суспільства.

Зрозуміло, що в сучасному цивілізованому світі, в якому величезна кількість видів діяльності людей супроводжується комп'ютерною підтримкою, проблема безпеки комп'ютерних систем є надзвичайно актуальною. Врахування усіх недоліків захисних механізмів, передбачення можливих наслідків та загроз безпеки інформаційних ресурсів може убезпечити комп'ютерних користувачів від небажаних впливів різноманітних обставин і сторонніх людей на їхнє життя. Саме тому в наш час професіоналам потрібно володіти навичками використання апробованих методів і надійних засобів захисту комп'ютерних даних та розумітися у проблемах захисту інформаційних ресурсів в усій їх багатогранності [1].

Активно користуючись мережевими ресурсами, в Інтернет можна натрапити на «крекерів», «кіберпанків», «фрікерів», «Інтернет-шахраїв», «мережевих шпигунів», «брейкерів», «кіберсквотерів», «крипто шантажистів» і т.п.

Інколи масштаби дій озброєних потужними комп'ютерами зловмисників, що добре знаються на різних технологіях програмування та вміють користуватися інструментами «*соціальної інженерії*», сягають рівня світових атак. Іноді потужні атаки навіть кваліфікують як «віртуальні війни».

Соціальна інженерія – це метод (атак) несанкціонованого доступу до даних або систем зберігання даних без використання технічних засобів. Метод заснований на використанні слабкості людського чинника і вважається дуже руйнівним. Зловмисник отримує дані, наприклад, шляхом збирання відомостей про службовців об'єкта атаки, за допомогою звичайного телефонного дзвінка або шляхом проникнення в організацію під виглядом її службовця [1].

Незважаючи на те, що поняття соціальної інженерії з'явилося нещодавно, люди в тій чи іншій формі користувалися її прийомами споконвіку. У Стародавній Греції та Римі у великій пошані були люди, які могли заговорити і переконати співрозмовника в «очевидній неправоті». Виступаючи від імені влади, вони вели дипломатичні переговори, а, підмішуючи в свої слова брехню, лестощі та вигідні аргументи, нерідко вирішували такі проблеми, які, у противному випадку, неможливо було вирішити без допомоги меча. У середовищі шпигунів соціальна інженерія завжди була головною зброєю. Видаючи себе за кого завгодно, агенти КДБ і ЦРУ могли вивідати найстрашніші державні таємниці.

На початку 70-х років, в період розквіту фрікінгу (*фрікінг*, (від англ. phreaking – сленговий вираз, що означає зламування телефонних автоматів і мереж, зазвичай з метою отримання безкоштовних дзвінків), деякі телефонні користувачі бавилися тим, що надзвонювали з вуличних автоматів операторам корпорації Bell і перевіряли співробітників стосовно їхніх компетентностей. Потім хтось, очевидно, зрозумів, що якщо трохи перебудувати фрази і подекуди використати неправдиві відомості, можна змусити технічний персонал (співробітників) не просто виправдовуватися, а видавати в пориві емоцій конфіденційні дані. Фрікери (люди, які спеціалізуються на фрікінгу) стали згодом експериментувати з деякими прийомами і до кінця 70-х років настільки відпрацювали прийоми маніпулювання непідготовленими операторами, що могли без проблем дізнатися у них практично все, що потрібно. Заговорювати людей використовуючи телефонні розмови, щоб отримати потрібні відомості або просто змусити їх щось зробити, прирівнювалося до мистецтва. Професіонали в цій галузі дуже пишалися своєю майстерністю. Дуже вправні соціальні інженери (сінжери) діяли експромтом, покладаючись на своє чуття. За правильно поставленим запитанням, з інтонації голосу вони (сінжери) могли визначити комплекси й страхи людини і, миттєво зорієнтувавшись, використати їх у своїх цілях. Наприклад, якщо зателефонувати молодій особі (співробітнику організації), яка нещодавно була зарахована на роботу, фрікер міг натякнути на можливі неприємності з керівництвом, для цього було досить представитися користувачем початківцем, якому все треба пояснити і розповісти. До кожного добирався свій підхід (ключ). З появою комп'ютерів багато фрікерів почали використовувати свої прийоми в комп'ютерних мережах і стали хакерами. Навички соціальної інженерії в новій галузі стали ще кориснішими. Якщо раніше потрібно було заговорити оператора для отримання деяких фрагментів даних з корпоративних довідників, то тепер стало можливим дізнатися пароль для входу в закриту комп'ютерну систему і завантажити звідти ті самі довідники та інші секретні дані. Причому, використовуючи такий спосіб, можна набагато швидше і простіше отримувати потрібні дані, ніж використовувати спеціальні програмно-технічні засоби. Не потрібно шукати вразливості в системах захисту, не треба чекати, поки за допомогою спеціальних програмних засобів буде віднайдений пароль і т. п... Достатньо зателефонувати і, при правильному підході, на іншому кінці телефонної лінії самі назвуть заповітне слово.

Наприклад зловмисник може зателефонувати працівникові компанії (під видом технічної служби) і вивідати пароль, вказавши на необхідність рішення невеликої проблеми в комп'ютерній системі. Дуже часто цей спосіб (трюк) проходить. Найкраща зброя в цьому випадку – приємний голос і акторські здібності. Зловмисник під виглядом службовця компанії телефонує у службу технічної

підтримки. Представляється від імені службовця, він просить нагадати свій пароль, або змінити його на новий, вказавши, що попередній пароль не може згадати. Імена службовців вдається довідатися після низки дзвінків і вивчення імен керівників на сайті компанії й інших джерел відкритих даних (звітів, реклами і т.п.). Далі справа техніки – використовуючи реальні імена в розмові зі службою технічної підтримки, зловмисник розповідає придуману історію, що наприклад, не може потрапити на важливу on-line нараду зі свого облікового запису віддаленого доступу.

Інший спосіб отримання даних може бути дослідження сміття організацій, віртуальних сміттєвих кошиків, крадіжка портативного комп'ютера або носіїв даних. Даний спосіб використовується, коли зловмисник намітив як жертву конкретну організацію (компанію).

Крім цього існують і інші способи отримання даних з використанням методів соціальної інженерії.

Всі методи соціальної інженерії засновані на особливостях прийняття людьми рішень, які ще відомі як когнітивні упередження. Ці упередження використовуються в різних комбінаціях, з метою створення найбільш придатної стратегії обману в кожному конкретному випадку. Але спільною рисою всіх цих методів є введення в оману, з метою змусити людину вчинити будь-яку дію, яка не вигідна їй і необхідна соціальному інженеру. Для досягнення поставленого результату зловмисник використовує цілий ряд усіляких тактик: видача себе за іншу особу, відволікання уваги, нагнітання психологічної напруги і т.д.

Розглянемо детальніше деякі атаки із використанням методів соціальної інженерії.

Претекстинг – це дія, відпрацьована за заздалегідь складеним сценарієм (претекстом). В результаті ціль (особа) повинна видати певні відомості, або зробити певну дію. Цей вид атак застосовується зазвичай за допомогою телефону. Часто в цьому методі використовуються неправдиві відомості, тому використання цього методу вимагає деяких попередніх досліджень (наприклад, персоналізації: дата народження, сума останнього рахунку та ін.), для того, щоб увійти у довіру. До цього ж виду атак відносять також атаки з використання програм месенджерів, наприклад ICQ, Skype та ін.

Фішинг – метод (атака), спрямований на шахрайське отримання конфіденційних даних. В більшості випадків зловмисник відправляє лист електронною поштою, підроблений під офіційний лист – від банку або платіжної системи – вимагаючи «перевірки» певних відомостей, або здійснення певних дій. Цей лист зазвичай містить посилання на фальшиву веб-сторінку, за якою імітується робота офіційної, з корпоративним логотипом і контентом, і містить форму, в якій потрібно ввести конфіденційні дані – від домашньої адреси до пін-коду банківської картки.

Троянський кінь – це метод (атака), в якому використовується зацікавленість або жадібність жертви (особи). Зловмисник відправляє лист електронною поштою, до якого прикріплений файл (додаток) з «важливими» оновленнями антивірусної програми або з «свіжим» компроматом на співробітника. Такий метод залишається ефективним, поки користувачі будуть не задумуючись використовувати будь-які вкладені файли в електронних листах.

Дорожнє яблуко – цей метод атаки є адаптацією троянського коня з використанням фізичних носіїв даних. Зловмисник може підкинути інфікований CD, або флеш-накопичувач, у місці, де носій може бути легко знайдений (туалет, ліфт, паркування). Цей носій підробляється під офіційний, і супроводжується підписом, який може викликати зацікавленість. Наприклад, зловмисник може підкинути CD з корпоративним логотипом і посиланням на офіційний сайт компанії жертви, і написом «Заробітна плата керівного складу 2014». Диск може бути залишений на підлозі ліфта або у вестибюлі. Співробітник через незнання може підібрати диск і використати його на комп'ютері, щоб задовольнити свою цікавість, або просто як «добрий самаритянин» віднесе диск у організацію.

Плечовий серфінг (англ. Shoulder surfing) – включає в себе спостереження особистих даних жертви (особи) через її плече. Цей тип атаки поширений в громадських місцях, таких як кафе, торгівельні центри, аеропорти, вокзали, а також у громадському транспорті.

«Кві про кво» (Qui pro Quo - латинський вираз, який буквально означає щось за щось) - зловмисник може зателефонувати за випадковим номером в організацію, і видати себе співробітником технічної підтримки, який опитує співробітників, чи є які-небудь технічні проблеми з комп'ютерною технікою. У випадку, якщо вони є, у процесі їх «вирішення» жертва вводить команди, за допомогою яких, хакер може запустити шкідливе програмне забезпечення.

Зворотна соціальна інженерія (reverse social engineering) – метою використання цього методу (атаки) є змусити ціль (особу) самій звернутися до зловмисника за «допомогою». Із цією метою хакер може застосовувати такі способи:

- *Диверсія.* Створення невеликої неполадки на комп'ютері жертви.
- *Реклама.* Зловмисник підсуває жертві оголошення виду «Якщо виникли неполадки з комп'ютером, зателефонуйте за таким номером» [2].

Відповідаючи на прохання, надати відомості

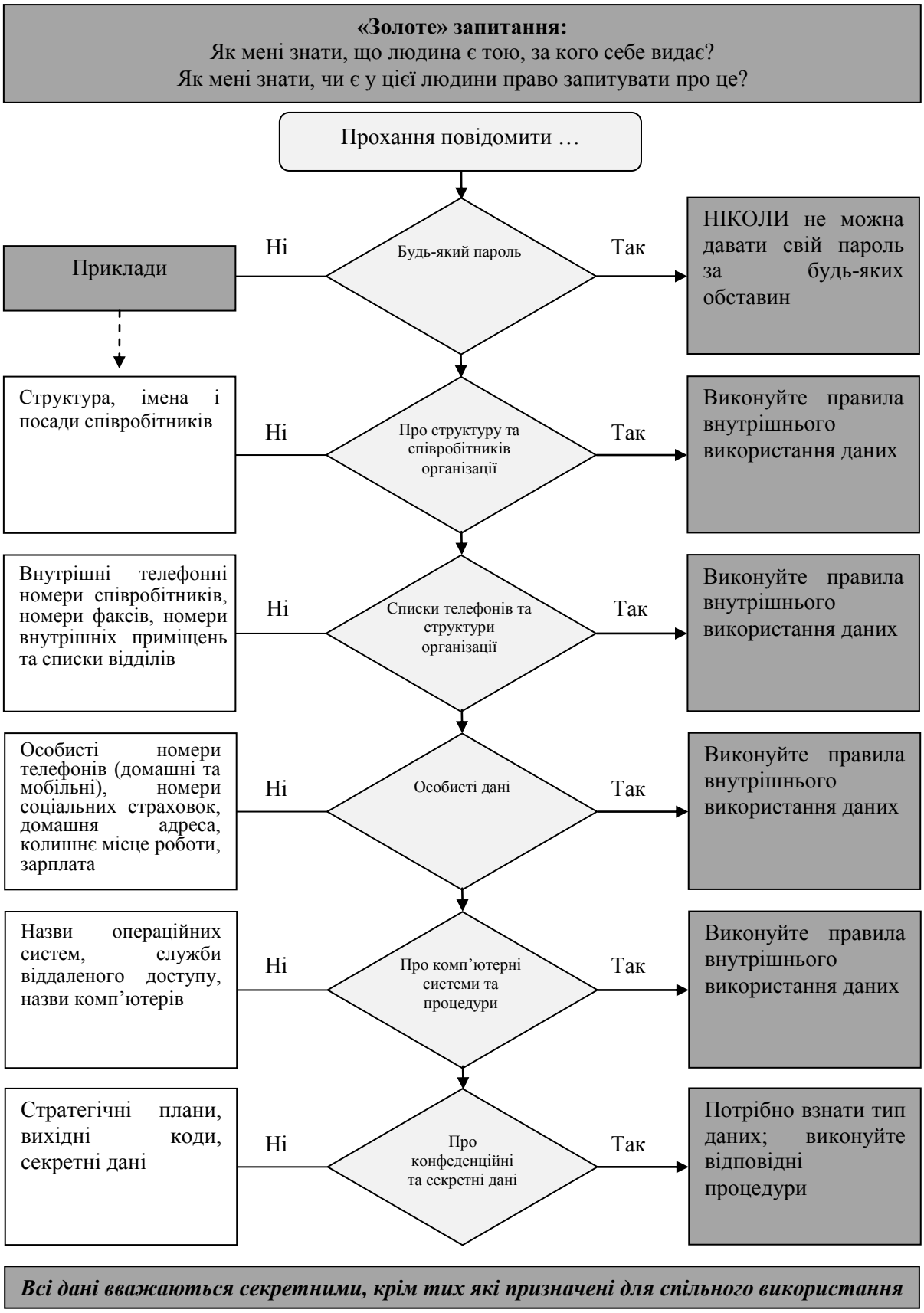

Рис. 1. Рекомендації щодо розкриття атаки**,** спрямованої на отримання даних

Відповідаючи на прохання, вчинення будь-яких дій

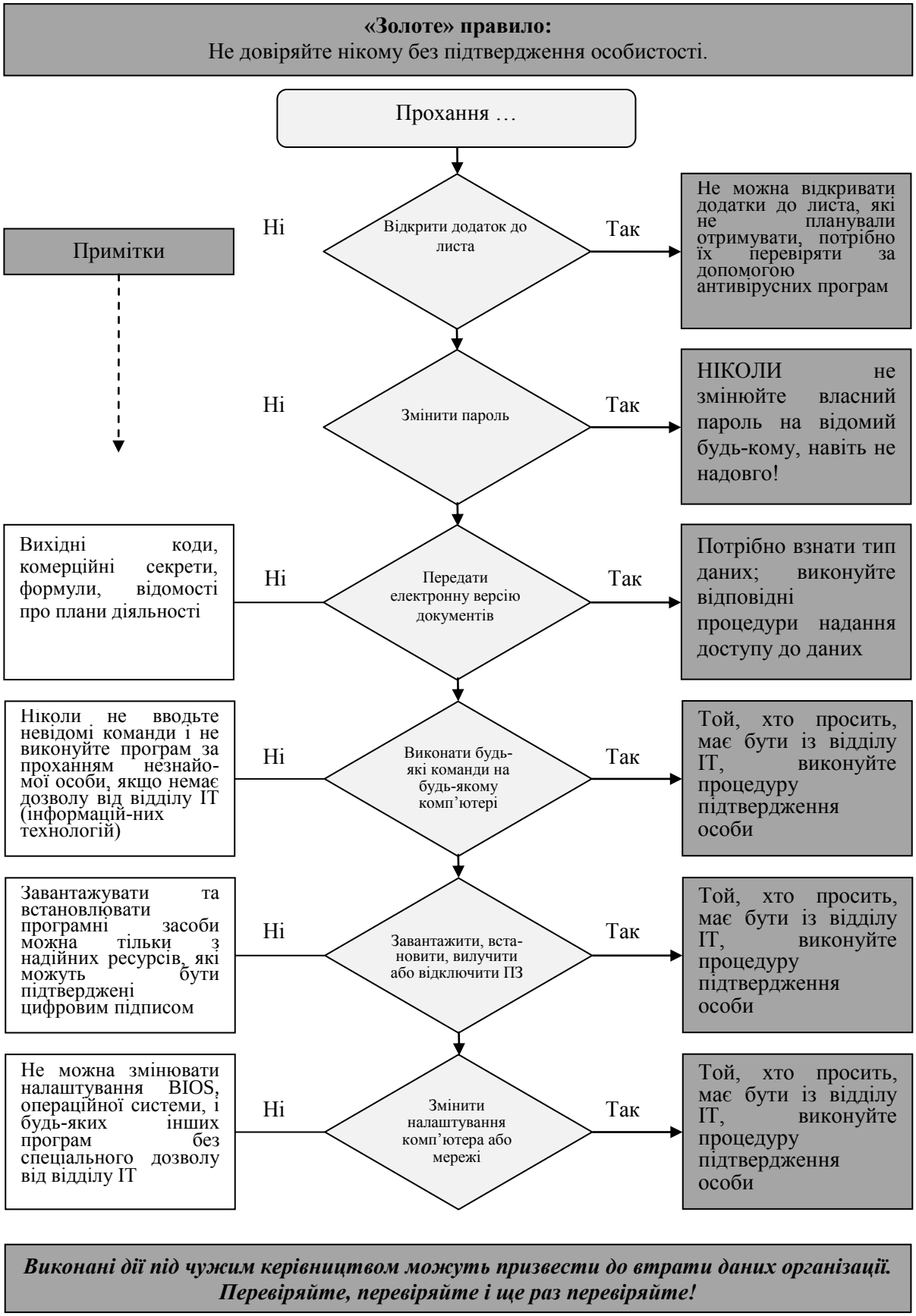

Рис. 2. Рекомендації щодо розкриття атаки**,** спрямованої на вчинення будь-яких дій

Для захисту користувачів від атак з використання методів соціальної інженерії можна застосовувати як антропогенні, так і технічні засоби.

Антропогенний захист. Найпростішими методами антропогенного захисту можна назвати:

- Залучення уваги користувачів до питань безпеки (Рис. 1).
- Усвідомлення користувачами всієї серйозності проблеми й прийняття політики безпеки організації.
- Вивчення й впровадження необхідних методів і дій для підвищення захисту інформаційного забезпечення (Рис. 2).

Дані засоби мають один загальний недолік: вони пасивні. Значний відсоток користувачів не звертає увагу на попередження, навіть написані найбільш помітним шрифтом.

Технічний захист. До технічного захисту можна віднести засоби, використовуючи які, заважають зловмиснику роздобути дані, і засоби, використовуючи які, заважають скористатися отриманими даними.

Найбільш поширеними серед атак з використанням методів соціальної інженерії є використання електронної пошти. Саме до таких атак можна з найбільшою ефективністю застосовувати обидва методи технічного захисту. Перешкодити зловмиснику отримати потрібні йому дані можна, аналізуючи як текст вхідних листів (імовірно, зловмисника), так і вихідних (імовірно, цілі атаки) за ключовими словами. До недоліків такого методу можна віднести велике навантаження на поштовий сервер і неможливість передбачити всі варіанти написання слів. Наприклад, якщо зловмисникові стає відомо, яка програма «реагує» на слово «пароль» і слово «вказати», зловмисник може замінити їх на «пассворд» і, відповідно, «ввести». Так само варто брати до уваги можливість написання слів із заміною кириличних літер латиницею для співпадаючих символів (а, с, е, о, р, х, у, А, В, С, Е, Н, К, М, О, Р, Т, Х). Засоби, за допомогою яких неможливо скористатися отриманими даними, можна поділити на ті, за допомогою яких повністю блокують використання даних, де б то не було, крім робочого місця користувача (може використовуватися прив'язка до серійних номерів або електронних підписів комплектуючих комп'ютера, до IP-адреси і т.д.), так і ті, за допомогою яких стає неможливим (або важко реалізувати) автоматичне використання отримання даних (наприклад, авторизація з використанням системи Captcha, коли в якості пароля потрібно ввести символи із спотвореного зображення) [3].

Але самий основний спосіб захисту від атак з використанням методів соціальної інженерії – це навчання. Тому що той, хто попереджений (навчений) – той озброєний. А незнання в свою чергу не звільняє від відповідальності. Всі співробітники організації повинні знати про небезпеки розкриття даних та способи їх запобігання. Крім того, співробітники організації повинні мати чіткі інструкції про те, як, на які теми говорити зі співрозмовником, які відомості для точної аутентифікації співрозмовника їм необхідно у нього отримати. З вище зазначеного можна виокремити деякі правила, які будуть корисні для співробітників організацій:

- Усі паролі користувача є власністю організації. Всім співробітникам повинно бути роз'яснено в день зарахування на роботу, що ті паролі, які їм видали, не можна використовувати в яких би то не було інших цілях, наприклад, для авторизації на сайтах (відомо, що людині важко тримати в пам’яті всі паролі і коди доступу, тому часто користуються одним паролем для різних ситуацій). Як така вразливість може бути використана в соціальній інженерії? Припустимо, співробітник організації став жертвою фішингу. У результаті його пароль на деякому сайті став відомий третім особам. Якщо цей пароль збігається з тим, який використовується в організації, виникає потенційна загроза безпеці самої організації. В принципі навіть не обов’язково, щоб співробітник організації ставав жертвою фішингу. Немає жодних гарантій, що на сайтах, де він авторизується, дотримуються необхідного рівня безпеки. Так що потенційна загроза завжди існує.
- Всі співробітники повинні бути проінструктовані, як поводитися з відвідувачами. Необхідні чіткі правила для встановлення особи відвідувача і його супроводу. Біля відвідувача завжди повинен знаходитися хтось із співробітників організації. Якщо співробітник організації зустрічає відвідувача, який просто сам ходить у приміщенні організації, то він повинен мати необхідні інструкції для коректного з'ясування того, з якою метою відвідувач опинився в цій частині приміщення і де його супровід.
- Має існувати правило коректного розкриття тільки дійсно необхідних даних у телефонних розмовах і під час особистої розмови, а так само процедура перевірки, чи є той, хто що-небудь запитує, дійсно співробітником організації. Не секрет, що більша частина відомостей добувається зловмисником під час безпосереднього спілкування з співробітниками організації. Треба врахувати ще той факт, що у великих організаціях співробітники можуть не знати один одного, тому зловмисник може легко «прикинутися» співробітником, якому потрібна допомога.

Всі описані вище заходи досить прості, однак більшість співробітників забувають про ці заходи і про той рівень відповідальності, який на них покладено під час підписання зобов'язань про нерозголошення комерційної таємниці. Організаціями витрачаються значні фінансові кошти на забезпечення інформаційної безпеки технічними методами, проте ці технічні перешкоди можуть бути подолані, якщо співробітники не будуть застосовувати заходи з протидії соціальним інженерам, а служби безпеки не будуть періодично перевіряти пильність персоналу організації. Тим самим кошти, спрямовані на забезпечення інформаційної безпеки, будуть витрачені марно.

У будь-якому випадку фахівцям-комп'ютерникам потрібно вміти надійно захищати інформаційні ресурси і всіляко уникати дій різного роду зловмисників. Для цього потрібно багатогранно досліджувати усі наявні технології та інструменти, до яких можуть вдатися хакери для доступу до даних, а також знатися на гарантованих прийомах і методах захисту даних та протидії їх пошкодженню.

Література

1. Смалько О.А. Захист інформаційних ресурсів: Монографія. – Кам'янець-Подільський: ПП Буйницький О. А., 2011. – 704 с.

2. Соціальна інженерія (безпека) [Електронний ресурс] – Режим доступу: http://uk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D1%8F_(%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0).

3. Соціальна інженерія [Електронний ресурс] – Режим доступу: http://wiki.tntu.edu.ua/%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D1%8F.

Біляй Ю.П.
Національний педагогічний університет імені М.П. Драгоманова

Дистанційне навчання баз даних

Сучасний світ інформаційних технологій неможливо уявити без використання баз даних. Практично всі системи пов'язані з функціями довготривалого зберігання та опрацювання даних. Тому бази даних – один з важливих курсів, пов'язаних з інформатикою.

Правильна постановка задачі, пошук і добір даних відіграє важливу роль у практичній діяльності людей багатьох професій, зокрема вчителів математичних та інформатичних дисциплін. Наприклад під час пошуку даних щодо використання Internet-технологій за відсутності вміння створювати правильні запити людина може отримати тисячі варіантів відповідей, або зовсім не отримати очікуваної відповіді на поставлений запит. Це свідчить про недостатнє розуміння принципу функціонування баз даних.

Підготовка кваліфікованих фахівців вимагає розвитку у них практичних навичок проектування і розробки баз даних. Курс «Бази даних» розрахований на один семестр, тому основна увага приділена питанням реалізації баз даних, а також розглядаються питання проектування правильної структури бази даних, відповідної моделі предметної галузі.

В процесі вивчення систем управління базами даних можуть виникнути певні проблеми, зокрема такі, що при формальному підході до вивчення баз даних після вивчення систем управління базами даних залишається не висвітленими у повній мірі призначення деяких операцій. На лекційних заняттях не обов'язково розглядати подробиці побудови подібної структури – вона може відрізнятися дуже високим рівнем складності (яку краще уточнювати на практиці в консолях баз даних або в процесі програмуванні додатків, де використовуються різні технології під'єднання баз даних).

Виникають утруднення під час вивчення правил роботи з кількома базами даних різного ступеня складності, часто абсолютно не пов'язаних між собою за змістом і призначенням. Крім того, нерідко використовується зайва кількість таблиць і зв'язків між ними, що ускладнює засвоєння основних понять відношення між таблицями.

За умов поступового подання навчального матеріалу здебільшого залишається мало часу на вивчення структурованої мов запитів – SQL (structured query language), на основі якої забезпечується управління структурою БД і роботи з даними, яка також є стандартним засобом доступу до віддалених БД.

За сформованою традицією вивчення теми «Бази даних. СУБД» будується на основі MS Access, з якою студенти знайомі ще зі школи. Проте через різний рівень підготовки, потрібно врахувати, що створення баз даних без використання СУБД може буди складним для деяких студентів. Тому в процесі навчання потрібно поєднувати вивчення теоретичного матеріалу разом із практичними