

КАДРОВА БЕЗПЕКА ПІДПРИЄМСТВА: СУТНІСТЬ ДЕФІНІЦІЇ ТА ІНДИКАТОРИ СТАНУ В УМОВАХ СТАНОВЛЕННЯ НОВОЇ ЕКОНОМІКИ

INSIDER THREAT MANAGEMENT: DEFINITION AND INDICATORS UNDER NEW ECONOMY

У статті розглянуто проблему визначення поняття «кадрова безпека», виділено основні підходи та складники кадрової безпеки. Запропоновано систему індикаторів кадрової безпеки для підприємства. Визначено основні складники системи індикаторів кадрової безпеки та проаналізовано її основні складники. Доведено, що діагностика стану кадрової безпеки дає змогу вчасно виявити ризики та загрози, які є похідними від діяльності персоналу, що допомагає вчасно реагувати на відновлення балансу в кадровій ситуації та попередити економічні збитки. Аналіз наукового доробку засвідчив, що в теоретичній конструкції цієї дефініції закладено дві ключові характеристики – належність до складників економічної безпеки підприємства та стан кадрової ситуації в контексті ризиків та загроз, що породжують соціально-економічні збитки для підприємства. Науково-прикладною платформою розроблення досконалих механізмів та інструментарію управління кадровою безпекою підприємства має стати її комплексний моніторинг із використанням низки індикаторів та відповідних показників.

Ключові слова: кадрова безпека, індикатори кадрової безпеки, зовнішні і внутрішні загрози, економічна безпека підприємства, система показників кадрової безпеки.

В статье рассмотрена проблема определения понятия «кадровая безопасность», выделены основные подходы и составляющие

кадровой безопасности. Предложена система индикаторов кадровой безопасности для предприятия. Определены основные составляющие системы индикаторов кадровой безопасности и проанализированы ее основные составляющие. Доказано, что диагностика состояния кадровой безопасности позволяет своевременно выявить риски и угрозы, которые являются производными от деятельности персонала, что позволяет своевременно реагировать на восстановление баланса в кадровой ситуации и предупредить экономический ущерб. Анализ научных работ показал, что в теоретической конструкции этой дефиниции заложены две ключевые характеристики – принадлежность к составляющим экономической безопасности предприятия и состояние кадровой ситуации в контексте рисков и угроз, порождающих социально-экономический ущерб для предприятия. Научно-прикладной платформой разработки совершенных механизмов и инструментария управления кадровой безопасностью предприятия должен стать ее комплексный мониторинг с использованием ряда индикаторов и соответствующих показателей.

Ключевые слова: кадровая безопасность, индикаторы кадровой безопасности, внешние и внутренние угрозы, экономическая безопасность предприятия, система показателей кадровой безопасности.

УДК 331.1

DOI: <https://doi.org/10.32843/bses.46-15>

Затонацький Д.А.

аспірант

Національний інститут стратегічних досліджень

Zatonatskiy Dmytro

National Institute for Strategic Studies

The article discusses the issues of defining the concept of «insider threat management», identifies the main approaches and elements of the insider threat management. The system of corporate insider threat management indicators is offered. The main elements of the insider threat management indicator system are identified and its main components are analyzed. The author shares the view of those scientists who consider the corporate insider threat management as a subsystem of its economic security that has as a purposes counteracting threats to the internal and external environment, aimed at achieving a dynamic equilibrium and interpreted from the point of view of the process of preventing negative effects of the economic risks threats to staff, their intellectual potential and social and labor relations in general. According to the author, the corporate insider threat management is a multidimensional process of personnel management at all its stages (search, selection, assessment of competence and identification of psycho-emotional qualities, motivation and formation of loyalty to the enterprise, etc.), which allows timely forecasting and identification of possible risks and threats by the staff, to ensure the economic security of the enterprise by creating a clear monitoring system for personnel processes and situations, which will allow to counter threats to the internal and external environment. It is proved that diagnostics of the insider threat management allows to identify in a timely manner the risks and threats that are derived from the activity of personnel, which allows timely response to the restoration of the balance in the personnel situation and to prevent economic losses. The analysis of scientific evidence showed that the theoretical construction of this definition contains two key characteristics – belonging to the components of economic security of the enterprise and the state of personnel situation in the context of risks and threats that cause socio-economic losses for the enterprise. A comprehensive platform for the development of perfect framework and tools for managing personnel safety of an enterprise should be its complex monitoring using a number of relevant indicators.

Key words: insider threat management, insider threat management indicators, external and internal threats, corporate economic security, system of insider threat management indicators.

Постановка проблеми. Нова економіка, становлення якої відбувається динамічними темпами в усьому світі, не лише створює нові можливості розвитку та горизонти обнадійливих перспектив, а й породжує нову масштабність існуючих загроз та принципово нові ризики різновекторних небезпек. Розвиток високих технологій та інформаційних систем, турбулентні траєкторії мінливої ринкової економіки, розгортання поведінкової економіки створюють передумови для виникнення численних загроз успішній діяльності підприємств.

Як свідчить досвід, найбільша частка збитків у діяльності підприємства спричинена незаконними та непрофесійними чи некомпетентними діями працівників, тобто переважна частина ризиків генерується співробітниками. Посилення ризиків та загроз економічній безпеці підприємства характерне для тих стадій життєвого циклу підприємства, коли виникає кризова ситуація чи розгортається криза, особливо системна. У таких умовах унаслідок складного фінансово-економічного стану та обмеженості бюджету на персонал

суттєво погіршується ступінь задоволеності роботою, знижується рівень реалізації потреб працівників, що спонукає до недобросовісної чи навіть протизаконної організаційної поведінки. Наведене дає змогу стверджувати про актуальність наукової проблематики кадрової безпеки підприємств як у цілому, так і щодо формування індикаторів її стану. Діагностика стану кадрової безпеки сприятиме вчасному виявленню ризиків та загроз, які є похідними від діяльності персоналу, що дасть змогу вчасно реагувати на відновлення балансу в кадровій ситуації та попередити економічні збитки.

Аналіз останніх досліджень і публікацій. Проблема кадрової безпеки є достатньо висвітленою в економічній літературі. Питанню визначення сутності кадрової безпеки присвятили свої дослідження такі вчені, як І. Бурда, О. Герасименко, О. Кириченко, А. Колот, В. Кравченко, Я. Криль, О. Литовченко, О. Ляшенко, Н. Логінова, Г. Назарова, О. Пацула, Ю. Чаплигіна. Своєю чергою, дослідженням індикаторів кадрової безпеки займалися Г. Гаваї, Ф. Грейтцер, А. Далтон, Л. Кангас, Д. Капеллі, А. Мур, К. Ноунан, Дж. Хенлі, К. Шрічаран тощо.

Постановка завдання. Авторське обґрунтування концепту кадрової безпеки підприємства базується на дослідженні цієї дефініції як органічної компоненти економічної безпеки. Мета дослідження – сформувати комплексне уявлення щодо сутності кадрової безпеки підприємства та індикаторів її стану в умовах становлення нової економіки.

Виклад основного матеріалу дослідження. Проблема кадрової безпеки підприємства в сучасному науковому середовищі опрацьована представниками різних наукових шкіл. Незважаючи на це, узагальнення точок зору різних авторів щодо визначення поняття «кадрова безпека» дає змогу стверджувати про відсутність полярних розбіжностей у баченні цього феномену. Більшість дослідників наголошує, що кадрова безпека є складовою частиною економічної безпеки підприємства, а її основною метою є захист підприємства від внутрішніх та зовнішніх загроз. У цілому можна виділити дві основні групи визначень кадрової безпеки (рис. 1).

Представники першої групи розглядають кадрову безпеку, передусім, як підсистему економічної безпеки, спрямовану на подолання загроз. Зокрема, О.М. Ляшенко визначає кадрову безпеку як «складову систему економічної безпеки підприємства, яка являє собою сукупність соціально-економічних, управлінських, соціальних та психологічних процесів, скерованих на убезпечення діяльності підприємства від загроз, зумовлених людським чинником» [1, с. 275]. І.Я. Бурда визначає кадрову безпеку як «підсистему економічної безпеки підприємства, що являє собою впорядковану сукупність елементів, які можуть

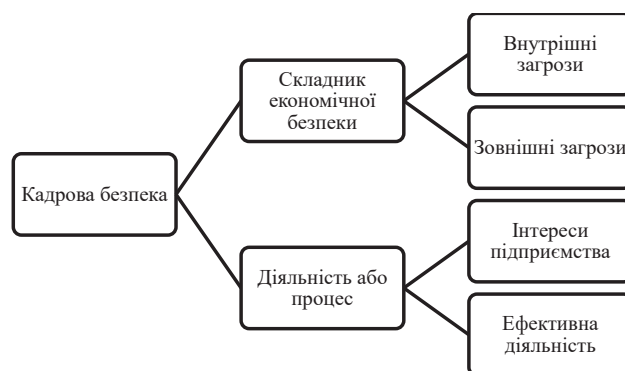


Рис. 1. Визначення поняття «кадрова безпека» підприємства

Джерело: побудовано автором

належати іншим підсистемам, комплексна взаємодія котрих слугує цілям протидії загрозам його внутрішнього та зовнішнього середовища та скерована на досягнення динамічної рівноваги всієї системи економічної безпеки» [2, с. 7]. Ю.С. Чаплигіна розглядає кадрову безпеку як «складник безпеки підприємства, що є кількісно-якісною характеристикою стану захищеності інтересів підприємства від внутрішніх та зовнішніх загроз і ризиків, пов'язаних із персоналом та використанням його людського, інтелектуального і соціального капіталу» [3, с. 102]. Н.І. Логінова бачить кадрову безпеку як «найважливішу складову частину економічної безпеки підприємства, яка має на меті виявлення, знешкодження, запобігання, відвернення та попередження загроз, небезпек і ризиків, які спрямовані на персонал та його інтелектуальний потенціал, і ті, які йдуть безпосередньо від нього, що повинно проявлятися в системі управління трудовими ресурсами та в кадровій політиці підприємства» [4, с. 372]. Своєю чергою, В.О. Кравченко наполягає, що, «будучи елементом економічної безпеки компанії, за умови, що в компанії присутні всі етапи організації та управління персоналом, кадрова безпека націлена на встановлення таких трудових і соціокультурних відносин, що забезпечують беззбиткову діяльність підприємства» [5, с. 302].

Натомість друга група дослідників розглядає кадрову безпеку як діяльність або процес, що складається з декількох основних елементів, спрямованих на забезпечення захисту інтересів підприємства. Наприклад, Г.В. Назарова визначає кадрову безпеку як «діяльність зі створення умов для його стабільного функціонування й розвитку, за яких забезпечують гарантовану законодавством захищеність інтересів підприємства, власників та персоналу від внутрішніх і зовнішніх загроз» [6, с. 35]. О.Ю. Литовченко вважає, що кадрова безпека – це «сукупність управлінських заходів, пов'язаних з ефективним формуванням та використанням кадрового потенціалу підпри-

емства з метою забезпечення та підтримки економічної стійкості та результативності господарської діяльності підприємства» [7, с. 8]. О.І. Пацула розглядає кадрову безпеку як «процес запобігання негативним впливам на економічну безпеку підприємства через ризики і погрози, пов'язані з персоналом, його інтелектуальним потенціалом і трудовими відносинами загалом» [8, с. 187]. О.А. Кириченко розглядає кадрову безпеку як «правове та інформаційне забезпечення процесу управління персоналом: вирішення правових питань трудових відносин, підготовка нормативних документів, що їх регулюють, забезпечення необхідною інформацією всіх підрозділів управління персоналом» [9, с. 130].

Таким чином, аналіз наукового доробку засвідчив, що в теоретичній конструкції цієї дефініції закладено дві ключові характеристики – належність до складників економічної безпеки підприємства та стан кадрової ситуації в контексті ризиків та загроз, що породжують соціально-економічні збитки для підприємства.

Автор поділяє точку зору тих науковців, які кадрову безпеку підприємства розглядають як підсистему його економічної безпеки, функціонування якої слугує цілям протидії загрозам внутрішнього та зовнішнього середовища, спрямовану на досягнення динамічної рівноваги, та трактують із погляду процесу запобігання негативним впливам на економічну безпеку підприємства через ризики і загрози, пов'язані з персоналом, його інтелектуальним потенціалом і соціально-трудовими відносинами загалом. На думку автора, кадрова безпека підприємства є багатовимірним процесом управління персоналом на всіх його стадіях (пошуку, підбору, оцінювання компетентності та виявлення психоемоційних якостей, мотивації та формування лояльності до підприємства тощо), який дає змогу вчасно прогнозувати та вияв-

ляти можливі ризики й загрози з боку персоналу, забезпечувати економічну безпеку підприємства шляхом створення чіткої системи моніторингу кадрових процесів та ситуацій, який дасть змогу протидіяти загрозам внутрішнього та зовнішнього середовища.

Із наведеного визначення слідує, що науково-прикладною платформою розроблення досконалих механізмів та інструментарію управління кадровою безпекою підприємства має стати її комплексний моніторинг із використанням низки індикаторів та відповідних показників. На нашу думку, індикатори кадрової безпеки можна представити чотирма блоками: досконалість організаційно-правового середовища, ступінь задоволеності працею, психологічна стійкість працівників, технічний рівень комунікацій (рис. 2).

Кожен із зазначених блоків відображає стан кадрової безпеки відповідно до джерел, що породжують ризики та загрози порушення рівноваги кадрової ситуації. Відповідно, моніторинг стану кадрової ситуації, що склалася на підприємстві, з використанням широкого спектру показників за наведеними індикаторами дасть змогу визначити сильні та слабкі сторони і сприятиме забезпеченню стійкого рівня кадрової безпеки на підприємстві. Кожен блок можна розглядати як рівнозначний складник забезпечення цілісної системи безпеки, тому питома вага кожного блока буде становити 0,25. На певній стадії життєвого циклу, у певній фінансово-економічній ситуації, у період організаційних змін, коли загострюються окремі питання кадрової безпеки за відповідним блоком, значущість відповідного індикатора посилюється. Вважаємо, що стартовим майданчиком розроблення науково-прикладного сценарію та запровадження практики діагностики кадрової безпеки підприємства має стати аналіз досконалості організаційно-правового середовища, що визначає



Рис. 2. Система індикаторів кадрової безпеки підприємства

Джерело: побудовано автором

стратегічні горизонти та політичну лінію, за якими формується система кадрової безпеки.

Індикатор «досконалість організаційно-правового середовища» на рівні підприємства, котре функціонує у відповідному правовому полі, формується з використанням показників, які окреслені та описані міжнародними стандартами. На думку автора, найбільш доцільним є запровадження стандарту ISO 27001, який містить набір показників, що слугують гарантіями під час прийняття на роботу нових працівників, визначають сферу їхніх повноважень та відповідальності, регламентують норми інформаційної безпеки працівників та вибудовують лінію захисту інтересів під час звільнення працівників. Під час використання стандарту ISO/IEC 27001 доцільно використовувати такі індикатори кадрової безпеки: перевірка, зобов'язання у трудовій угоді, відповідальність керівництва, знання вимог з інформаційної безпеки, дисциплінарні стягнення, припинення або зміна зобов'язань співробітника.

Таким чином, розроблення та імплементація відповідної документації згідно з ISO/IEC 27001 дасть змогу створити набір показників, за якими можна визначати рівень досягнутої кадрової безпеки. Отримання сертифікату ISO/IEC 27001 посилюватиме конкурентні переваги підприємства, особливо на міжнародному ринку [10].

Ступінь задоволеності працею як індикатор кадрової безпеки на підприємстві визначається шляхом проведення мотиваційного моніторингу, сценарій якого має бути орієнтований на компоненти концепту гідної праці. За наявними науковими напрацюваннями, гідна праця на рівні підприємства – це зайнятість, за якої працівник має змогу отримувати прийнятний трудовий дохід, розвивати свій потенціал і самореалізовуватися, а роботодавець – підвищувати конкурентоспроможність та забезпечувати збалансований розвиток. На думку автора, зазначені ознаки з доповненням характеристик прояву гідної праці на індивідуальному рівні мають становити основу мотиваційного моніторингу. Слід погодитися з твердженням, що розуміння компонент гідної праці на індивідуальному (особистісному) рівні має враховувати ступінь задоволеності базових потреб і статусу працівника [11].

Індикатор «психологічна стійкість працівників», що передбачає проведення аналізу психологічного стану працівника та визначення його динаміки у часі, сформувано на підставі гіпотези про те, що зміна емоційного та психосоціального стану працівника може

становити загрозу йому особисто та підприємству в цілому. Наприклад, закритість у поведінці та конфліктність у спілкуванні з колегами працівника-екстраверта може бути свідченням шантажу або мобінгу, що може призвести до загрози втрати конфіденційності інформації чи спричинення шкоди та збитків в інший спосіб.

В основу формування показників за зазначеним індикатором можуть бути покладені різні психологічні моделі чи дослідження. Зокрема, п'ятифакторна модель OCEAN та темна тріада як найбільш популярні сучасні моделі, які містять показники найбільш важливих психологічних індикаторів людини (рис. 3).

Для оцінювання психологічної стійкості працівників необхідне проведення спеціального психологічного тестування та моніторингу діяльності працівників із боку лінійних керівників та фахівців департаменту управління персоналом. На практиці в найкращому разі відбувається усереднення оцінок за тестами та власних суджень людей, що взаємодіють із певним працівником.

Інновацією в індикації психологічної стійкості працівників може стати розроблення та запровадження спеціальної інформаційної системи, куди будуть заноситися результати оцінювання психологічного стану працівника, що з використанням додаткових алгоритмів дасть змогу визначити ступінь ризику для кадрової безпеки. Такий програмний продукт може бути створений власними зусиллями із залученням додаткового людського ресурсу. Проте подібний проект займе багато часу на реалізацію та може бути неефективним із погляду надійності кінцевих результатів. Доцільно запровадити наявне програмне забезпечення. Зокрема, продукти та послуги Midot призначені для забезпечення благонадійності персоналу протягом усього його життєвого циклу в організації, починаючи від найму працівника, протягом усього

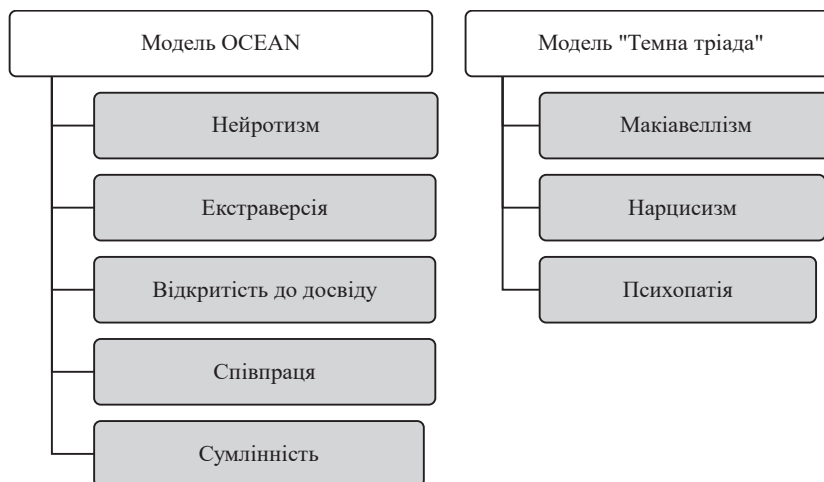


Рис. 3. Індикатори психологічної стійкості працівників у моделях OCEAN та «Темна тріада»

Джерело: побудовано автором на основі [12; 13]

періоду зайнятості в організації та до моменту його звільнення [14]. Продукт Ехабеат надає рішення у сфері безпеки й управління, які допомагають організаціям будь-яких масштабів діяльності захищати їх найціннішу інформацію [15].

За індикатором «технічний рівень комунікацій» має бути налагоджено моніторинг та аналіз усіх процесів, які працівник здійснює зі зверненням до корпоративної мережі. Показниками за зазначеним індикатором можна підтвердити аномальність поведінки, що слугуватиме підтвердженням наявності кадрової загрози з боку певного співробітника. Зокрема, авторизація у корпоративній мережі кілька разів у нічний час або пересилання листа з великими масивами вкладеної інформації можуть свідчити, що такі дії є нетиповими для працівника і, таким чином, він може здійснювати контрпродуктивну для підприємства діяльність.

Формування переліку показників за згаданим індикатором потрібно здійснювати виходячи з наявної системи адміністрування та характеру діяльності відповідних департаментів. Загальний поділ цих індикаторів можна здійснити за такими категоріями: використання електронної пошти, вміст електронної пошти, поведінка входу в систему/виходу із системи, робота з програмами і вебдіяльність [16].

Для проведення моніторингу кадрової безпеки підприємства за індикатором «технічний рівень комунікацій» пропонується покроковий алгоритм дій:

1) визначення переліку показників за індикаторами кожного блоку відповідно до поставлених завдань та специфіки діяльності кожного підрозділу підприємства;

2) розроблення та запровадження автоматизованої системи моніторингу та бази даних, де будуть створені архіви даних з урахуванням календарних термінів;

3) підготовка звітів із періодичністю один раз на тиждень/місяць із констатацією виявлених фактів та аналізом тенденцій по кожному працівнику.

Підтвердженням досягнення цілі щодо технічної підтримки системи кадрової безпеки може вважатися запровадження моніторингу кадрової безпеки підприємства за індикатором «технічний рівень комунікацій» із налаштуванням щотижневих результатів аналізу зміни поведінки кожного працівника стосовно використання ним корпоративної мережі. Імплементация на підприємстві технічної підсистеми кадрової безпеки передбачає, що керівник підприємства чи начальник служби безпеки зможуть у будь-який час із відповідним доступом отримати звіт щодо динаміки відповідних показників по кожному працівнику.

Висновки з проведеного дослідження. Формування досконалих механізмів та інструментів управління кадровою безпекою як підсистемою економічної безпеки підприємства неможливе без оновлення та поглиблення теоретико-методичних

засад. Дефініція «кадрова безпека» у сучасному науковому середовищі трактується переважно з погляду стану кадрової ситуації в контексті ризиків та загроз, що породжують збитки для підприємства. Авторське бачення теоретичної конструкції поняття «кадрова безпека підприємства» базується на його доповненні як підсистеми економічної безпеки, яка скерована на досягнення динамічної рівноваги та протидії загрозам внутрішнього та зовнішнього середовища, запобігання ризикам і загрозам, пов'язаним із персоналом, його інтелектуальним потенціалом і соціально-трудовими відносинами загалом. За авторським концептом кадрова безпека підприємства є багатовимірним процесом ефективного управління персоналом на стадіях формування, використання та розвитку людського ресурсу. Досконалість кадрових механізмів, інструментів та технологій дає змогу забезпечувати економічну безпеку підприємства. Передумовою цього слугує моніторинг кадрових процесів та ситуацій, який дасть змогу вчасно виявляти можливі ризики й загрози з боку персоналу, прогнозувати їх наслідки, протидіяти загрозам внутрішнього та зовнішнього середовища, тим самим попереджуючи або мінімізуючи соціально-економічні збитки підприємства.

Брак комплексних наукових підходів до кількісної характеристики рівня кадрової безпеки, важливість діагностики кадрової ситуації за джерелами формування потенційних ризиків та загроз в умовах становлення нової економіки є свідченням необхідності моніторингу кадрової безпеки. Індикатори стану кадрової безпеки за блоками «досконалість організаційно-правового середовища», «ступінь задоволеності працею», «психологічна стійкість працівників», «технічний рівень комунікацій» із відповідними показниками діагностики дадуть змогу провести цілісне та комплексне дослідження ризиків та загроз, що породжують кадрову небезпеку за різними джерелами її виникнення.

Подальші наукові дослідження автора будуть спрямовані на формування комплексної системи показників рівня кадрової безпеки, структурованої за індикаторами, що викладені у даній статті. Одним із напрямів подальших досліджень стане розроблення пропозицій щодо вдосконалення механізмів та оновлення і модернізації інструментарію управління кадровою безпекою підприємств.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Ляшенко О.М., Криль Я.М. Кадрова безпека у системі економічної безпеки підприємства. *Економіка. Менеджмент. Підприємництво*. 2013. № 25(II). С. 274–279.

2. Бурда І.Я. Кадрова безпека у системі економічної безпеки видавничо-поліграфічних підприємств : автореф. дис. ... канд. екон. наук : 21.04.02 ; Східно-укр. нац. ун-т ім. В. Даля. Луганськ, 2014. 20 с.

3. Чаплигіна Ю.С. Етимологічний аналіз категорії «кадрова безпека». *Управління розвитком*. 2011. № 4(101). С. 102–104.

4. Логінова Н.І. Місце кадрової безпеки в економічній безпеці підприємства. *Коммунальное хозяйство городов*. 2009. № 87. С. 371–376.

5. Кравченко В.О. Кадрова безпека – основа економічної безпеки підприємства. *Соціально-трудова відносина: теорія та практика*. 2014. № 1. С. 301–305.

6. Назарова Г.В. Передумови створення системи кадрової безпеки підприємства. *Регіональні аспекти розвитку продуктивних сил України*. 2010. Вип. 15. С. 34–37.

7. Литовченко О.Ю. Формування кадрової безпеки підприємств АПК : автореф. дис. ... канд. екон. наук : 08.00.04 ; Приват. ВНЗ «Європ. ун-т». Київ, 2010. 22 с.

8. Пацула О.І. Аналіз соціальних витрат підприємства у системі забезпечення його кадрової безпеки. *Вісник Національного університету «Львівська політехніка»*. 2012. № 722. С. 186–189.

9. Кириченко О.А. Менеджмент зовнішньоекономічної діяльності : навчальний посібник. Київ : Знання-Прес, 2002. 384 с.

10. Information technology – Security techniques – Information security management systems – Requirements. ISO/IEC 27001:2013. URL : http://k504.khai.edu/attachments/article/1406/iso_mek_27001-2013.pdf (дата звернення: 10.10.2019).

11. Колот А.М., Герасименко О.О. Теоретико-методологічні засади гідної праці: проблеми та напрями розвитку. *Соціально-трудова відносина: теорія та практика*. 2015. № 2(10). С. 21–42.

12. Moore A.P., Cappelli D.M., Trzeciak R.F. The “Big Picture” of Insider It Sabotage across U.S. Critical Infrastructures. *Insider Attack and Cyber Security*, eds. S.J. Stolfo, et al. Springer US. 2008. Vol. 39. P. 17–52.

13. Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats / F.L. Greitzer et al. 2012 45th Hawaii International Conference on System Sciences. 2012. DOI : 10.1109/hicss.2012.309 (дата звернення: 10.10.2019).

14. Midot : офіційний вебсайт. URL : <https://www.midot.com/russian/> (дата звернення: 10.10.2019).

15. Next Gen SIEM, UEBA and Automated Incident Response. URL : <https://www.exabeam.com/> (дата звернення: 10.10.2019).

16. Supervised and unsupervised methods to detect insider threat from enterprise social and online activity data / G. Gavai et al. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*. 2015. Vol. 6. № 4. P. 47–63.

REFERENCES:

1. Liashenko O. M., Kryl Ya. M. (2013) Kadrova bezpeka u systemi ekonomichnoi bezpeky pidpriemstva [Insider threat management in the corporate economic security system]. *Ekonomika. Menedzhment. Pidpriemnytstvo : zb. nauk. pr.*, 25 (II), pp. 274-279.

2. Burda I. Ya. (2014) Kadrova bezpeka u systemi ekonomichnoi bezpeky vydavnycho-polihrafichnykh pidpriemstv [Insider threat management in the economic security system of the publishing enterprise] (PhD Thesis) *Nauk. Skhidnoukr. nats. un-t im. V. Dalia, Luhansk.*

3. Chaplyhina Yu.S. (2011) Etymolohichnyi analiz katehorii “kadrova bezpeka” [Etymology of the notion “insider threat management”]. *Upravlinnia rozvytkom*, no. 4 (101), pp. 102-104.

4. Lohinova N. I. (2009) Mistse kadrovoy bezpeky v ekonomichnii bezpetsi pidpriemstva [The role of the insider threat management in the corporate economic security]. *Kommunal'noe khazyaystvo gorodov: Nauchno-tekhnicheskyy sbornik*, no. 87, pp. 371-376.

5. Kravchenko V. O. (2014) Kadrova bezpeka – osnova ekonomichnoi bezpeky pidpriemstva [Insider threat management as the basis of the corporate economic security]. *Sotsialno-trudovi vidnosyny: teoriia ta praktyka*, no. 1, pp. 301-305.

6. Nazarova H. V. (2010) Peredumovy stvorennia systemy kadrovoy bezpeky pidpriemstva [Prerequisites to creating corporate insider threat management system]. *Rehionalni aspekty rozvytku produktyvnykh syl Ukrainy*, Vyp.15, pp. 34-37.

7. Lytovchenko O. Yu. (2010) Formuvannia kadrovoy bezpeky pidpriemstv APK [Creating insider threat management for agricultural enterprise] (PhD Thesis) *Pryvat. VNZ “Yevrop. un-t”*.

8. Patsula O. I. (2012) Analiz sotsialnykh vytrat pidpriemstva u systemi zabezpechennia yoho kadrovoy bezpeky [Social costs analysis for corporate system of insider threat management]. *Visn. Nats. un-tu “Lviv. politekhnik”, no. 722*, pp. 186-189.

9. Kyrychenko O. A. (2002) Menedzhment zovnishnoekonomichnoi diialnosti [Management of the foreign economic activities]: *Navch. posibnyk*. K.: Znannia-Prs. (in Ukrainian)

10. Information technology – Security techniques – Information security management systems – Requirements. ISO/IEC 27001:2013. URL: http://k504.khai.edu/attachments/article/1406/iso_mek_27001-2013.pdf (accessed 10 October 2019).

11. Kolot A. M., Herasymenko O. O. (2015) Teoretyko-metodolohichni zasady hidnoi pratsi: problemy ta napriamy rozvytku [Theories of the principles of decent work: issues and development]. *Sotsialno-trudovi vidnosyny: teoriia ta praktyka*. Kyiv: KNEU, № 2 (10), pp. 21-42. (

12. Moore A. P., Cappelli D. M., Trzeciak R. F. (2008) The “Big Picture” of Insider It Sabotage across U.S. Critical Infrastructures. *Insider Attack and Cyber Security*, eds. S.J. Stolfo, et al. Springer US, vol. 39, pp. 17-52.

13. 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. URL: doi:10.1109/hicss.2012.309 (accessed 10 October 2019).

14. Midot: official web-site. URL: <https://www.midot.com/russian/> (in Russian) (accessed 10 October 2019)

15. Next Gen SIEM, UEBA and Automated Incident Response. URL: <https://www.exabeam.com/> (accessed 10 October 2019).

16. Gavai G., Sricharan K., Gunning D., Hanley J., Singhal M., Rolleston R. (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.