11. Буч Грейди. Язык UML. Руководство пользователя = The Unified Modeling Language user guide / Грейди Буч, Джеймс Рамбо, Айвар Джекобсон. – Изд. 2-ое, [перераб. и доп.]. – М.-СПб. : ДМК Пресс, изд-во "Питер", 2004. – 432 с.

12. Буч Г. UML. Классика CS : пер. с англ. / Г. Буч, А. Якобсон, Дж. Рамбо. – Изд. 2-ое, [перераб. и доп.] / под общ. ред. проф. С. Орлова. – СПб. : Изд-во "Питер", 2006. – 736 с.

13. Пукач А.І. Розроблення спеціалізованої комп'ютерної системи для автоматичного контролю величини резистивних параметрів мікроелектромеханічних систем / А.І. Пукач, В.М. Теслюк, Р.-А.Д. Іванців // Збірник наукових праць ІППМЕ ім. Г.Є. Пухова НАН України. – К. : Вид-во ІППМЕ ім. Г.Є. Пухова, 2012. – Вип. 64. – С. 197-202.

Пукач А.И., Теслюк В.Н., Теслюк Т.В. **Разработка микроконтроллера специализированной компьютерной системы автоматического контроля величины резистивных параметров микроэлектромеханических систем**

Разработан микроконтроллер на базе микроконтроллера семейства Arduino, и соответствующее программное обеспечение (ПО), для специализированной компьютерной системы (СКС) автоматического контроля величины резистивных параметров микроэлектромеханических систем. Для обеспечения максимального соответствия разработанного ПО аппаратной составляющей разработанной системы был применен подход с использованием унифицированного языка моделирования UML.

Ключевые слова: система, автоматизация, контроль, МЭМС, резистор, Arduino, UML, модель.

Pukach A.I., Teslyuk V.M., Teslyuk T.V. **Development of microcontroller of specialized computer system for automatic control of micro-electro-mechanical system resistive parameters value**

In this article a microcontroler of the specialized computer system for automatic control of MEMS resistive parameters value, based on Arduino microcontrollers family, and related software, are developed. For ensuring maximal accordance between developed software and appropriate hardware component of developed system the Unified Modeling Language (UML) approach was applied.

Keywords: system, automation, control, MEMS, resistor, Arduino, UML, model.

УДК 004.056:061.68

Студ. А.І. Кунинець, магістрант;
проф. Ю.І. Грицюк, д-р техн. наук – Львівський ДУ БЖД

ІНФОРМАЦІЙНІ ЗАГРОЗИ ТА ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОМИСЛОВИХ КОМПАНІЙ

Розглянуто причини виникнення сучасних інформаційних загроз та проблеми забезпечення інформаційної безпеки (ІБ) промислових компаній. З'ясовано, що проблема забезпечення ІБ будь-якої компанії є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій (ІТ), вона супроводжується постійними інформаційними загрозами – як зовнішніми, так і внутрішніми. Тому керівники служб ІБ мають прийняти як аксіому твердження про те, що звичайна оперативність реагування на сучасні загрози ІБ вже не є достатньою для запобігання їм чи знешкодження з найменшими втратами.

Ключові слова: інформаційні загрози, інформаційна безпека, інформаційні технології, джерела загроз, промислова компанія.

Вступ. У процесі своєї діяльності будь-яка компанія оперує інформацією як специфічним товаром значної вартості. Володіння достовірною і своєчасною інформацією, а також її оптимальне використання забезпечує ефективне функціонування суб'єкта господарювання як цілісного комплексу [4]. Тому проблема забезпечення інформаційної безпеки (ІБ) будь-якої компанії [2] є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій (ІТ), яка супроводжується постійними інформаційними загрозами – як зовнішніми, так і внутрішніми [1].

Загрози ІБ – це сукупність умов і чинників, що створюють небезпеку життєво важливим інтересам компанії в інформаційній сфері [1]. Дослідження причин виникнення загроз, їх характеристик, особливостей впливу на корпоративні мережі та інформаційні ресурси сприяє розробленню ефективних заходів їх захисту, спрямованих на забезпечення нормальної господарської діяльності компаній [4, 7, 10]. Управління ІБ та стійкістю функціонування компаній залежить від глибини прогнозу соціально-економічних наслідків небезпечних ситуацій та своєчасного планування та виконання низки запобіжних і захисних заходів [8].

Згідно з даними звіту "Глобальне дослідження інформаційної безпеки, 2012 рік", який 29 жовтня 2012 р. опублікувала компанія "Ернст енд Янг[1]", для захисту компаній від загроз ІБ, які є наслідком дії наявних і впровадження нових ІТ, потрібно докорінно змінити підхід до забезпечення їх ІБ [5, 6]. Цей звіт (вже п'ятнадцятий за рахунком) є одним з найбільш повних досліджень в галузі ІБ, який базується на відповідях понад 1850 респондентів – керівників інформаційно-комунікаційних мереж і служб ІБ з 64 країн світу.

Хоча на сьогодні керівники практично всіх компаній поступово нарощують свій потенціал у вирішенні короткотермінових завдань [10], пов'язаних із проблемою забезпечення ІБ, але при цьому не приділяють уваги проблемам, вирішення яких є доцільним вже зараз для зниження загрози ІБ в майбутньому. Насамперед відчувається потреба в створенні надійної архітектури ІБ, про наявність якої зголосилися тільки 31 % респондентів і відзначили збільшення кількості випадків її порушення протягом останніх двох років. Тим не менш, в 63 % компаній така архітектура не створена, і тільки 16 % респондентів вважають, що їх система ІБ повністю відповідає потребам захисту власних корпоративних мереж та інформаційних ресурсів [3].

Це означає, що керівники служб ІБ мають прийняти як аксіому твердження про те, що звичайна оперативність реагування на сучасні загрози ІБ вже не є достатньою для їх попередження чи знешкодження з найменшими втратами [2, 4, 6, 8]. Швидкість і складність динаміки джерел загроз ІБ промислових компаній зростає з роками колосальними темпами. І без того непроста ситуація у сфері ІБ ускладнюється впливом ринків нових ІТ, кількість яких стрімко розвиваються, тривалою нестабільністю в економіці та політиці, офшорній діяльності багатьох промислових компаній і посиленням нормативних вимог у сфері ІБ.

1. Збільшення кількості загроз інформаційній безпеці. У багатьох керівників служб ІБ промислових компаній на сьогодні вже є розуміння того, що сама природа і характер ризиків втрат інформаційних ресурсів швидко мі-

[1] Компанія "Ернст енд Янг" є міжнародним лідером з аудиту, оподаткування, супроводу угод і консультування. Колектив компанії нараховує 167 000 співробітників у різних країнах світу, яких об'єднують спільні цінності та високі стандарти якості послуг.

няються, а разом із збільшенням частоти появи загроз ІБ зростає і кількість порушень та інцидентів ІБ [2, 7]. Приблизно 77 % респондентів різних компаній підтвердили зростання ризику зовнішніх хакерських атак, проте вони не є єдиним джерелом занепокоєння для вирішення глобальних проблем ІБ, позаяк 46 % респондентів відзначають, що внутрішня уразливість інформаційних ресурсів також невпинно зростає за рахунок інсайдерів. Постійне зростання обсягу VoIP-продуктів змушує керівників служби ІБ швидше реагувати на появу нових витоків конфіденційної інформації [9, 10].

Компанія Sophos[1] опублікувала "Дослідження загроз у сфері ІБ – 2013", в якому було проведено детальний аналіз подій в області ІТ-безпеки за 2012 року та зроблено прогноз на 2013 рік [6]. Зокрема, зазначалося, що 80 % хакерських атак у 2012 році використали переадресацію з нібито благонадійних сайтів різних організацій, а майже 18 % доменів – з експлойт Blackhole, які знаходилися в Росії. За словами фахівців цієї компанії, 2012 рік був роком нових програмних платформ і нових хакерських загроз. Якщо зовсім недавно основною операційною системою в світі була Windows, то тепер на зміну їй прийшла нова різноманітність програмних платформ. Розробники шкідливого ПЗ активно користуються цією ситуацією, придумуючи нові неприємні сюрпризи для працівників відділу ІТ та служби ІБ промислових компаній.

Незахищені комп'ютери схильні до атак різного шкідливого ПЗ, яке поширюється мережею Інтернет [2]. Шкідливе ПЗ (англ. malware, malicious software – шкідлива програма, зловмисне ПЗ) – будь-яке ПЗ, призначене для отримання несанкціонованого доступу до обчислювальних ресурсів самого комп'ютера або до інформаційних ресурсів, які зберігаються на ньому, призначене для несанкціонованого власником їх використання чи спричинення шкоди (нанесення збитку) власникові комп'ютера, інформації чи комп'ютерній мережі шляхом копіювання, спотворення даних, видалення або підміни інформації.

Термін "шкідлива програма" (malware – це скорочення від "malicious software") за трактуванням корпорації Microsoft зазвичай використовується як загальноприйнятий термін для позначення будь-якого ПЗ, спеціально створеного для того, щоб заподіювати збиток окремому комп'ютеру, серверу, або комп'ютерній мережі, незалежно від того, чи є воно вірусом, шпигунською програмою і т. д.

Шкідливі програми за нанесеним збитком поділяються на такі, що:

1) Створюють перешкоди в роботі зараженого комп'ютера: починаючи від відкриття-закриття піддону CD-ROM і закінчуючи знищенням даних і поломкою апаратного забезпечення; блокування антивірусних сайтів, антивірусного ПЗ і адміністративних функцій ОС з метою ускладнення їх лікування; саботаж виробничих процесів, керованих комп'ютером (цим відомий черв'як Stuxnet).

[1] *Sophos* – розробник/виробник засобів захисту інформації для настільних комп'ютерів, серверів, поштових систем і мережевих шлюзів. Компанія створює програмні та апаратні продукти для фільтрації спаму, боротьби з вірусами і шпигунським ПЗ, а також розробляє криптографічні засоби і DLP-системи. Заснована компанія у 1985 році, штат налічує близько 1500 працівників.

2) Виконують інсталяцію іншого шкідливого ПЗ: завантаження з мережі (downloader); розпаковування іншої шкідливої програми, що вже міститься усередині файлу (dropper).

3) Здійснюють крадіжку, шахрайство, здирство і шпигунство за користувачем. Для крадіжки може застосовуватися сканування жорсткого диска, реєстрація натиснень клавіш (Keylogger) і перенаправлення користувача на підроблені сайти, в точності повторюючи вихідні ресурси. Викрадання даних, які представляють цінність або таємницю. Крадіжка аккаунтів різних служб (електронної пошти, мессенджерів, ігрових серверів.). Аккаунти застосовуються для розсилання спаму, а через електронну пошту можна роздобути паролі від інших аккаунтів, водночас як віртуальне майно можна продати в MMOG (Massively multiplayer online game). Крадіжка аккаунтів платіжних систем.

Шкідливе ПЗ створюють блокування комп'ютера, шифрування файлів користувача з метою шантажу і здирства грошових коштів (Ransomware[1]). Здебільшого після оплати комп'ютер або не розблоковується, або незабаром блокується другий раз. Шкідлива програма використовує телефонний модем для здійснення дорогих дзвінків, що спричиняє за собою значні суми в телефонних рахунках. Платне ПЗ, яке імітує, наприклад, антивірус, але нічого корисного для цього не робить (fraudware або scareware).

4) Виконують іншу незаконна діяльність: отримання несанкціонованого (і дармового) доступу до ресурсів самого комп'ютера або третіх ресурсів, доступних через нього, у т.ч. пряме управління комп'ютером (так званий backdoor). Організація на комп'ютері відкритих релеїв і загальнодоступних проксі-серверів. Заражений комп'ютер (у складі ботнета) може бути використаний для проведення DDoS-атак. Збирання адрес електронної пошти і поширення спаму, у т.ч. у складі ботнета[2]. Накручування електронних голосувань, клацань по рекламних банерах. Генерування монет платіжної системи Bitcoin. Використання ефекту 25-го кадру для зомбування людини.

5) Записують файли, які не є істинно шкідливими, але здебільшого небажані: жартівливе ПЗ, тобто робить які-небудь речі, що непокоять користувача. Наприклад, програма Adware показує рекламу, а програма Spyware посилає через мережу Інтернет інформацію, несанкціоновану користувачем. Створюють видимість "отруєння" документів, які дестабілізують ПЗ, що відкриває їх (наприклад, архів розміром менше мегабайта може містити гігабайти даних, а при його архівуванні може надовго "зависнути" архіватор). Програми віддаленого адміністрування можуть застосовуватися як для того, щоб дистанційно вирішувати проблеми з комп'ютером, так і для зловмисних цілей. Rootkit (руткіт, від англ. root kit, тобто "набір root'a") програма або набір програм, призначений для приховування слідів присутності зловмисника або шкідливого ПЗ від сторонніх очей.

[1] Ransomware (від англ. ransom – викуп і software – програмне забезпечення) – це шкідливе ПЗ, яке працює як здирник.

[2] Ботнет (англ. botnet від robot і network) – це комп'ютерна мережа, яка складається з деякої кількості хостів, із запущеними ботами – автономним ПЗ. Найчастіше бот у складі ботнета є програмою, яка приховано встановлюється на комп'ютері жертви і дає змогу зловмисникові виконувати певні дії з використанням ресурсів інфікованого комп'ютера.

Інколи шкідливе ПЗ для власного "життєзабезпечення" встановлює додаткові утиліти: IRC-клієнти, програмні маршрутизатори, відкриті бібліотеки перехоплення клавіатури. Таке ПЗ шкідливим не є, але через те, що за ним часто знаходиться більш шкідлива програма, яка детектується антивірусами. Буває навіть, що шкідливим є тільки скрипт з одного рядка, а останні програми сповна легітимні.

Шкідливі програми за методом розмноження поділяються на:

1) Експлойт[1] – теоретично нешкідливий набір даних (наприклад, графічний файл або мережевий пакет), що некоректно сприймається програмою, яка працює з такими даними. Тут шкоду наносить не сам файл, а неадекватна поведінку ПЗ з помилкою. Також експлойтом називають програму для генерування подібних "отруєних" даних.

2) Логічна бомба в програмі спрацьовує за певної умови, є невід'ємною від корисної програми-носія.

3) Троянська програма не має власного механізму розмноження.

4) Комп'ютерний вірус розмножується в межах комп'ютера і через змінні диски. Розмноження через локальну мережу можливо, якщо користувач сам викладе заражений файл в мережу. Віруси, водночас, поділяються за типом файлів, що заражаються (файлові, завантажувальні, макро-файлові, такі, що автозапускаються); за способом прикріплення до файлів (паразитні, супутні і такі, що перезаписують) і т.д.

5) Мережевий черв'як здатний самостійно розмножуватися мережею. Поділяється на IRC[2], поштові, такі, що розмножуються за допомогою експлойтів і т.д.

Шкідливе ПЗ може утворювати ланцюжки: наприклад, за допомогою експлойта (1) на комп'ютері жертви розгортається завантажувач (2), який встановлює з мережі Інтернет черв'яка (3)

Міжнародна мережа центрів досліджень в галузі ІБ SophosLabs компанії Sophos на основі аналізу мережевого трафіку створила рейтинг країн з найбільшим і найменшим ризиками (індекс поширеності шкідливого ПЗ розрахований на основі кількості хакерських атак комп'ютерів за останні три місяці 2012 року) [8]:

- з найбільшим ризиком: Гонконг – 23,54 %; Тайвань – 21,26 %; Арабські Емірати – 20,78 %; Мексика – 19,81 %; Індія – 17,44 %.
- з найменшим ризиком: Норвегія – 1,81 %; Швеція – 2,59 %; Японія – 2,63 %; Великобританія – 3,51 %; Швейцарія – 3,81 %.

Фахівці компанії Sophos вважають, якщо до цього моменту безліч хакерських атак не завдавали істотної шкоди компаніям, то в 2013-му, з розвитком різних програмних платформ для тестування наборів експлойтів – шкідливого ПЗ, ситуація може кардинально змінитися – традиційні системи ІБ корпоративних мереж перестануть їх захищати від нових загроз. Деякі виробники подібних платформ навіть гарантують покупцям повернення коштів у разі невдачі їх продуктів. Внаслідок цього очікується збільшення кількості інцидентів, коли шахраї отримають доступ до корпоративних мереж і активно користуватимуться ними.

[1] Експлойт (від англ. exploit – експлуатувати) – це комп'ютерна програма, фрагмент програмного коду або послідовність команд, що використовують вразливості в ПЗ та призначені для проведення атаки на обчислювальну систему. Метою атаки може бути як захоплення контролю над системою (підвищення привілеїв), так і порушення її функціонування (DoS-атака).

[2] IRC (від англ. Internet Relay Chat) – сервіс мережі Інтернет, який надає користувачам можливість спілкування шляхом надсилання текстових повідомлень багатьом людям з усього світу одночасно (в режимі реального часу).

Також для 2013 р. в галузі ІБ буде характерно:

- збільшення кількості критичних помилок для систем ІБ у налаштуваннях веб-серверів;
- зростання обсягів шкідливого ПЗ, яке важко аналізувати;
- поява інструментів для створення хакерських програм з новими сервісами;
- спрощення процесу виявлення експлойтів – шкідливого ПЗ;
- проблеми інтеграції, конфіденційності інформації та її безпеки.

Поява нових ІТ відкривають перед компаніями не тільки небачені можливості, але й піддають їх потенційним загрозам з невідомих раніше джерел [1, 7, 10]. Хмарні комп'ютерні технології як і раніше є головним джерелом інновацій в сучасному інформаційному середовищі: за останні декілька років кількість компаній, які використовують хмарні обчислення, збільшилася майже удвічі. Тим не менше, 38 % таких компаній не вжили жодних заходів щодо зниження ризиків витоку інформації, зокрема не забезпечили більш строгого нагляду за управлінням контрактами з провайдерами, які надають послуги з хмарного оброблення даних, або застосування методів шифрування [9].

Ще однією новою ІТ, яка заслуговує на увагу, є мобільні пристрої для роботи в мережі Інтернет, технологічну досконалість яких, а також пов'язані з ними переваги для бізнесу, забезпечили стрімке зростання їх популярності [4]. Станом на 2012 рік 44 % різних компаній давали змогу своїм працівникам використовувати корпоративні або особисті планшети (аналогічний показник за 2001 рік становив 20 %), за допомогою яких співробітники відправляли і отримували значні обсяги інформації, що істотно ускладнювало контроль за ІБ не тільки корпоративної мережі, але й всієї компанії загалом.

Керівники служб ІБ визнають, що мобільним технологіям потрібно приділяти більш пильну увагу [9]. При цьому засоби забезпечення ІБ і спеціальне програмне забезпечення, яке б відстежувало трафік мобільних пристроїв, як і раніше досить рідко застосовуються на динамічному ринку мобільних технологій. Тільки 40 % різних компаній використовують той чи інший метод шифрування даних на мобільних пристроях.

2. Витрати на забезпечення ІБ більші – ефективність менша. Більшість керівників різних компаній відповідають на зростання ризиків і збільшення кількості інформаційних систем, які підлягають захисту, збільшенням бюджетів на їх обслуговування та зміною пріоритетів [5, 6]. 51 % керівників різних компаній повідомили, що в 2013 році планують збільшити бюджет на 5 %. 32 % компаній вклали в розвиток системи ІБ більше 1 млн $, однак обсяг інвестицій істотно відрізняється залежно від регіону: 48 % американських компаній витратили на ІБ більше 1 млн $, водночас як у Азіатсько-Тихооке-

анському регіоні, країнах Європи, Близького Сходу, Африки і в Індії (EMEIA) частка таких компаній становила 35 % і 26 % відповідно. Що стосується розподілу бюджету, то головними статтями витрат є отримання нових ІТ (55 %) і забезпечення безперервності бізнесу (47 %).

Однак заплановане збільшення бюджету на удосконалення системи ІБ виявиться ефективним тільки в разі належного розподілу обов'язків між відповідальними за прийняття рішень. У багатьох компаніях питанням забезпечення ІБ як і раніше займаються інформаційно-технологічні відділи: 63 % респондентів повідомили, що відповідальність за ІБ в їх компаніях знаходиться на фахівцях у області ІТ [9]. Оскільки забезпечення ІБ починає виходити за рамки традиційних можливостей ІТ, в даний час потрібно приймати рішення про вибір дещо інших інструментів, процесів і методів моніторингу джерел загроз ІБ, оцінювання ефективності роботи персоналу служби ІБ, пошуку прогалин у системі ІБ, що і визначає потребу перерозподілу відповідальності.

Станом на 2012 рік тільки 5 % компаній стверджують, що забезпечення ІБ належить до компетенції керівника служби управління ризиками [7]. У багатьох компаніях такі служби не забезпечені наявними формалізованими механізмами оцінювання ризиків. Як наслідок, 52 % компаній не мають у своєму розпорядженні програм аналізу та збирання даних про ризики. Збільшення їх кількості та розриву між рівнями уразливості та захищеності компанії вимагає використання декількох джерел та (або) функцій оцінювання стану ІБ, в т.ч. і внутрішній аудит, внутрішню самооцінку і оцінку третіх сторін.

При прийнятті рішень щодо забезпечення ІБ керівники деяких компаній враховують питання наявності кваліфікованих кадрів і їх відповідна підготовка, рівня зрілості працівників щодо організації ІБ, виділення бюджету на їх ефективне функціонування [10]. Але ці очевидні питання, як і численні обхідні рішення, що дають змогу задовольнити потреби ІБ в короткотерміновій перспективі, приховують більш серйозну проблему інформаційно-комунікаційної вразливості будь-якої компанії.

Практика роботи керівників різних компаній України щодо ІБ загалом не відрізняється в кращий бік від загального її стану, які спостерігаються в країнах ближнього і дальнього зарубіжжя. Більшість компанії в основному проводять реактивні дії на ті, чи інші інциденти ІБ; різні підрозділи, які в рамках однієї компанії так чи інакше займаються питаннями оцінювання загроз та управління ІБ, діють найчастіше роз'єднано й фрагментарно покривають тільки явно видимі проблеми; інформаційні процеси ніби і контролюються, але далеко не всі, які варто було б відстежувати. Внаслідок цього виходить як за Райкіним – гудзики пришиті відмінно, кишені на місці, але костюм при цьому "якийсь не такий".

Щодо перспектив удосконалення системи ІБ, то тут можна констатувати таке: фахівцям з відділу ІТ і служби ІБ вдалося виявити декілька сучасних проблем, але на горизонті виникають нові, серед яких – посилення ролі державних органів управління та посилення регулятивних вимог щодо управління ІБ загалом [10]. Якщо найближчим часом керівники компаній не

приймуть заходів щодо розроблення всеосяжної системи ІБ, наслідки сучасних і майбутніх проблем тільки додадуть джерел загроз ІБ в майбутньому.

Таким чином, використання наявних ІТ в повсякденній діяльності різних компаній значно підвищує ефективність виробничих процесів, зменшує затрати на їх проведення, проте водночас зумовлює виникнення нових загроз ІБ для успішного їх функціонування. Отже, ІБ фактично відображається у ступені захищеності важливої для компанії інформації від впливу дій випадкового або навмисного характеру, які можуть завдати збитків компанії. Оптимальним варіантом забезпечення ІБ компанії є дотримання систематичного поєднання правових, організаційних і програмно-технічних методів у процесі управління ІБ.

Висновки:

1. З'ясовано, що проблема забезпечення інформаційної безпеки (ІБ) будь-якої компанії є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій (ІТ), яка супроводжується постійними інформаційними загрозами – як зовнішніми, так і внутрішніми. Тому керівники служб ІБ мають прийняти як аксіому твердження про те, що звичайна оперативність реагування на сучасні загрози ІБ вже не є достатньою для їх попередження чи знешкодження з найменшими втратами.

2. Встановлено, що поява нових ІТ відкривають перед компаніями не тільки небачені можливості, але й піддають їх потенційним загрозам з невідомих раніше джерел. Хмарні комп'ютерні технології як і раніше є головним джерелом інновацій в сучасному інформаційному середовищі: за останні декілька років кількість компаній, які використовують хмарні обчислення, збільшилася майже удвічі.

3. Виявлено, що заплановане збільшення бюджету на удосконалення системи ІБ виявиться ефективним тільки в разі належного розподілу обов'язків між відповідальними за прийняття рішень. У багатьох компаніях питанням забезпечення ІБ як і раніше займаються інформаційно-технологічні відділи. Оскільки забезпечення ІБ починає виходити за рамки традиційних можливостей ІТ, в даний час потрібно приймати рішення про вибір дещо інших інструментів, процесів і методів моніторингу джерел загроз ІБ, оцінювання ефективності роботи персоналу служби ІБ, пошуку прогалин у системі ІБ, що і визначає потребу перерозподілу відповідальності.

Література

1. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій / Г.Я. Аніловська. [Електронний ресурс]. – Доступний з http://nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf

2. Бєгун А.В. Інформаційна безпека / А.В. Бєгун. – К. : Вид-во КНЕУ, 2008. – 280 с.

3. В 63% организаций отсутствует архитектура системы безопасности. [Электронный ресурс]. – Доступный с http://www.cnews.ru/news/2012/11/01/v_63_organizaciy_otsutstvuet_arhitektura_sistemy _bezopasnosti_508436

4. Герасименко О.В. Інформаційна безпека підприємства: поняття та методи її забезпечення / О.В. Герасименко, А.В. Козак. [Електронний ресурс]. – Доступний з http://intkonf.org/ken-gerasimenko-ov-kozak-av-informatsiyna-bezpeka-pidpriemstva-ponyattya-ta-metodi-yiyi-zabezpechennya/

5. Глобальное исследование информационной безопасности. [Электронный ресурс]. – Доступный с http://www.gosbook.ru/node/64161

6. Глобальное исследование инцидентов внутренней информационной безопасности. [Электронный ресурс]. – Доступный с http://www.securitylab.ru/analytics/291018.php

7. Гриджук Г.С. Систематизація методів інформаційної безпеки підприємства / Г.С. Гриджук. [Електронний ресурс]. – Доступний з http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf

8. Компании ищут способы оперативного реагирования на современные угрозы и больше не могут обеспечивать информационную безопасность путем решения отдельных задач. [Электронный ресурс]. – Доступный с http://www.ey.com/RU/ru/Newsroom/News-releases/Press-Release---2012-10-29-2

9. Мониторинг утечек информации. [Электронный ресурс]. – Доступный с http://www.infowatch.ru/analytics/leaks_monitoring

10. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко. [Електронний ресурс]. – Доступний з http:// nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

Кунинец А.И., Грыцюк Ю.И. **Информационные угрозы и проблемы обеспечения информационной безопасности промышленных компаний**

Рассмотрены причины возникновения современных информационных угроз и проблемы обеспечения информационной безопасности (ИБ) промышленных компаний. Выяснено, что проблема обеспечения ИБ любой компании чрезвычайно актуальна на современном этапе развития информационных технологий (ИТ), она сопровождается постоянными информационными угрозами – как внешними, так и внутренними. Поэтому руководители служб ИБ должны принять как аксиому утверждение о том, что обычная оперативность реагирования на современные угрозы ИБ уже не является достаточной для их предупреждения или обезвреживания с наименьшими потерями.

Ключевые слова: информационные угрозы, информационная безопасность, информационные технологии, источники угроз, промышленная компания.

Кипупес А.І., Grycyuk Yu.I. **Information threats and issues of information security of industrial companies**

The reasons for the emergence of modern information threats and problems of information security (IS) manufacturing companies. It was found that the issue of information security of any company is extremely topical at the present stage of development of information technology (IT), followed by constant information threats – both external and internal. Therefore, security service managers must take for granted the claim that the usual quick response to modern threats IS is no longer sufficient to prevent them or neutralization with minimal losses.

Keywords: information threats, information security, information technology, threat sources, industrial company.

УДК 336.26

Доц. Н.І. Власюк, канд. екон. наук – Львівська КА

ІНТЕГРАЛЬНЕ ОЦІНЮВАННЯ ЙМОВІРНОСТІ БАНКРУТСТВА ПІДПРИЄМСТВ

З використанням математичних методів на базі системи коефіцієнтів оцінювання фінансового стану підприємств проведено інтегральний аналіз ймовірності банкрутства. Запропонована методика дасть змогу на основі аналізу фінансової звітності передбачити фінансову кризу на підприємстві.

Ключові слова: банкрутство, фінансовий стан, модель побудови інтегрального показника, еталонні показники, стандартизація показників, локальні інтегральні показники.

Постановка проблеми. В умовах нестабільного економічного середовища функціонування значної кількості суб'єктів господарювання в Україні відбувається на межі банкрутства. Згідно з інформацією, яка надходить до Державного департаменту з питань банкрутства, протягом 2010 р. порушено 14642 справ про банкрутство підприємств різної форми власності, тоді як у 2009 р. ця кількість становила 15642 справ, тобто відбулось певне зменшення. З них справ про банкрутство державних підприємств та підприємств з державною часткою понад 25 % порушено на 6 % більше, ніж за 2009 р. (204 та 217 відповідно). Станом на кінець 2011 р. загальна кількість підприємств, які перебували у процедурах банкрутства, становила 17178, що на 2536 більше, ніж у 2010 р., та на 1536 – ніж у 2009 р. [5]. Спад національної економіки, посилення конкуренції, збільшення цін на ресурси, зменшення попиту на продукцію та недоліки в управлінні підприємством – основні чинники, які найчастіше призводять до виникнення кризової ситуації на підприємстві. У зв'язку з цим виникає необхідність постійного моніторингу фінансово-економічного стану та діагностики банкрутства суб'єкта господарювання з метою запобігання кризовим явищам на підприємстві.

Аналіз останніх досліджень та публікацій. Зарубіжна та вітчизняна практика характеризується різноманітними підходами до діагностики банкрутства підприємства, формами та інструментами її реалізації [1-4]. Найбільш поширеними для цілей прогнозування банкрутства є багатофакторні дискримінантні моделі. Зокрема, моделі Е. Альтмана, Таффлера і Тішоу, Р. Ліса, Р. Сайфуліна та Г. Кадикова, О. Терещенка та інші. Проте зарубіжні моделі не завжди дають об'єктивну оцінку прогнозування банкрутства підприємств в Україні. Саме тому актуальною є розроблення вітчизняних методик такого прогнозування, що базуються на показниках фінансової звітності підприємств [7].

Метою роботи є уточнення переліку та складу діагностичних індикаторів фінансового стану підприємства та проведення на їх основі інтегральної оцінки прогнозування банкрутства підприємств.

Виклад основного матеріалу. Ефективність функціонування підприємств різних видів економічної діяльності оцінюють за допомогою індикаторів, що характеризують їхній фінансовий стан та його окремі складові (платоспроможність, прибутковість, структуру капіталу, оборотність тощо). Діагностика діяльності підприємства на засадах фінансових індикаторів є найбільш показовою та найпростішою у плані доступу до інформації. Уточнивши попередньо перелік найбільш репрезентативних показників, що характеризують фінансовий стан та результати діяльності суб'єктів господарювання, сформуємо модель для розрахунку інтегрального показника ймовірності банкрутства підприємства, яка включатиме основні етапи (рис.).

Вихідні дані (фінансові індикатори) для побудови матриці (І етап) попередньо згрупуємо:

1 група – показники платоспроможності;
2 група – показники фінансової незалежності;
3 група – показники забезпеченості власним капіталом;
4 група – показники стану та джерел формування основних засобів;
5 група – показники ділової активності.