provide guaranteed survival and development of the national industrial enterprises in the conditions of instability and the growing influence of the environment on the internal parameters of their development.
industrial enterprise, viability, functioning support, development support, stability, reliability, economic security, adaptation

Одержано (Received) 4.11.2016 *Прорецензовано (Reviewed)* 24.11.2016
Прийнято до друку (Approved) 28.11.2016

УДК 351.746:007:658:001.8

О.І. Волот, доц., канд.екон. наук
Чернігівський національний технологічний університет, м. Чернігів, Україна

Методологічні аспекти безпеки інформаційних потоків підприємства

Запропоновано методичне підґрунтя моделі побудови збалансованої системи інформаційної безпеки підприємства, описано взаємозв'язки між інформаційними потоками, визначено загрози інформаційній безпеці підприємства і оцінено вірогідність реалізації даних загроз. Доведено необхідність удосконалення існуючих методів впровадження інформаційних систем в умовах формування інформаційних потоків підприємства.
економічна безпека, модель, інформаційні потоки підприємства

Е.И. Волот, доц., канд. экон. наук
Черниговскийнациональныйтехнологическийуниверситет, г. Чернигов, Украина

Методологические аспекты безопасности информационных потоков предприятия

Предложена методологическая основа модели построения сбалансированной системы информационной безопасности предприятия, описаны взаимосвязи между информационными потоками, определены угрозы информационной безопасности предприятия и оценена вероятность реализации данных угроз. Доказана необходимость усовершенствования существующих методов внедрения информационных систем в условиях формирования информационных потоков предприятия.
экономическая безопасность, модель, информационные потоки предприятия

Постановка проблеми. Зростання ролі інформаційних потоків в діяльності сучасного підприємства обумовлено наступними основними причинами. Перш за все, інформацією, яка є основним джерелом виявлення інтересів, мотивів, ідей та дій усіх учасників зовнішнього середовища, що для економічної безпеки підприємства має важливе значення. Від обсягу, швидкості та якості обробки інформації значною мірою залежить ефективність управлінських рішень, зростає значення методів управління з використанням інформаційних технологій соціальними та економічними процесами, фінансовими і товарними потоками, аналізу та прогнозування розвитку внутрішнього і зовнішніх ринків. Пошук нових методів та моделей побудови збалансованої системи інформаційної безпеки підприємства, які орієнтовані на прийняття ефективних управлінських рішень є одним з першочергових завдань для багатьох промислових підприємств на даному етапі розвитку економіки України, що обумовлює актуальність та доцільність теми дослідження.

Аналіз останніх досліджень і публікацій. Серед праць, котрі присвячені дослідженням проблем забезпечення інформаційної безпеки підприємств, особливе місце займають теоретичні розробки О.В. Ареф'євої [1], В.В. Буряковського [2], М.І. Камлика [3], В.Л. Ортинського [4], С.М. Шкарлета [5] та інших. Однак, враховуючи наявні теоретичні розробки, проблеми удосконалення в розрізі інформаційної безпеки інформаційних потоків на підприємствах розглянуті недостатньо.

Постановка завдання. Метою статті є обґрунтування загальних методологічних підходів формування моделі побудови збалансованої системи інформаційної безпеки підприємства, а також визначення загроз цій системі і оцінка вірогідності реалізації даних загроз.

Викладення основного матеріалу. На сьогоднішній день своєчасна та об'єктивна інформація є важливим фактором виробництва, який розглядають як один з основних ресурсів розвитку суспільства. Широкі можливості інформаційних систем та технологій дозволяють автоматизувати процеси моніторингу та управління державними, економічними, соціальними, оборонними та іншими об'єктами і системами, отримувати, накопичувати, обробляти і передавати інформацію про ці процеси практично з будь-якої необхідною швидкістю, в будь-якій кількості.

Інформаційна безпека підприємства – стан захищеності інформаційного середовища підприємства, який забезпечує його формування, використання та розвиток. Такі складові інформаційного середовища України, як інформаційні ресурси (у тому числі й інформаційні технології) та інформаційна інфраструктура (як матеріально-технічна основа створення, розповсюдження і використання інформаційних ресурсів), які входять до складу національного інформаційного потенціалу, сьогодні значною мірою визначають рівень і темпи соціально-економічного, науково-технічного і культурного розвитку країни [6].

Можна виділити цілу низку джерел загроз інформаційній безпеці сучасного підприємства:

- протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації;
- порушення встановлених регламентів збору, обробки та передачі інформації;
- навмисні дії та ненавмисні помилки персоналу інформаційних систем;
- помилки в проектуванні інформаційних систем;
- відмова технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах тощо [7].

Поняття «інформаційні потоки», в загальному розумінні, є сукупністю циркулюючих на підприємстві відомостей, необхідних для підготовки, прийняття та контролю реалізації управлінського рішення. Такі відомості можуть існувати у вигляді усних повідомлень та паперових або електронних документів, які на практиці формуються у систему усного інформування (у формі доповідей, засідань, нарад, бесід з підлеглими, консультантами тощо), систему паперового документообігу та комп'ютеризовану (автоматизовану) інформаційну систему відповідно [8]. Звідси очевидно, що інформаційні потоки на підприємстві здійснюються за допомогою основних видів інформаційних технологій: усної, письмової та комп'ютеризованої (тобто комп'ютерної та телекомунікаційної технологій). Як правило, комп'ютерні інформаційні системи частково замінюють або дублюють усну та паперову систему інформування.

На практиці цей аналіз здійснюється у декілька етапів. Перший – обстеження, другий – побудова й аналіз інформаційної структури організаційної або виробничої системи. Основу для проектування інформаційної системи становлять результати обстежень інформаційних потоків і документообігу підприємства. Таким чином, інформаційна безпека інформаційних потоків підприємства є невід'ємною складовою ефективної діяльності підприємства.

Головною метою будь-якої системи інформаційної безпеки підприємства є забезпечення стійкого функціонування підприємства, запобігання погрозам його безпеці, захист законних інтересів від протиправних посягань, недопущення

розкрадання фінансових коштів, розголошування, втрати, спотворення і знищення службової інформації, забезпечення нормальної виробничої діяльності всіх підрозділів об'єкту. Досягнення заданих цілей можливе в ході вирішення таких основних завдань [9]:

– виділення і віднесення інформації з найбільш важливих інформаційних потоків до категорії обмеженого доступу, тобто комерційної таємниці;

– прогнозування і своєчасне виявлення загроз безпеці інформаційним ресурсам, причин і умов, які ведуть до фінансового, матеріального і морального збитку, порушення нормального функціонування і розвитку підприємства;

– створення умов функціонування з найменшою вірогідністю реалізації загроз безпеці інформаційним ресурсам і нанесення різних видів збитку;

– створення механізму й умов оперативного реагування на загрози інформаційній безпеці і прояви негативних тенденцій у функціонуванні, ефективне припинення посягань на ресурси на основі правових, організаційних і технічних засобів забезпечення безпеки;

– створення умов для максимально можливого відшкодування і локалізації збитків, які спричиняються неправомірними діями фізичних і юридичних осіб, послаблення негативного впливу наслідків порушення інформаційної та економічної безпеки на досягнення стратегічних цілей.

На рисунку 1 представлена модель побудови системи інформаційної безпеки підприємства.

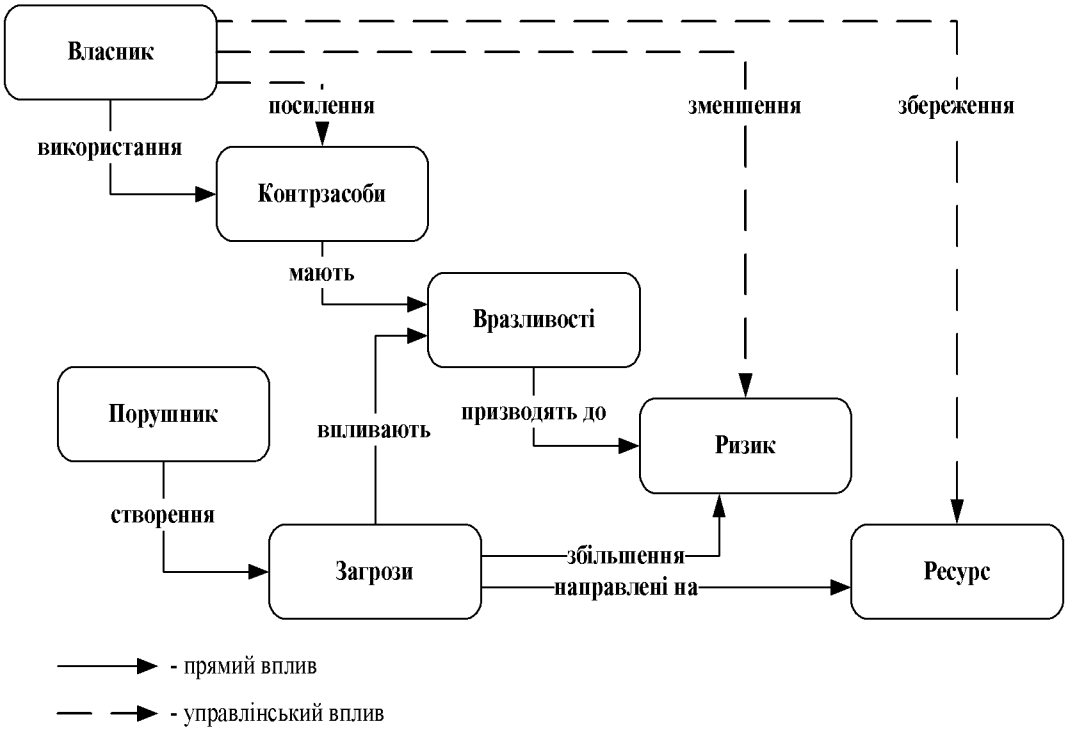

Рисунок 1 – Модель побудови системи інформаційної безпеки підприємства

Джерело: розроблено автором на основі [4].

Модель відповідає спеціальним нормативним документам з забезпечення інформаційної безпеки, прийнятим міжнародним стандартам ISO/IEC 15408 "Інформаційна технологія – методи захисту – критерії оцінки інформаційної безпеки", стандарту ISO/IEC 27002 "Управління інформаційною безпекою" і враховує тенденції розвитку вітчизняної нормативної бази щодо питань інформаційної безпеки [10, 11].

Представлена модель інформаційної безпеки – це сукупність об'єктивних зовнішніх і внутрішніх чинників та їх вплив на інформаційну безпеку на підприємстві і на збереження матеріальних та інформаційних ресурсів. До цих об'єктивних чинників належать наступні:

– загрози інформаційній безпеці, які характеризуються вірогідністю виникнення, і реалізації загроз;

– вразливості інформаційної системи або системи контрзаходів, які впливають на вірогідність реалізації загроз для підприємства;

– економічний ризик – чинник, що відображає можливі збитки підприємства в результаті реалізації загрози інформаційній безпеці: витік інформації і неправомірне її використання, і як наслідок, вірогідні прямі та непрямі фінансові збитки.

Принципами побудови збалансованої системи інформаційної безпеки підприємства є:

– аналіз ризиків у сфері інформаційної безпеки,

– визначення оптимального рівня ризику для підприємства на основі заданого критерію,

– вибір таких контрзаходів, які можуть забезпечити досягнення заданого рівня ризику.

Така методика дає змогу проаналізувати вимоги щодо гарантування інформаційної безпеки підприємства. Для досягнення поставленої мети необхідне вирішення певних завдань:

– розподілення інформації за рівнями доступу;

– прогнозування і своєчасне виявлення загроз безпеці інформаційних ресурсів;

– створення умов, при яких найменш вірогідна загроза безпеці інформаційних ресурсів;

– створення механізму і умов оперативного реагування на загрози інформаційній безпеці, забезпечення проведення робіт в короткі терміни;

– створення механізму і умов для максимально можливого відшкодування і локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб;

– забезпечення оптимального вибору заходів протидії;

– оцінка ефективності контрзаходів, порівняння різних варіантів.

Для побудови збалансованої системи інформаційної безпеки підприємства спочатку передбачається провести аналіз ризику в області безпеки інформаційних потоків. Потім визначити оптимальний рівень ризику для підприємства на основі заданого критерію. Система інформаційної безпеки підприємства повинна бути побудова таким чином, щоб досягти заданого рівня ризику.

При побудові моделі необхідно враховувати взаємозв'язки між ресурсами: для виділених ресурсів визначається їх цінність як з точки зору можливих фінансових збитків, так і з точки зору можливого збитку репутації підприємства, дезорганізації його діяльності, нематеріального збитку від розголошування конфіденційної інформації тощо. Далі необхідно описати взаємозв'язки між інформаційними потоками, визначити загрози інформаційній безпеці підприємства і оцінити вірогідність реалізації даних загроз.

Запропонований методичний підхід дозволяє:

– повністю проаналізувати і документально оформити вимоги, пов'язані із забезпеченням інформаційної безпеки підприємства;

– уникнути витрат на зайві заходи безпеки, які можливі при суб'єктивній оцінці ризику;

– надати допомогу в плануванні і здійсненні захисту на всіх стадіях життєвого циклу інформаційної системи підприємства;

– забезпечити проведення робіт в стислі терміни;

– представити обґрунтування для вибору засобів протидії та інші.

На основі побудованої моделі можна обґрунтовано вибрати систему контрзаходів, які знижують ризики до допустимих рівнів і мають найбільшу економічну ефективність. Частиною системи контрзаходів є рекомендації щодо проведення перевірок ефективності системи захисту.

Забезпечення вимог до інформаційної безпеки припускає відповідні заходи на всіх етапах життєвого циклу системи інформаційних потоків підприємства. Перелік вимог до системи інформаційної безпеки формується в технічній документації, до якої належать такі документи: ескізний проект, план захисту, який містить набір вимог до інформаційної безпеки підприємства, профілі економічного захисту тощо.

У загальному вигляді розробка технічної документації включає:

– уточнення функцій захисту;

– вибір архітектурних принципів побудови системи інформаційної безпеки;

– розробку логічної структури системи економічної безпеки;

– уточнення вимог функцій забезпечення ефективності;

– розробку методики і програми випробувань на відповідність вимогам [9].

На останньому етапі проводиться оцінка досягнутої захищеності через оцінку ступеня гарантії інформаційної безпеки підприємства, яка ґрунтується на оцінці, з якою після виконання рекомендованих заходів можна довіряти системі інформаційних потоків підприємства.

Базові положення даної методики припускають, що ступінь гарантії виходить з ефективності зусиль при проведенні оцінки безпеки.

Збільшення зусиль оцінки припускає:

– значне число елементів інформаційного середовища об'єкта, що беруть участь у процесі оцінки;

– розширення типів проектів і описів деталей виконання при проектуванні системи забезпечення безпеки;

– строгість, що полягає в застосуванні більшого числа інструментів пошуку і методів, направлених на виявлення менш очевидних уразливостей або на зменшення вірогідності [9].

Висновки і перспективи подальших досліджень. Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, обробки, зберігання, пошуку та надання користувачам. Ці технології мають враховувати особливості інформації, які роблять її цінною, а також давати змогу користувачам різних категорій ефективно працювати з інформаційними ресурсами.

У цілому розглянутий методичний підхід дозволяє оцінити або переоцінити рівень поточного стану інформаційної безпеки інформаційних потоків підприємства, виробити рекомендації по забезпеченню інформаційної безпеки підприємства, знизити потенційні витрати підприємства шляхом підвищення стійкості системи інформаційних потоків, розробити концепцію і політику інформаційної безпеки підприємства. А також запропонувати плани захисту внутрішніх і зовнішніх інформаційних потоків, які створюються на підприємстві та передаються по різного роду каналах зв'язку і захистити інформацію підприємства від умисного спотворення, несанкціонованого доступу, копіювання або використання, що є перспективою подальших досліджень.

Список літератури

1. Ареф'єва О.В. Планування економічної безпеки підприємств [Текст] / О.В. Ареф'єва ; Європейський ун-т. - К. : Вид. Європейського ун-ту, 2004. – 169 с.
2. Буряковський В.В. Національна економіка [Текст] : навч. посібник для студ. вищих навч. закл. / В.В. Бурковський ; Дніпропетровський національний ун-т. – Д. : Наука і освіта, 2007. – 310 с.
3. Камлик М.І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект [Текст] : навч. посібник / М.І. Камлик. – К. : Атіка, 2005. – 432с.
4. Ортинський В.Л. Економічна безпека підприємств, організацій та установ / В.Л. Ортинський, І.С. Керницький, З.Б. Живко – К. : Правова єдність, 2009. – 544 с.
5. Шкарлет С.М. Економічна безпека підприємства: інноваційний аспект [Текст] : моногр. / С.М. Шкарлет. – К. : Книжкове видавництво Національного авіаційного ун-ту, 2007. – 436 с.
6. Бабінська М.С. Проблеми інформаційної безпеки України / М.С.Бабінська // Вісник Наукового інформаційно-аналітичного центру НАТО Прикарпатського національного університету ім. В.Стефаника. – Івано-Франківськ: Прикарпатський національний університет ім. В.Стефаника, 2009. – Вип.2. – С. 11–15.
7. Литвинюк А.А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування / А.А. Литвинюк // Вісник Центральної виборчої комісії. – Київ: Центральна виборча комісія, 2008. – Вип.4(14). – С. 18–21.
8. Бутко М.П. Моделювання інформаційного забезпечення в процесі прийняття управлінського рішення / М.П. Бутко, О.І.Волот // Зб. наук. пр. Науково-дослідного економічного інституту «Формування ринкових відносин в Україні». – Київ: НДЕІ, 2011. – Вип.10. – С. 3–7.
9. Єрмоленко О.А. Економічна безпека системи інформаційних потоків підприємства [Текст] / О.А. Єрмоленко // Економіка: проблеми теорії та практики : зб. наук. праць / ДНУ. – 2009. – Т. 1. Вип. 253. – С. 82–89.
10. ISO/IEC 15408:2008 – Information technology – Security techniques – Evaluation criteriafor IT security [Електронний ресурс] – Режим доступу: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46414.
11. ISO/IEC 27002:2005 – Information technology – Security techniques – Code of practice for information security management [Електронний ресурс] – Режим доступу: http://www.iso.org/iso/catalogue_detail?csnumber=50297

References

1. Arefieva, O.V. (2004). *Planuvannia ekonomichnoi bezpeki pidpriemstv [Planning Economic Security of enterprises].* Kyiv: Vydavnytstvo Ievropeiskoho universitetu [in Ukrainian].
2. Buriakovskyi, V.V. (2007). *Natsionalna ekonomika [National economy].* Dnipropetrovsk: Naukaiosvita [in Ukrainian].
3. Kamlik, M.I. (2005). *Ekonomichna bezpeka pidpriemnitskoi diialnosti. Ekonomiko-pravovyi aspect [The economic security of entrepreneurship. Economic and legal aspects].* Kyiv: Atika [in Ukrainian].
4. Ortynskyi, V.L. (2009). *Ekonomichna bezpeka pidpriemstv, orhanizatsii ta ustanov [The economic security of enterprises, organizations and institutions].* Kyiv: Pravovaednist [in Ukrainian].
5. Shkarlet, S.M. (2007). *Ekonomichna bezpeka pidpriemstva: innovatsiinyi aspect [The economic security of the enterprise: innovative aspects].* Kyiv: Vydavnytstvo Natsionalnooho aviatsiinoho universitetu [in Ukrainian].
6. Babinska, M.S. (2009). Problemy informatsiinoi bezpeky Ukrainy [The problems of information security Ukraine]. *Visnyk Naukovoho informatsiino-analitichnoho tsentru NATO Prikarpatskoho natsionalnoho universitetu im. V.Stefanika - Bulletin of information-analytical center of NATO Carpathian National University. V.Stefanyk, 2,* 11-15 [in Ukrainian].
7. Lytvyniuk, A.A. (2008). Osnovy informatsiinoi bezpeky. Kompleksna systema zakhystu informatsii: struktura, vstanovlennia ta pidtrymka funktsionuvannia [Fundamentals of information security. The complex system of information security: structure, installation and supporting the functioning]. *Visnyk Tsentralnoi vyborchoi komisii - Bulletin of the Central Election Commission, 4(14),* 18-21 [in Ukrainian].
8. Butko, M.P., & Volot, O.I. (2011). Modeluvannia informatsiinogo zabezpechennia v protsesi priiniattia upravlinskogo rishennia [Modeling information support in process making management decisions] *Zbirnyk naukovykh prats Naukovo-doslidnogo ekonomichnogo instytutu "Formuvannua rynkovykh vidnosyn v Ukraini - Collection Scientific Papers of Economic Research Institute "The formation of market relations in Ukraine", 10,* 3-7, [in Ukrainian].
9. Yermolenko, O.A. (2009). Ekonomichna bezpeka systemy informatsiinykh potokiv pidpryiemstva [Economic security of system information flows enterprise]. *Zbirnyk naukovykh prats Donetskogo*

Natsionalnoho universitetu "Ekonomika: problem teorii ta praktyky" - Collection Scientific Papers of Donetsk National University "Economy: problems of theory and practice", 253, Vol. 1, 82-89 [in Ukrainian].
10. ISO/IEC 15408:2008. Information technology. Security techniques. Evaluation criteria for IT security. *www.iso.org.* Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46414 [in Switzerland].
11. ISO/IEC 27002:2005. Information technology. Security techniques. Code of practice for information security management. *www.iso.org.* Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=50297 [in Switzerland].

Olena Volot, Associate Professor, PhD in Economics (Candidate of Economic Sciences)
Chernihiv National University of Technology, Chernihiv, Ukraine

Methodological Aspects of the Security of Information Flows of an Enterprise

The methodological basis of the model for the formation of a balanced system of information security at the enterprise was suggested. The relationship among information flows was described and the threats to the information security of the enterprise were defined. The probability of realization of the threats was estimated.

The presented model of information security is a set of objective external and internal factors and their impact on the information security at the enterprise including safety of material and information resources.

On the whole the methodical approach under consideration allows assessing or overestimating the level of the current state of information security of information flows at the enterprise, to develop recommendations on providing information security of the enterprise and to reduce possible costs of the enterprise by increasing the stability of the system of information flows. The approach also helps to develop the concept and policy of information security of the enterprise and offers protective plans for internal and external information flows which are created at the enterprise and transmitted by different kinds of communication channels protecting information of the enterprise from intentional distortion, unauthorized access, copying or use.

economic security, model, information flows of the enterprise

Одержано (Received) 8.11.2016 *Прорецензовано (Reviewed)* 24.11.2016
Прийнято до друку (Approved) 28.11.2016

УДК 330.341.1:332.122:338.49

Л.М. Фільштейн, доц., канд. екон. наук
В.В. Будулатій
А.І. Бережньова
Кіровоградський національний технічний університет, м. Кропивницький, Україна

Стан розвитку та особливості функціонування інноваційної інфраструктури в Кіровоградському регіоні

Досліджено стан розвитку та особливості функціонування інноваційної структури в Кіровоградському регіоні в контексті необхідності забезпечення реалізації державної регіональної політики та створення системи суб'єктів, здатних забезпечити ефективне здійснення інноваційної господарської діяльності в інтересах всього суспільства. Здійснено критичний аналіз умов функціонування діючих об'єктів інноваційної інфраструктури регіону. Визначені основні напрямки розвитку інноваційної інфраструктури Кіровоградської області.

інноваційна діяльність, інноваційна інфраструктура, бізнес-інкубатор, технопарк, кластер, регіон

Л.Н. Фильштейн, доц., канд. экон. наук
В.В. Будулатий
А.И. Бережнева
Кировоградский национальный технический университет, г. Кропивницкий, Украина

Состояние развития и особенности функционирования инновационной инфраструктуры в Кировоградском регионе