9. UNCTAD (2009). Training Manual on Statistics for FDI and the Operations of TNCs. Volume II Statistics on the Operations of Transnational Corporations. New York and Geneva, United Nations Publications. Retrieved from https://unctad.org/en/Docs/diaeia20092_en.pdf

10. UNCTAD (2007). The Universe of the Largest Transnational Corporations. New York and Geneva, United Nations Publications. Retrieved from http://unctad.org/en/Docs/iteiia20072_en.pdf

11. United Nations (2002). Manual on Statistics of International Trade in Service. Statistical Papers Series M no. 86, New York, United Nations Publications. Retrieved from http://www.oecd.org/sdd/its/2404428.pdf

12. United Nations (2010). Manual on Statistics of International Trade in Service 2010. New York, United Nations Publications. Retrieved from https://unstats.un.org/unsd/publication/seriesm/seriesm_86rev1e.pdf

13. Folfas, Pawel. (2009). Intra-Firm Trade and non-Trade Intercompany Transactions: Changes in Volume and Structure During 1990–2007. Warsaw, Warsaw School of Economics, Institute of International Economics. Retrieved from http://www.etsg.org/ETSG2009/papers/folfas.pdf

14. UNCTAD (1998). World Investment Report 1998. Trends and Determinants. New York and Geneva, United Nations Publishing. Retrieved from https://unctad.org/en/Docs/wir1998_en.pdf

15. Vernon, R. (1979). The Product Cycle Hypothesis in a New International Environment. *Oxford Bulletin of Economics and Statistics.* Volume 41, issue 4. Retrieved from https://pdfs.semanticscholar.org/1b25/2b3a40c639bf00413d7e91e988f0b0e5f30c.pdf

16. Cowling, K. Sugden, R. (1987). Market Exchange and the Concept of a Transnational Corporation: Analysing the Nature of the Firm. *British Review of Economic.* Issues, 9, 20: 57-68.

17. UNCTAD (2004). World Investment Report 2004. The Shift Towards Services. New York and Geneva, United Nations Publishing. Retrieved from https://unctad.org/en/docs/wir2004_en.pdf

18. UNCTAD (2007). World Investment Report 2007. Transnational Corporations, Extractive Industries and Development. New York and Geneva, United Nations Publishing. Retrieved from https://unctad.org/en/Docs/wir2007_en.pdf

19. UNCTAD (2008). World Investment Report 2007. Transnational Corporations and the Infrastructure Challenge. New York and Geneva, United Nations Publishing. Retrieved from https://unctad.org/en/docs/wir2008_en.pdf

20. UNCTAD (2017). World Investment Report 2007. Investment and the Digital Economy. New York and Geneva, United Nations Publishing. Retrieved from https://unctad.org/en/PublicationsLibrary/wir2017_en.pdf

Bulletin of Taras Shevchenko National University of Kyiv. Economics, 2019; 3(204): 20-27
УДК 331.1
JEL classification: J28, M50
DOI: https://doi.org/10.17721/1728-2667.2019/204-3/3

Д. Затонацький, асп.
ORCID iD 0000-0002-4828-9144
Національний інститут стратегічних досліджень, Київ, Україна

ДІАГНОСТИКА ІНСАЙДЕРСЬКИХ РИЗИКІВ І ЗАГРОЗ В УПРАВЛІННІ КАДРОВОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Проаналізовано зарубіжні підходи до діагностики ризиків і загроз у системі управління кадровою безпекою підприємства, виявлено сильні та слабкі сторони моделей у межах цих підходів, обґрунтовано сферу їхнього застосування. Наведено рекомендації щодо запровадження комплексної та цілісної системи кадрової безпеки для поліпшення практики психологічної діагностики та моніторингу дій співробітників, зокрема – удосконалення систем збору інформації щодо поведінкових індикаторів співробітників у корпоративному середовищі та за його межами.

Ключові слова: кадрова безпека, економічна безпека, управління кадровою безпекою, моделі кадрової безпеки, управління персоналом.

Вступ. Сучасний світовий досвід підтверджує пріоритетність людського ресурсу серед інших джерел економічного розвитку й чинників забезпечення конкурентоспроможності національних економік. Персонал, як носій інтелектуального та інноваційного потенціалу, нині стає головною конкурентною перевагою кожного підприємства. Від рівня компетентності та ступеня мотивованості працівників залежить результативність функціонування й динаміка розвитку підприємства.

Актуальність. Наявність проблемних зон і невирішеність проблем щодо якісного кадрового забезпечення діяльності підприємства створює передумови для порушення балансу економічної безпеки, що актуалізує наукову проблематику управління кадровою безпекою підприємства. У розумінні автора, управління кадровою безпекою підприємства є комплексним процесом запобігання негативним впливам на його економічну безпеку шляхом попередження ризиків і загроз, зумовлених потенціалом і поведінкою персоналу, управлінням працею й регулюванням соціально-трудових відносин на підприємстві, а також мінімізації негативних наслідків у разі настання цих ризиків і загроз.

Постановка проблеми. До першочергових науково-практичних завдань, що підлягають розв'язанню, варто віднести виявлення ризиків і загроз як компоненти забезпечення кадрової безпеки підприємства з метою попередження їхнього виникнення та нівелювання чи мінімізації наслідків у разі настання та прояву їх дії.

Невирішені раніше частини загальної проблеми. У сучасному науковому доробку бракує комплексного та системного дослідження альтернативних підходів і моделей, застосування яких дозволить виявити потенційні ризики та загрози економічній безпеці підприємства в частині її кадрової компоненти, що зумовлено людським фактором – низьким рівнем потенціалу чи девіантною поведінкою працівників.

Метою дослідження є критичний аналіз зарубіжних моделей виявлення інсайдерських ризиків і загроз та обґрунтування можливості їхньої імплементації у вітчизняну практику управління кадровою безпекою підприємства.

Огляд літератури. Теоретичні засади та практичні аспекти кадрової безпеки є предметом дослідження багатьох вітчизняних та іноземних науковців і фахівців-практиків. В українських наукових колах проблематика ризиків і загроз у системі кадрової безпеки підприємства розглядається як складова моделі забезпечення кадрової безпеки [1]; визначено комплекс загроз для суб'єктів господарювання, що походять від діяльності персоналу [2] і вдосконалено класифікації ризиків і загроз кадровій безпеці підприємства [3]; уточнено джерела і фактори загроз за характеристиками персоналу [4]; розроблено методику мон

видавничо-поліграфічної галузі [5]. Розглянуто актуальні аспекти питання кадрової безпеки організацій як одного зі складників економічного розвитку підприємства; ризики й загрози, пов'язані з персоналом, його інтелектуальним потенціалом і трудовими відносинами [6]; сформована формалізована модель дій інсайдерів у системі кадрової безпеки суб'єктів господарювання, побудована на основі міжнародного стандарту методології функціонального моделювання IDEF0 [7]. Доводиться, що для сталого розвитку установи, закладу, підприємства, а також суспільства в цілому важливе значення мають виявлення, запобігання та своєчасна нейтралізація реальних і потенційних загроз кадровому потенціалу [8]. При цьому управління кадровою безпекою підприємства розглядається як складова частина менеджменту персоналу, націлена на виявлення, знешкодження й попередження ризиків і загроз, які можуть бути спричинені персоналом і призвести до негативних наслідків для [9]. Кадрова безпека трактується як сукупність соціально-економічних, управлінських, соціальних і психологічних процесів, скерованих на убезпечення діяльності підприємства від загроз, зумовлених людським чинником [10].

Узагальнення наукового доробку засвідчило, що в іноземній науковій літературі сформувалось декілька підходів до діагностики ризиків і загроз як інструменту управління кадровою безпекою підприємства. Одна група дослідників переконливо доводить, що для забезпечення ефективної кадрової безпеки необхідно створювати інформаційні системи й системи управління доступом до даних таким чином, щоб унеможливити ймовірність нанесення шкоди підприємству з боку його працівників. Такий підхід, зокрема, розглядається у роботі Al-Dhahri, S., Al-Sarti, M. & Abdul, A. (2017), де висвітлено питання ефективності використання міжнародних систем управління інформаційною безпекою як один зі способів ефективного управління кадровою безпекою [11]. Інша група дослідників здійснює моделювання впливу різних факторів на можливість витоку даних, в основному шляхом поширення конфіденційної інформації персоналом компанії, із використанням сучасних математичних підходів і методів. Фундаментальною в цьому напрямі є наукова праця Frank L. Greitzer, Lars J. Kangas, Christine F. Noonan, Angela C. Dalton, Ryan E. Hohimer (2012), які застосували та порівняли кілька алгоритмів дата майнінгу для дослідження проблеми інсайдерських ризиків [12]. Унаслідок чого згаданими авторами аргументовано найвищі показники ефективності байєсівського підходу та представлено архітектуру системи моніторингу дій персоналу CHAMPION для ефективного управління кадровою безпекою.

Методологія досліджень. Теоретико-методологічною основою дослідження є фундаментальні положення сучасної теорії управління персоналом, праці вітчизняних та іноземних учених у галузі управління кадровою безпекою. Для досягнення поставленої мети й розв'язання визначених завдань використано загальнонаукові та спеціальні методи наукового пізнання: *порівняльного аналізу* – для визначення сильних і слабких сторін різних моделей діагностики інсайдерських ризиків і загроз; *кластерного аналізу* – для виявлення особливостей підходів, які об'єднують спектр різних моделей виявлення передумов кадрової небезпеки; *аналізу й синтезу* – для розроблення пропозицій щодо можливості імплементації зарубіжного досвіду діагностики інсайдерських ризиків і загроз у вітчизняну практику управління кадровою безпекою підприємств.

Основні результати. Ретроспектива започаткування й поширення науково-прикладних засад управління кадровою безпекою підприємств засвідчує, що сучасні методики діагностики ризиків і загроз як складової системи управління кадровою безпекою підприємства, що знайшли висвітлення в іноземних джерелах, можна об'єднати у два підходи:

1. Психосоціальний підхід.
2. Моніторинг "комп'ютерної" активності працівника (використання комп'ютера, електронної пошти, веб-браузера тощо).

Розглянемо кожен із підходів та опишемо відповідні інструменти й моделі діагностики інсайдерських ризиків і загроз.

Основою психосоціального підходу є припущення про можливість передбачати поведінку працівників, яка може становити загрозу підприємству (внаслідок несанкціонованого поширення та "продажу" конфіденційних даних), на основі аналізу їхнього психічного й емоційного стану. Натепер існує достатня кількість наукових досліджень, результатом яких є виявлення взаємозв'язку між походженням і мотивами інсайдерів і певними особливостями поведінки працівника [13–15].

Незважаючи на зростаючий обсяг досліджень у сфері психології та мотивації працівників, існують певні труднощі з передбаченням працівників, що становлять загрозу для кадрової безпеки й можуть здійснити шахрайські дії [16]. Shaw та Fischer констатують, що більшість загроз у їхньому дослідженні можна було б уникнути своєчасними й ефективними діями, спрямованими на усунення гніву, болю, тривоги або психологічного погіршення стану правопорушників, які проявляли ознаки вразливості або ризику задовго до скоєного злочину [15].

У роботі Gudaitis наводиться аргумент, що "збір, оцінка та профілювання даних працівника" повинні бути синтезовані й інтегровані з методами інформаційної безпеки для досягнення ефективного загального способу забезпечення кадрової безпеки [17]. Згаданий автор рекомендує застосовувати спеціальні інструменти, які вимірюють особистісні та поведінкові характеристики – тести, які не лише фокусуються на придатності до роботи і навичках, а й не містять очевидних психіатричних питань, які легко вибрати та відповісти на них відповідним чином. Gudaitis наполягає на використанні цих типів тестів як методичного інструментарію відбору співробітників, припускаючи, що навіть цей підхід має недоліки в значній мірі через непередбачуваність життєвих і службових обставин співробітників.

У роботі Moore, Cappelli, Trzeciak було доведено взаємозв'язок між вимірами особистості, які визначаються п'ятифакторною моделлю (OCEAN), і контрпродуктивною поведінкою на роботі [13]. Ця модель описує такі п'ять особистісних факторів як емоційна стабільність, екстраверсія, відкритість до досвіду, співпраця, сумлінність. У цій роботі було виявлено значну кореляцію між певними елементами моделі OCEAN (відкритість і співпраця) і безвідповідальною або контрпродуктивною поведінкою. Іншими словами, кожна з п'яти рис вказує на континуум між двома крайніми характеристиками. Наприклад для показника екстраверсії такими полярними характеристиками є самотність і доброзичливість/відкритість. На рис. 1 також показано, що кожна риса особистості має зворотний бік. Наприклад, якщо хтось є спокійним, що здається позитивною рисою, то він також буде скептичним.

Таким чином, взаємозв'язок характеристик кожної з п'яти рис формує певний рівень загрози для цільового показника – ризику кадрової безпеки.

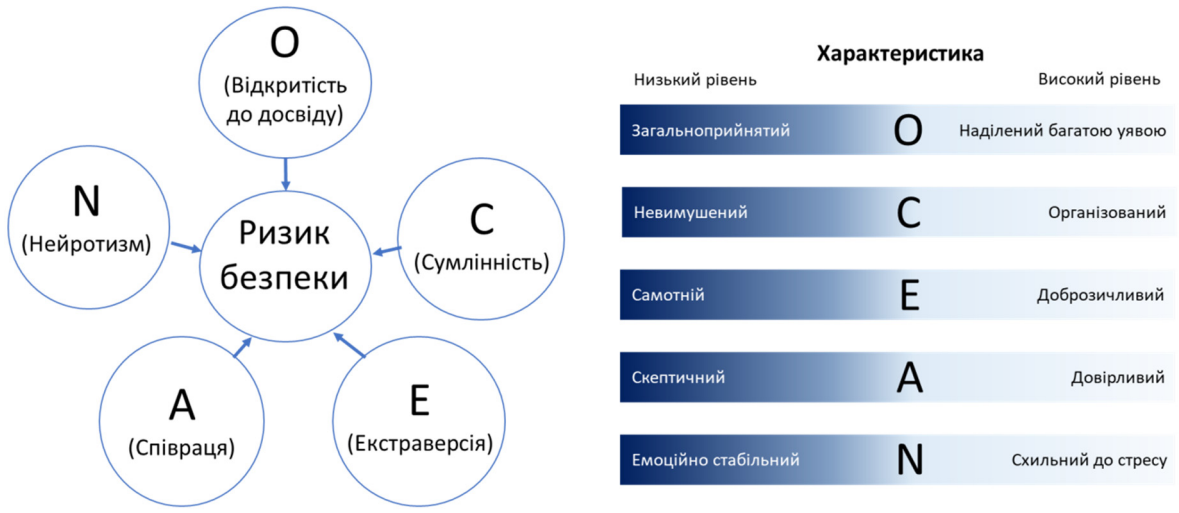

Рис. 1. Графічне представлення моделі OCEAN

Джерело: складено автором на основі [13].

Одним із найбільш відомих натепер для оцінки особистісних і поведінкових характеристик є п'ятифакторний особистісний опитувальник (більш відомий як "Велика п'ятірка"), розроблений американськими психологами Р. МакКрае і П. Коста [18]. Цей тест являє собою набір із 75 парних, протилежних за своїм значенням, висловлювань, що характеризують поведінку людини. На основі цього тесту можливо точно визначити тип поведінки людини за моделлю OCEAN (емоційна стабільність, екстраверсія, відкритість до досвіду, співпраця, сумлінність). Приклад частини тесту проведений автором у ході дослідження кадрової безпеки підприємства наведено в табл. 1.

Таблиця 1. **Тест "Великої п'ятірки"**

1. Мені подобається займатися фізкультурою	–2	–1	0	1	2	Я не люблю фізичні навантаження
2. Люди вважають мене чуйною та доброзичливою людиною	–2	–1	0	1	2	Деякі люди вважають мене холодним і черствим
3. Я в усьому ціную чистоту й порядок	–2	–1	0	1	2	Іноді я дозволяю собі бути неохайним
4. Мене часто турбує думка, що що-небудь може трапитися	–2	–1	0	1	2	"Дрібниці життя" мене не турбують
5. Усе нове викликає в мене інтерес	–2	–1	0	1	2	Часто нове викликає в мене роздратування
6. Якщо я нічим не зайнятий, то це мене турбує	–2	–1	0	1	2	Я людина спокійна й не люблю метушні
7. Я намагаюся проявляти дружелюбність до всіх людей	–2	–1	0	1	2	Я не завжди й не з усіма доброзичливий
8. Моя кімната завжди охайно прибрана	–2	–1	0	1	2	Я не дуже намагаюся стежити за чистотою й порядком
9. Іноді я впадаю в розпач через дрібниці	–2	–1	0	1	2	Я не звертаю уваги на дрібні проблеми
10. Мені подобаються несподіванки	–2	–1	0	1	2	Я люблю передбачуваність подій
11. Я не можу довго залишатися в нерухомості	–2	–1	0	1	2	Мені не подобається швидкий стиль життя
12. Я тактовний відносно інших людей	–2	–1	0	1	2	Іноді жартома я зачіпаю самолюбство інших
13. Я методичний і пунктуальний у всьому	–2	–1	0	1	2	Я не дуже обов'язкова людина
14. Мої почуття легко вразливі й ранимі	–2	–1	0	1	2	Я рідко тривожуся й рідко чого-небудь боюся
15. Мені не цікаво, коли відповідь зрозуміла заздалегідь	–2	–1	0	1	2	Я не цікавлюся речами, які мені не зрозумілі
16. Я люблю, щоб інші швидко виконували мої розпорядження	–2	–1	0	1	2	Я не виконую чужі розпорядження, не поспішаючи
17. Я поступлива та схильна до компромісів людина	–2	–1	0	1	2	Я люблю посперечатися з оточуючими
18. Я проявляю наполегливість при розв'язанні важке завдання	–2	–1	0	1	2	Я не дуже наполеглива людина
19. У важких ситуаціях я напружуюсь	–2	–1	0	1	2	Я можу розслабитися в будь-якій ситуації
20. У мене дуже жива уява	–2	–1	0	1	2	Я завжди віддаю перевагу реально дивитися на світ

Джерело: складено автором.

Підтвердженням проведеного автором тестування є висновки в роботі Willison [14], а саме, невдоволення на робочому місці й незадоволеність працівника визначаються як дві основні причини організаційної злочинності. Коли людина має незадоволені очікування від організації, у неї може з'явитися мотивація, щоб виправдати очікування за допомогою зловмисних дій проти організації. Незадоволені очікування можуть включати організаційні чинники, такі як рівень заробітної плати, потенціал просування по службі чи політика організації щодо вирішення конфліктів. Позаорганізаційні чинники, такі як сімейні проблеми чи особисті фінансові труднощі, також можуть впливати на інтенсивність незадоволеності. Ва-

жливими є висновки в роботі Keeney, et al., які показують, що 85 % інсайдерів, тобто людей, що є загрозою кадровій безпеці, відчували невдоволення до здійснення нападів, і в 92 % випадків саботажу незадоволеність пов'язувалася з працевлаштуванням [19].

У роботі Workman показано, що негативні відносини співробітників у колективі є провісниками навмисної контрпродуктивної й підривної поведінки працівника, від абсентеїзму до різних форм відплати [20]. У своєму дослідженні Wells вказує на те, що незадоволеність працівників організацією праці є потужним предиктором шахрайства на робочому місці [21]. Спираючись на літературу з організаційного правосуддя, Willison продемонстрував, як несправедливість у розподільній, процедурній, інтерактивній, міжособистісній та інформаційній сферах усередині організації може спровокувати інсайдерський злочин і витік конфіденційної інформації [14]. Також у цій роботі показано, що існує суттєвий зв'язок між сприйняттям співробітниками несправедливості на робочому місці та їхньою девіантною поведінкою, такою як злодійство чи саботаж.

У разі, коли працівник намагається отримати фінансову вигоду, використовуючи інтелектуальну власність підприємства, прагнення до помсти може викликатися задоволенням від заподіяння підприємству величезних збитків, але воно також може включати мотиви власної фінансової вигоди. У будь-якому випадку у працівника може бути стрес або одна з форм незадоволеності певними обставинами цієї людини в організації. Ці фактори, якщо їх належним чином своєчасно оцінити, можуть попередити організацію про розвиток кадрової злочинності серед працівників.

Підхід на основі виявлення співробітників, які демонструють підвищений ризик кадрової загрози, має дві переваги: запобігання непотрібних витрат для роботодавця внаслідок втрати конфіденційної інформації й допомога працівникові до того, як негативний фактор стане критичним. Правильно організоване втручання допоможе знайти рішення, яке принесе користь обом сторонам. Таким чином, психосоціальна модель приносить користь як працівникам, так і роботодавцям, якщо ця модель прийнята підприємством як один з інструментів забезпечення кадрової безпеки та включена як інструмент у процедуру регулярного оцінювання персоналу.

У сучасній науковій літературі можна виокремити кілька напрямів та інструментів, що розкривають сутність психосоціального підходу.

Однією з найбільш поширених і важливих проблем управління кадровою безпекою, що пов'язана як із внутрішніми, так і з зовнішніми ризиками, є проблема витоку даних або проблема інсайдерських ризиків. У роботі Frank L. Greitzer, Lars J. Kangas, Christine F. Noonan, Angela C. Dalton, Ryan E. Hohimer (2012) описано модель оцінки поведінки співробітників на основі набору із 12 поведінкових показників, для виявлення тих працівників, що мають підвищений інсайдерський ризик (тобто тих, хто може нанести шкоду організації або її співробітникам) [12]. Збір даних і тестування моделі проводилося за допомогою експертів HR департаменту. Цей набір із 12 показників було обрано для того, щоб його було легко контролювати й регулярно реєструвати.

Згаданими вище авторами протестовано байєсівську модель, нелінійну модель нейронної мережі зі зворотним зв'язком (ANN) і лінійну регресію, факторами, у яких були певні психологічні показники людини, які умовно доступні в кожній компанії. Унаслідок дослідження найкращою з погляду стабільності, наочності та якості прогнозів було обрано модель Байєса. Ця модель може робити прогнози ймовірності загрози кадровій безпеці з боку кожного працівника на основі аналізу та поєднання цих поведінкових факторів.

Також, у цій роботі наголошено на необхідності використання систем збору даних користувачів компанії, що може також реєструвати психологічні й поведінкові показники працівників, для забезпечення комплексного рішення та можливості реалізації раніше охарактеризованої моделі. Так, автори описують можливу архітектуру такої системи CHAMPION, яка забезпечує справедливий і послідовний підхід до моніторингу співробітників і приносить користь як працівникам, так і роботодавцям.

Система CHAMPION (Columnar Hierarchical Autoassociative Memory Processing In Ontological Networks) містить ієрархічну структуру міркувань, організовану семантичним шаром, який забезпечує теоретико-графові методи розпізнавання образів. На відміну від підходів типового семантичного графа з монолітним аргументом, який необхідний для аргументації всіх концепцій, представлених у всьому семантичному графі, кожен аргумент у мережі CHAMPION працює лише на невеликому наборі релевантних концепцій. Кожен компонент системи CHAMPION управляється онтологією (отриманою з експертних знань); структура міркувань виконує процес абстракції, який послідовно аналізує шаблони більш високого порядку, одночасно поєднуючи кілька областей даних. Це допоможе аналітику зіставляти дані у просторі й часі, а також із різних джерел даних, знизити когнітивне навантаження на аналітика й зосередити увагу на діях, які представляють найбільш критичні потенційні ризики для кадрової безпеки.

Модель може включати кілька типів даних, які генеруються з різних "пристроїв" моніторингу співробітників, які тепер пропонуються в комерційних продуктах, від журналів подій безпеки і системи управління інформацією до веб-журналів і систем захисту/запобігання втрати даних. Система CHAMPION також може включати дані, отримані з поведінкових і психосоціальних даних (хоча вони вимагають більш формальних методів збору). Дані вводяться в семантичний граф системи окремими компонентами прийому даних ("рефлекторами"), які адаптовані до пристрою та типу даних, що надходять у систему.

До основних переваг цієї моделі можна віднести відносну простоту реалізації та зручність користування. До того ж, байєсівська модель заснована на ймовірностях, тому може давати передбачення навіть за відсутності реальних даних спостереження (наприклад, для нових співробітників). Також, урахування особливостей кожного працівника допомагає краще оцінити ймовірність загрози, тому така модель є більш практичною в багатьох компаніях. До недоліків можна віднести відносну суб'єктивність оцінювання поведінкових факторів із боку інших працівників компанії, які не завжди можуть оцінити наявність або відсутність певної характеристики у свого колеги. Із-поміж недоліків варто виділити певну обмеженість в оцінках, оскільки багато психологічних характеристик можуть бути не чітко виражені, а тому вважатись як відсутні в цього працівника.

Інша модель психосоціального підходу представлена в роботі Sokolowski та Banks, основою якої є методологія агентного моделювання [22]. У цьому дослідженні співробітники організації розглядаються як агенти, які взаємодіють з іншими співробітниками й організацією в середовищі. Потенціал кожного агента (працівника) розглядається як комбінація з трьох поведінкових

компонентів: емоційного, раціонального й соціального. Ці три компоненти об'єднуються, формуючи загальне ставлення агента до ситуації та прийняття ним рішення, яке розглядається як бінарне відношення. Ця структура використовувалася для представлення кожного працівника (інсайдера) як людини, що може негативно впливати на безпеку компанії в певний момент, чи звичайного працівника, що не представляє загрози.

Реалізація емоційної компоненти представляється як різниця між очікуваннями інсайдера й досягненням цих очікувань щодо його положення в компанії. Раціональна складова зазвичай реалізується як імовірність, пов'язана з класичною теорією прийняття рішень і обмеженою раціональністю. Соціальна складова є сумою зважених диспозицій інших агентів у моделі. Ці зважені диспозиції демонструють, наскільки співробітник залежить від колег. У цій моделі сукупність трьох складових кожного агента може перевищити його особистий поріг і стати активною загрозою для компанії (інсайдерський ризик).

Загалом, процес моделювання, викладений у згаданій вище праці, включає дослідження відсотка співробітників, які можуть стати інсайдерською загрозою для компанії при певному наборі умов. Для ініціалізації моделі були використані такі значущі початкові параметри: афективна вага, відношення до ризику, поріг загрози, цінність винагороди й організаційні зміни. Модель була створена і протестована в організації кількістю 300 співробітників. Було показано, що значення таких параметрів як афективна вага, поріг загрози майже не змінюються, а отже, вони найбільш суттєво впливають на кадрову безпеку на підприємстві.

Перевагою цієї моделі є її динамічна природа, яка дозволяє розглядати зміну рівня кадрової безпеки з плином часу, а не у статичному положенні. Простота моделювання й інтерпретація результатів також є сильними сторонами цієї моделі. У той же час, дана модель має суттєвий недолік, який проявляється в нівелюванні суб'єктивної складової кожного співробітника й неможливості врахувати особливості діяльності кожної людини. Більш того, неточності при складанні поведінкових рівнянь, від яких залежить поведінка всієї системи, може призвести до суттєвих негативних наслідків і неправильних висновків. Окрім того, імітаційний характер моделювання не враховує особливостей діяльності організації, що може призводити до одних і тих самих результатів при моделюванні діяльності різних компаній.

У той же час, збиранню даних тільки із внутрішньої інформаційної системи компанії стає замало для комплексної оцінки ризиків витоку даних. Так, Alahmadi, B. A., Legg, P. A., and Nurse, J. R. дослідили як активність у мережі Інтернет (блоги, історія відвідування веб-сайтів) може використовуватися для прогнозування психологічних характеристик людини з метою виявлення потенційних інсайдерських загроз [23].

Це дослідження ґрунтується на припущенні, що на основі аналізу історії перегляду веб-сторінок, можна зробити висновок про особливості поведінки конкретної особистості. Унаслідок чого, відхилення в такій поведінці можуть означати зміну особистості, що може характеризувати внутрішню загрозу. Такий підхід може використовуватися організаціями для моніторингу своїх співробітників, щоб виявити будь-яке раптове відхилення, яке потенційно може вказувати на підвищену імовірність інсайдерської атаки.

Основою такого підходу є два компоненти:

1) аналіз історії переглядів, зіставлення ключових слів цих сайтів із рисами характеру в моделі OCEAN. Для реалізації цієї частини використовується технології Web Scraping і Content Extraction. Далі проводиться категоріальний аналіз сайтів для визначення його категорії на основі міжнародного словника LIWC. Після цього використовуються алгоритми машинного навчання для класифікації кожного сайту та відповідної йому психологічної характеристики OCEAN. Результат таких експериментів дає значущі знання й розуміння. Наприклад, люди, які незадоволені своєю вагою та часто шукають рішення в Інтернеті на відповідних сайтах, можуть відчувати занепокоєння і депресію, що призводить до високих показників невротизму [24].

2) створення профілю особистості кожного працівника для оцінки на предмет відхилень у їхніх психологічних рисах із плином часу. Використовуючи такий профіль, система внутрішніх загроз компанії могла б відстежувати зміни в індивідуальній поведінці людини з плином часу та виявляти будь-які відхилення в їхній звичайній структурі. Це, у свою чергу, може сигналізувати про потенційну загрозу кадровій безпеці на підприємстві з боку цього працівника. Така система може допомогти виявити людей, які ймовірно стануть інсайдерами інформації.

До того ж, створений профіль особистості за таким методом може використовуватися як метрика в комплексній структурі кадрової безпеки. Наприклад, було встановлено, що такі особистісні якості, як нарцисизм і макіавеллізм, пов'язані з внутрішніми загрозами й деструктивною поведінкою [25]. Крім того, люди, які мають ознаки нарцисизму, виявляють надмірну значущість для себе, сильну потребу в захопленні та відсутність емпатії – досить поширені риси у поведінці людей, які вчинили інсайдерські атаки [26].

До позитивних сторін цієї моделі належать такі:

1) більша об'єктивність оцінки психологічного портрету працівника порівняно із суб'єктивною оцінкою його поведінки з боку інших людей;

2) можливість динамічно відслідковувати зміну психологічного стану працівника та вчасно виявляти загрозу кадровій безпеці.

У той же час ця модель має суттєві недоліки:

1) моніторинг активності користувача може порушувати права співробітника на недоторканість особистого життя (етичні та правові наслідки);

2) динамічність сайтів і велика "зашумленість" даних, неможливість правильно класифікувати категорію сайту;

3) відсутність адекватної заміни словника LIWC для класифікації вітчизняних сайтів українською чи російською мовами, що унеможливлює використання цього методу для вітчизняних підприємств.

Інший поширений підхід діагностики інсайдерських ризиків і загроз полягає у використанні різноманітних технічних стратегій аналізу поведінки працівника як користувача комп'ютерної техніки, більшість із яких використовує методи виявлення аномалій у характеристиках поведінки користувача.

Традиційні методи виявлення загроз кадровій безпеці в основному використовують методи з систем виявлення вторгнень (IDS). Ці системи розгортаються для виявлення реальних контактів у мережі чи хост-системах. Основним принципом IDS є виявлення аномалій, що полягає в позначенні всіх аномальних поведінок як вторгнення. Colombe and Stephens дослідили використання методів візуалізації для фільтрації помилкових позитивних результатів, створених IDS-системами при виявленні інсайдерських атак [27]. У цьому методі виявлення

аномалії проводилося шляхом розрахунку типової оцінки для кожного сигналу тривоги в кожному з факторів моделі. Більш низькі показники розглядалися як аномалії, а більш високі значення вважалися нормальними. Ця модель може розглядатися як інтегрована модель для підходу IDS із можливостями візуалізації для виявлення кадрової загрози. Проте, цій системі притаманні деякі недоліки. По-перше, така модель потребує використання великої кількості даних для адекватної оцінки, що може бути досить суттєвим обмеженням для вітчизняних підприємств. По-друге, реалізація у формі контактів із мережами чи хост-системами потребує інтеграції й постійного адміністрування, що може бути складним і дорогим процесом для вітчизняних підприємств.

Інший підхід на основі соціальних графіків для виявлення шкідливих внутрішніх загроз працівників був запропонований у роботі Eberle and Holder [28]. Вони розробили три окремі алгоритми виявлення аномалій на основі графіків, щоб виявити три різні аномалії – вставки, модифікації та видалення. Наявність у динаміці даних несподіваної вершини або краю розглядалася авторами дослідження як вставка, існування несподіваної мітки на вершині або краю – як модифікація, а неочікувана відсутність вершини або краю – як видалення. Для оцінки запропонованих методів виявлення аномалій на основі графіків було використано методи імітаційного моделювання, тобто оцінювання проводилося на основі деяких потенційних шкідливих дій з урахуванням різних сценаріїв. Унаслідок цього, на початку згенеровані аномалії були виявлені принаймні одним із трьох алгоритмів, які досліджували автори. Перевагою цього методу є його наочність і зрозумілість для кінцевого користувача. Також, такий метод є досить об'єктивним і допомагає вчасно виявити такі можливі загрози кадрової безпеки як шахрайство чи підозріла діяльність у мережі певного співробітника. У той же час, такий підхід є дорогим за фінансовими витратами й потребує використання найновітнішої обчислювальної техніки, що в свою чергу збільшує витрати для багатьох компаній. Також, обмеження цього підхожу полягає лише у використанні даних мережі, тобто розглядається тільки система взаємозв'язків між різними підрозділами.

У науковій праці Gavai, Sricharan та інших описана модель виявлення інсайдерської загрози на основі аналізу даних про соціальну й інтерактивну діяльність працівників підприємств [29]. Для цього було сформовано набір відповідних ознак, які можуть свідчити про загрозу кадровій безпеці на підприємстві. До таких ознак належать 42 ряди даних у п'яти категоріях: використання електронної пошти, вміст електронної пошти, поведінка входу в систему, програмна активність і веб-діяльність. Далі застосовуються методи навчання без вчителя для виявлення поведінки щодо цих ознак, які відхиляються від нормальних значень, використовуючи найсучасніші методи виявлення аномалій. У згаданій праці для виконання поставленого завдання використовувався метод "ізоляційних лісів". Унаслідок моделювання було створено панель візуалізації, яка дозволяє швидко ідентифікувати працівників із високими оцінками ризику й загрози, які дозволять їм приймати відповідні профілактичні заходи та обмежувати ризик кадрової безпеки. Перевагою цього методу є його простота, динамічність і відносна легкість у реалізації. Також, цей метод є об'єктивним, тобто спирається на автоматизований аналіз даних на основі сучасних алгоритмів машинного навчання. У той же час, цей метод є досить нестабільним і може давати зміщені результати при аналізі великої кількості працівників.

Висновки. Імовірність ризиків і загроз у порушенні рівноваги кадрової підсистеми діяльності підприємств, і як наслідок – значних економічних втрат, зумовлює потребу виявлення передумов настання цих ризиків і загроз, зокрема й з боку інсайдерів.

У практиці управління кадровою безпекою підприємств натепер сформовано потужний науково-методичний базис аналізу кадрової ситуації з метою виявлення потенційних небезпек для фінансової стабільності й позитивної динаміки економічного розвитку. Зокрема, існує широкий спектр інструментів діагностики інсайдерських ризиків і загроз, які можна згрупувати у два блоки – психосоціальні моделі та моделі на основі моніторингу активності працівника при використанні різноманітної комп'ютерної техніки. Моделі першого блоку побудовані на взаємозв'язку оцінки поведінкових характеристик працівника та ймовірності завдати збитків підприємству з боку працівника. З урахуванням сильних і слабких сторін моделей із цього блоку можна стверджувати, що в сучасних умовах для українських підприємств найбільш доцільно використовувати байєсівську модель, оскільки вона є простою в реалізації, дозволяє враховувати особливості діяльності кожного працівника та не має етичних і юридичних обмежень. Більшість інструментів другого підходу пов'язані з аналізом динаміки різних даних працівника як користувача інформаційно-комунікаційними засобами й мережами, починаючи від простої авторизації за комп'ютером і до середньої довжини і кількості спеціальних символів у службовій переписці цього співробітника. Для цих моделей характерно використання різноманітних методів машинного навчання, що пов'язані з проблемою виявлення аномалій у даних. Візуалізація цих аномалій може слугувати аргументацією девіантної поведінки працівника, що є свідченням імовірності кадрової небезпеки з боку працівника. Критичний аналіз моделей, що застосовуються у практиці виявлення інсайдерських ризиків і загроз, створює підстави для висновку про те, що для українських підприємств ефективним інструментом діагностування таких ризиків може бути модель на основі аналізу даних про соціальну й інтерактивну діяльність працівників підприємств як маловитратна.

Перспективи подальших досліджень у цьому напрямі. Горизонт подальших наукових розвідок автора статті визначено розробленням інноваційних за змістом механізмів та інструментів управління кадровою безпекою на підприємствах як передумови забезпечення їхньої економічної безпеки на основі задіяння потенціалу державних і договірних важелів регулювання соціально-трудових відносин, оновленого управлінського інструментарію посилення мотивованості працівників, а також реалізації ідеології підвищення конкурентоспроможності робочої сили та поліпшення якості трудового життя. Для досягнення такої мети передбачається здійснити критичне узагальнення методичних підходів і наявного інструментарію оцінювання рівня кадрової безпеки на підприємстві, сформувати аналітично-методичне забезпечення подальшого розвитку інструментарію управління персоналом у структурі економічної безпеки підприємства, розробити пропозиції щодо вдосконалення системи індикаторів оцінки кадрової безпеки на державному підприємстві. Із метою виявлення домінант впливу серед факторів кадрової безпеки на показники економічної діяльності підприємства припускається розробити багатофакторну економіко-математичну модель, яка дозволить здійснювати прогноз щодо нових можливостей і нових загроз для економічного зростання підприємств під впливом кадрового забезпечення.

Список використаних джерел:

1. Герасименко О. М. Моделювання системи забезпечення кадрової безпеки суб'єкта господарювання / О. М. Герасименко // Актуальні проблеми економіки. – 2012. – № 2. – *С.* 118–124.
2. Зачосова Н. В. Напрями забезпечення надійності персоналу та кадрової безпеки суб'єктів господарської діяльності. / Н. В. Зачосова, Я. М. Надточій // Причорноморські економічні студії. – 2017. – Вип. 21. – С. 82–86.
3. Семенченко А. В. Удосконалення кадрової безпеки як елементу посилення фінансово-економічної безпеки підприємства / А. В. Семенченко // Бізнес Інформ. – 2015. – № 9. – С. 428–433.
4. Кавтиш О. П. Системна природа кадрової безпеки підприємства. / О. П. Кавтиш // Економ. вісн. Нац. техн. ун-ту України "Київський політехнічний інститут". – 2015. – № 12. – С. 181–189.
5. Бурда І. Я. Моніторинг кадрової безпеки підприємств видавничо-поліграфічної галузі: методичні засади та результати апробації. / І. Я. Бурда // Наук. вісн. Львів. держ. ун-ту внутрішніх справ. Сер. економічна. – 2011. – Вип. 2. – С. 239–247.
6. Шевченко В. Є. Кадрова безпека підприємства: організаційно-психологічні аспекти / В. Є. Шевченко // Правничий вісник Ун-ту "КРОК". – 2012. – Вип. 14. – С. 124–129.
7. Панченко В. А. Схематика дій інсайдерів у системі кадрової безпеки суб'єктів господарювання / В. А. Панченко // Підприємництво і торгівля. – 2018. – Вип. 22. – С. 101-107.
8. Чередниченко О. Ю. Актуальні питання забезпечення кадрової безпеки як важливої складової системи безпеки установи, закладу, підприємства / О. Ю. Чередниченко // Честь і закон. – 2017. – № 4. – С. 44–48.
9. Черчик Л. Управління кадровою безпекою в системі менеджменту персоналу підприємства./ Л. Черчик // Економічний часопис Східноєвропейського нац. ун-ту імені Лесі Українки. – 2017. – № 4. – С. 57–61.
10. Ляшенко О. М. Кадрова безпека у системі економічної безпеки підприємства. / О. М. Ляшенко // Економіка. Менеджмент. Підприємництво. – 2013. – № 25(2). – С. 274–279.
11. Al-Dhahri S., Al-Sarti M. & Abdul, A.. Information Security Management System. // International Journal of Computer Applications. – 2017. – Volume 158 – No 7. – P. 29–33. [Electronic resource]. – Access mode: https://www.researchgate.net/publication/312518367_Information_Security_Management_System
12. Greitzer F. L., Kangas L. J., Noonan C. F., Dalton A. C. & Hohimer R. E. Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats. // 45th Hawaii International Conference on System Sciences. – 2012. – P. 2392–2401. [Electronic resource]. – Access mode: https://www.researchgate.net/publication/261527163_Identifying_At-Risk_Employees_Modeling_Psychosocial_Precursors_of_Potential_Insider_Threats
13. Moore, AP, DM Cappelli, and RF Trzeciak. 2008, "The "Big Picture" of Insider It Sabotage across U.S. Critical Infrastructures." in Insider Attack and Cyber Security, eds. SJ Stolfo, et al., Vol 39. P. 17–52. Springer US.
14. Willison R. 2009, Motivations for Employee Computer Crime: Understanding and Addressing Workplace Disgruntlement through the Application of Organisational Justice. Technical Rpt. Working Paper No. 1, Copenhagen Business School, Department of Informatics, Copenhagen, Denmark.
15. Shaw ED, and LF Fischer. 2005, Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders. Report 1 – Overview and General Observations. Technical Rpt. TR 0504.
16. Kramer LA, RJ Heuer Jr., and KS Crawford. 2005, Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage. Technical Rpt. TR 05–10, Defense Personnel Security Research Center, Monterey, CA.
17. Gudaitis TM. 1998, "The Missing Link in Information Security: Three Dimensional Profiling." CyberPsychology & Behavior 1:321–40.
18. Пятифакторный личностный опросник МакКрае-Коста ("Большая пятёрка") [Електроний ресурс]. – Режим доступу: https://fc.vseosvita.ua/0010bc-73ae.pdf
19. Keeney M/, et al. 2005, Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. Technical, U.S. Secret Service and Carnegie-Mellon University, Software Engineering Institute, CERT Coordination Center.
20. Workman M. 2009, "A Field Study of Corporate Employee Monitoring: Attitudes, Absenteeism, and the Moderating Influences of Procedural Justice Perceptions." Information and Organization 19:218-32.
21. Wells JT. 2001, "Enemies Within." Journal of Accountancy 192:31-35.
22. Sokolowski J. A., & Banks C. M. Agent implementation for modeling insider threat. // Proceedings of the 2015 Winter Simulation Conference. – 2015. – P. 266–275 [Electronic resource]. – Access mode: https://www.researchgate.net/publication/302479872_Agent_implementation_for_modeling_insider_threat
23. Alahmadi B. A., Legg P. A. & Nurse J. R. Using Internet Activity Profiling for Insider-threat Detection. // Proceedings of the 17th International Conference on Enterprise Information Systems. – 2015. – P. 709–720 [Electronic resource]. – Access mode: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220%2f0005480407090720
24. Davis, C. and Fox, J. (1993). Excessive exercise and weight preoccupation in women. Addictive Behaviors, 18(2):201-211.
25. Axelrad, E. T., Sticha P. J., Brdiczka O., and Shen J. (2013). A bayesian network model for predicting insider threats. In Security and Privacy Workshops (SPW), 2013 IEEE. P. 82–89.
26. Shaw E., Ruby K., and Post J. (1998). The insider threat to information systems: The psychology of the dangerous insider. Security Awareness Bulletin, 2(98):1–10.
27. J.B. Colombe. 2004, "Statistical profiling and visualization for detection of malicious insider attacks on computer networks," in Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, Washington DC, USA.
28. W. Eberle and L. Holder, "Applying graph-based anomaly detection approaches to the discovery of insider threats," in Intelligence and Security Informatics, 2009. ISI '09. IEEE International Conference on, 2009. P. 206–208.
29. G. Gavai, K. Sricharan, D. Gunning, J. Hanley, M. Singhal, and R. Rolleston. 2015. "Supervised and unsupervised methods to detect insider threat from enterprise social and online activity data," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), vol. 6, no. 4. P. 47–63.

Received: 26/01/2019
1st Revision: 20/02/19
Accepted: 10/03/2019

Author's declaration on the sources of funding of research presented in the scientific article or of the preparation of the scientific article: budget of university's scientific project

Д. Затонацкий, асп.
Национальный институт стратегических исследований, Киев, Украина

ДИАГНОСТИКА ИНСАЙДЕРСКИХ РИСКОВ И УГРОЗ В УПРАВЛЕНИИ КАДРОВОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

Проанализированы зарубежные подходы к диагностике рисков и угроз в системе управления кадровой безопасностью предприятия, выявлены сильные и слабые стороны моделей в рамках этих подходов, обосновано сферу их применения. Приведены рекомендации по внедрению комплексной и целостной системы кадровой безопасности для улучшения практики психологической диагностики и мониторинга действий сотрудников, в том числе – совершенствование систем сбора информации о поведенческих индикаторов сотрудников в корпоративной среде и за его пределами.

Ключевые слова: кадровая безопасность, экономическая безопасность, управление кадровой безопасностью, модели кадровой безопасности, управление персоналом.

D. Zatonatskiy, PhD student
The National Institute for Strategic Studies, Kyiv, Ukraine

DIAGNOSTICS OF INSIDER RISKS AND THREATS IN PERSONNEL SECURITY MANAGEMENT OF THE ENTERPRISE

In today's fast-changing world, the issues of personnel security management are becoming increasingly important in order to protect enterprises against internal and external threats. The article analyzes modern foreign approaches to the detection of risks and threats in the system of personnel security management of the enterprise, identifies the strengths and weaknesses of the models within these approaches, and justifies the scope of their application. The aim of the paper is to analyze critically the models of identifying insider risks and threats and to substantiate the possibility of their implementation in the national practice of personnel security management of the enterprise. It is proved that the introduction of modern modeling methods will contribute to the strengthening of the systemic nature of the practice of providing personnel security under the influence of external and internal threats. The conducted analysis of the current toolkit for diagnosing insider risks and threats has shown the expediency of clustering existing models in two blocks-psychosocial models and the models based on the use of modern information and communication technologies to monitor the employee's activity. By argumentation of the positive and negative aspects of each model, it has been proved that in modern conditions

for the Ukrainian enterprises it is most expedient to use the Bayesian model because it is simple in implementation, allows for the individuality of each employee's activity and does not have ethical and legal constraints. Recommendations for introducing comprehensive and integrated personnel security systems for domestic enterprises to improve the practice of psychological diagnostics and monitoring of employee's actions are given, in particular, improvement of systems for collecting information about employees' behavioral indicators in the corporate environment and beyond. The necessity of using modern toolkit for diagnosing risks and threats, for instance, OCEAN and CHAMPION systems, is proved, that significantly improves personnel security management in the systems of economic safety of enterprises. It has been determined that according to the criterion of the expenditure, an effective toolkit for identifying insider risks and threats can be a model based on data on social and interactive activities of enterprise employees.

Keywords: personnel security, economic security, personnel security management, personnel security models, personnel management.

References (in Latin): Translation / Transliteration / Transcription:

1. Herasymenko, O.M., 2012. Modeling of the personnel security system of the subject of management. *Actual problems of economics*, 2, pp. 118-124.

2. Zachosova, N.V. and Nadtochii, Ya. M., 2017. Areas of ensuring the reliability of personnel and personnel security of economic entities. *Black Sea Economic Studies*, 21, pp. 82-86.

3. Semenchenko, A V., 2015. Improvement of personnel security as an element of strengthening of financial and economic security of the enterprise. *Business Inform*, 9, pp. 428-433.

4. Kavtysh, O. P., 2015. Systemic nature of personnel security of the enterprise. *Economic bulletin of NTUU "KPI"*, 12, pp. 181-189.

5. Burda, I. Ya., 2011. Monitoring personnel security of enterprises of the publishing and printing industry: methodical principles and results of testing. *The Scientific Bulletin of Lviv State University of Internal Affairs (economic series)*, 2, pp. 239-247.

6. Shevchenko, V. Ye., 2012. Personnel security of the enterprise: organizational and psychological aspects. *Scientific Notes of "KROK" University*, 14, pp. 124-129.

7. Panchenko, V.A., 2018. Scheme of actions of insiders in the system of personnel security of business entities. *Entrepreneurship and Trade*, 22, pp. 101-107.

8. Cherednychenko O. Yu., 2017. Topical issues of personnel security as an important component of the security system of an institution, institution, enterprise. *Honor and Law*, 4, pp. 44-48.

9. Cherchyk, L., 2017. Personnel Security Management in the Enterprise Personnel Management System. *Economic Journal Lesya Ukrainka Eastern European National University*, № 4. pp. 57-61.

10. Liashenko, O.M., 2013. Human security in the system of economic security of the enterprise. *Economics, Entrepreneurship, Management*, 25(2), pp. 274-279.

11. Al-Dhahri, S., Al-Sarti, M. & Abdul, A. (2017). Information Security Management System. *International Journal of Computer Applications, 158*(7), 29-33.

12. Greitzer, F.L., Kangas, L.J., Noonan, C.F., Dalton, A.C., & Hohimer, R.E. (2012). Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats. *45th Hawaii International Conference on System Sciences*. Retrieved from https://www.researchgate.net/publication/261527163_Identifying_At-Risk_Employees_Modeling_Psychosocial_Precursors_of_Potential_Insider_Threats

13. Moore, A.P, Cappelli, D.M and Trzeciak R.F, 2008. "The "Big Picture" of Insider It Sabotage across U.S. Critical Infrastructures." in Insider Attack and Cyber Security, eds. SJ Stolfo, et al., Vol 39, pp. 17-52. Springer US.

14. Willison, R, 2009. Motivations for Employee Computer Crime: Understanding and Addressing Workplace Disgruntlement through the Application of Organisational Justice. Technical Rpt. Working Paper No. 1, Copenhagen Business School, Department of Informatics, Copenhagen, Denmark.

15. Shaw, ED, and LF Fischer, 2005. Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders. Report 1 – Overview and General Observations. Technical Rpt. TR 0504.

16. Kramer, LA, RJ Heuer, Jr., and KS Crawford, 2005. Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage. Technical Rpt. TR 05-10, Defense Personnel Security Research Center, Monterey, CA.

17. Gudaitis, T.M., 1998. "The Missing Link in Information Security: Three Dimensional Profiling." CyberPsychology & Behavior 1:321-40.

18. *Five-factor personal questionnaire McCrae-Costa ("Big Five")*. [pdf] Project "Vseosvita". Available at: <https://fc.vseosvita.ua/0010bc-73ae.pdf> [Accessed 04 May 2019].

19. Keeney, M, et al, 2005. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. Technical, U.S. Secret Service and Carnegie-Mellon University, Software Engineering Institute, CERT Coordination Center.

20. Workman, M, 2009. "A Field Study of Corporate Employee Monitoring: Attitudes, Absenteeism, and the Moderating Influences of Procedural Justice Perceptions." Information and Organization 19:218-32.

21. Wells, J.T., 2001. "Enemies Within." Journal of Accountancy 192:31-35.

22. Sokolowski, J.A., & Banks, C.M. (2015). Agent implementation for modeling insider threat. *Proceedings of the 2015 Winter Simulation Conference*. Retrieved from https://www.researchgate.net/publication/302479872_Agent_implementation_for_modeling_insider_threat

23. Alahmadi, B.A., Legg, P.A., & Nurse, J.R. 2015. Using Internet Activity Profiling for Insider-threat Detection. *Proceedings of the 17th International Conference on Enterprise Information Systems*. Retrieved from http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220%2f0005480407090720

24. Davis, C. and Fox, J. 1993. Excessive exercise and weight preoccupation in women. Addictive Behaviors, 18(2):201-211.

25. Axelrad, E.T., Sticha, P.J., Brdiczka, O., and Shen, J. 2013. A bayesian network model for predicting insider threats. In Security and Privacy Workshops (SPW), 2013 IEEE, pages 82-89.

26. Shaw, E., Ruby, K., and Post, J. 1998. The insider threat to information systems: The psychology of the dangerous insider. Security Awareness Bulletin, 2(98):1-10.

27. J. B. Colombe, 2004. "Statistical profiling and visualization for detection of malicious insider attacks on computer networks," in Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, Washington DC, USA,

28. W. Eberle and L. Holder, "Applying graph-based anomaly detection approaches to the discovery of insider threats," in Intelligence and Security Informatics, 2009. ISI '09. IEEE International Conference on, 2009, pp. 206-208.

29. G. Gavai, K. Sricharan, D. Gunning, J. Hanley, M. Singhal, and R. Rolleston, 2015. "Supervised and unsupervised methods to detect insider threat from enterprise social and online activity data," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), vol. 6, no. 4, pp. 47-63.