УДК 004.056:159.95
Нікіфорова Л.О.
Вінницький національний технічний університет

МЕТОД РОЗРАХУНКУ РІВНЯ ВМОТИВОВАНОСТІ СПІВРОБІТНИКІВ ЩОДО ЗБЕРЕЖЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ В ЗАДАЧАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В статті у розрізі задач інформаційної безпеки розроблено метод розрахунку рівня вмотивованості співробітників підприємства на основі модифікації соціометричних показників шляхом додаткового врахування кількісних показників із Internet та соціальних мереж. Даний метод дає можливість не лише кількісно оцінити рівень вмотивованості співробітників щодо збереження конфіденційності інформації, але й попередити виникнення можливих вразливостей та загроз зі сторони персоналу щодо забезпечення інформаційної безпеки на підприємстві.
Ключові слова: менеджмент, інформаційна безпека, мотивація, конфіденційна інформація, захист інформації, метод, модель.

Вступ. Основним елементом сучасних стандартів серії ISO/IEC 27000-27037 Information technology – Security techniques є система менеджменту (управління) інформаційної безпеки (СМІБ) підприємства. Підкреслюється, що до забезпечення інформаційної безпеки підприємства повинні залучатися всі співробітники.

Для ефективності діяльності СМІБ на підприємстві повинна бути створена потужна система мотивації діяльності співробітників у цьому напрямку. Про необхідність цього свідчить, наприклад, та обставина, що на сайті організації Вікілікс виставлено декілька мільйонів *конфіденційних* документів [1], причому деякі із них відносяться до рівня державної таємниці.

Це свідчить про те, що сотні тисяч людей, які *були попереджені* про необхідність збереження конфіденційності чи державної таємниці, *свідомо* порушили свої зобов'язання перед підприємством чи державою. Для цього потрібен досить високий *рівень* їх мотивації. Таким чином, виникає необхідність наукового дослідження проблеми виявлення рівня вмотивованості співробітників до збереження конфіденційності та виконання вимог СМІБ. Ця задача має не тільки наукову актуальність, але й високий рівень практичної значимості.

Аналіз останніх досліджень і публікацій. В [2-4] описано загальні методи для мотивації співробітників підприємства. В [2] основна увага зосереджена на методах, які використовуються в управлінні персоналом підприємства, але детально специфічні аспекти використання методів управління мотивацією в задачах інформаційної безпеки не розглядаються. В [3] детально описані методи мотивації співробітників підприємства, які є перспективними для використання в рамках СМІБ, але самі методи використання мотивації не розглянуто. В [4] подано постановку загальної задачі про роль мотивації в забезпечення інформаційної безпеки підприємства, але методи для цього детально не описано.

В [5] подано основні існуючі сьогодні моделі захисту інформації. В цих моделях вимоги до суб'єктів інформаційного захисту – а саме ними є співробітники підприємства – подано у вигляді певних *вимог* до їх поведінки. Наголошується, що тільки за виконанням цих вимог, які зводяться до того, що співробітник повинен *строго* виконувати задані правила, модель здатна гарантувати захист інформації. Проте, як свідчить наявність сайту Вікілікс [1], реальна ситуація свідчить про *масові* порушення умов існуючих моделей захисту інформації.

Для можливості використання в моделях захисту інформації, показники та характеристики мотивації повинні мати *кількісний* вираз. Сьогодні існує дуже мала кількість таких психолого-соціологічних показників, які можна виміряти кількісно.

Найбільш поширеними є так звані соціометричні показники, запропоновані в кінці 1950-х років [6,7]. Дослідження підприємств, здійснені за допомогою цих методів,

засвідчили їх придатність до використання в якості кількісного виміру рівня вмотивованості співробітників підприємств в умовах України [7].

Метою статті є розробка методу розрахунку рівня вмотивованості співробітників підприємства на основі модифікації соціометричних показників шляхом додаткового врахування кількісних показників із Intranet та соціальних мереж для використання в задачах інформаційної безпеки.

Модифікація методу розрахунку соціометричних показників. Традиційно в соціометриці для кожного співробітника визначають, як саме вибраний i-тий співробітник відноситься до інших співробітників: позитивне відношення позначається як $R^{+}_{i\to j}(=1)$, негативне як $R^{-}_{i\to j}(=1)$, а нейтральне – як $R^{0}_{i\to j}(=0)$ [7].

Ці характеристики відношень дозволяють ввести два типи показників. Перший тип визначає, кількість тих співробітників, до яких заданий i-тий співробітник відноситься позитивно. Він розраховується за такою формулою.

$$P_{i\to} = \frac{1}{N-1}\sum_{j=1,\, j\neq i}^{N-1} R^{+}_{i\to j} \tag{1}$$

де N – загальна кількість співробітників.

До першого типу показників слід віднести також той, який визначає кількість тих співробітників, до яких i-тий співробітник відноситься негативно. Аналогічно (1), він розраховується за такою формулою.

$$M_{i\to} = \frac{1}{N-1}\sum_{j=1,\, j\neq i}^{N-1} R^{-}_{i\to j} \tag{2}$$

До другого типу показників відносяться ті показники, які визначають, скільки співробітників відносяться до i-того співробітника позитивно $(P_{i\leftarrow})$ та негативно $(M_{i\leftarrow})$. Вони задаються такими формулами.

$$P_{i\leftarrow} = \frac{1}{N-1}\sum_{j=1,\, j\neq i}^{N-1} R^{+}_{j\to i} \tag{3}$$

$$M_{i\leftarrow} = \frac{1}{N-1}\sum_{j=1,\, j\neq i}^{N-1} R^{-}_{j\to i} \tag{4}$$

Показники (1)-(4) приймають значення на відрізку $[0,1]$. Також, слід відмітити, що показники (1)-(4) були розроблені і активно використовувалися ще тоді, коли комунікації між людьми могли здійснюватися лише при особистому контакті. Сьогодні ж значно зросла кількість каналів для здійснення таких комунікацій: їх можна здійснювати через внутрішню мережу підприємства Intranet, а також через велику кількість різних соціальних мереж (Facebook, Твіттер, Інстаграм, Вконтакте, Одноклассники, Livejournal, професійні соціальні мережі тощо). Більш того: в соціальних мережах часто є можливість відслідковувати позитивне чи негативне відношення як до певного мессаджа, так і до певної особи (наприклад, так звані «лайки»). В деяких соціальних мережах навіть можна встановити особу, яка виразила своє відношення.

Враховуючи вищесказане, формули (1)-(4) можуть бути узагальнені для урахування різних каналів здійснення комунікацій між співробітниками таким чином.

$${}_{k}P_{i\to} = \frac{1}{N_k-1}\sum_{j=1,\, j\neq i}^{N-1} {}_{k}R^{+}_{i\to j} \tag{5}$$

$${}_{k}M_{i\to} = \frac{1}{N_k-1}\sum_{j=1,\, j\neq i}^{N-1} {}_{k}R^{-}_{i\to j} \tag{6}$$

$$ {}_kP_{i\leftarrow} = \frac{1}{N_k - 1} \sum_{j=1,\, j\neq i}^{N-1} {}_kR^{+}_{j\rightarrow i} \tag{7} $$

$$ {}_kM_{i\leftarrow} = \frac{1}{N_k - 1} \sum_{j=1,\, j\neq i}^{N-1} {}_kR^{-}_{j\rightarrow i} \tag{8} $$

Через N_k позначена кількість співробітників, які *зареєстровані* в k-тій соціальній мережу. В формулах (5)-(8) всі величини ${}_kR$ є загальною кількістю визначених відношень між i-тим та j-тим співробітниками, відповідно до сенсу показника (який визначається верхніми та нижніми індексами, які подано після показника). Індекс «k» нумерує номер каналу комунікації. Загальна кількість каналів для i-го співробітника позначається як K_i.

Показники (5)-(8) є більш інформативними, аніж широко використовувані показники (1)-(4). При визначення стандартних соціометричних індексів (1)-(4) здійснюється пряме анкетування співробітників підприємства. При цьому співробітники *зобов'язані* давати відповідь. Але вони можуть бути не певні в тому, що збережеться конфіденційність їх відповідей, – а справа йде про їх відношення до інших співробітників, і навіть – до їх керівників. Тому існує висока ймовірність того, що будуть отримані недостовірні первинні дані.

Навпаки, у мережі Intranet співробітники спілкуються в межах здійснення спільної діяльності, за своїм бажанням висловлюючи підтримку, не підтримку чи ігнорування *ділових* пропозицій інших співробітників. Вони самостійно висловлюють своє ставлення до інших співробітників.

Аналогічно в соціальних мережах співробітники також самі приймають рішення про підтримку чи не підтримку повідомлення (фотографії, відео сюжету тощо) інших співробітників. Також вони вільно приймають рішення щодо своєї участі в дискусіях, які започатковуються іншим співробітником підприємства. Вони також приймають рішення щодо того, щоб *відслідковувати* публікації в соціальних мережах інших співробітників («підписки»), - причому як таких, до яких у них є позитивне відношення, так і до тих, до яких вони відносяться негативно («щоб покритикувати»).

Веб-ресурси сучасних соціальних мереж дозволяють фіксувати описану вище інформацію, що дозволяє отримати досить швидко достатньо великі та представницькі бази даних. Це суттєво підвищує статистичну надійність результатів. До того ж, постійне спілкування співробітників в соціальних мережах дозволяє здійснювати моніторинг ситуації, досить швидко фіксуючи зміни.

Таким чином, використання модифікованих показників (5)-(8) дозволяє підвищити надійність та достовірність отриманих даних у порівнянні із стандартними соціометричними показниками, за рахунок наявності власної мотивації співробітників до висловлювання їх відношень до інших співробітників підприємства та за рахунок відсутності психологічного тиску на ці висловлювання. Це дозволяє підвищити об'єктивність отриманих результатів.

Метод врахування величини рівня вмотивованості співробітників в задачах інформаційної безпеки. Використання величини рівня вмотивованості співробітників в задачах інформаційної безпеки розпадається на два етапи.

Під час першого етапу здійснюється вимірювання показників, які характеризують вмотивованість співробітників. В нашому випадку – це формування такого кортежу.

$$ M = \langle R_s, R_{sn} \rangle \tag{9} $$

де R_s – множина стандартних соціометричних показників, яка розраховується за формулами (1)-(4);

R_{sn} – множина узагальнених показників, які вимірюються в соціальних мережах та розраховуються за формулами (5)-(8).

В кортежі (9) враховуються всі показники кожного із співробітників в контексті інформаційної безпеки.

Для використання кортежу (9) з метою захисту інформації, необхідно привести показники кортежу R_{sn} до такого вигляду, який було б зручно використовувати в розрахунках. Це необхідно зробити внаслідок того, що числові значення показників кортежу R_s належать до відрізку $[0,1]$, тоді як показники кортежу R_{sn} належать до відрізку $[0,\infty]$.

Розглянемо для кожного із каналів кількість позитивних/негативних висловлювань i-го співробітника $N_{k,i\rightarrow}^{+/-}$ та висловлювань інших працівників про нього $N_{k,i\leftarrow}^{+/-}$. Введемо максимальні значення для висловлювань за такими формулами.

$$N_{k,i\rightarrow}^{+/-} = \max_{i,j} N_{k,i\rightarrow}^{+/-} \tag{10}$$

$$N_{k,i\leftarrow}^{+/-} = \max_{i,j} N_{k,i\leftarrow}^{+/-} \tag{11}$$

Тоді узагальнені показники (5)-(8) приводяться для кожного каналу до інтервалу $[0,1]$ шляхом ділення на числа (10) та (11), відповідно.

В результаті кортеж (9) буде мати такий вигляд.

$$M^{\text{mod}} = \langle R_s, R_{sn}^{\text{mod}} \rangle \tag{12}$$

Другий етап полягає у використанні кортежу (12) для задач інформаційної безпеки. В загальному випадку цей кортеж можна використати для того, щоб визначити співробітників, які відносяться до так званої «групи ризику», - тобто тих, які є найменш мотивованими для збереження конфіденційності інформації.

Для цього розглянемо таке *припущення*: до групи ризику можна віднести співробітників, для яких виконується хоча б одне із таких тверджень:

1) їх агрегований показник позитивних відносин до інших співробітників (агрегований коефіцієнт позитивної мотивації або позитивної емоційної експансивності), розрахований за кортежем (12), є меншим за певну, знайдену із проведеного експерименту, величину (загальну методику проведення якого наведено в [7]);

2) їх агрегований показник негативних відносин до інших співробітників (агрегований коефіцієнт негативної мотивації або негативної емоційної експансивності), розрахований за кортежем (12), є більшим за певну, знайдену із експерименту, величину [7];

3) їх агрегований показник нейтральних відносин до інших співробітників (агрегований коефіцієнт нейтральної мотивації), розрахований за кортежем (12), є більшим за певну, знайдену із експерименту, величину [7];

4) агрегований показник позитивних відносин до них в боку інших співробітників (агрегований коефіцієнт позитивного сприйняття колективом або позитивного соціометричного статусу), розрахований за кортежем (12), є меншим за певну, знайдену із проведеного експерименту, величину (загальну методику проведення якого наведено в [7]);

5) агрегований показник негативних відносин до них з боку інших співробітників (агрегований коефіцієнт негативного сприйняття колективом або негативного соціометричного статусу), розрахований за кортежем (12), є більшим за певну, знайдену із експерименту, величину;

6) агрегований показник нейтральних відносин до них з боку інших співробітників (агрегований коефіцієнт нейтрального сприйняття колективом), розрахований за кортежем (12), є більшим за певну, знайдену із експерименту, величину.

Моделі агрегації показників кортежу (12). Вибір моделі для агрегації показників кортежу визначається, в загальному випадку, вимогами задачі із захисту інформації. Наведемо декілька прикладів можливих моделей агрегації.

Модель 1. Для її використання на підприємстві повинна бути визначена людина, до якої більшість співробітників відноситься позитивно. Назвемо її «позитивний лідер», а її показники визначимо за зразок для конкретної групи співробітників.

У цьому випадку для кожного i-го співробітника заданої групи знаходимо коефіцієнт автокореляції між його показниками та показниками позитивного лідера із кортежу (12). При відсутності співробітника у соціальній мережі відповідний коефіцієнт вважається рівним нулю. Так як показники обох співробітників додатні, то коефіцієнт автокореляції належить до відрізку $[0,1]$.

Можна запропонувати таку класифікацію співробітників за рівнем їх належності до «групи ризику»:

1) якщо $K_{li} > 0,7$, то співробітник не належить до групи ризику;

2) якщо $0,4 < K_{li} < 0,7$, то у співробітника мала мотивація до порушення конфіденційності інформації (але вона збільшується із зменшенням величини K_{li});

3) якщо $K_{li} < 0,4$, то у співробітника високий рівень мотивації до порушення конфіденційності інформації (і він збільшується із зменшенням величини K_{li}).

Модель 2. Спочатку визначаємо в кортежі (12) ті соціальні мережі, в яких зареєстровані *усі* співробітників під ніками, що ідентифікуються (для прикладу мережа «Однокласники»).

Потім для кожного із співробітників розраховуємо суму всіх позитивних і негативних показників, які залишені лише членами його колективу. У цьому випадку агрегування перетворюється в просте додавання.

Впорядковуємо працівників по зменшенню значення агрегованого показника.

До групи ризику віднесемо співробітників, які належать до найменшого децилю.

Модель 3. Врахуємо те, що різні співробітники можуть приймати участь у різній кількості соціальних мереж.

У цьому випадку суму показників для i-го співробітника ділимо на кількість соціальних мереж K_i, у яких він приймає участь.

Впорядковуємо працівників по зменшенню значення агрегованого показника.

До групи ризику віднесемо співробітників, які належать до найменшого децилю.

Зауваження до моделей. Границі можуть встановлюватися, виходячи із даних спеціально проведених експериментів.

Порівняння із існуючими методами. Існуючі сьогодні методи визначення груп ризику мають своє походження або із психології, або із менеджменту, або із соціології [2-4]. Порівняння розробленого в статті методу із існуючими наведено в табл. 1.

Таблиця 1.

Порівняння існуючих та розробленого в статті методу.

№ п/п		Психологічні	Соціологічні	Менеджменту	Розроблені в статті
	Характеристики методу				
1	Вимагають виключно прямого опитування	+	+	+	–
2	Можуть здійснюватися таємно від співробітника	–	–	–	+
3	Залучають соціальні мережі	–	–	–	+
4	Допускають різні моделі агрегації	–	–	–	+
5	Дозволяють здійснювати моніторинг	–	–	–	+

В мережі Internet сьогодні існує ряд веб-сайтів [8,9], на яких розташовані програмні продукти. Проте вони дозволяють тільки здійснити анкетування працівників, автоматично розрахувати стандартні соціометричні показники та представити результати у стандартному соціометричному вигляді [6].

Висновки. Як було зауважено, сьогодні ж значно зросла кількість каналів для здійснення таких комунікацій: їх можна здійснювати через внутрішню мережу підприємства Intranet, а також через велику кількість різних соціальних мереж (Facebook, Твіттер, Інстаграм, Вконтакте, Одноклассники, Livejournal, професійні соціальні мережі тощо). Більш того: в соціальних мережах часто є можливість відслідковувати позитивне чи негативне відношення як до певного мессаджа, так і до певної особи, а в деяких соціальних мережах навіть можна встановити особу, яка виразила своє відношення. Також перевагою використання таких мереж для визначення рівня вмотивованості співробітників є те, що вони існує висока вірогідність того, що збережеться конфіденційність їх відповідей, на відміну від класичних соціометричних показників, які ґрунтуються на чіткій ідентифікації особистості і вагомим своїм недоліком мають високу ймовірність недостовірної первинної інформації. Саме тому в основу розробленого методу були покладені модифіковані показники (5)-(8), які враховують існуючи недоліки класичних підходів до досліджуваної проблеми і орієнтовані на сучасні інформаційні технології. Також, виходячи із припущень щодо кортежу (12) було запропоновано три моделі агрегації даного показника, з плаваючими границями, конкретні кількісні значення яких, за необхідності, можуть бути встановлені виходячи із даних спеціально проведених експериментів.

Отже, таким чином розроблений метод дає можливість в розрізі задач інформаційної безпеки на основі модифікації соціометричних показників шляхом додаткового врахування кількісних показників із Intranet та соціальних мереж не лише кількісно оцінити рівень вмотивованості співробітників щодо збереження конфіденційності інформації, але й попередити виникнення можливих вразливостей та загроз зі сторони персоналу щодо забезпечення інформаційної безпеки на підприємстві.

Література

1. Вікілікс. Режим доступу в Інтернет: https://wikileaks.org/.
2. Ожиганова М. І. Управління персоналом / М. І. Ожиганова, В. О. Хорошко, Ю. Є. Яремчук, В. В. Карпінець. – Вінниця : ВНТУ, 2014. – 188 с.
3. Андреєв В. І. Стратегія управління інформаційною безпекою / В. І. Андреєв, В. Д. Козюра, Л. М. Скачек, В. О. Хорошко. – К. : ДУІКТ, 2007. – 277 с.
4. Андреєв В.І. Основи інформаційної безпеки / В. І. Андреєв, В. О. Хорошко, В. С. Чередниченко, М. Є. Шелест. – К. : Вид. ДУІКТ, 2009. – 292 с.
5. Богуш В. М., Довидьков О. А., Кривуца В. Г. Теоретичні основи захищених інформаційних технологій / В. М. Богуш, О. А. Довидьков, В. Г. Кривуца. – К. : ДУІКТ, 2010. – 454 с.
6. Морено Я. Л. Социометрия: Экспериментальный метод и наука об обществе / Я. Л. Морено. – М. : Академический Проект, 2001. – 384 с.
7. Мороз О. В. Соціально-психологічні чинники мотивування працівників приладобудівних підприємств / О. В. Мороз, Л. О. Нікіфорова, А. А. Шиян. – Вінниця : ВНТУ, 2011. – 252 с.
8. Комп'ютерна програма координатно-соціаграмного аналізу колективу Соціометрія. Режим доступу в Інтернет: http://www.ait.org.ua/socuometriya/.
9. Компьютерная программа для автоматизации расчета данных социометрии SociometryPro. Режим доступу в Інтернет: http://www.ledisgroup.com/ru/sociometryproru.

Рецензент: проф., д.т.н. Корченко О.Г. Надійшла 03.09.2014