- принцип стимулювання, що припускає зацікавленість усіх сторін у досягненні максимального результату: збільшення фінансових потоків і підвищення ефективності їх використання;
- принцип транспарентності, що дає змогу одержати достовірну і повну інформацію про фінансові потоки всіх суб'єктів економічної системи території.

Таким чином, для виконання вимог оптимальності та системності під час управління фінансовим потенціалом території необхідно дотримуватись всіх основних принципів оптимізованого управління, й оцінювати не лише окремі коефіцієнти, але і їх співвідношення, структуру, що дасть змогу звести та відобразити процес формування фінансового потенціалу території і зрештою –виявити слабкі та сильні сторони.

Висновки. Сутність фінансового потенціалу території полягає в можливості керівних органів держави та місцевого самоврядування консолідувати та генерувати наявні й потенційні фінансові ресурси економічної системи з метою забезпечення економічного розвитку території в інтересах його населення.

Формування достатнього рівня фінансового потенціалу території є метою кожного органу місцевого самоврядування й передумовою їхнього успішного функціонування, ефективної діяльності, виступає основою забезпечення належного рівня фінансової стійкості території. Сформована передумова запровадження концепції оптимізованої системи управління фінансового потенціалу території, а також виділено та охарактеризовано основні принципи функціонування системи управління фінансовим потенціалом території.

Література

1. Возняк Г.В. Фінансовий потенціал реального сектора економіки регіону: підходи до формування та використання / Г.В. Возняк // Регіональна економіка : наук.-практ. журнал. – 2012. – № 1. – С. 107-116.

2. Карпінський Б.А. Негативна синергічність фінансової продуктивності регіонів України за впливу глобальних фінансових викликів / Б.А. Карпінський // Вісник Львівської державної фінансової академії. – Сер.: Економічні науки. – 2010. – № 18. – С. 133-142.

3. Карпінський Б.А. Збалансованість фінансової системи: методологія, оцінка, порівняння : монографія / Б.А. Карпінський. – Львів : Вид-во "Логос", 2005. – 496 с.

4. Карпінський Б.А. Оцінювання і порівняння фінансової продуктивності національного господарства в умовах глобальних фінансових викликів: методологія та практика / Б.А. Карпінський // Наукові праці НДФІ : наук. зб. – 2010. – Вип. 1(50). – С. 80-90.

5. Руденко Л.В. Фінансовий ресурс як компонент динамічної системи ресурсного забезпечення транснаціональних корпорацій / Л.В. Руденко // Економіка і управління : наук. журнал. – 2006. – № 1. – С. 15-23.

6. Свірський В. Фінансовий потенціал: теоретико-концептуальні засади / В. Свірський // Світ фінансів : наук. журнал. – 2007. – № 4 (13). – С. 43-51.

7. Чуницька І.І. До питання формування і реалізації фінансового потенціалу держави / І.І. Чуницька // Інвестиції: практика та досвід. – 2007. – № 13. – С. 28-32.

8. Фінанси регіону: теорія, проблеми, практика : монографія / М.А. Козоріз, А.Я. Кузнєцова, І.З. Сторонянська, Г.В. Возняк. – К. : Вид-во УБС НБУ, 2010. – 222 с.

Карпинский Б.А., Григоренко В.О. **Концепция оптимизированной системы управления финансовым потенциалом территории**

Выделены функциональная зависимость и сущность финансового потенциала территории. Определены основы формирования новой системы управления финансовым потенциалом территории, которая базируется на концепции оптимизированного управления. Рассмотрены основные стадии процесса управления финансовым потенциалом. Определены базовые принципы процесса управления.

Ключевые слова: финансы, финансовый потенциал территории, концепция управления, оптимизированное управление, фактор, принципы, формы проявления, финансовые ресурсы.

Karpinsky B.A., Grigorenko V.O. **The concept of optimized system management by financial potential on the territory**

The functional dependence and the essence of the financial capacity on the territory are selected. The basics of forming a new system of management by financial potential of the territory, which is based on the concept of optimized control are outlined. The basic stages of managing by financial potential are considered. The basic principles of management are presented.

Keywords: a finance, financial potential of the territory, the concept of governance, optimized management, a factor, the principles, the forms of manifestation, financial resources.

УДК 004.056:061.68

Курсант Н.В. Чудінова; проф. Ю.І. Грицюк, д-р техн. наук – Львівський ДУ БЖД

ОСОБЛИВОСТІ ВИКОРИСТАННЯ МЕРЕЖІ ІНТЕРНЕТ ДЛЯ ОТРИМАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Прагнення людей до спілкування, особливо в соціальних мережах, закладене в самій природі людини. З появою мережі Інтернет люди не поміняли своїх звичок, продовжуючи вирішувати особисті проблеми через корпоративні засоби зв'язку. Позаяк використання поштової скриньки у власних потребах не створює видимих фінансових витрат, то в багатьох державних установах такий стан речей взагалі не вважають проблемою, тому просто її тимчасово ігнорують, позаяк приділяють увагу вирішанню інших нагальних проблем. Проте користь подібного явища на перевірку інформаційної безпеки багатьох установ виявилася хибною, тобто не завжди це обходиться без наслідків для фірм чи держави.

Ключові слова: інформаційні загрози, інформаційна безпека, конфіденційна інформація, джерела загроз, промислова компанія.

Вступ. Останнім часом набуло широкого розповсюдження спілкування людей в мережі Інтернет, електронною поштою Skype, на форумах і в чатах, не замислюючись при цьому про місцезнаходження співбесідників [15]. Велика швидкість передачі даних і збільшена продуктивність комп'ютерів дають змогу користувачам за мінімальних витрат не тільки обмінюватися текстовими повідомленнями в реальному часі[1], але й здійснювати аудіо- і відеозв'язок [14]. Проте, як це часто трапляється, з вирішенням попередніх проблем з'являються нові, позаяк охочі до розмов не поміняли своїх звичок. Наприклад, якщо раніше з робочих телефонів обговорювалися здебільшого домашні та особисті проблеми, то сьогодні до цього додалося використання корпоративної електронної адреси як у робочих, так і в особистих потребах.

Оскільки використання поштової скриньки не створює видимої фінансової проблеми, то в багатьох державних установах, в т.ч. структурних підрозділах ДСНС України, такий стан речей взагалі не вважають проблемою, тому просто її тимчасово ігнорують, позаяк приділяють увагу вирішанню ін-

[1] Під спілкуванням у реальному часі, як правило, розуміють такий процес обміну інформацією, при якому у тих, що спілкуються, є можливість отримувати у відповідь повідомлення з мінімальною затримкою в часі.

ших нагальних проблем. Проте користь подібного явища на перевірку ІБ багатьох установ виявилася хибною. Значна кількість прикладів [1, 3, 11, 13], виявлених фахівцями з аудиту ІБ, висвітлює проблеми ІБ установ, які були створеними виключно прагненням людей до спілкування на фоні бездіяльності керівників служб ІБ. Є факти, коли безграмотне користування корпоративною електронною поштою дало змогу фахівцям з конкурентної розвідки відносно швидко ідентифікувати відповідних осіб – носіїв конфіденційної інформації установи і зробити все можливе для того, щоб отримати від них потрібні дані, навіть, не прикладаючи до цього великі зусилля [13].

В усіх наведених нижче випадках відповідні особи, які потрапили в поле зору фахівців з аудиту ІБ, використовували в особистих цілях корпоративну електронну пошту, яка містить в адресі мережеве ім'я (нік, nickname) користувача і доменне ім'я установи. Для того, щоб результати дослідження виявилися правдоподібними, а також допитливому читачеві стали зрозумілими висновки, які знаходяться в основі прийнятих рішень фахівців з аудиту ІБ, вигадані далі в роботі особисті імена та їхні адреси повністю відповідають реальним.

Фахівці з аудиту ІБ провели два окремих дослідження за допомогою відкритих джерел інформації з використанням пошукових систем Yandex, Rambler і Google. У першому випадку потрібно було здійснити аудит фірми з метою виявлення несанкціонованої керівництвом інформації про неї в мережі Інтернет. У другому випадку проводилося дослідження фірми-конкурента стосовно витоку конфіденційної інформації про деякі особливості її роботи.

Досліджувалася фірма "СофтСервіс", яку було засновано у Львові в 2003 році зі спеціалізацією на складанні комп'ютерів з комплектних деталей, завезених переважно з країн Східної Азії. Запит "СофтСервіс комп'ютери" був розміщений в кожній з пошукових систем. Серед перших знайдених сторінок виявився сайт її фірми – http://softservice.com.ua, а також адреса офісу та відповідні телефони приймальної керівника та відділу маркетингу. За допомогою послуги перевірки доменного імені на Web-сервері компанії Soft-Maximum було встановлено, що ім'я дійсно зареєстроване на дану фірму. Після цього у зазначених пошукових системах було внесено таку фразу: "softservice.com.ua"&&+(форум|чат|оголошення|куплю|продам|знайомства|foum|chat).

Внаслідок такого пошуку було отримано посилання на декілька форумів і чатів, де розміщувалися оголошення про купівлю-продаж комп'ютерів, комплектних деталей і офісної техніки, а також деякі співробітники цієї фірми залишали свої повідомлення. Більшість з них для потреб дослідження не мали інформаційної цінності, проте увагу привернули дві особи, які не часто були присутні на форумах і в чатах, проте привернули увагу фахівців з ІБ.

1. Професійні поради на форумах і в чатах. Перший співробітник фірми "СофтСервіс" фігурував під псевдонімом Edic_Soft, був постійним відвідувачем форуму, присвяченому комп'ютерам і їхнім проблемам. У своїх реєстраційних даних він вказав адресу електронної пошти edic@softservice.com.ua. Аналіз його повідомлень дав змогу фахівцям з аудиту ІБ зрозуміти, що це кваліфікований працівник у області комп'ютерної інженерії, мережевих технологій і операційних систем. Зважаючи на ім'я користувача (нік softservice) в електронній пошті, було зроблено висновок, що йдеться можливо про системного адміністратора фірми "СофтСервіс", якого звати Едуард. Як показує практика [7], користувачі досить часто пов'язують нік зі своїм справжнім іменем, прізвищем або посадою. Зокрема, командна посада часто знаходить своє втілення в ніку: manager, finance, sys_admin, editor.

Щоб переконатися, що Едуард справді працює на фірмі "СофтСервіс" і на якій посаді, фахівцям з аудиту ІБ довелося зателефонувати в приймальну директора фірм, представитися представником навчальної установи і попросити зв'язатися з системним адміністратором Едуардом з приводу налагодження комп'ютерної мережі. На що секретар люб'язно відповіла, що "...Едуарда Григоровича сьогодні на роботі немає – він у відрядженні". Проте, нею ж було запропоновано зв'язатися з його заступником, який спробує вирішити усі наші питання. Виявляється, ще й секретар з легкістю видає інформацію, яка не входить в її компетенцію.

Інформація про те, що ім'я системного адміністратора корпоративної мережі стало швидко відоме стороннім особам (в нашому випадку фахівцям з аудиту ІБ), виявилася для директора фірми "СофтСервіс" несподіванкою. Він не очікував й того, що Едуард на форумі досить детально розповідав відвідувачам, наприклад, про принципи налаштувань захисту уявного мережевого сервера, організація мережевої інфраструктури для уникнення загроз інформаційній безпеці тощо. Системний адміністратор, який знає практично все про захист інформаційних ресурсів фірми, – це не та особа, яка мала б виставляти себе на загальний огляд у соціальній мережі та ще й давав професійні поради у сфері ІТ та ІБ.

Директор фірми "СофтСервіс" визнав, що інцидент потребує ретельного аналізу, зважаючи на його потенційну небезпеку [2]. Проте, через свою поблажливість, або, можливо, з інших міркувань, він не був схильний ускладнювати ситуацію до такої міри, аби приймати організаційні висновки. Водночас було зрозуміло, що ситуацію треба негайно виправляти, бажано без зайвого розголосу. Йшлося саме про виправлення, а не про профілактику рецидиву [3], оскільки системний адміністратор, розуміючи краще за багатьох інших небезпеку скоєного, визнав свою провину і заявив, що надалі не допустить повторення подібних промахів.

Окрім цього, як для керівника фірми, так і для системного адміністратора було очевидне, що прибрати з мережі інформацію, яка вже потрапила в неї, швидше за все не вдасться. Більше цього, не було впевненості в тому, що інформація вже не потрапила в руки зацікавлених осіб з конкурентних фірм.

Захист інформаційних ресурсів за "принцип Алі-Баби". Фахівці з аудиту ІБ запропонували керівнику фірми "СофтСервіс" застосувати стандартну схему, направлену на запобігання витоку інформації з первинних джерел [9]. Така схема є виправданою в разі її виявлення, наприклад, каналами зв'язку або за допомогою "жучків" – закладних пристроїв. Адже, в описуваному прикладі склалася дещо сприятливіша ситуація, ніж при виявленні "жучків", коли де-факто невідомо, що саме працівники фірм встигли "наговорити в мік-

рофон". Обсяг витоку інформації у соціальній мережі був очевидний, хоча, ймовірність того, що потенційний зловмисник вже зміг знайти щось таке, що аудитори випустили з уваги, залишалася великою.

Запропонований аудиторами варіант захисту інформаційних ресурсів називається "принципом Алі-Баби": якщо неможливо стерти хрестик на своїх дверях, то треба його намалювати на всіх інших [6]. У нашому випадку було б неправильно переривати спілкування в соціальній мережі та на форумах. Тому було прийнято рішення – продовжувати видавати інформацію, але не достеменну, а дещо спотворену, поступово відхилюючи правдоподібність фактів і висновків від реальних. Робити це слід до тих пір, поки, внаслідок таких логічних відхилень, інформація не перестане відповідати дійсному стану справ на фірмі "СофтСервіс". При цьому потрібно створити ілюзію поступового згортання активності Едуарда Григоровича на форумі, мотивуючи це якоюсь правдоподібною причиною. Зважаючи на його обізнаність в ІТ і зайву балакучість, здійснити це було достатньо легко.

Після того, як було оцінено загальну кількість його публікацій на форумі за останні три місяці (їх виявилося 16) і кількість тих з них, де розповідалося про налаштування системи захисту мережевого сервера, було прийнято рішення протягом наступних двох місяців дати ще 13-15 публікацій на загальні теми з ІТ, поступово зменшуючи їхній обсяг. При цьому в трьох повідомленнях першої десятки йшлося про деякі правдоподібні зміни в налаштуваннях захисту сервера, а в 11-му – про те, що придбано новий мережевий сервер з надзвичайно потужними можливостями (коротка інформація про нього була взята з мережі Інтернет), а також у 13 повідомленні – про те, що Едуард змушений змінити місце роботи, позаяк іде на підвищення. Одночасно зі "зміною місця роботи" змінилася і адреса його електронної пошти на kisa@gmail.com.ua. Оскільки системний адміністратор не вважав за потрібне все ж таки залишатися на форумі, то він заздалегідь зареєструвався під іншим псевдонімом і зберіг свою присутність тільки під новим іменем. Причина в тому, що на деяких форумах їх учасники отримують "звання" та "регалії", що для багатьох співбесідників виявляється досить важливим, тому безболісно прибрати з форуму охочого поговорити в on-line режимі не завжди вдається [5].

Вочевидь, цей інцидент заставив системного адміністратора фірми "СофтСервіс" задуматися над своїми діями і, насамперед, визначити недопустимість своєї поведінки. Він перестав публікувати свої повідомлення, які стосувалися його безпосередньої роботи, наводити приклади реальних налаштування мережевого сервера тощо. Водночас, керівник фірми за порадою фахівців з аудиту ІБ вирішив піти на такі надмірні, за відношенням до масштабів витоку інформації, заходи, виходячи з двох причин [13].

По-перше, особа системного адміністратора фірми в соціальній мережі взагалі має бути засекречена, або не афішуватися взагалі. Інакше, при здійсненні недружніх дій відносно фірми "СофтСервіс" фахівців з конкурентної розвідки, з'являється можливість швидкої нейтралізації тим або іншим способом посадової особи, яка в змозі знаходити, знищувати або змінювати

інформацію в корпоративній мережі, що різко знижує здатність фірми до опору [6]. Системний адміністратор – носій інформації про системні доступи практично до всіх конфіденційних даних, тому при певних обставинах він може бути підданий певному шантажу представниками конкурентної розвідки, внаслідок чого результати подальших його дій матимуть кримінальний характер. Водночас, знання посади, імені та електронної адреси системного адміністратора часто відкриває широкий простір для діяльності "соціальних аналітиків", які навчені маніпулювати співрозмовниками і моделювати уявні ситуації для того, щоб змусити їх видати потрібну інформацію [8]. Подібні знання дають змогу фахівцю з конкурентної розвідки ставити питання користувачам корпоративної мережі фірми "СофтСервіс" про паролі доступу в систему від імені адміністратора мережі. При цьому зробити це можна як телефоном, так і електронною поштою. Рідкісний працівник, побачивши, що електронний лист прийшов з адреси системного адміністратора, стане перевіряти його правдоподібність і зворотну адресу, особливо в кінці робочого дня та за наявності зовні достовірного формулювання запитання.

По-друге, директор фірми "СофтСервіс", почувши від фахівців з аудиту ІБ про існування типових рішень для виходу з подібних ситуацій, захотів провести свого роду "навчання" співробітників з виявленої проблеми.

3. Охочий до флірту з чарівними дівчатами. Другий співробітник фірми "СофтСервіс", який потрапив у поле зору фахівців з аудиту ІБ, регулярно продавав уживані комп'ютери та старі комплектні деталі, і, окрім цього, активно спілкувався з чарівними співрозмовниками. Завдяки його "старанням" адреса електронної пошти fedir@softservice.com.ua і характерний нік FedirTP за кількістю згадок у мережі наближалася до десяти сторінок Веб-сайту. Більше цього, на одному з Інтернет-ресурсів, присвяченому знайомствам, поряд з розповіддю про свою роботу на фірмі "СофтСервіс", ілюструючи її перспективи співпраці з азійськими комп'ютерними фірмами, було виставлене фото цього балакуна біля свого авто при вході на роботу. Для отримання його імені не довелося нікого й запитувати – Тарас Петрович сам написав його поряд зі своїм фото, а Федір, як виявилося – його прізвище. Керівник фірми "СофтСервіс", побачивши це фото, впізнав у ньому провідного фахівця відділу маркетингу, допущеного до всієї інформації про її міжнародні проекти. Чим це могло бути потенційно небезпечним для фірми, здогадатися необізнаному читачеві важко, тому для точнішої відповіді на це запитання, наведено трохи теорії та деяких аналогій з подібних ситуацій.

Згідно з класичними поглядами [13], одне з найважливіших завдань конкурентної розвідки – надання своєму керівництву інформації про те, де відносно конкурентів знаходиться фірма зараз і де вона виявиться завтра. Зрозуміло, знання планів конкурента дає змогу керівникові фірми прийняти найбільш правильне рішення про стратегію подальших дій. Це настільки важливо, що, наприклад, крупні американські компанії, які торгують зерном, витрачають значні суми на придбання знімків з космосу, на яких зображені поля в країнах-виробниках сільськогосподарської продукції. Внаслідок такого контролю є можливість раніше і точніше за конкурентів прогнозувати си-

туацію на ринку сільськогосподарської продукції. У нашій ситуації ставки набагато менші, але відмінності обмежуються тільки масштабами товарообігу. Для керівництва компанії-конкурента мати джерело інформації про рішення, прийняті усередині фірми "СофтСервіс", – справжній успіх. Якщо до цього додати, що для регулярного отримання подібної стратегічної інформації достатньо тільки трохи віскі (про те, що цей маркетолог є великим прихильником цього напою, він сам люб'язно повідомив на форумі, розповідаючи про їхні марки, смаки і ціни), то конкуренти в особі такого фахівця могли знайти цінне джерело інформації про ринки збуту комп'ютерного обладнання, тендерні пропозиції, потенційні замовлення тощо.

Для отримання регулярної інформації достатньо було вийти з віртуального світу в реальний, скориставшись схильністю маркетолога вступати на форумах у суперечку з будь-якого приводу, і укласти з ним парі на пляшку віскі про що завгодно, головне – зі свідомо програшним результатом для фахівця з конкурентної розвідки. Після особистого знайомства, найімовірніше, за чаркою віскі контакт буде налагоджено і можна розраховувати на те, що такі зустрічі стануть постійним приводом для будь-яких дискусій – ну як же в такій ситуації не заговорити про роботу!

Подібне отримання інформації – зовсім не примарні фантазії. Артур Вайс, англійський консультант і тренер з конкурентної розвідки [6], який постійно веде відкриті та корпоративні семінари, наводить такий приклад. На одному із західних підприємств була технологічна проблема, над вирішенням якої протягом півтора роки працювали його інженери. Керівництво конкурентної фірми залучило для виявлення суті проблеми фахівців підрозділу, один з якого порадив керівникові відділу маркетингу підприємства на зборах, де присутні співробітники різних служб, публічно поскаржитися на те, що інженери підприємства не можуть впоратися з проблемою. При цьому потрібно було підкреслити, що в одного з конкурентів ця проблема якось вирішена і то вже давно. Внаслідок цього за два тижні технологічна проблема стала відомою конкурентній фірмі, позаяк один із співробітників фірми грав у футбол разом з інженером підприємства і як би ненавмисно розпитав його про проблему, яку вони не можуть вирішити. Виявляється на Заході можливо навіть те, що друзі розмовляють про роботу під час відпочинку. Тобто, не варто забувати про різні способи отримання потрібної інформації на форумах, у чатах або в приватних розмовах. Якщо ви активний учасник жвавих дискусій з приводу деяких робочих проблем, то кваліфікованому аналітику не буде великих проблем взнати про роботу вашої фірми за опосередкованою інформацією [3]. Тому, якщо ви надто говіркий, то є зміст у таких дискусіях час від часу плутати факти, видавати дезінформацію, не згадувати прізвища конкретних фахівців, посилаючись на деякі проблеми з пам'яттю.

Пристрасть маркетолога до віски та спілкування з прекрасною статтю, на думку керівника фірми "СофтСервіс", давно заважала його ефективній роботі, але ні дисциплінарні стягнення, ні позбавлення премії не допомагали. Виявлений факт поведінки співробітника у мережі став останнім китайським попередженням – маркетолог був переведений на іншу, менш інформативну роботу, з якої він згодом звільнився за власним бажанням.

4. Дослідження фірми-конкурента. Це дослідження проводилося відносно головного конкурента фірми "СофтСервіс" – компанії "НеоСервіс", що, з одного боку, позбавляло фахівців з аудиту ІБ можливості повторної перевірки отриманої інформації, але з іншого – давало їм змогу переконатися в ефективній діяльності фахівців з конкурентної розвідки. Робота велася з особами, вказаними замовником дослідження, тобто директором фірми "СофтСервіс", а не в режимі "вільного полювання", як у попередньому прикладі.

Після дослідження сайту компанії "НеоСервіс" був проведений пошук за доменним іменем як фрагмента адреси електронної пошти – "neoservise.com.ua". Одна із знайдених сторінок була книгою відгуків на першій сторінці сайту організації, що займається навчанням. У книзі було зафіксовано повідомлення, пов'язане з адресою yuliya_pari@neoservise.com.ua і вказівка на те, що автор відгуку – працівник компанії "НеоСервіс", відносно якої проводилося дослідження. Після цього було проведено пошук за ніком "yuliya_pari", і на одному з форумів, присвяченому банківській діяльності, виявилася учасниця з таким самим ніком, але з іншою адресою електронної пошти yuliya_pari@gmail.com.ua, яка давала детальні пояснення щодо діяльності компанії, а також поради з приводу різних схем роботи з банками і лізинговими організаціями. Про те, що це фахівець своєї справи, свідчили тексти її відповідей, в яких вона коротко, лаконічно і в доступній формі давала різні пояснення.

На момент проведення дослідження у форумі було шість її повідомлень, які відповідали на питання його відвідувачів і розповідали про плюси і мінуси конкретної фінансової схеми. Кожен учасник форуму міг поставити практично будь-яке запитання та отримати конкретну відповідь. З високим ступенем ймовірності можна було передбачити, що у своїх відповідях цей фінансовий фахівець, насамперед використовував свій досвід роботи в компанії "НеоСервіс". В усякому разі, в попередніх відповідях вона прямо посилалася на досвід роботи свого відділу, вживаючи в пропозиціях фрази: "наша компанія робить це так…" або "за моїм досвідом…". Люди, як правило, підсвідомо схильні приховувати інформацію, що стосується прямо їхньої діяльності, якщо не впевнені в тому, як вона буде використана, але водночас легко її видають, якщо не відчувають загрози.

Все це виявилося вельми доречним для фірми "СофтСервіс", директор якої півтора роки намагався дізнатися про те, як конкретно його конкурент реалізує фінансові схеми, що обговорювалися на форумі, маючи більші прибутки при значно меншому попиті на комп'ютерне обладнання. Методика, про яку люб'язно розповіла на форумі пані з ніком yuliya_pari, з одного боку, відкривала доступ до деяких фінансових махінацій, а з іншого – вимагала реалізації заходів, проведення яких ставило б під загрозу фінансову стабільність компанії.

Інформація, виявлена фахівцями з аудиту, сама по собі ще не давала фірмі "СофтСервіс" можливості почати роботу з новими партнерами за новою схемою і т.д. Проте вона заповнювала прогалини в досвіді роботи директора цієї фірми щодо проведення фінансових операцій, а також давала шанс згодом анонімно уточнити відповіді на різні додаткові запитання. Аудитори змогли також з'ясувати ім'я фінансового директора компанії-конкурента –

Юлія Пархоменко. Гіпотезу про те, що йдеться саме про цю персону, висунув один з аудиторів, який подзвонив у компанію "НеоСервіс" за номером контактного телефону. Дзвінок потрапив у відділ маркетингу і був переадресований секретареві генерального директора. Фахівець з аудиту пояснив, що хоче звернутися до фінансового директора з листом-замовленням на придбання партії комп'ютерного обладнання і уточнює його прізвище та ініціали. Інформація про те, що фінансовий директор компанії "НеоСервіс", Юлія Пархоменко та yuliya_parі – одна і та ж особа, отримала остаточне підтвердження.

5. Поради та рекомендації. Істотні зміни в засобах комунікації не тільки полегшили спілкування людей між собою, незважаючи на чималу відстань і відсутність особистого знайомства між людьми. Вони створили нові можливості для отримання конфіденційної інформації через достатньо очевидні прогалини в системі захисту корпоративних мереж та ІБ самих установ [4]. Звичайно, це не заклик обмежити спілкування, проте слід прийняти ряд заходів для того, аби, зберігши плюси такого спілкування, позбавитися від очевидних мінусів:

- заборонити співробітникам у особистих інтересах використовувати адресу електронної пошти на корпоративному домені;
- рекомендувати співробітникам застосовувати в корпоративних іменах нейтральні ніки, які ускладнюють ідентифікацію користувача, який вирішив публікуватися на інших інформаційних ресурсах;
- проводити із співробітниками роз'яснювальну роботу про важливість дотримання правил ІБ;
- регулярно проводити моніторинг корпоративної мережі для своєчасного виявлення порушень працівниками встановлених правил її використання.

Одного дня складений запит, який дає високий релевантний результат, можна використовувати багато разів для автоматичного моніторингу інформації, наявної в мережі Інтернет із заданої проблеми. Наприклад, найбільш цінною для фірми "СофтСервіс" була інформація про реалізацію фінансових схем і посадові особи компанії-конкурента, а також пов'язані з ними події: інтерв'ю, участь в інформаційних оглядах, рекламі і т.п. Такий моніторинг може проводитися за допомогою програм Check&Get або WebSite Watcher, які дають змогу автоматично повторювати пошук через вказані проміжки часу, які не тільки сигналізуватимуть про те, на яких сайтах сталися зміни, але відзначають час і дату цих змін [3]. Це дає змогу вчасно отримувати ту чи іншу інформацію, піддавати її ретельному аналізу, синтезувати нові знання і приймати відповідні рішення.

Перефразовуючи один з відомих афоризмів, зазначимо – хто володіє достовірною інформацією, той володіє реальною ситуацією, що склалася. А це на сьогодні не маловажно в бізнесовій діяльності товаровиробників і наданні послуг.

Література

1. Бармута Андрей. Утечка информации в корпоративной сети: угроза виртуальная, защита реальная / Андрей Бармута. [Электронный ресурс]. – Доступный с http://www.itsec.ru/articles2/in-ch-sec/ytechka-informacii-v-korporativnoi-seti-ygroza-virtyalnaya-zashita-realnaya

2. Защита информации от внутренних угроз. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/informationnaya_bezopasnost.php

3. Защита от инсайдеров и утечки информации // ISO27000.RU Искусство управления информационной безопасностью. [Электронный ресурс]. – Доступный с http://www.iso27000.ru/chitalnyi-zai/zaschita-ot-insaiderov

4. Использование программ для слежения за компьютерами в локальной сети с целью снижения внутренних угроз корпоративной безопасности. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/internal-threat.php

5. История нашего клиента: как я поймал инсайдера. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/insider.php

6. Корпоративная информационная безопасность: виды IT-угроз. [Электронный ресурс]. – Доступный с http://www.razumny.ru/stat/it-ugrozy.html

7. Корпоративная культура. [Электронный ресурс]. – Доступный с http://www.b-seminar.ru/article/show/469.htm

8. Надо ли следить за персоналом?. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/monitiring-personal.php

9. Перехват сообщений и скрытое наблюдение за сотрудниками. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/perehvat_soobshniy_skrytoe_nablyudenie.php

10. Статьи о Staffcop. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/

11. Утечка информации – угроза корпоративной безопасности. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/Information_leakage.php

12. Учет рабочего времени сотрудников и контроль персонала – важная составляющая эффективной организации. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/personnelcontrol.php

13. Ющук Евгений. Брешь в конфиденциальности (Практика использования сети Интернет в конкурентной разведке) / Евгений Ющук. [Электронный ресурс]. – Доступный с http://citcity.ru/17017/

14. Skype – программа для голосового общения или отличный троян?. [Электронный ресурс]. – Доступный с http://hackzona.ru/hz.php?name=News&file=article&sid =6680.

15. 50 million concurrent users online! // Skype Numerology. [Electronic resource]. – Mode of access http://skypenumerology.blogspot.com/2013/01/50-million-concurrent-users-online.html

Чудинова Н.В., Грыцюк Ю.И. **Особенности использования сети Интернет для получения конфиденциальной информации**

Стремление людей к общению, особенно в социальных сетях, заложено в самой природе человека. С появлением сети Интернет люди не поменяли своих привычек, продолжая решать личные проблемы, используя при этом корпоративные средства связи. Поскольку использование почтового ящика в собственных нуждах не создает видимых финансовых затрат, то во многих учреждениях такое положение вещей вообще не считают проблемой, поэтому просто его временно игнорируют, поскольку уделяют внимание решению других неотложных проблем. Однако польза подобного явления на проверку информационной безопасности многих учреждений выяснилась ошибочной, то есть не всегда это обходится без последствий для фирм или государства вообще.

Ключевые слова: информационные угрозы, информационная безопасность, конфиденциальная информация, источники угроз, промышленная компания.

Chudinova N.V., Grycyuk Yu.I. **Features of the Internet for the exchange of confidential information**

The desire of people to communicate, especially in social networks, inherent in human nature. With the advent of the Internet people have not changed their habits, continuing to solve personal problems, using corporate communications. As the use of a mailbox in their own needs no perception of financial costs, many institutions such a situation do not consider a problem, so just ignore it temporarily, because paying attention to address other pressing issues. However, the benefits of this phenomenon to test information security of many institutions became clear mistake, that is not always without their impacts for the companies or the state in general.

Keywords: information threats, information security, confidential information, industrial company.