УДК 004.056:159.95 **Л.О. Нікіфорова**

УЗАГАЛЬНЕНА МОДЕЛЬ ОЦІНКИ РІВНЯ ВМОТИВОВАНОСТІ АГЕНТІВ ЗАГРОЗ В ЗАДАЧАХ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ НА МІКРО ТА МАКРОРІВНЯХ

В статті розроблено модель, яка дає змогу охопити функціональні області найбільш розповсюджених вразливостей забезпечення безпеки об'єкта на макро і мікрорівнях при недостатньому рівні вмотивованості агента загрози. Також в статті розроблено метод, що дозволяє не лише оцінити рівня вмотивованості агентів загрозщодо збереження безпеки об'єкта на різних рівнях, але й попередити виникнення можливих вразливостей та загроз.

Ключові слова: агент, загроза, вразливість, безпека, мотивація, захист, інформація, метод, модель, рівень.

Вступ

Найбільш вразливою ланкою в системі безпеки будь-яких об'єктів, насамперед, є люди, їхні слабкості [1]. Гарним прикладом є Германія часів Другої світової війни, коли оператори машини Enigma, для полегшення своєї роботи, використовували стандартні скорочення, що дало можливість дешифровки закодованої інформації. Тобто шифрувальники були недостатньо вмотивовані виконувати трудомістку працю з найвищим рівнем захисту і ця виникла вразливість відкрила шлях для створення загрози витоку інформації, що і сталося в реальності. Тому задача виявлення потенційних вразливостей та загроз через недостатній рівень вмотивованості людей є задачею, яка має не тільки наукову актуальність, але й високий рівень практичної значимості.

Аналіз останніх досліджень і публікацій

В [2-5] описано загальні методи для мотивації працівників підприємства. В [2] основна увага зосереджена на методах, які використовуються в управлінні персоналом підприємства, але детально різнорівневі фактори, які впливають на рівень вмотивованості працівників в задачах забезпечення безпеки підприємств чи структур не розглядаються. В [3, 5] описані загальні методи та моделі мотивації працівників підприємства, які є перспективними для використання в рамках системи менеджменту інформаційної безпеки, але самі методи оцінки вмотивованості працівників не розглянуто. В [4] подано постановку загальної задачі про роль мотивації в забезпечення інформаційної безпеки підприємства, але методи для цього детально не описано. В джерелі [8] розроблено загальну модель для вибору оптимального методу протидії загрозам інформаційної безпеки, але окремо вплив мотивації на ці загрози не розглянуло.

Метою статті є розробка моделі, яка дає змогу охопити функціональні області найбільш розповсюджених вразливостей забезпечення безпеки об'єкта на макро і мікрорівнях при недостатньому рівні вмотивованості агента загрози (РВА) та, на її основі, розробка методу, який дозволяє оцінити цей рівень.

Викладення основного матеріалу

Традиційно вразливістю вважається потенційний шлях для здійснення будь-яких загроз щодо порушення безпеки об'єкта [6]. Найчастіше вразливості пов'язують лише з комп'ютерними системами та мережами [7], що є не зовсім вірним, адже найчастіше найбільшою загрозою для безпеки об'єкта, яка з'являється при виникненні вразливості, є людина [1].

Як правило, загрозою вважається дія або подія, яка в змозі порушити безпеку будь-якої системи. Основними складовими загроз є [7];

1. Цілі – компоненти безпеки, які підлягають атаці.
2. Агенти – люди або організації, які можуть створювати загрозу.
3. Подія – дії, які створюють загрозу.

Розглянемо більш розлого такий компонент загрози безпеки об'єкта, як агенти. Агентами загроз є люди, які свідомо або підсвідомо можуть чи намагаються нанести збиток організації чи структурі. Для цього вони повинні мати наступне [6]:

- Доступ.
- Знання.
- Мотивацію.

Як бачимо, первинним компонентом виникнення загроз є мотивація агента для здійснення певних дій. Мотивація є спонукаючою дією, її можна визначити як первісну ціль. В даному випадку мотивацію для досягнення загрози безпеки об'єкта слід розглядати як деструктивний фактор для підприємства чи іншої структури, чия безпека потенційно може бути порушена. Як правило, деструктивною мотивацією є незадоволеність потреб агента щодо його матеріальних або моральних цінностей, тобто можна сказати, що основною причиною виникнення агента загрози є недостатній рівень вмотивованості такого працівника щодо збереження своєї посади і тих благ, які вона несе, а отже і не має достатнього рівня мотивації щодо збереження безпеки підприємства на якому такий агент прац.

Відобразимо у вигляді функції рівень вмотивованості агентів загроз (*РВА*):

$$РВА = f(ІП; НРП; СПР; КІС; ОБП; ВП; СФ), \quad (1.1)$$

де *ІП* – імідж посади;
НРП – наявність ресурсів, що знаходяться у підпорядкуванні;
СПР – рівень самостійності в прийнятті рішень;
КІС – рівень комунікативної діяльності в різних ієрархічних структурах управління;
ОБП – офіційні бонуси посади;
ВП – винагорода за працю;
СФ – специфічні об'єктивні фактори для різних країн.

На кожен вище визначений фактор першого порядку, який впливає на рівень вмотивованості агента та задоволення своєю посадою, в свою чергу, діють фактори другого та третього порядку. Узагальнена модель управління мотивацією агента відображено на рис.1.

На рис. 1 пунктиром зображено функціональну область в межах якої діють фактори другого та третього порядків. Так як модель є узагальненою, то на ній не відображено функціональні зв'язки між факторами першого порядку, так як вони є достатньо складними і потребують окремих досліджень. Наприклад, відкликання права носіння на зброю охороні агента не лише прямо вплине на імідж його посади, але й спричинить опосередкований вплив на неформальний ієрархічний рівень агента у внутрішній структурі управління підприємством чи організацією, що є прямим шляхом для створення загрози безпеки через виникнення вразливості [7], яка з'явилась через незадоволення агента даним рішенням і бажанням змінити ситуацію.

Розглянемо більш детально функціональні області, в межах яких діють фактори першого порядку.

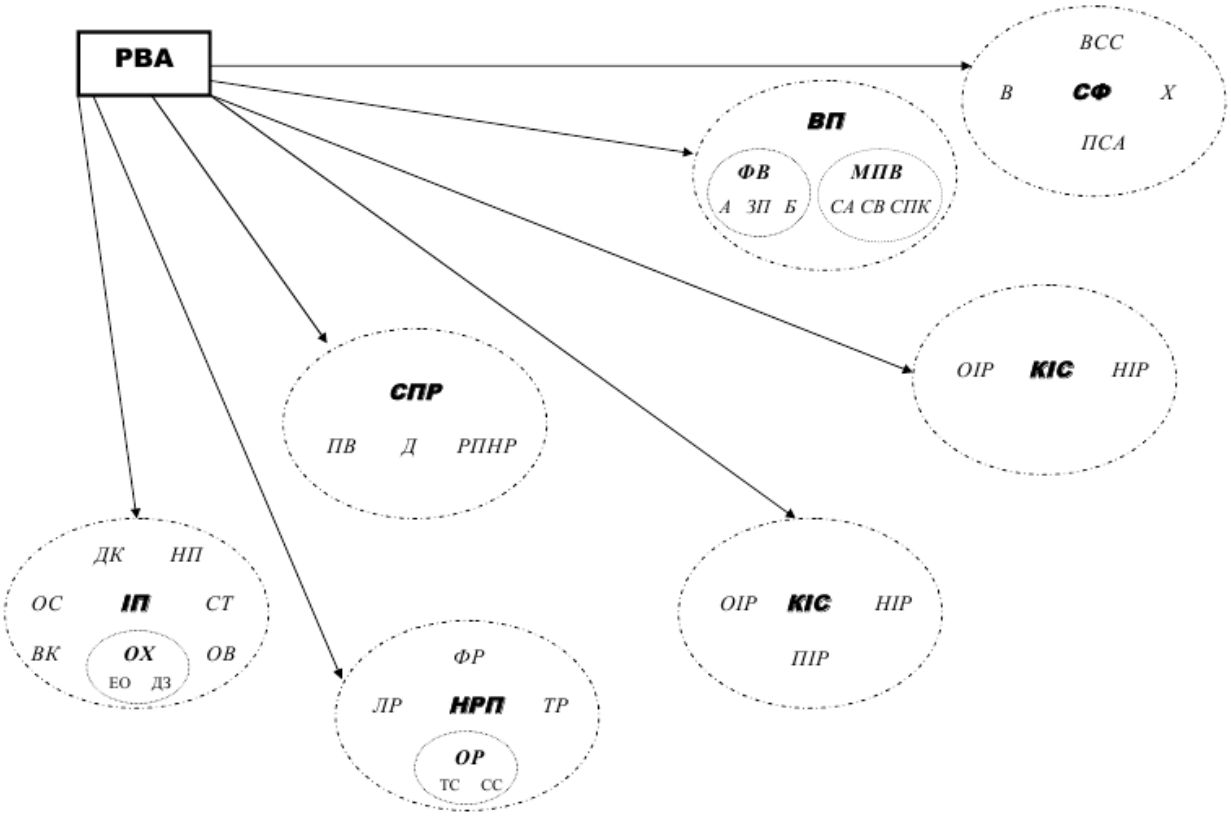

Рис. 1. Узагальнена модель управління мотивацією агента загрози

1. Будь-який агент на підприємстві чи в організації займає певну посаду, імідж якої залежить від багатьох факторів, а отже є відкритим для багатьох вразливостей, які виникають при цьому. В формулі (2) описано найбільш поширені вразливості, які можуть призвести до виникнення загрози загальної безпеки об'єкта (на мікрорівні – підприємства, організації, фірми і т. п., на макрорівні – області, регіону, країни тощо) шляхом виникнення демотивації агента.

$$ІП = f\ (ОС;\ ВК;\ ДК;\ НП;\ ОХ;\ СТ;\ ОВ), \qquad (2)$$

де *ОС* – особистий секретар (помічник);
ВК – власний кабінет;
ДК – дизайн кабінету;
НП – назва посади;
СТ – марка службово транспорту;
ОВ – особистий водій;
ОХ – особиста охорона, яка, в свою чергу, залежить від таких факторів третього порядку:

$$ОХ = f\ (ЕО;\ ДЗ), \qquad (3)$$

де *ЕО* – ескорт для охорони;
ДЗ – дозвіл на носіння та користування вогнепальної зброї.

2. Формула (4) описує найбільш поширені вразливості різних рівнів, які можуть виникнути через доступ агента до ресурсів, на які знаходяться у його безпосередньому підпорядкуванні.

$$НРП = f\ (ОР;\ ЛР;\ ФР;\ ТР), \qquad (4)$$

де *ЛР* – людські ресурси;

ФР – фінансові ресурси;

ТР – технічні ресурси;

ОР – організаційні ресурси, у кількісному вираженні, які, в свою чергу, залежить від таких факторів третього порядку:

$$ОР = f\ (ТС\ ;\ СС), \tag{5}$$

де *ТС* – типові структури: бухгалтерія, кадри, різні відділи і т.д.

СС – спеціалізовані структури: аналітики, референти, іміджмейкери, секретаріат, перекладачі тощо.

3. Рівень самостійності в прийнятті рішень є фактором, який найбільш чинить вплив на *РВА* саме на макрорівні, наприклад, якщо агент займає посаду депутата чи міністра країни. Для даного фактору достатньо важко виділити об'єктивні показники другого рівня, які теоретично мають найбільший вплив на цей показник. В формулі (6) подано основні з них:

$$СПР = f\ (ПВ;\ Д;\ РПНР), \tag{6}$$

де *ПВ* – можливість підвищення кваліфікації, інтерактивне навчання;

Д – можливість отримання досвіду (тренінги, відрядження, стимулятори, використання СППР тощо);

РПНР – ризик прийняття невірного рішення (розраховується на основі попередньо прийнятих рішень).

Для *СПР* фактори другого порядку є найбільш тісно взаємопов'язаними та послідовними, такими, що не є взаємо компенсованими. Якщо агент не має можливості постійно підвищувати свою кваліфікацію, не має нових сучасних знань, то він автоматично не має можливості набуття досвіду, що призводить до збільшення ризику прийняття невірного рішення, що, в свою чергу, призводить до зниження рівня самостійності в прийнятті рішень і до де мотивації агента.

4. Будь-який агент на підприємстві чи в організації комунікує з іншими агентами і займає певний ієрархічний рівень у структурі управління, який залежить від багатьох факторів, а отже є відкритим для вразливостей, які виникають при цьому. В формулі (7) описано найбільш поширені з них:

$$КІС = f\ (ОІР;\ НІР;\ ПІР), \tag{7}$$

де *ОІР* – офіційний ієрархічний рівень агента у внутрішній структурі управління об'єктом (підприємством, організацією, регіоном, країною тощо);

НІР – неформальний ієрархічний рівень агента у внутрішній структурі управління об'єктом;

ПІР – персональний ієрархічний рівень агента у зовнішній комунікативній системі «об'єкт-партнери».

5. Ще одним фактором, який чинить вплив на *РВА* саме є офіційні бонуси посади агента:

$$ОБП = f\ (ЛІА;\ ПОБ), \tag{8}$$

де *ЛІА* – лобіювання інтересів інших внутрішніх чи зовнішніх агентів;

ПОБ – перспективи отримання офіційних благ після залишення даної посади.

6. Формула (9) описує найбільш поширені вразливості різних рівнів, які можуть виникнути через незадоволення агентом винагородою за свою працю:

$$ВП = f\ (ФВ;\ МПВ),\qquad (9)$$

де *ФВ* – фінансова винагорода;
МПВ – морально-психологічна винагорода
Дані фактори, в свою чергу складаються із таких факторів третього рівня:

$$ФВ = f\ (А;\ ЗП;\ Б),\qquad (10)$$

де *А* – акції;
ЗП – основна заробітна плата;
Б – різноманітні бонуси у вигляді премій, доплат, надбавок тощо.

$$МПВ = f\ (СА;\ СВ;\ СПК),\qquad (11)$$

де *СА* – самоактулізація;
СВ – самовираження;
СПК – соціально-психологічна комфортність [9].

7. Розглянемо специфічні об'єктивні фактори для різних країн на прикладі України. Фактори другого порядку, які подані в формулі (12) є найбільш розповсюдженими на території України і особливої загрози набувають на макрорівні На мікрорівні вони, як правило, є найбільш розповсюдженими в організаціях та службах державної форми власності.

$$СФ = f\ (В;\ Х;\ ВСС;\ ПСА),\qquad (12)$$

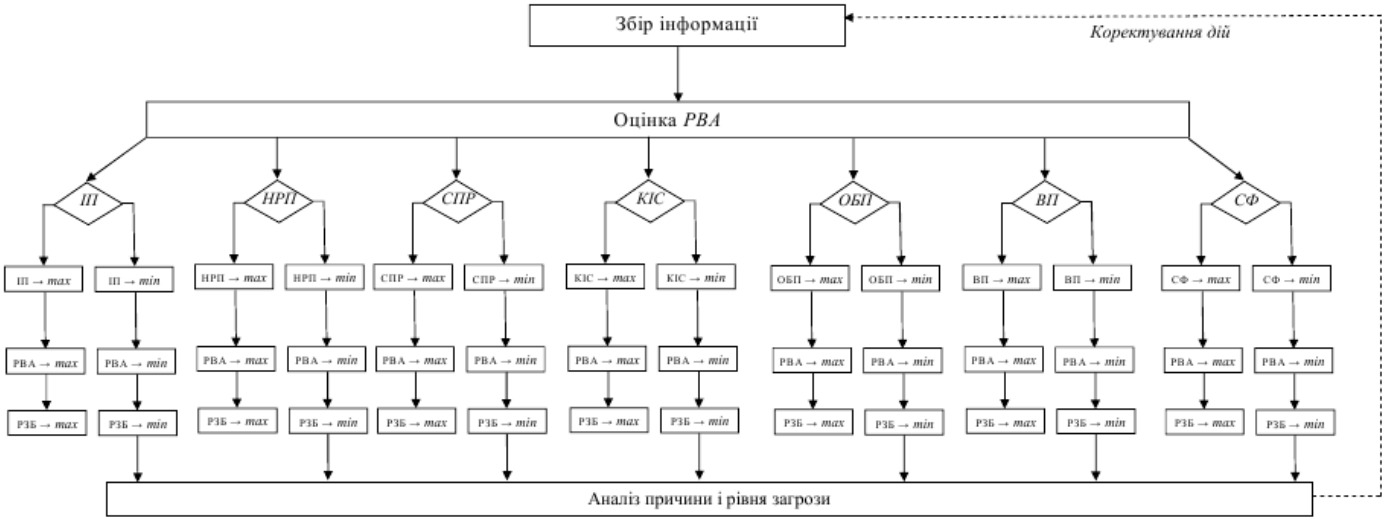

Рис. 2 – Узагальнений функціональна схема методу оцінки рівня вмотивованості агентів загроз

де *В* – можливість «відкатів»;
Х – можливість отримання хабарів;
ВСС – використання службового становища в особистих цілях;
ПСА – надання послуг стороннім взаємопов'язаним організаціям.

Метод оцінки рівня вмотивованості агентів безпеки, представлений на рис. 2 у вигляді узагальненої функціональної схеми дій, дає можливість, крім оцінювання *РВА,* також

оцінити рівень забезпечення безпеки (*РЗБ*) на аналізованому об’єкті та завчасно попередити виникнення можливих вразливостей та загроз шляхом коригуючи дій.

Висновки

Отже, таким чином розроблена модель дає змогу охопити функціональні області найбільш розповсюджених вразливостей забезпечення безпеки об’єкта на макро і мікрорівнях при недостатньому рівні вмотивованості агента. В свою чергу, розроблений метод дозволяє не лише оцінити рівень вмотивованості агента щодо збереження безпеки підприємства (організації) чи країни (регіону), але й попередити виникнення можливих вразливостей та загроз.

Література

1. Мэйволд Э. Информационная безопасность: Курс лекцій [Электронный ресурс] – Национальный Открытый Университет "ИНТУИТ", режим доступа: www.intuit.ru.

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. Таланова А.В., Владимиров С.Р. Основные подходы к управлению персоналом организации // Экономика и менеджмент инновационных технологий. – 2014, № 2 [Электронный ресурс]. – режим доступа: http://ekonomika.snauka.ru/2014/02/3673

6. Анисимов А.А. Менеджмент в сфере информационной безопасности: Учебное пособие – М.: АЭРО, 2014. – 180 с.

7. Граничин О.Безопасность информационных систем: Курс лекцій / О Граничин., В. Кияев– М.: АЭРО, 2010. – 85 с.

8. Нікіфорова Л.О. Моделювання вибору оптимального методу протидії загрозам інформаційній безпеці / Л. О. Нікіфорова, Ю. Є. Яремчук, А. А. Шиян // Реєстрація, зберігання і обробка даних. – 2014. – Т.16, № 4. – С. 28-33.

9. Нікіфорова Л.О. Метод розрахунку рівня вмотивованості співробітників щодо збереження конфіденційності інформації в задачах інформаційної безпеки // Інформаційна безпека. – 2014. – № 4 (16). – С.175-182.

Надійшла 28.10.2015 р. Рецензент: д.т.н., проф. Богданович В.Ю.