Leykhiff, Dzh. M. *Biznes-kommunikatsii: Strategii i navyki* [Business communication: strategies and skills]. St. Petersburg: Piter, 2013.

"Marketing communications methods" Interactive advertising and marketing association. http://marketing.about.com/od/marketingmethods

Polanyi, K. *The great Transformation: the political and economic origins of our time.* Boston: Beacon Press; Beacon Hill, 1944.

Sharkov, F. I. *Integrirovannye PR-kommunikatsii: Sviazi s obshchestvennostiu kak komponent integrirovannykh marketingovykh kommunikatsiy* [Integrated PR-communications: Public Relations as a component of integrated marketing communications]. Moscow: RIP-kholding, 2004.

Zaplatynskyi, V. M. I*NTERNET – suchasna informatsiina tekhnolohiia dlia marketynhu* [INTERNET – modern information technology to marketing]. Lviv, 2008.

УДК 658.5:338.2(004.9)

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ

© 2015 **ЯРЕМИК Х. Я., ЯРЕМИК М. І.**

УДК 658.5:338.2(004.9)

Яремик Х. Я., Яремик М. І. Організація інформаційно-аналітичного забезпечення фінансово-економічної безпеки

Мета статті полягає в дослідженні функціонування інформаційно-аналітичного забезпечення фінансово-економічної безпеки підприємств в умовах сучасного стану розвитку інформаційних технологій. На основі аналізу наукових поглядів учених було уточнено основні завдання інформаційно-аналітичного забезпечення фінансово-економічної безпеки. Обґрунтовано, що в умовах розвитку засобів комунікацій, PDA-пристроїв, перенесення частини бізнесу в соціальні мережі виникла необхідність застосування спеціалізованого програмного забезпечення як інструменту інформаційно-аналітичного забезпечення. Визначено, що основним елементом має бути DLP-система, яка повинна інтегруватися із SEIM-системами, Business intelligence, HRM та Anti-Fraud-системами. Перспективами подальших досліджень у даному напрямі є визначення можливості інтеграції DLP-систем з інструментами конкурентної розвідки (пошуковими системами), що дозволить автоматизувати аналіз потенційних зовнішніх загроз фінансово-економічній безпеці, а також дослідження місця IT-аудиту в інформаційно-аналітичному забезпеченні фінансово-економічної безпеки.

Ключові слова: *фінансово-економічна безпека, інформаційна-аналітичне забезпечення, конкурентна розвідка, DLP-системи, SIEM-системи.*
Бібл.: *17.*

Яремик Христина Ярославівна *– кандидат економічних наук, доцент кафедри фінансово-економічної безпеки, обліку і аудиту, Українська академія друкарства (вул. Підголоско, 19, Львів, 79020, Україна)*
E-mail: *khyaremyk@i.ua*

Яремик Мирослав Іванович *– кандидат економічних наук, доцент, доцент кафедри фінансово-економічної безпеки, обліку і аудиту, Українська академія друкарства (вул. Підголоско, 19, Львів, 79020, Україна)*
E-mail: *jaremyk_m@i.ua*

УДК 658.5:338.2(004.9)

Яремик Х. Я., Яремик М. И. Организация информационно-аналитического обеспечения финансово-экономической безопасности

Цель статьи заключается в исследовании функционирования информационно-аналитического обеспечения финансово-экономической безопасности предприятий в условиях современного состояния развития информационных технологий. На основе анализа научных взглядов ученых были уточнены основные задачи информационно-аналитического обеспечения финансово-экономической безопасности. Обосновано, что в условиях развития средств коммуникаций, PDA-устройств, переноса части бизнеса в социальные сети возникла необходимость применения специализированного программного обеспечения как инструмента информационно-аналитического обеспечения. Определено, что основным элементом должна быть DLP-система, которая интегрируется с SEIM-системами, Business intelligence, HRM и Anti-Fraud- системами. Перспективами дальнейших исследований в данном направлении являются определение возможности интеграции DLP-систем с инструментами конкурентной разведки (поисковыми системами), что позволит автоматизировать анализ потенциальных внешних угроз финансово-экономической безопасности, а также исследование места ИТ-аудита в информационно-аналитическом обеспечении финансово-экономической безопасности.

Ключевые слова: *финансово-экономическая безопасность, информационно-аналитическое обеспечение, конкурентная разведка, DLP-системы, SIEM-системы.*
Библ.: *17.*

Яремик Христина Ярославовна *– кандидат экономических наук, доцент кафедры финансово-экономической безопасности, учета и аудита, Украинская академия печати (ул. Подголоско, 19, Львов, 79020, Украина)*
E-mail: *khyaremyk@i.ua*

Яремик Мирослав Иванович *– кандидат экономических наук, доцент, доцент кафедры финансово-экономической безопасности, учета и аудита, Украинская академия печати (ул. Подголоско, 19, Львов, 79020, Украина)*
E-mail: *jaremyk_m@i.ua*

UDC 658.5:338.2(004.9)

Yaremyk Kh. Ya., Yaremyk M. I. Organization of Information-Analytical Provision of Financial-Economic Security

The article is aimed at studying the functioning of information-analytical provision of the financial-economic security of enterprises in conditions of the current stage of development of information technology. On the basis of the analysis of scientific views of scientists, the main tasks of the information-analytical provision of financial-economic security have been clarified. It has been substantiated that, in the conditions of communications development, PDA devices, partial transfering of business into social networks, it became necessary to use specialized software as a tool for information-analytical provision. It has been determined that the main element has to be a DLP system that integrates with SIEM systems, Business intelligence, CRM and Anti-Fraud-systems. Prospects for further research in this area is to determine the possibility of integration of DLP-systems with competitive intelligence tools (search engines) that will automate the analysis of potential external threats to financial-economic security, as well as to study the place of IT-auditing in the information-analytical providing the financial-economic security.

Key words: *financial-economic security, information-analytical provision, competitive intelligence, DLP systems, SIEM systems.*
Bibl.: *17.*

Yaremyk Khrystyna Ya. *– Candidate of Sciences (Economics), Associate Professor of the Department of Financial and Economic Security, Accounting and Auditing, Ukrainian Academy of Printing (vul. Pidgolosko, 19, Lviv, 79020, Ukraine)*
E-mail: *khyaremyk@i.ua*

Yaremyk Myroslav I. *– Candidate of Sciences (Economics), Associate Professor, Associate Professor of the Department of Financial and Economic Security, Accounting and Auditing, Ukrainian Academy of Printing (vul. Pidgolosko, 19, Lviv, 79020, Ukraine)*
E-mail: *jaremyk_m@i.ua*

Проблема протидії загрозам фінансовій безпеці підприємницьких структур є важливою для усіх країн. Особливо гостро ця проблема стоїть на порядку денному вітчизняних підприємств, що можна пояснити їх правовою незахищеністю, рейдерством, значним рівнем корумпованості влади та правоохоронної системи, відсутністю інформаційно-аналітичних систем (аналогів кредитних бюро), зростанням злочинності, існуванням недобросовісної конкуренції та промислового шпіонажу. Отже, від вміння отримувати швидко достовірну та актуальну інформацію про зовнішні та внутрішні загрози фінансовій безпеці багато в чому буде залежати ефективність господарської діяльності підприємства та його економічна безпека. Тому застосування засобів автоматизації процесу пошуку, обробки, узагальнення інформації, а також її захисту є досить актуальним у сучасних умовах господарювання.

Визначення місця та ролі інформаційно-аналітичного забезпечення в системі економічної безпеки підприємств, вивчення принципів його організації розглядаються вітчизняними та зарубіжними науковцями і практиками в роботах [2, 7, 8, 11, 12], проте в більшості цих робіт не розглядаються питання забезпечення інформаційної складової безпеки на підприємствах. Зокрема, Є. Позднишев визначає, що метою інформаційно-аналітичного забезпечення безпеки підприємств є «…виявлення на ранній стадії заходів безпосередньої підготовки певних ворожих сил з метою нанесення економічних збитків підприємству та забезпечення відповідних їм дій за допомогою добування необхідної інформації для планування, підготовки і проведення заходів задля недопущення можливих дій» [11]. Натомість інша група учених, зокрема: З. Гуцайлюк, В. Цимбалюк, О. Сороківська, В. Гевко та ін., навпаки, зосереджує свої дослідження на технічному боці, а саме: питаннях ефективного захисту інформації та зниження ризиків її ураження від стороннього доступу [4, 13, 15]. При цьому інформаційну безпеку розглядають лише як формування інформаційних ресурсів та організацію гарантованого їх захисту [15]. Але, погоджуючись з І. Копєлєвим, до проблем інформаційної безпеки слід віднести не лише захист інформації (протидія загрозам втрати, витоку чи викривлення інформації), але і захист від поширення неправдивої інформації (запобігання інформаційним загрозам) [5].

Опрацювання робіт як вітчизняних, так і зарубіжних авторів у сфері застосування інформаційних систем і технологій забезпечення фінансової безпеки дозволило виявити, що недостатньо досліджено проблему підвищення ефективності інформаційно-аналітичного забезпечення шляхом застосування спеціалізованих програмних продуктів на усіх його напрямках.

Метою даної статті є дослідження напрямків підвищення ефективності інформаційно-аналітичного забезпечення з використанням спеціалізованих програмних продуктів.

Виходячи із загальновідомого твердження, що інформаційно-аналітична діяльність – це процес систематизації розрізненої інформації з метою отримання якісно нової інформації у вигляді аналітичних документів [5], при визначенні її місця в системі фінансово-економічної безпеки (ФЕБ) важливим є встановлення об'єктів інформаційної уваги ФЕБ.

У результаті аналізу наукових поглядів, поданих в економічній літературі, можна зробити висновок про відсутність єдиних підходів щодо визначення об'єктів фінансово-економічної безпеки. Ряд авторів, зокрема Т. Г. Васильців, В. І. Волошин, О. Р. Бойкевич [14], О. В. Іващенко, П. М. Четвєріков [3] до основних об'єктів інформаційної уваги ФЕБ відносять лише внутрішні об'єкти: фінансові, кадрові, інформаційні, матеріальні та інтелектуальні ресурси (технології, ноу-хау, нематеріальні активи), а також техніко-економічні показники діяльності підприємств, тобто ресурси, на яких базується фінансово-господарська діяльність підприємства. Але, погоджуючись з І. П. Мойсеєнко та О. М. Марченко у тому, що «фінансово-економічна безпека підприємства – це такий його фінансово-економічний стан, який забезпечує захищеність його фінансово-економічних інтересів від внутрішніх і зовнішніх загроз і створює необхідні фінансово-економічні передумови для стійкого розвитку в поточному та довгостроковому періодах» [8, с. 28], до об'єктів інформаційної уваги ФЕБ слід віднести також і зовнішні, які умовно поділяються на об'єкти:

- макросередовища (інформація про загальний стан економіки держави та галузі, інфляція, купівельна спроможність населення, курсові коливання, інвестиційний клімат, міжнародні угоди, економічні рішення уряду, тощо);
- мікросередовища (інформація про власників, акції підприємства, конкурентів, покупців, постачальників та партнерів, контактних аудиторій, банків, тощо);
- інформація про бізнес-процеси у виробничій сфері, маркетинговій діяльності, корпоративному управлінні, індикатори фінансового стану підприємств [8, с. 34–35].

Не можна цілком погодитися з думкою авторів [5, 11] про те, що головною метою інформаційно-аналітичного забезпечення безпеки підприємництва є лише своєчасне виявлення загроз нанесення економічних збитків підприємству та забезпечення відповідних їм протидій, а також отримання необхідної інформації для планування, підготовки і проведення контрзаходів. Ми притримуємося поглядів, що інформаційно-аналітичне забезпечення передбачає також моніторинг його фінансового стану за системою показників, що враховують специфічні галузеві особливості, найбільш характерні для даного підприємства і мають для останнього важливе стратегічне значення [9].

На сьогодні існує два підходи до створення інформаційно-аналітичного забезпечення ФЕБ, а саме:

- підхід як до процесу створення та захисту інформаційної складової економічної безпеки підприємств;
- підхід як до системи з формування інформаційного ресурсу діяльності підприємств з метою забезпечення функціонування системи економічної безпеки [2].

Застосування першого підходу, на наш погляд, є дискусійним, оскільки у сферу об'єктів інформаційної уваги повинна включатися інформація лише про стан захищеності інформаційних ресурсів, а не інформаційна безпека підприємства. Інформаційна безпека – поняття значно ширше і передбачає також організацію захисту інформаційних ресурсів (включаючи технічні аспекти та застосування програмних продуктів) [4, 13, 15].

Отже, з огляду на вищезазначене, можна окреслити такі основні завдання інформаційно-аналітичного забезпечення ФЕБ:

1) пошук, збір, систематизація та узагальнення достовірної та актуальної інформації про:

- стан захищеності фінансових, кадрових, матеріальних та інтелектуальних ресурсів підприємства;
- стан організації захисту інформаційних ресурсів та потенційні загрози щодо її знищення, викрадення, викривлення чи відмові в доступі до неї;
- потенційні загрози ФЕБ підприємств зовнішнього (як макро-, так і мікро-) середовища;
- бізнес-процеси в усіх сферах його фінансово-економічної діяльності та корпоративному управлінні;

2) моніторинг фінансового стану підприємства з урахуванням специфічних галузевих особливостей;

3) аналіз основних індикаторів ефективності фінансово-господарської діяльності та їх вплив на стан ФЕБ підприємства.

Оскільки інформаційно-аналітичне забезпечення належить до забезпечуючих підсистем управління ФЕБ, то зрозуміло, що від його якості безпосередньо залежить якість управління ФЕБ, де основними є процеси прийняття рішень на основі отримуваної інформації. В епоху глобальної інформатизації суспільства та застосування інформаційних технологій автоматизації основних бізнес процесів, розвитку засобів комунікацій ефективність функціонування підсистеми інформаційно-аналітичного забезпечення неможлива без використання сучасних спеціалізованих продуктів.

За даними Аналітичного центру InfoWatch «Дослідження витоків конфіденційної інформації у 2014 році», у світі за означений рік зареєстровано 1395 випадків витоку конфіденційної інформації, що на 22 % більше 2013 р. (у тому числі в Україні зареєстровано 15). При цьому серед усіх витоків 50,1 % випадкові, 43,2 % умисні. У 54 % випадків винуватцями витоків є теперішні, а лише у 0,9 % – колишні співробітники; 25,8 % – зовнішні зловмисники. Понад 1 % порушників складає керівний склад підприємств (керівники відділів, топ-менеджери).

За характером дій розподіл порушень вказує, що: 80,5 % – це втрата контролю над даними, 7,8 % – несанкціонований доступ до інформації, 11,7 % – зловживання з використанням інформації [10]. На наш погляд, реальні дані є значно більшими, оскільки багато компаній не бажають розголошувати інформацію щодо витоку інформації, щоб не дискредитувати свій імідж.

Наведені результати дослідження Аналітичного центру InfoWatch вказують на потребу проведення детальних розслідувань інцидентів витоку інформації. Основною проблемою побудови захисту інформації при сучасному розвитку технологій у галузі IT-індустрії є обробка інформації, оскільки кількість джерел, що забезпечують надходження актуальної інформації за поточним станом захищеності, безперервно зростає. Як спеціалізоване програмне забезпечення аналізу інцидентів можуть бути використані DLP-системи. DLP (*Data Loss Prevention*) – це спеціалізований програмний продукт, що запобігає витоку конфіденційної інформації за межі корпоративної мережі. Хоча основне призначення таких систем – запобігання витоку інформації, у сучасних DLP-системах акцент змістився до розвитку аналітичних інструментів розслідування та аналізу інцидентів. Сучасні DLP-системи дозволяють:

- виявити зловмисників, осіб, які займаються промисловим шпигунством, халатності персоналу при роботі з конфіденційною інформацією;
- здійснювати контроль діяльності персоналу та визначити ступень їх лояльності до компанії (включно з тими, що можуть передати інформацію конкурентам) за допомогою інструментів аналізу і бізнес-розвідки (BI – *Business Intelligence*);
- оперативно відстежувати стан інформаційної безпеки за допомогою звітності;
- оперативно виявляти кризові ситуації як всередині периметра компанії, так і за її межами;
- отримати повну систематизовану картину інформаційного фону компанії в Інтернеті [10].

На сьогодні світовими лідерами є програмні продукти Symantec Data Loss Prevention (Symantec Corp.), RSA (подразделение EMC Corp.), Verdasys Inc, Websense Triton (Websense Inc.), McAfee. Серед російських DLP-систем слід виділити: InfoWatch Traffic Monitor (InfoWatch), Дозор-Джет (компнія Инфосистемы Джет), Zecurion (SecureIT), Falcongaze SecureTower (ООО «Фалконгейз»), «Гарда Предприятие» (МФИ Софт) [1, 17].

Для контролю за подіями в мережі в режимі реального часу, виявлення вразливих точок на основі вивчення кореляції між різними типами подій доцільною є інтеграція DLP і SIEM систем. SIEM (*Security information and event management*) – об'єднання двох термінів, що позначають область застосування SIM – *Security information management* – управління інформаційною безпекою і SEM – *Security event management* – управління подіями безпеки. Оскільки SIEM-система містить архів записів про події (лог-файли), спільна робота DLP і SIEM дозволить при необхідності відновити історію подій, що буває необхідно, наприклад, у випадку службового розслідування. SIEM здатна виявляти: мережеві атаки, вірусні зараження, невидалені віруси, трояни, спроби несанкціонованого доступу до конфіденційної інформації, вразливості, шахрайство та інше. На сьогодні найбільш відомі SIEM-системи: IBM Security QRadar SIEM (виявлення неправильного використання додатків, внутрішнього шахрайства і сучасних невеликих погроз, які можна не помітити серед мільйонів подій); HP ArcSight Security Intelligence (комплексне рішення забез-

печує збір і фільтрацію подій, рішення для виявлення і запобігання шахрайства у сфері інтернет-банкінгу та банківських (пластикових) карток); McAfee NitroSecurity (рішення Enterprise Security Manager, яке здійснює збір, кореляцію, оцінку і розподіл пріоритетів подій безпеки); Symantec SSIM (Система автоматизації виявлення та реагування на інциденти інформаційної безпеки контролю переміщення конфіденційної інформації); RSA Envision (Унікальна інфраструктура збору, зберігання і аналізу мережевого трафіку і журналів подій, що дозволяє зі значно більш високою швидкістю обробляти дані організації будь-яких масштабів); Open Source Information Security Management (OSSIM) (є безкоштовною SIEM-системою); «НВО «Ешелон» КОМРАД (для оперативного оповіщення і реагування на внутрішні та зовнішні загрози безпеки автоматизованих систем, а також контролю виконання вимог безпеки інформації) [16].

Оскільки завданням інформаційно-аналітичної діяльності у ФЕБ, поряд з аналізом інцидентів, є також виявлення потенційних витоків інформації, то доцільним є інтеграція DLP з аналітичними системами класу BI (Business Intelligence), зокрема системами Security Intelligence, які працюють з будь-якими видами інформації та дозволяють виявляти тенденції і прогнози, а також ERP-системами чи системами управління персоналом (HRM-системами, Human Resource Management), що дозволить відслідковувати комунікації працівників з майбутніми чи теперішніми контрагентами. Як правило, HR-модулі є в більшості ERP-системах (зокрема SAP ERP, Oracle Hyperion, Microsoft Dynamics), але можуть застосовуватись окремі програмні рішення (Megapolis фірми ТОВ «Софтлайн-ІТ»).

Указані системи здебільшого дозволяють аналізувати потенційні загрози, які стосуються інформаційної складової ФЕБ, але не менш важливим є отримання інформації про потенційні загрози зовнішнього середовища. Традиційні методи аналізу бізнесу, такі як: фінансові прогнози, аналіз витрат і фінансових результатів, як правило, не дають уявлення про вплив зовнішніх чинників на успішність діяльності підприємства та не допоможуть використовувати можливості чи нейтралізувати загрози, що раптово виникли, а також виявити потенційних конкурентів. На такі питання може дати відповідь конкурентна розвідка. Ефективність конкурентної розвідки забезпечується застосуванням пошукових інструментів, серед яких слід виділити: Competitive Research&Keyword Research Gadget (аналіз стратегії конкурентів та ключових слів); InfiniGraph (відстеження активності конкурентів у соціальних мережах); Google Alerts (відстеження згадувань), Marketing Grader та Topsy (аналіз активності конкурентів у соціальних медіа та блогосфері), SpyOnWeb (виявлення сайтів з одним і тим самим власником), WhatRunsWhere (моніторинг реклами), Open Site Explorer (виявлення усіх, хто посилається на даний сайт), SimilarWeb (аналіз популярності сайтів) [6].

Для конкурентної розвідки важливо не лише відшукати необхідні дані, але й правильно інтерпретувати параметри зовнішнього середовища для процесу прийняття стратегічних рішень. Для цього використовують: метод альтернативних результатів, аналіз можливостей, метод аналізу подій, аналіз конкуруючих гіпотез. Підвищити ефективність аналізу результатів конкурентної розвідки може інтеграція її пошукових інструментів з DLP-системами. Інтенсивність контактів, період їх ведення та повноваження учасників і автоматизоване зіставлення цих факторів дозволить відділу ФЕБ своєчасно виявляти потенційно загрози.

ВИСНОВКИ

Розвиток інформаційних технологій, з одного боку, розширив бізнес-можливості компаній, а з іншого – створив додаткові загрози для фінансово-економічної безпеки підприємств. Організація інформаційно-аналітичного забезпечення із застосуванням спеціалізованого програмного забезпечення, зокрема DLP-систем, дозволить отримувати інформацію про стан інформаційної безпеки, основні канали витоку інформації, а також виявити потенційних зловмисників серед персоналу. У сучасних умовах призначення DLP-систем розглядають не тільки як інструмент запобігання витоку конфіденційної інформації, а більшою мірою – як засіб контролю корпоративних комунікацій. Для автоматизації аналізу інформації доцільним є інтеграція їх з SEIM-системами, системами класу Business Intelligence, HRM та Anti-Fraud системами. Найбільш перспективним напрямком є інтеграція DLP-систем і програмних інструментів конкурентної розвідки. ■

ЛІТЕРАТУРА

1. Акимов Е. DLP в деле безопасности бизнеса / Е. Акимов // Jet Info. – 2015. – № 9 [Электронный ресурс]. – Режим доступа : http://www.jetinfo.ru/jetinfo_arhiv/dlp-so-znakom/dlp-v-dele-bezopasnosti-biznesa/2015

2. Баланда А. Л. Інформаційно-аналітичне забезпечення економічної безпеки суб'єктів підприємницької діяльності: стан та перспективи розвитку / А. Л. Баланда // Управління проектами та розвиток виробництва : зб. наук. пр. – Луганськ : Вид-во СНУ ім. В. Даля, 2011. – № 1 (37). – С. 150–155 [Електронный ресурс]. – Режим доступу : http://www.pmdp.org.ua/images/Journal/37/11balspr.pdf

3. Іващенко О. В. Система фінансово-економічної безпеки підприємства / О. В. Іващенко, П. М. Четвєріков // Scientific researches and their practical application. modern state and ways of development (2–12 October 2012) [Електронний ресурс]. – Режим доступу : http://www.sworld.com.ua/index.php/ru /conference/he-content-of- conferences/archives-of-individual-conferences/oct-2012.

4. Копєлєв І. Ю. Інформаційні загрози: суть і проблеми / І. Ю. Копєлєв, М. О. Живко // Системи обробки інформації. – 2010. – Вип. 3. – С. 130–131 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/j-pdf/soi_2010_3_55.pdf

5. Кузнецов И. Н. Учебник по информационно-аналитической работе / И. Н. Кузнецов. – М. : ООО Изд-во «Яуза», 2001. – 320 с.

6. Мельник А. 24 инструмента конкурентной разведки в интернете: выявление, мониторинг и анализ конкурентов / А. Мельник // Веб-сайт «Ловим сетью» [Электронный ресурс]. – Режим доступа : http://lovim.net/2014/03/slezhka-za-konkurentami-v-internete/#dsq-content

7. Минаев С. Информационно-аналитическое обеспечение безопасности / С. Минаев [Электронный ресурс]. – Режим доступа : http://www.it2b.ru/blog/arhiv/34.html

8. Мойсеєнко І. П. Управління фінансово-економічною безпекою підприємства : навч. посібник / І. П. Мойсеєнко, О. М. Марченко. – Львів, 2011. – 380 с.

9. Отенко І. П. Економічна безпека підприємства : навчальний посібник / І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Х. : Вид. ХНЕУ, 2012. – 251 с.

10. Офіційний сайт InfoWatch [Електронний ресурс]. – Режим доступу : http://www.infowatch.ru/ analytics/reports

11. Позднишев Є. В. Інформаційно-аналітичне забезпечення безпеки підприємництва (методи та їх застосування) : навч. посібник. Кн. 1 / Є. В. Позднишев. – К. : Позднишев, 2007. – 86 с. [Електронний ресурс]. – Режим доступу : http://ir.kneu.edu.ua:8080/handle/2010/106

12. Сорока Р. С. Значення інформаційно-аналітичної діяльності в забезпеченні економічної безпеки підприємства / Р. С. Сорока, М. П. Сорока // Науковий вісник НЛТУ України. – 2012. – Вип. 22.13. – С. 317–322 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/j-pdf/nvnltu_2012_22.13_56.pdf

13. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісник Хмельницького національного університету. – 2010. – № 2, Т. 2. – С. 32–35 [Електронний ресурс]. – Режим доступу : http://archive.nbuv.gov.ua/portal/soc_gum/Vchnu_ekon/2010_2_2/032-035.pdf

14. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення : монографія / Т. Г. Васильців, В. І. Волошин, О. Р. Бойкевич ; за ред. Т. Г. Васильціва. – Львів, 2012. – 386 с.

15. Цимбалюк В. С. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальні кіберцивілізації) / В. С. Цимбалюк // Підприємництво, господарство і право. – 2007. – № 3. – С. 88–91.

16. Шелестова О. Что такое SIEM? / О. Шелестова // Информационный портал по безопасности SecurityLab.ru [Электронный ресурс]. – Режим доступа : http://www.securitylab.ru/analytics/430777.php

17. Шабанов И. Расширенный анализ рынка DLP-систем в России / И. Шабанов // Информационно-аналитический центр Anti-Malware.ru [Электронный ресурс]. – Режим доступа : http://www.anti-malware.ru/analytics/Market_Analysis/extended_analysis_ russian_dlp_market

REFERENCES

Akimov, E. "DLP v dele bezopasnosti biznesa" [DLP in the security business]. http://www.jetinfo.ru/jetinfo_arhiv/dlp-so-znakom/dlp-v-dele-bezopasnosti-biznesa/2015

Balanda, A. L. "Informatsiino-analitychne zabezpechennia ekonomichnoi bezpeky subiektiv pidpryiemnytskoi diialnosti: stan ta perspektyvy rozvytku" [Information-analytical economic security of business entities: state and prospects]. http://www.pmdp.org.ua/images/Journal/37/11balspr.pdf

Ivashchenko, O. V., and Chetvierikov, P. M. "Systema finansovo-ekonomichnoi bezpeky pidpryiemstva" [The system of financial and economic security]. http://www.sworld.com.ua/index.php/ru/conference/he-content-of-conferences/archives-of-individual-conferences/oct-2012

InfoWatch. http://www.infowatch.ru/ analytics/reports

Kuznetsov, I. N. *Uchebnik po informatsionno-analiticheskoy rabote* [Tutorial for information and analysis]. Moscow: Yauza, 2001.

Kopieliev, I. Yu., and Zhyvko, M. O. "Informatsiini zahrozy: sut i problemy" [Information threats: essence and problems]. http://nbuv.gov.ua/j-pdf/soi_2010_3_55.pdf

Minaev, S. "Informatsionno-analiticheskoe obespechenie bezopasnosti" [Information-analytical security]. http://www.it2b.ru/blog/arhiv/34.html

Moiseienko, I. P., and Marchenko, O. M. *Upravlinnia finansovo-ekonomichnoiu bezpekoiu pidpryiemstva* [Financial and economic security]. Lviv, 2011.

Melnik, A. "24 instrumenta konkurentnoy razvedki v internete: vyiavlenie, monitoring i analiz konkurentov" [24 competitive intelligence tool on the Internet: the identification, monitoring and analysis of competitors]. Lovim setiu. http://lovim.net/2014/03/slezhka-za-konkurentami-v-internete/#dsq-content.

Otenko, I. P., Ivashchenko, H. A., and Voronkov, D. K. *Ekonomichna bezpeka pidpryiemstva* [Economic security]. Kharkiv: Vyd-vo KhNEU, 2012.

Pozdnyshev, Ye. V. "Informatsiino-analitychne zabezpechennia bezpeky pidpryiemnytstva (metody ta ikh zastosuvannia)" [Information-analytical security business (methods and applications)]. http://ir.kneu.edu.ua:8080/handle/2010/106

Soroka, R. S., and Soroka, M. P. "Znachennia informatsiino-analitychnoi diialnosti v zabezpechenni ekonomichnoi bezpeky pidpryiemstva" [The value of information-analytical activities to ensure economic security]. http://nbuv.gov.ua/j-pdf/nvnltu_2012_22.13_56.pdf

Sorokivska, O. A., and Hevko, V. L. "Informatsiina bezpeka pidpryiemstva: novi zahrozy ta perspektyvy" [Information security company: new challenges and prospects]. http://archive.nbuv.gov.ua/portal/soc_gum/Vchnu_ekon/2010_2_2/032-035.pdf

Shelestova, O. "Chto takoe SIEM?" [What is the SIEM?]. http://www.securitylab.ru/analytics/430777.php

Shabanov, I. "Rasshirennyy analiz rynka DLP-sistem v Rossii" [Advanced analysis of the market of DLP-systems in Russia]. http://www.anti-malware.ru/analytics/Market_Analysis/extended_analysis_>russian_dlp_market

Tsymbaliuk, B. C. "Informatsiina bezpeka pidpryiemnytskoi diialnosti: vyznachennia sutnosti ta zmistu poniattia za umov vkhodzhennia Ukrainy do informatsiinoho suspilstva (hlobalni kibertsyvilizatsii)" [Information security business: determining the nature and meaning of the conditions of entry of Ukraine to the information society (global ciber civilization)]. *Pidpryiemnytstvo, hospodarstvo i pravo*, no. 3 (2007): 88-91.

Vasyltsiv, T. H., Voloshyn, V. I., and Boikevych, O. R. *Finansovo-ekonomichna bezpeka pidpryiemstv Ukrainy: stratehiia ta mekhanizmy zabezpechennia* [The financial and economic security of Ukraine: Strategy and mechanisms of support]. Lviv, 2012.