УДК 658.012.2

DOI: https://doi.org/10.32782/2304-0920/6-79-12

Судакова О. І.
Формалюк В. Д.
Черевко В. О.
ДВНЗ «Придніпровська державна академія будівництва та архітектури»

МЕТОДОЛОГІЧНІ АСПЕКТИ ОРГАНІЗАЦІЇ ЕФЕКТИВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Досліджено методологічні аспекти організації ефективної інформаційної безпеки підприємства. Виділено, що детермінантою інформаційної безпеки є положення про захищеність процесів зміни властивостей інформації, а також процесів, пов'язаних із різними формами її обробки. Наведено властивості інформації, які в першу чергу визначають рівень її захищеності, визначаються суб'єктами, що провадять цю інформацію, а також виробленими ними інформаційними продуктами і послугами. Розроблено поняття інформаційного простору, інформаційних (внутрішніх і зовнішніх) полів підприємства, схеми взаємодії, у яких визначено суб'єкти взаємодії, їхні структури й елементи, що піддаються дії загроз, що формують категоріальний базис інформаційної безпеки підприємства. Це дає змогу сформувати єдиний понятійний апарат для його включення в систему визначень економічної безпеки підприємства у цілому.
Ключові слова: інформація, безпека, інформаційний продукт, інформаційна послуга, інформаційна інфраструктура, інформаційний простір економічного об'єкта, підприємство.

Постановка проблеми. В Україні проблема інформаційної безпеки набула особливої значущості, особливо в умовах широкого застосування автоматизованих інформаційних систем, заснованих на використанні комп'ютерних і телекомунікаційних засобах. У зв'язку із цим в Україні розробляється широкий спектр напрямів, пов'язаних зі стратегічними та оперативними завданнями у сфері інформатизації суспільства. Запобігання негативному впливу комплексу зовнішніх і внутрішніх загроз можливе шляхом забезпечення своєчасної реакції на них і створення умов для безпечного розвитку підприємства через ефективне управління економічною безпекою. Це зумовлює системний характер впливу на інформаційну безпеку великої сукупності різних обставини, які мають до того ж різну фізичну природу, переслідують різні цілі і викликають різні наслідки, призводять до необхідності комплексного підходу до вирішення даної проблеми. Задоволення цих вимог можливе на основі інформаційної безпеки у контексті чинників забезпечення стратегії розвитку підприємства за рахунок упровадження її до механізму управління безпекою підприємства.

Аналіз останніх досліджень і публікацій. Сьогодні в науковій літературі значна увага приділяється питанню дослідження методологічних, сутнісних

та змістовних основ інформаційної безпеки. Вагомий внесок у дослідження, пов'язані з проблемами інформаційної безпеки, зробили такі вітчизняні і зарубіжні науковці: Н.С. Безугла, О.Р. Бойкевич, Т.Г. Васильців, Г.Б. Веретенникова, О.А. Грунін, С.О. Грунін, Я.А. Жаліло, А.В. Іванов, А.В. Кірієнко, Р.М. Качалов, Г.Б. Клейнер, Г.В. Козаченко, Т.Б. Кузенко, В.А. Ліпкан, В.Я. Пригунов, А.С. Соснін, А.Г. Шаваєв, В.В. Шликов, В.І. Ярочкін, В.М. Ячменьова та ін. [1–4]. Дослідження вітчизняних та зарубіжних учених показують, що для підприємства більш важливим є не уникнення загрози взагалі, а вміння вчасно і точно її передбачити, щоб ужити необхідних заходів. Це стосується як підприємств, що знаходяться у кризовому стані, так і успішно працюючих підприємств.

Виділення не вирішених раніше частин загальної проблеми. Однак залишилася невирішена проблема – недостатньо розкрито застосування інформаційної безпеки та впровадження її до механізму управління безпекою підприємства.

Мета статті. Головною метою цієї роботи є обґрунтування змісту та ролі інформаційної безпеки у контексті чинників забезпечення стратегії розвитку підприємства за рахунок упровадження її до механізму управління безпекою підприємства.

Виклад основного матеріалу. У зв'язку зі зростаючою роллю інформаційних ресурсів у житті сучасного суспільства, а також через реальність численних загроз із погляду їх захищеності проблема інформаційної безпеки вимагає до себе постійної й більшої уваги.

Аналіз поняття «інформаційна безпека» здійснимо на основі аналізу категорій «безпека» та «інформація».

Згідно з існуючим і досліджуваним у сучасній літературі визначенням безпеки [1–4], у доповнення до розглянутого та у зв'язку з необхідністю виявлення відносин між цими поняттями, виділимо такі аспекти, в яких воно диференціюється:

– психологічний: відчуття, переживання, необхідність захисту життєво важливих потреб та інтересів людей;

– філософський: стан, тенденції розвитку, умови життєдіяльності соціуму, його структур та інститутів, за яких забезпечується їх якісна визначеність;

– юридичний: система встановлених законами гарантій захищеності особистості й суспільства, що забезпечує нормальну життєдіяльність, права та свободу.

Таким чином, є такі детермінанти, що визначають зазначені аспекти: система, захищеність індивіда і суспільства, інтереси та потреба, здатність підтримувати нормальну життєдіяльність, розвивати цю здатність у процесі вдосконалювання структур та інститутів суспільства й економіки у цілому.

Безпека визначається також як відсутність небезпеки або стан, за якого є захист від небезпеки й результатом дії якого є неможливість завдання збитків об'єкту загрози або як «відбивання» загроз та існуючих небезпек, а також їх відсутність. Дане положення вказує на той факт, що мають існувати засоби, що прогнозують і запобігають потенційним загрозам та небезпекам, які наносять збиток особистості або суспільству.

Узагальнення результатів та їх аналіз дають змогу запропонувати таку схему формування змісту «об'єкт безпеки» (рис. 1).

Аналіз наведеної на рис. 1 структури дає змогу виявити особливість, що не відзначалася авторами досліджень у сфері інформаційної безпеки: відсутність зв'язку «суб'єкти загроз – суб'єкти забезпечення безпеки». На практиці вона визначає необхідність проведення превентивних дій (заходів) із боку суб'єктів, що забезпечують безпеку, стосовно суб'єктів загроз (небезпек). Методологічний висновок полягає у необхідності розробляти такі схеми взаємодії, які дадуть змогу зменшувати ризики за рахунок навмисного превентивного впливу на можливі суб'єкти загроз.

Перейдемо до поняття «інформація» як об'єкта впливу загроз, що носять характер внутрішніх і зовнішніх взаємодій об'єкта. Аналіз існуючих досліджень показав, що під інформацією розуміють «інформаційний вимір», що характеризує особистість, індивіда, соціум, суспільство, націю, культуру або ж поле, де функціонують зазначені суб'єкти, яке характеризується як інформаційне та використовується в соціальних і технічних системах. Зрозуміло, що це поле має свої характеристики (параметри), які можуть бути змінені та модифіковані відповідно до механізмів, що зумовлені взаємодією суб'єктів і об'єктів загроз, а також суб'єктів загроз і суб'єктів забезпечення безпеки. Такий підхід дає змогу включити в розгляд нові ідеї безпеки, згідно з якими стабільність інформаційного поля характеризується сферою, яка включає у себе локальне поле взаємодії зазначених суб'єктів.

Уведемо поняття «інформаційний об'єкт» як об'єкт, характер функціонування якого визначається його інформаційними властивостями: інформаційним продуктом, що є результатом діяльності індивіда, суспільства, соціуму, складом і характером інформаційних послуг та інформаційною інфраструктурою, у якій зазначені елементи функціонують.

Відповідно до цього, структуру поняття «інформаційний об'єкт» можна представити у вигляді схеми (рис. 2).

Інформаційна структура, своєю чергою, містить у собі засоби забезпечення виробництва і реалізації інформаційних продуктів та інформаційних послуг окремими суб'єктами й суспільством у цілому, а також засоби забезпечення їх ефективного функціонування в процесах виробництва, відтворення й комунікацій (передачі).

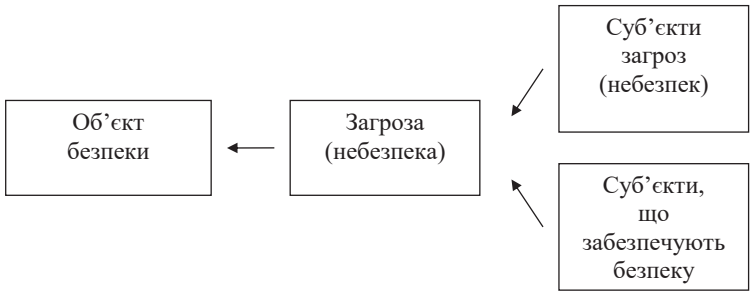

Рис. 1. Схема формування змісту «об'єкт безпеки»

Результатом інформаційних взаємодій може бути одержання інформації з метою власного розвитку, з метою створення умов для розширення власного життєвого простору, а також навмисного (прямого) або ненавмисного впливу на цю інформацію з метою її перекручування та й впливу на інформаційну інфраструктуру одного із суб'єктів інформаційної взаємодії (іншого об'єкта).

Структура зовнішнього інформаційного поля визначається зовнішнім інформаційним образом підприємства, що містить у собі:

– імідж, торговельну марку (бренд), репутацію;

– канали доставки образу: ЗМІ, конференції, PR-акції;

– інформаційні технології: технології, інновації, нововведення;

– диференціацію продукції як засіб розширення свого життєвого простору;

– конкурентоздатність у сфері його діяльності;

– доступ до сучасних міжнародних інформаційних комунікацій.

Структура внутрішнього інформаційного поля визначається існуючою інформаційною інфраструктурою об'єкта.

Таким чином, отримуємо таку структуру поняття «інформаційний простір економічного об'єкта» (рис. 3).

Схему взаємодії інформаційних просторів наведено на рис. 4.

Механізми протидії інформаційній зброї та інформаційним війнам повинні базуватися на посиленні позитивних чинників: інформаційної інфраструктури і зменшенні (нейтралізації) негативних факторів, перепрограмуванні інформаційної інфраструктури на основі таких дестабілізуючих дій, як навмисна модифікація та інтерпретація інформаційних продуктів та їхніх похідних для виділення таких процедур, технологій маніпулювання ними, які дали б змогу досягти переваги в матеріальній сфері.

Це завдання може бути вирішене за допомогою протидії і нейтралізації загроз інформаційних війн, які призвели б до посилення «розтискаючої» сили внутрішніх і зовнішніх інформаційних полів (позитивних чинників) і зменшення впливу «стискаючої» сили з боку інших суб'єктів інформаційної взаємодії (негативних чинників) (рис. 5).

Протидії можуть носити пасивний (нейтралізуючий) і активний характер.

Пасивні протидії можуть містити у собі вирішення таких завдань:

1. Кількісна і/або якісна оцінка поточного та необхідного рівня інформаційної безпеки за заданих рівнів конфіденційності інформації для різних рівнів управління підприємством.

2. Розроблення заходів щодо реінжинірингу системи безпеки інформаційної системи для досягнення її заданого рівня.

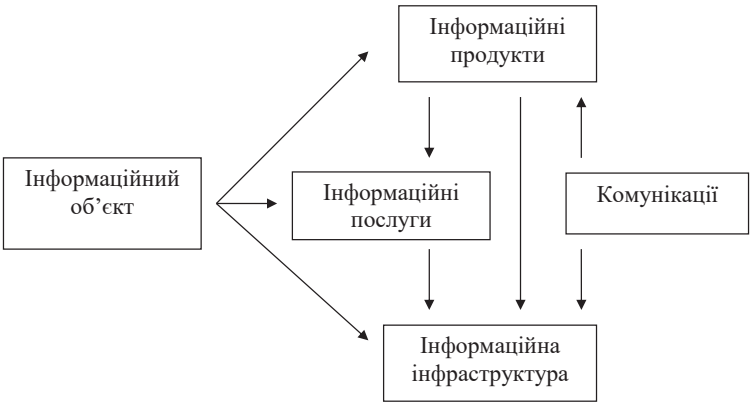

Рис. 2. Структура поняття «інформаційний об'єкт»

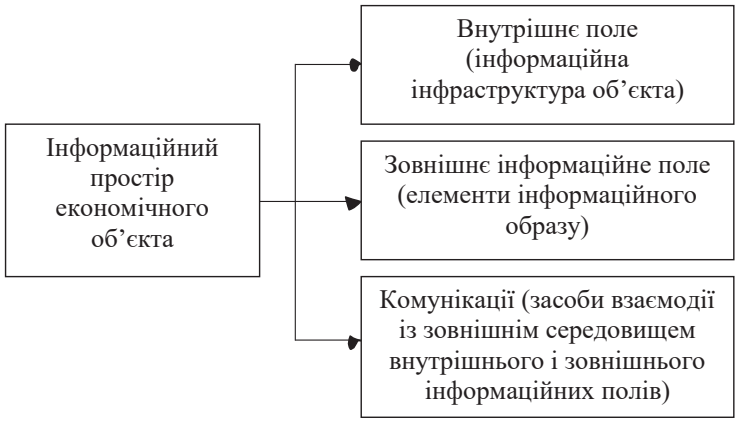

Рис. 3. Структура поняття «інформаційний простір економічного об'єкта»

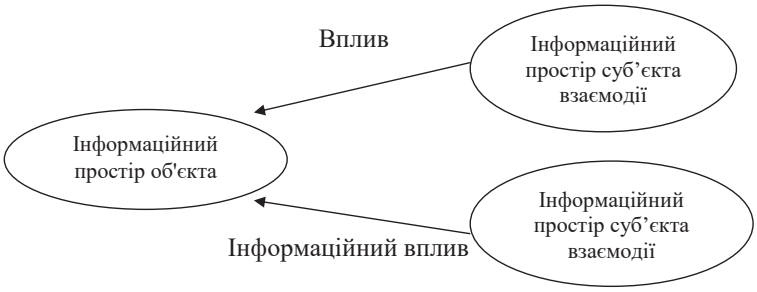

Рис. 4. Схема взаємодії інформаційних просторів суб'єктів інформаційної взаємодії

3. Проведення аудиту і сертифікації компонентів інформаційної системи у цілому на відповідність вимогам та існуючим стандартам інформаційної безпеки.

4. Розроблення зон відповідальності для взаємодії служб і підрозділів зі службою інформаційної безпеки підприємства. Розроблення організаційно-розпорядницької документації з координації і реалізації заходів щодо забезпечення необхідного рівня захисту з припустимими рівнями ризиків.

5. Розроблення політики і концепції забезпечення інформаційної безпеки підприємства на період 3–5 років із визначенням осіб, відповідальних за її реалізацію.

Активні протидії являють собою сукупність методів, засобів, правил надання впливу на інформаційні простори (інформаційні інфраструктури) суб'єктів взаємодії з метою запобігання і нейтралізації інформаційних атак та вироблення власної політики в інформаційній сфері для забезпечення стабільного розвитку підприємства.

До основних завдань у забезпеченні активної протидії належать:

1. Збільшення «своїх» засобів і каналів інформаційного впливу на суспільну думку (захоплення, перехоплення й постановка під свій вплив різних засобів масової інформації).

2. Протидія і розроблення цільових заходів із недопущення витоку інформації.

3. Підвищення іміджу й репутації підприємства за рахунок публікації достовірної й об'єктивної інформації про підприємство в урядових, регіональних засобах масової інформації, що мають високий рівень репутації.

4. Постійна сертифікація наявного та придбаного ліцензійного устаткування, рівень інформа-

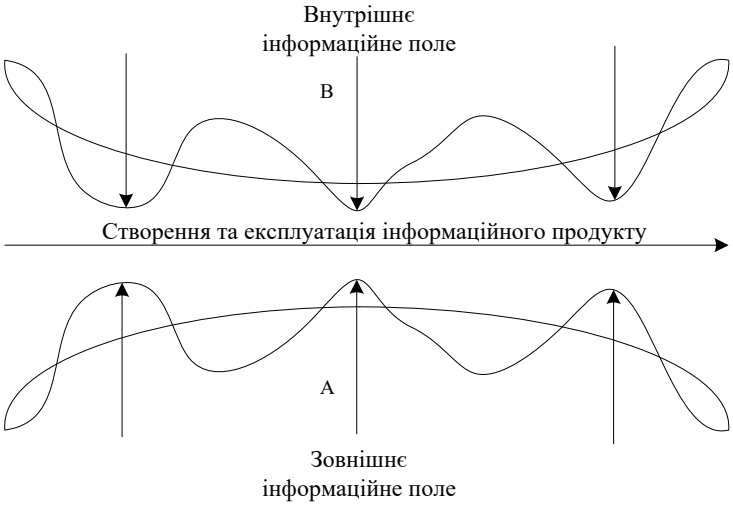

Рис. 5. Схема «стискаючих» (А) і «розтискаючих» (В) сил як чинників негативного/позитивного впливу

ційної безпеки якого гарантується, що дасть змогу забезпечити імідж підприємства як такого, що має високий рівень захищеності.

5. Широке використання засобів контррозвідувальної діяльності для визначення місцезнаходження підслуховуючих пристроїв, засобів радіоелектронної війни, комп'ютерної хакерської діяльності.

6. Постійний контроль точок входу зовнішніх комунікаційних систем в інформаційну систему підприємства, особливо в корпоративних системах, що використовують віддалені комп'ютерні термінали, для виявлення спрямованого інформаційного впливу для порушення їхньої діяльності.

Висновки і пропозиції. Інформаційна безпека визначається такими поняттями, як «інформація», «безпека», «інформаційний продукт», «інформаційна послуга», «інформаційна інфраструктура». Детермінантою інформаційної безпеки є положення про захищеність процесів зміни властивостей інформації, а також процесів, пов'язаних із різними формами її обробки. Властивості інформації, які в першу чергу визначають рівень її захищеності, визначаються суб'єктами, що провадять цю інформацію, а також виробленими ними інформаційними продуктами і послугами. Поняття інформаційного простору, інформаційних (внутрішніх і зовнішніх) полів підприємства, схеми взаємодії, у яких визначено суб'єкти взаємодії, їхні структури й елементи, що піддаються дії загроз, які формують категоріальний базис інформаційної безпеки підприємства. Усе це дає змогу сформувати єдиний понятійний апарат для його включення в систему визначень економічної безпеки підприємства у цілому.

Список використаних джерел:

1. Кавун С.В. Економічна безпека підприємства: інформаційний аспект. Харків, 2014. 312 с.
2. Ковтун О.І. Стратегія підприємства : навчальний посібник. Київ, 2014. 680 с.
3. Судакова О.І., Щеглова О.Ю., Гасенко О.О. Головна характеристика механізму управління економічною безпекою розвитку підприємства. *Науковий вісник Міжнародного гуманітарного університету. Серія «Економіка і* менеджмент». 2017. № 24. С. 11–14.
4. Чумак О.В., Андрющенко І.С. Управління витратами в інформаційно-аналітичній системі підприємств ресторанного господарства : монографія. Харків, 2016. 268 с.

References:

1. Kavun C. V. (2014) EkonomIchna bezpeka pidpriemstva [Economic security of the enterprise]. Kharkiv. (in Ukrainian)
2. Kovtun O. I. (2014) Strategiya pidpriemstva [Strategy of the enterprise]. Kyiv. (in Ukrainian)
3. Sudakova O. I., Scheglova O. Yu., Gasenko O. O. (2017) Golovna harakteristika mehanizmu upravlinnya ekonomichnoyu bezpekoyu rozvitku pidpriemstva [The main characteristic of control mechanism of the economic security enterprise]. *Scientific bulletin of the International Humanitarian University. Series: "Economics and Management"*.no. 24, pp. 11-14.
4. Chumak O. V., Andrjushhenko I. S. (2016) Upravlinnja vytratamy v informacijno-analitychnij systemi pidpryjemstv restorannogo gospodarstva [Cost Management in the Information and Analytical System of Restaurant Enterprises]. Harkiv. (in Ukrainian)

Судакова О. И.
Формалюк В. Д.
Черевко В. А.
ГВУЗ «Приднепровская государственная академия строительства и архитектуры»

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ОРГАНИЗАЦИИ ЭФФЕКТИВНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Резюме
Исследованы методологические аспекты организации эффективной информационной безопасности предприятия. Выделено, что детерминантом информационной безопасности является положение о защищенности процессов изменения свойств информации, а также процессов, связанных с различными формами ее обработки. Приведены свойства информации, которые в первую очередь определяют уровень ее защищенности, определяются субъектами, которые осуществляют эту информацию, а также производимыми ими информационными продуктами и услугами. Разработаны понятия информационного пространства, информационных (внутренних и внешних) полей предприятия, схемы взаимодействия, в которых определены субъекты взаимодействия, их структуры и элементы, подвергающиеся воздействию угроз, которые формируют категориальный базис информационной безопасности предприятия, что позволяет сформировать единый понятийный аппарат для его включения в систему определений экономической безопасности предприятия в целом.
Ключевые слова: информация, безопасность, информационный продукт, информационная услуга, информационная инфраструктура, информационное пространство экономического объекта, предприятие.

Sudakova Oksana
Formaliuk Vladislav
Cherevko Vitaljy
Pridneprovsk State Academy of Civil Engineering and Architecture

THE METHODOLOGICAL ASPECTS OF EFFECTIVE INFORMATION SECURITY OF THE ENTERPRISE

Summary
In Ukraine, the problem of information security received particular importance, especially in the context of widespread use of automated information systems based on the use of computer and telecommunication facilities. Due to the increasing role of information resources in the life of modern society, as well as because of the reality of numerous threats from the point of view of their security, the problem of information security requires constant and greater attention. The systematic nature of the impact on the information security of a large set of different circumstances, which are also of different physical nature, pursuing different goals and causing different consequences, lead to the need for a comprehensive approach to solving this problem. Using the system approach to the organization of processes of providing information security of the enterprise based on the provisions of the theory of information, clarifying the concept of information resource and defining information security as a support system for information resources - the most important task of improving the efficiency of information security of the enterprise. Therefore, the article explores the methodological aspects of the organization of effective information security of the enterprise. It is emphasized that the determinant of information security is the provision on the security of the processes of changing the properties of information, as well as the processes associated with various forms of its processing. The properties of information, which establish the level of its security, are determined by the entities that produce this information, as well as the information products and services produced by them. The concept of information space, information (internal and external) fields of the enterprise, schemes of interaction in which the subjects of interaction are defined, their structures and elements that are exposed to threats that form the categorical basis of information security of the enterprise are developed. This allows us to form a single conceptual system for its inclusion in the structure of definitions of economic security of the enterprise as a whole. The proposed interpretation of the security development strategy is based on the concepts of security of the enterprise information infrastructure, information products and services produced in it, formalization of procedures for identifying threats, and inclusion of organizational mechanisms for managing enterprise security.
Keywords: information, security, information product, information service, information infrastructure, information space of economic object, enterprise.

УДК 65.016.7

DOI: https://doi.org/10.32782/2304-0920/6-79-13

Ткачук М. П.
Коваль Л. А.
Артюшок В. С.
ПВНЗ «Міжнародний економіко-гуманітарний університет
імені академіка Степана Дем'янчука»

УПРАВЛІННЯ ЗМІНАМИ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ СТАЛОГО РОЗВИТКУ ПІДПРИЄМСТВА

У статті досліджено, що об'єктивними умовами забезпечення сталого розвитку підприємства є впровадження системних змін та ефективне управління цим процесом. Установлено, що реальне проведення змін потребує мобілізації матеріальних, фінансових, інформаційних, людських і організаційних ресурсів на здійснення інноваційної діяльності в управлінні суб'єктами господарювання. З'ясовано різні наукові підходи до визначення сутності понять «зміни» та «управління змінами». На основі їх систематизації та узагальнення розглянуто трактування поняття змін із позиції чотирьох його складників: змістовного, процесного, об'єктного й організаційного; уточнено визначення управління змінами як інтеграції процесного, системного і структурного підходів. Досліджено і структуровано ідеологічні, організаційні, кадрові, ресурсні та інформаційні передумови здійснення змін на підприємстві. Доведено, що втіленню змін повинна передувати комплексна діагностика за всіма зазначеними напрямами щодо визначення готовності підприємства до здійснення процесу впровадження змін.
Ключові слова: зміни, управління змінами, інструменти управління змінами, механізми управління змінам, сталий розвиток, інноваційні технології управління.

Постановка проблеми. В умовах ринкових відносин, зростаючої невизначеності та динамічності зовнішнього оточення сучасним інструментом, який здатний забезпечити сталий розвиток підприємства, є ефективне управління змінами в умовах сьогодення. Системне впровадження змін у розвиток підприємства відображається у різних формах: у виробничій і фінансовій діяльності, культурі організації, організаційному забезпеченні, трансформації, реструктуризації, а також у бізнес-плануванні, реінжинірингу, бенчмаркінгу тощо.

Управління змінами в контексті досягнення сталого розвитку підприємства зумовлює необхідність сучасних і комплексних змін у його діяльності, зокрема у технологіях, що використо-