личини ресурсного потенціалу дає змогу швидко і об'єктивно оцінити динаміку та стан розвитку ресурсного потенціалу, проводити моніторинг його за складовими елементами, дозволяє швидко та оперативно реагувати на проблеми діяльності підприємства.

Список літератури:
1. Трегобчук В. Відтворення та ефективне використання ресурсного потенціалу АПК (теоретичні та практичні аспекти) /
1. В. Трегобчук [та ін.] – К. : Інститут економіки НАН України, 2003. – 259 с.
2. Мельник Б.А. Економіка, організація та стратегія розвитку промислового птахівництва в Україні / Б.А. Мельник – Київ : «ПоліграфІнко», 2006. – 270 с.
3. Статистичний збірник «Тваринництво України 2013» / За редакцією Н.С. Власенко [Електронний ресурс]. Режим доступу : http://ukrstat.org/druk/publicat/kat_r/publ7_r.htm. Назва з екрану.
4. Клейнер Г.Б. социально-экономические системы и сбалансированное управление [Електронний ресурс]. – Режим доступу : http://www.kleiner.ru/skrepk/spb-2005.pdf Назва з екрану.
5. Ковалева А.М. Финансы фирмы : учебник. 2-е изд. доп. и перераб. / А.М. Ковалева, М.Г. Лапуста, Л.Г. Скамай. – М. : Финансы и статистика, 1997. – 384 с.
6. Балабанов И.Т. Основы финансового менеджмента. Как управлять капиталом? / И.Т. Балабанов. – М. : Финансы и статистика, 1997. – 384 с.

Вяткина Т. Г.
Луганский национальный аграрный университет

ОЦЕНКА ВЕЛИЧИНЫ РЕСУРСНОГО ПОТЕНЦИАЛА ПРЕДПРИЯТИЙ ПТИЦЕВОДЧЕСКОЙ ОТРАСЛИ

Резюме
В статье обобщены характеристики ресурсного потенциала предприятия. Раскрыто экономическое содержание ресурсного потенциала, опирающегося на внутренние, внешние факторы, взаимодействие элементов материальной и нематериальной сферы. Предложена методика оценки величины ресурсного потенциала предприятий птицеводческой отрасли.
Ключевые слова: ресурсный потенциал, внутренняя среда, внешняя среда, показатели оценки ресурсного потенциала.

Viatkina T. G.
Lugansk National Agrarian University

EVALUATING THE CAPACITY OF RESOURCE POTENTIAL OF POULTRY INDUSTRY ENTERPRISES

Summary
This paper summarizes the characteristics of the resource potential of the company. The economic content of the resource potential, which is based on internal, external factors, interaction elements of material and non-material sphere is discovered. It proposed the method of estimation of resource potential businesses poultry industry.
Key words: resources, internal environment, external environment, index of evaluation of resource potential.

УДК 65.012.8:001.102

Ганущак Т. В.
Університет економіки та права «КРОК»

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ТА УМОВИ ЇЇ ЗАБЕЗПЕЧЕННЯ

У статті досліджено інформаційну безпеку підприємства. Дано визначення поняттям «інформація», «інформаційна безпека підприємства», «ризик», «загроза». Визначено основні заходи у забезпечені інформаційної безпеки підприємства. Систематизовано заходи попередження комп'ютерних злочинів.
Ключові слова: підприємство, інформація, інформаційна безпека підприємства, загроза, ризик, комп'ютерні злочини.

Постановка проблеми. В умовах фінансово-економічної кризи сьогодення вітчизняні підприємства функціонують при невизначеності зміни кон'юнктури ринку, недосконалості фінансово-економічного й організаційно-правового механізму забезпечення економічної безпеки підприємства, а зокрема і її інформаційної складової. Рівень загроз та ризиків інформацій безпеці підприємства постійно зростають. Особливо це пов'язано з розвитком сучасних технологій, численними інформаційними злочинами, шпигунством, промисловим шпіонажем. Господарюючі суб'єкти взаємодіють з великою кількістю контрагентів, які прагнуть реалізувати власні інтереси, і є великими загрозами зовнішнього середовища, які намагаються законним та незаконним

шляхом отримати інформацію про фінансовий стан підприємства, плани на перспективу розвитку, інформацію про процес виробництва та збуту товару, постачальників, партнерів. Часто, переманюючи персонал або влаштовуючи свого працівника, конкуренти намагаються незаконним шляхом отримати інформацію про суб'єкта господарювання. Тому заради забезпечення інформаційної безпеки підприємства необхідно застосовувати превентивні заходи як юридичного так і фінансового характеру. Механізм забезпечення інформаційної безпеки суб'єктів господарювання має формуватися й реалізовуватися на практиці шляхом комплексного розв'язання проблем, пов'язаних із багатофакторністю важко контрольованого й прогнозованого сучасного середовища функціонування системи інформаційної безпеки підприємств. Сучасні умови підприємницької діяльності вимагають створення інформаційно-забезпеченої системи управління. Саме тому питання інформаційної безпеки підприємства є досить актуальним питанням сьогодення.

Аналіз останніх досліджень і публікацій. Забезпечення інформаційної безпеки суб'єкта господарювання як основи захисту його інтересів від екзогенних та ендогенних факторів впливу в сучасних умовах невизначеності є предметом вивчення, про що свідчить значна кількість наукових праць. Дослідженням інформації та інформаційної безпеки підприємства займалися наступні вчені, зокрема: Азрилиян А.М., Башняніна Г.І., Бобров Є.А., Гевко В.Л., Гнилицька Л.В., Григорьєв В.А., Дегтярьова Л.М., Живко З.Б., Живко М.О., Іфтемчук В.С., Качинська А.Б., Керн ицицький І.С., Керницька М.І., Кіслов Б.А., Коваль А.П., Конончук О.В., Кудрицький В.Д., Кудря І.В., Кириченко О.А., Манич М.І., Мелесик С.В., Мельник С.І., Ніколаюк С.І., Ортинський В.Л., Сороковська О.А., Степанова О.М., Франчук В.І., Цуп М.Ю., Цюрюпа С.В., Шевченко С.Ю., Шутак Г.Д. та інші.

Виділення невирішених раніше частин загальної проблеми. Розвинуті країни світу витрачають близько 9-12% від свого прибутку на забезпечення безпеки бізнесу [1, с. 8]. В Україні на підприємствах нерідко забезпечення безпеки підприємства зводиться лише до наявності охоронця.

Незважаючи на значну кількість публікацій, і досі існують нерозв'язані проблеми, пов'язані з забезпеченням інформаційної безпеки суб'єктів господарювання, потребою модернізації існуючих методів і засобів розв'язання завдань у сучасних умовах розвитку фінансово-економічної системи країни. Розв'язання цього завдання ускладнюється через відсутність єдиного наукового системного підходу із врахуванням специфіки галузі досліджуваного суб'єкта виробничо-господарської діяльності та єдиного понятійно-категоріального апарату. Необхідно систематизувати заходи попередження комп'ютерних злочинів.

Мета статті. Головною метою цієї роботи є:

- визначення поняття «інформація»;
- опрацювання підходів до дефініції «інформаційна безпека», «ризик»;
- дослідити процес оцінювання ризиків інформаційної безпеки на підприємстві;
- дати визначення поняттю «загроза»;
- визначити найбільш розповсюджені загрози інформаційній безпеці підприємств;
- систематизувати заходи попередження комп'ютерних злочинів.

Виклад основного матеріалу. В англійській мові слово «information» вперше з'явилося у 1387 р. Сучасного написання це слово набуло в XVI ст. У східнослов'янські мови слово «інформація» прийшло із Польщі у XVII ст. У середині XX ст. інформація стала загальнонауковим поняттям, але досі в науковій сфері воно залишається досить дискусійним. Загальноприйнятного визначення інформація не існує, і воно використовується переважно на інтуїтивному рівні [2, с. 449].

Правовою основою визначення терміну «інформація» є Закон України «Про інформацію» та Цивільний кодекс України.

Так, відповідно до Закону України «Про інформацію», під поняттям «інформація» розуміється будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [3].

Враховуючи тлумачення терміну «інформація» Цивільним кодексом, під цим терміном розуміються документовані або публічно оголошені відомості про події та явища, що мали або мають

Таблиця 1

Підходи до дефініції «інформаційна безпека»

Автор	Зміст підходу
В.С. Іфтемчук, В.А. Григорьєв, М.І. Маниліч, Г.Д. Шутак [7, с. 55]	забезпечення захисту інформації від випадкового чи навмисного доступу осіб, що не мають на це права; інтегральна властивість інформації, що характеризується конфіденційністю, цілісністю і приступністю; захищеність пристроїв, процесів, програм, середовища і даних, що забезпечує цілісність інформації, яка обробляється, зберігається і передається цими засобами; властивість середовища забезпечити захист інформації.
А.Н. Азрилиян [8, с. 56]	забезпечення захисту інформації від випадкового чи навмисного доступу осіб, які не мають на це право; інтегральна властивість інформації, яка характеризується конфіденційністю, цілісністю і доступністю; захист приладів, процесів, програм, даних, середовища, що забезпечує цілісність інформації, яка обробляється, зберігається і передається цими засобами; властивість середовища забезпечувати захист інформації.
С.І. Мельник, М.Ю. Цуп [9]	це стан захищеності інформаційного середовища організації від внутрішніх та зовнішніх загроз. Зміст інформаційної безпеки полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності підприємства. Відповідні служби виконують при цьому певні функції, які в сукупності характеризують процес створення та захисту інформаційної складової економічної безпеки.
О.М. Степанова, Л.М. Дегтярьова [10]	захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних дій природного або випадкового характеру, які можуть завдати збитку власникам інформаційного ресурсу або користувачам інформації і підтримуючої інфраструктури
О.А. Сороковська, В.Л. Гевко [11, с. 33-34]	суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності.
Д.В. Кіслов [12, с. 40]	стан захищеності від впливу та використання інформації, що може гальмувати чи перешкоджати їх використанню та реалізації.

місце у суспільстві, державі та навколишньому середовищі [4, ст. 200].

Існує безліч тлумачень терміну «інформація» вченими, але дослідимо деякі з них.

Зокрема, Цюрюпа С.В. вважає, що інформація – це один з найважливіших ресурсів разом з матеріальними, енергетичними та людськими ресурсами [5, с. 231].

Кортич Б.А. користується думкою, що інформація – це певні відомості, сукупність яких-небудь даних, знань [6, с. 41].

Обидва трактування мають право на існування, не заперечують один одного, а лише доповнюють.

В умовах постійного розвитку інформаційного середовища підприємства необхідним є забезпечення його інформаційної безпеки на всіх стадіях діяльності. Існують різні підходи вчених-економістів щодо терміну «інформаційна безпека» (таблиця 1).

Аналізуючи наведені погляди на дефініції «інформаційна безпека», слід відзначити, що вони ні в якому разі не суперечать один одному, а лише розглядають різні аспекти забезпечення інформаційної безпеки, та фактично доповнюють один одного.

Така кількість підходів тлумачення інформаційної безпеки свідчить про роль, яку вона виконує в процесі ефективного розвитку підприємства, тому що забезпечує захист інформації у всіх сферах діяльності підприємства.

Особливу роль у забезпеченні інформаційної безпеки суб'єкта господарювання є мінімізація ризиків щодо втрати інформаційних потоків на підприємстві. Тому доцільно розглянути економічну категорію «ризик» (таблиця 2).

Підвищені вимоги до інформаційної безпеки припускають відповідні заходи на всіх етапах життєвого циклу інформаційних технологій. Планують ці заходи після закінчення етапу аналізу ризиків і вибору контрзаходів. Обов'язковою складовою частиною цих планів є періодична перевірка відповідності існуючого режиму інформаційної безпеки політиці безпеки, сертифікації інформаційної системи (технології) на відповідність вимогам певного стандарту безпеки. Мета процесу оцінювання ризиків полягає у визначенні їх характеристик в інформаційній системі та її ресурсах. На основі таких даних обирають необхідні засоби управління інформаційною безпекою.

Процес оцінювання ризиків складається з кількох етапів: опис об'єкта і заходів захисту; ідентифікація ресурсу та оцінювання його кількісних показників (визначення потенційної негативної дії на бізнес); аналіз загроз інформаційній безпеці; оцінювання слабких місць; оцінювання існуючих і перспективних засобів гарантування інформаційної безпеки; оцінювання ризиків [18].

Ключовим фактором у забезпеченні інформаційної безпеки підприємства є його персонал. Основними заходами при роботі з яким є: проведення аналітичних процедур при прийомі і звільненні; навчання і інструктаж практичним діям по захисту інформації; контроль за виконанням вимог по захисту інформації, стимулювання відповідального відношення до збереження інформації та ін. [19].

Діяльність будь-якого підприємства підлягає впливу різних загроз. Чим більше підприємство, тим більше загроз як екзогенного, так і ендогенного характеру на діяльність цього суб'єкта господарювання.

На всіх рівнях безпеки необхідно виявити загрозу чи загрози, які негативно впливають чи вплинуть у майбутньому на діяльність об'єкта. Загроза – підтверджена доказами очевидна сутність збитку завданого державі, галузі економіки чи підприємству [20, с. 622].

Загроза – це дія дестабілізуючих природних і суб'єктивних чинників, пов'язаних з недобросовісною конкуренцією, порушенням законів, норм, які можуть спричинити потенційні або реальні втрати, що здатні викликати небезпеку для корпоративної системи [21, с. 149].

Найбільш розповсюдженими і небезпечними загрозами доступності є ненавмисні помилки постійних користувачів, операторів, системних адміністраторів та інших осіб, що обслуговують інформаційні системи. Саме такі помилки зазвичай і стають загрозами (неправильно введені дані чи помилка в програмі, що призвела до краху системи), іноді вони створюють слабкі місця, якими можуть скористатися зловмисники. Статистика свідчить, що близько 65% втрат – наслідок ненавмисних помилок. Виходячи з цього, найбільш радикальний спосіб боротьби з ненавмисними помилками – максимальна автоматизація і строгий контроль.

На другому місці за розмірами збитків – крадіжки та підробки. За даними, що обертаються серед фахівців, у 2006 році внаслідок подібних протиправних діянь з використанням персональних комп'ютерів американським організаціям було завдано загальної шкоди у розмірі 1 млрд 882 млн дол. США. Можна припустити, що справжній розмір шкоди набагато більший, оскільки багато фірм зі зрозумілих причин приховують такі інциденти. У більшості розслідуваних випадків винуватцями виявлялися штатні співробітники фірм, добре обізнані з режимом роботи і заходами безпеки [22].

Головним завданням на підприємстві є вчасне виявлення загроз та запобігання їм. Одними із таких завдань керівництва є ряд заходів щодо попередження комп'ютерних злочинів. Їх розмежовують на технічні, організаційні та правові (таблиця 3).

Таблиця 2

Підходи до визначення економічної категорії «ризик»

Назва підходу	Зміст підходу
Фінансовий [13, с. 197; 14, с. 209]	ймовірність настання збитку в результаті проведення яких-небудь операцій у фінансово-кредитній і біржовій сферах, здійснення операцій з цінними паперами, тобто ризику, що випливає з природи цих операцій; значною мірою залежать від обраної ними політики взаємовідносин з боржником після того, як стало відомо, що він опинився у фінансовій кризі.
Медичний [15]	це комплекс дій для вивчення, аналізу та ідентифікації механізмів виникнення явищ, які мають великий вплив на спосіб життя та стан здоров'я людини, з метою запобігання згаданим явищам або протидії їх виникненню.
Виникнення надзвичайної ситуації [16, с. 324]	ймовірність або частота виникнення джерела надзвичайної ситуації, що визначається відповідними показниками
Інноваційний [17, с. 13]	можливість втрат, що виникають внаслідок вкладення підприємством коштів у виробництво нових товарів (послуг), які, можливо, не знайдуть попиту на ринку.

Таблиця 3

Заходи попередження комп'ютерних злочинів

Технічні	Організаційні	Правові
1.захист від несанкціонованого доступу до системи; 2. резервування особливих комп'ютерних підсистем; 3. організація обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок; 4. встановлення устаткування для виявлення і гасіння пожежі; 5. вживання конструктивних заходів захисту від крадіжок, саботажу, диверсій,вибухів; 6. встановлення сигналізації.	1. охорона обчислюваних центрів; 2. ретельний добір персоналу; 3. наявність плану відновлення працездатності обчислювального центру після виходу його з ладу; 4. універсальність засобів захисту від усіх користувачів (в тому числі вищих посадових осіб); 5. виключення випадків проведення особливо важливих робіт лише однією людиною; 6. організація обслуговування обчислювального центру сторонньою організацією або особами, що не зацікавленні у приховуванні фактів порушень засобів центру.	1. захист авторських прав програмістів; 2. контроль за контроль розробниками комп'ютерних систем; 3. удосконалення адміністративного, цивільного, законодавства в галузі комп'ютерного права.

Джерело: складено автором на основі [22, с. 193-194]

Висновки і пропозиції. Дослідивши підходи щодо таких дефініцій, як «інформація», «інформаційна безпека», «загроза», «ризик», можна зробити висновки, що на сьогоднішній день немає єдиної точки зору щодо визначення цих понять. Досліджені визначення доповнюють один одного, не суперечать, мають різне направлення, залежно від застосування в певній галузі. На думку автора, інформація – це письмові, усно передані або збережені на електронних носіях відомості про конкретний досліджуваний об'єкт; інформаційна безпека підприємства – це захищеність всіх видів інформації про діяльність підприємства від несанкціонованого доступу, викрадення, використання та розголошення; загроза – це економічна категорія, яка негативно впливає на діяльність підприємства і є ймовірністю понесення збитку; ризик – це визначена економічна категорія, що носить ймовірнісний характер щодо настання негативної події, яка безпосередньо пов'язана з загрозою та величиною завданого збитку, залежить від зовнішніх та внутрішніх факторів впливу.

На підприємстві необхідно вживати заходи попередження комп'ютерних злочинів: технічні, організаційні, правові. На думку автора, головною загрозою в забезпеченні інформаційної безпеки підприємств є промисловий шпіонаж, непідписання договорів про нерозголошення комерційної таємниці. Необхідно збільшити відрахування з чистого прибутку підприємств на забезпечення інформаційної безпеки підприємств.

Список літератури:

1. Гнилицька Л.В. Теоретико-методологические и прикладные основы обеспечения экономической безопасности субъектов хозяйственной деятельности : монография / Л.В. Гнилицька; Университет экономики и права «КРОК» ; Учебно-научный институт менеджмента безопасности. – К. : Дорадо-друк, 2011. –289 с.
2. Ортинський В.Л. Економічна безпека підприємств, організацій та установ / В.Л. Ортинський, І.С. Керницький, З.Б. Живко, М.І. Керницька, М.О. Живко. – К. : Правова єдність, 2009. – 541 с.
3. Закон України «Про інформацію» [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2657-12.
4. Цивільний кодекс України: чинне законодавство зі змінами та допов. на 1 січн. 2005 р. / Верховна Рада України. – Офіц. вид. Паливода А.В. – К. : 2005. – 336 с. – (Кодекси України)
5. Цюрюпа С.В. Класифікація інформації та способи її відображення для використання в діяльності підприємства / С.В. Цюрюпа // Вчені записки Університету «КРОК» / Вищий навчальний заклад «Університет економіки та права «КРОК». Вип. 1. (1997). – Вип. 33. – К., 2013. – С. 231-235.
6. Генеза ринкової економіки: словник-довідник [авт.-уклад. В.С. Іфтемчук, В.А. Григор'єв, М.І. Маниліч, Г.Д. Шутак] / Г.І. Башняніна В.С. Іфтемчук. – К. : «Магнолія плюс», 2004. – 688 с.
7. Новый экономический словарь / [А.Н. Азрилиян]. – М. : Институт новой экономики, 2006. – 1088 с.
8. Мельник С.І. Інформаційна безпека як складова економічної безпеки підприємства / С.І. Мельник, М.Ю. Цуп [Електронний ресурс]. – Режим доступу : http://www.rusnauka.com/6_PNI_2013/Economics/9_130048.doc.htm.
9. Степанова О.М. Інформаційна безпека в умовах розвитку інформаційної системи / О.М. Степанова, Л.М. Дегтярьова [Електронний ресурс]. – Режим доступу : http://dspace.snu.edu.ua:8080/jkovskaspui/bitstream/123456789/685/1/11.pdf.
10. Сороковська О. А. Інформаційна безпека підприємства: нові загрози та перспективи/ О. А. Сороковська, В. Л. Гевко // Вісник Хмельницького національного університету. – Вип. 2, Т. 2. – 2010. – С. 33-34.
11. Кіслов Д. В. Інформаційні війни : монографія / Д.В. Кіслов. – К. : Київ. нац. торг. екон. ун-т, 2013. – 300 с.
12. Кортич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посібник. – К. : Кондор, 2004. – 384 с.
13. Bobrov Yevgeniy. Finance./Yevgeniy Bobrov. – K. : «KROK» University, 2008. – 220 p.
14. Аналіз ризику – методологічна основа для розв'язання проблем безпеки людини та довкілля [Електронний ресурс] / Визначення та формалізація терміну «ризик» // Режим доступу : http://www.niss.gov.ua/book/kachin/1-3.htm.
15. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / А.Б. Качинський. – К:, 2003. – 472 с.
16. Концепція економічної безпеки антикризового управління економікою України. Науково-аналітична доповідь. – К. : «Дорадо-Друк», 2009. – 64 с.
17. Конончук О.В. Економічна безпека суб'єктів зовнішньоекономічної діяльності України в умовах фінансової кризи. Науково-аналітична доповідь./ О.В. Конончук, В.Д. Кудрицький, І.В. Кудря, С.В. Мелесик / Науковий редактор д.е.н, професор О.А. Кириченко. – К. : Університет економіки та права «КРОК», 2009. – 76 с.
18. Модель побудови системи інформаційної безпеки [Електронний ресурс]. – Режим доступу : http://pidruchniki.ws/1237070651274/ekonomika/model_pobudovi_sistemi_informatsiynoyi_bezpeki.
19. Шевченко С.Ю. Формування системи управління інформаційної безпеки підприємства [Електронний ресурс]. – Режим доступу : kneu.edu.ua/…/ec…/ShevchenkoS.rtf.docx.
20. Коваль А.П. Методичні підходи до оцінювання фінансової безпеки підприємства / А.П.Коваль // Науковий вісник Національного лісотехнічного університету України. – Вип. 7(22). – 2012 – С. 208-212.
21. Франчук В.І. Загрози когнітивної безпеки як об'єкт дослідження // Актуальні проблеми економіки. – 2009. – № 9. – С. 148-154.
22. Поняття та класифікація загроз безпеки інформації [Електронний ресурс]. – Режим доступу : http://pidruchniki.ws/12631113/ekonomika/ponyattya_klasifikatsiya_zagroz_bezpeki_informatsiyi.
23. Ніколаюк С.І. Безпека суб'єктів підприємницької діяльності / Серія бібліотека оперативного працівника / С.І. Ніколаюк, Д.Й. Никифорчук. – К. : КНТ, 2005. – 320 с.

Ганущак Т. В.
Университет экономики и права «КРОК»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ И УСЛОВИЯ ЕЕ ОБЕСПЕЧЕНИЯ

Резюме
В статье исследована информационная безопасность предприятия. Дано определение понятиям «информация», «информационная безопасность предприятия», «риск», «угроза». Определены основные мероприятия в обеспечении информационной безопасности предприятия. Систематизированы мероприятия по предупреждению компьютерных преступлений.
Ключевые слова: предприятие, информация, информационная безопасность предприятия, угроза, риск, компьютерные преступления.

Ganushchak T. V.
University of Economy and Law «KROK»

ENTERPRISE INFORMATION SECURITY AND CONDITIONS OF ITS SOFTWARE

Summary
The article tackles the topic about enterprise information safety. The following definitions of the «information», «information safety», «risk», «threat» have been given. There have been started the main tools in providing the information security at an enterprise, as well as systematized the means of computer crime warnings.
Key words: enterprise, information, information safety of an enterprise, threat, risk, computer crimes.

УДК 339.338.13

Горняк О. В.
Одеський національний університет імені І. І. Мечникова

СТРУКТУРНІ ЗРУШЕННЯ В ЕКОНОМІЦІ ТА РОЗВИТОК СУЧАСНИХ ПІДПРИЄМСТВ

У статті досліджується вплив структурних зрушень в економіці на діяльність сучасних підприємств. Виокремлено такі чинники, як глобалізація, інформаційні технології, Інтернет, що докорінно змінили традиційні підприємства і сприяли розвитку нової фірми, яка відрізняється від них якісно новими рисами.
Ключові слова: глобалізація, інформаційні технології, Інтернет, підприємство, нова фірма.

Протягом останніх десятиліть у національній та світовій економіці відбуваються кардинальні зрушення, що сформували глобальну економіку, яка визначає динаміку і нові риси економічних процесів на мікро-, макро-, мезо- та мегарівнях. В основі якісних змін знаходяться інформаційні технології, їх ресурси, сфери їх використання та можливості, які найбільш повною мірою реалізуються у всесвітній мережі Інтернет.

Глобалізація та інформаційні технології тісно пов'язані між собою, оскільки за допомогою інформаційних технологій значно скорочуються витрати, перш за все, комунікаційні та трансакційні, а також глобалізуються промислове виробництво, сфера послуг, ризики. З іншого боку, глобалізація розширює рамки конкурентного середовища, стимулює нововведення та їх розповсюдження. Особливо суттєвий вплив структурних зрушень відчутний на мікрорівні економіки, оскільки впровадження новітніх технологій відбувається, перш за все, на підприємствах.

Дослідженням структурних зрушень на різних рівнях економіки займаються провідні економісти. Їх здобутки надали можливість розкрити наслідки структурних зрушень на різних рівнях економіки. Це такі економісти, як В. Ардисланов, О. Воробйова, В. Горбатов, Х. Клодт, Е. Кіріченко, О. Лебедєва, Д. Лук'яненко, Т. Фролова, Ю. Уманців та інші.

У той же час потребує подальших досліджень вплив структурних зрушень економіки на підприємства, на їх цілі, функції, напрями діяльності, організаційні структури управління, форми. Тому метою даної статті є розкриття тих аспектів структурних зрушень економіки, які безпосередньо впливають на діяльність і розвиток підприємств, на зміну їх місця та ролі в економічній системі.

Формування нової економіки [1] відбувається завдяки широкій комп'ютеризації господарства, на основі використання засобів зв'язку і телекомунікацій в усіх сферах і на всіх рівнях. Починаючи з середини 90-х років у результаті розробки стандартів цифрових мереж і комерціалізації мережі Інтернет, значно знизилися різного роду витрати і були створені умови для інноваційного розвитку і підвищення ефективності компаній будь-якого розміру [2, с. 47].

Інтернет одночасно є найважливішим рушієм формування нової економіки і її реальним результатом. Створення світової телекомунікаційної мережі є результатом глибоких технологічних та економічних зрушень, і в той же час Інтернет та пов'язані з ним мережеві технології формують середовище для розвитку нової економіки, де змінюються традиційні уявлення про оптимальний розмір фірми, принципи організації виробництва і реалізації продукції на різних рівнях. В реальній економіці використовуються механізми досконалого ринку, а також розширюється простір діяльності природних монополій за рахунок мережевого ефекту. Широке використання інформаційних технологій змінює умови ведення бізнесу і формує