МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЖИТОМИРСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

В.В. Нонік,
А.П. Дикий,
О.С. Дика

ІНФОРМАЦІЙНА МОДЕЛЬ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

МОНОГРАФІЯ

ЖИТОМИР
Вид. О.О. Євенок
2017

УДК 657:005.922.1
ББК 65.052.21
Н81

Рекомендовано до друку Вченою радою
Житомирського державного технологічного університету
Протокол № 12 від 27 березня 2017 р.

Рецензенти:

д.е.н., проф. Л.В. Гнилицька

ДВНЗ "Київський національний економічний університет
імені Вадима Гетьмана"
(м. Київ)

д.е.н., проф. С.З. Мошенський

Житомирський державний технологічний університет
(м. Житомир)

Н81 Нонік В.В., Дикий А.П., Дика О.С. Інформаційна модель управління економічною безпекою суб'єктів господарювання: монографія / В.В. Нонік, А.П. Дикий, О.С. Дика. – Житомир: Вид. О.О. Євенок, 2017. – 248 с.
ISBN 978-617-7483-78-5

Забезпечення захисту облікових даних суб'єкта господарювання є важливою передумовою, спрямованою на забезпечення економічної безпеки підприємства. Особливого значення набуває проблема організації бухгалтерського обліку у формуванні системи економічної безпеки підприємства щодо забезпечення управління обліковою інформацією для прийняття управлінських рішень та належного рівня захисту майна підприємства від прояву негативних чинників з боку різних користувачів.

В монографії сформовано науково обґрунтовані теоретичні засади та практичні рекомендації щодо організації бухгалтерського обліку як інструменту забезпечення економічної безпеки підприємств з метою захисту бухгалтерської інформації та майна підприємства від внутрішніх і зовнішніх загроз, що сприятиме реалізації принципу безперервності діяльності.

Видання призначене для докторантів, аспірантів, магістрів, наукових співробітників, які вивчають проблеми теорії та методології бухгалтерського обліку.

УДК 657:005.922.1
ББК 65.052.21

ISBN 978-617-7483-78-5

ЗМІСТ

ВСТУП

На формування економічної безпеки підприємства впливають зміни, які відбуваються як у зовнішньому, так і внутрішньому середовищі його функціонування. Ці зміни характеризуються нестабільністю та потребують швидкої адаптації підприємств до сучасних умов господарювання з урахуванням чинників невизначеності та нестійкості економічного середовища. Вирішення проблемних питань із забезпечення захисту облікових даних підприємства є важливою передумовою, спрямованою на забезпечення економічної безпеки підприємства як на даному етапі розвитку, так і в майбутньому.

За даними Головного контрольно-ревізійного управління України протягом 2008 р. виявлено порушення, які призвели до втрат фінансових і матеріальних ресурсів на загальну суму понад 3,7 млрд. грн. Загалом протягом І півріччя 2009 р. майже у всіх з перевірених підприємств, установ і організацій усіх форм власності виявлено незаконні та не за цільовим призначенням проведені витрати, недостачі коштів та матеріальних цінностей, а також недоотримання фінансових ресурсів на загальну суму понад 1,6 млрд. грн. З них на 7,2 тис. об'єктів контролю встановлено незаконне і нецільове витрачання коштів і матеріальних цінностей, їх недостачі на загальну суму понад 1 млрд. грн. (або 61,9 % від загальної суми виявлених порушень, що призвели до втрат). Відповідно, особливого значення набуває проблема організації бухгалтерського обліку у формуванні системи економічної безпеки підприємства щодо забезпечення управління обліковою інформацією для прийняття управлінських рішень та належного рівня захисту майна підприємства від прояву негативних чинників з боку різних користувачів.

Дослідженням питань організації бухгалтерського обліку займалися такі вчені як: О.М. Галаган, Я.М. Гальперін, В.Б. Івашкевич, Ю.Я. Литвин, П.П. Німчинов, В.Ф. Палій, Я.В. Соколов, В.В. Сопко та ін. Однак вченими не приділено належної уваги розгляду проблемних питань щодо організації бухгалтерського обліку як інструменту забезпечення економічної безпеки підприємств.

Значний внесок у розробку концепції економічної безпеки зробили такі дослідники, як Л.І. Абалкін, В.І. Аверченков, В.А. Богомолов, Е.А. Олейніков, Г.А. Пастернак-Таранушенко, І.П. Плетникова, В.П. Пономарьов, В.К. Сенчагов, А.І. Соловйов, В.Л. Тамбовцев. У сфері бухгалтерському обліку питання захисту облікової інформації знайшли своє відображення в наукових працях В.П. Бондаря, Б.І. Валуєва, В.В. Євдокимова, М.Д. Корінька, М.Ф. Кропивка, Я.Д. Крупки, С.З. Мошенського, О.В. Олійник, В.О. Осмятченка, О.І. Паламарчука, М.С. Пушкара, М.Г. Чумаченка. Серед зарубіжних дослідників питання захисту бухгалтерської інформації розглядалися в працях В.Б. Івашкевича, В.Ф. Палія, Я.В. Соколова. Питання щодо захисту бухгалтерської інформації в комп'ютерному середовищі розглядалися польськими вченими З. Ідзікевич (Z. Idzikiewicz), А. Соколовські (A. Sokolowski).

Наявність невирішених проблемних питань, пов'язаних з організацією бухгалтерського обліку для забезпечення економічної безпеки підприємства у сучасних умовах господарювання, зумовили необхідність розробки науково обґрунтованих рекомендацій з удосконалення вітчизняної теорії та практики організації облікової системи щодо забезпечення захисту бухгалтерської інформації, яка входить до складу комерційної таємниці. Розробка науково обґрунтованих рекомендацій з вирішення даних питань, враховуючи напрацювання вітчизняних і зарубіжних вчених, визначають актуальність та основні напрями дослідження.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ: ОБЛІКОВИЙ ВИМІР

1.1. Наукова ідентифікація економічної безпеки

Сучасна динаміка розвитку світового господарства, національних економік, окремих галузей та підприємств пов'язана не лише з новітніми технологіями, появою нових засобів виробництва, інноваційними управлінськими рішеннями. Одним з найважливіших компонентів сучасного прогресу є економічна безпека суб'єктів економічних відносин всіх рівнів, як домінуюча потреба.

Актуальність проблеми економічної безпеки обумовлена змінними умовами функціонування економічних суб'єктів, які постійно висувають нові вимоги до кількісних та якісних параметрів економічної сфери. Залежно від того, наскільки високим є ступінь економічної безпеки, настільки передбачуваним буде можливий позитивний результат. Таким чином, економічна безпека є основою раціональної поведінки в умовах ринкових ризиків, неодмінною умовою задоволення економічних потреб суспільства.

Суспільний розвиток країн вимагає розвитку економічної безпеки на національному рівні, оскільки світова конкуренція з року в рік стає жорсткішою. Тому кожен суб'єкт економічних відносин певною мірою прагне зберігати та посилювати свою економічну безпеку усіма доступними для нього законними засобами, причому на національному рівні економічна безпека інтегрує потреби всіх включених рівнів, виступаючи, таким чином, інтегрованою суспільною потребою.

Термін "економічна безпека" вперше з'явився в XX столітті та досить швидко отримав розповсюдження у розвинених капіталістичних країнах. Саме тоді, відстоюючи реалістичну оцінку міжнародної ситуації, яка склалася на той час, представники передусім країн Західної Європи виступили за використання економічних методів забезпечення національної безпеки. Одним із найголовніших завдань економічної безпеки на національному рівні є збереження та посилення позицій держави у світовій економічній системі.

У соціально-економічних умовах глобалізації економіки та формування постіндустріальної системи виникла нова потреба у визначенні місця і ролі економічної безпеки, у пошуку нових напрямів її вдосконалення та стратегічної реалізації.

Дослідження економічної безпеки має глибоке історичне коріння, оскільки прагнення захистити державу та власника, власні багатства та мати можливість розвинути свій добробут – все це було актуальним як в глибокому минулому, так і в епоху індустріалізації. Тому окремі підходи до визначення значення, ролі та форм економічної безпеки або її окремих складових можна зустріти у Дж.М. Кейнса, Т. Мальтуса, А. Маршалла, Д.С. Мілля, А. Пігу, Платона, Д. Ріккардо, А. Сміта.

Загальні основи поняття економічної безпеки були закладені у класичних працях М. Вальраса, Дж.М. Кейнса, Ф. Ліста, Т. Мальтуса, К. Маркса, А. Маршалла, Д. Норта, В. Ойкена, А. Сміта, їх роботи містять ґрунтовні теоретичні висновки та пропозиції щодо узгодження інтересів різних суб'єктів господарювання, джерел конфліктів та загроз, способів стабілізації господарського розвитку та підтримки економічної рівноваги.

Так, А. Сміт відзначав, що узгодження інтересів та забезпечення необхідної стійкості економічних відносин є функцією так званої, "прихованої руки" ринку. Переслідуючи особисті інтереси, кожна людина досить часто "дієво служить суспільним інтересам, а ніж тоді, коли прагне це робити свідомо" [1, с. 331-332]. Безпека ринкових об'єктів, що раціонально діють, – це їх природний стан, свідоме втручання в нього лише зіпсує справу.

Неокласична школа конкретизувала підхід А. Сміта, запропонувавши концепцію загальної рівноваги. У соціально-економічному відношенні рівновага учасників ринку означає гнучке динамічне узгодження їх інтересів, досягнення балансу між попитом і пропозицією, виробництвом і споживанням, заощадженнями і інвестиціями. Також відзначимо, що у А. Маршалла в науковому обороті вперше з'являється категорія безпеки. Зокрема, він розглядає безпеку як умову для заощадження: "У далекому минулому марнотратство значною мірою обумовлювалося відсутністю безпеки, невпевненістю тих, хто здатний відкладати на майбутнє, що вони можуть скористатися своїми запасами; лише ті, хто вже був багатий, володіли

[1] Смит А. Исследование о природе и принципах богатства народов / А. Смит. – М.: Соц-экгиз, 1962. – 654 с.

достатньою силою, щоб захистити свої заощадження" [2, с. 304]. Маршалл А. прямо пов'язує безпеку з наявністю деякої сили, достатньої для її забезпечення. Принципи загальної рівноваги при цьому формально дотримуються, але сила, що забезпечує безпеку учасників економічних відносин, може бути віднесена як до ресурсів ринку, так і до ресурсів держави.

Залучення можливостей держави для впорядковування, стабілізації господарської системи і забезпечення її безпеки стає однією з провідних тем у вченні Дж. М. Кейнса та його послідовників. Необхідно відзначити розширювальний підхід кейнсіанської школи до трактування небезпек, що з'являються на шляху учасників ринку. Зокрема, спроба забезпечити ефективний попит на основі застосування інструментів грошової політики може завести ситуацію на ринку в своєрідну безвихідь, так звану "пастку ліквідності". Зниження відсоткової ставки практично зупиняється після отримання певної кількості грошової маси. Подальше збільшення грошової маси здатне лише посилити проблему фінансової нестійкості.

Задля стимулювання ефективного попиту, Дж.М. Кейнс запропонував збільшити витрати держави, державні інвестиції, а також зменшити податки. Розрахунок полягав в тому, що держава братиме на себе все більшу відповідальність за пряму організацію інвестицій [3, с. 151]. Фактично мова йшла про участь держави в забезпеченні стійкого, безпечного соціально-економічного розвитку. Характерним є те, що основні практичні заходи державної економічної політики орієнтовані у Дж.М. Кейнса та його послідовників на урівноваження та нейтралізацію тих небезпек, з якими не справляється механізм ринкового саморегулювання, це можуть бути безробіття та неефективність попиту, дефіцит інвестицій тощо.

Нова інституційна теорія, в основу якої закладено положення про синтез економічних, політичних, соціально-культурних відносин, орієнтована на пошук адекватних такому синтезу та ефективних способів впорядковування даних відносин. Сучасні визначення фундаментальної категорії нової інституційної теорії – інституту – спираються зазвичай на поняття норми або правила різних аспектів діяльності суб'єктів господарювання та їх форм спільності [4, с. 11-13].

---

[2] Маршалл А. Принципы экономической науки: [пер. с англ, Т.1] / А. Маршалл. – М.: "Прогресс", 1993. – 415 с.

[3] Кейнс Дж.М. Избранные произведения / Дж.М. Кейнс. – М.: Прогресс, 1993. – 544 с.

[4] Норт Д. Институциональные изменения: рамки анализа / Д. Норт // Вопросы экономики. – 1997. – № 3. – С. 11-13.

Норми та правила діяльності, оскільки вони встановлені та закріплені, є специфічними межами безпеки, нехтування яких призводить до появи ризиків та загроз самому існуванню даної діяльності та її суб'єктів. Недаремно в центрі уваги інституціоналізму знаходяться особливі форми порушення умов економічної безпеки – інституційні пастки, що трансформують енергію функціонування та розвитку системи в енергію підриву її основ і саморуйнування. При цьому прихильники інституційного напряму рідко використовують саму категорію економічної безпеки.

У 60-х роках XX століття економічна безпека опинилася в центрі уваги дослідників, об'єднаних у складі Римського клубу (М. Месаровіч, Д. Мідоуз, Р. Мюрдаль, А. Печчеі тощо), які зробили акцент на екологічному аспекті даної проблеми, а також на вирішенні конфлікту між бідними і багатими країнами.

Протистояння багатства і бідності по осі "Північ – Південь", як показав Г. Мюрдаль, веде до того, що невтручання багатих країн в ситуацію найбідніших країн призведе зовсім не до саморозвитку в останніх ринкової економіки, а до консервації і навіть до спричинення економічних розривів, що склалися, до відтворення бідності у розширеному масштабі [5, с. 192]. "Прихована рука" ринку не справляється з загрозами, які виникли в світовому господарстві, що глобалізується. Необхідно відзначити специфічний пласт проблем економічної безпеки, піднятий Г. Мюрдалем, – глобальну безпеку економічного розвитку в умовах масштабних розривів та необхідність модернізації господарства багатьох країн світу.

Трансформація економіки ініціювала дослідження проблеми економічної безпеки у вітчизняній літературі. Розпад СРСР, входження пострадянських країн в глобальне світове господарство поставили перед вченими завдання формування концепції економічної безпеки та обґрунтування ефективних стратегій стійкого розвитку країни (праці Л. Абалкіна, Е. Бухвальда, С. Глаз'єва, А. Ілларіонова, Д. Львова, В. Сенчагова, В. Тамбовцева та ін.).

Основними елементами системи економічної безпеки виступають потреби, інтереси та ідеї суб'єктів господарювання, детерміновані відносинами власності. Сама безпека трактується як захисна властивість, обумовлена наявністю синергетичних зв'язків між різними суб'єктами на різних рівнях суспільної ієрархії.

[5] Мюрдаль Г. Современные проблемы "третьего мира" (Asian Drama) / Г. Мюрдаль. – М.: Прогресс, 1972. – 767 с.

З позиції масштабності можна виділити наступні рівні економічної безпеки:

– особистості, організації (мікрорівень),

– галузі, регіону (мезорівень),

– суспільства та держави (макрорівень).

В свою чергу економічна безпека має наступну функціональну структуру: науково-технічна безпека; інформаційна безпека; інтелектуальна безпека; енергетична безпека; фінансова безпека; інвестиційна безпека; безпека зовнішньоекономічної діяльності тощо.

Суб'єктами економічної безпеки виступають окремі індивіди, соціальні групи, колективи, держава. Об'єктами економічної безпеки виступають їх економічні інтереси. Звідси витікає цілком обґрунтований висновок про те, що економічна безпека за своєю суттю виражає відношення із захисту інтересів суб'єктів національної економіки в умовах невизначеності та небезпеки.

Можна виділити рівні організації суб'єкта економічної безпеки (індивіда, домогосподарства, місцевого господарства, регіонального господарського комплексу, національної економіки тощо), а також рівні організації середовища безпечного функціонування та розвитку (нано-, мікро-, мезо-, макро-, мегасередовище).

Узагальнення результатів аналізу еволюції підходів до дослідження економічної безпеки дозволяє сформувати сукупність фундаментальних висновків:

– сутність економічної безпеки полягає в тому, що система економічних відносин володіє власним потенціалом самооновлення, самоорганізації і саморозвитку у взаємодії із зовнішнім середовищем її існування;

– оскільки кожній економічній системі властива невизначеність, проблема безпеки носить універсальний характер;

– невизначеність є природним середовищем існування небезпеки, тому кожен учасник системи економічних відносин повинен активно діяти з метою нейтралізації і подолання існуючих небезпек;

– економічна безпека є найважливішою системною характеристикою, втрата якої ставить господарське життя під загрозу позбавлення цілісності, самодостатності, руйнує її;

– ризики, загрози, конфлікти є формами прояву єдиного процесу руйнування економічної безпеки. Цим формам мають протистояти адекватні

інструменти підтримки і забезпечення економічної безпеки, оскільки інакше система економічних відносин втрачає рівновагу і починає рух по траєкторії саморуйнування;

– потреба в безпеці є однією з фундаментальних потреб існування суб'єкта господарювання будь-якого рівня. Незадоволення даної потреби виводить суб'єктів господарювання за рамки ефективної і стійкої участі в суспільно-господарському житті, позбавляє їх природного захисту;

– системний характер економічної безпеки, необхідність забезпечувати динамічний баланс між формами її руйнування та інструментами її забезпечення, а також фундаментальний характер потреби в безпеці для будь-якого суб'єкта господарювання зумовлюють застосування відтворювального підходу до дослідження даного явища.

Економічна безпека не може бути адекватно відображена в теоретичному відношенні та забезпечена в повному обсязі в практичному відношенні, якщо абстрагуватися від процесуального, динамічного характеру суспільно-господарського життя, а також поєднання мінливості та стійкості у функціонуванні і розвитку, якій притаманні властивості безпеки системи економічних відносин. Будь-які разові, невідновні інструменти забезпечення безпеки захищають систему від ризиків, загроз та конфліктів лише на нетривалий час. Стратегічний підхід до економічної безпеки передбачає її власне відтворення.

Сучасні зарубіжні вчені також розглядають сутність економічної безпеки, перспективи та умови її розвитку в особі таких учених як Е. Ласло, А. Маслоу, Р. МакЕлвейн, Р. Міллер, П. Самуельсон, Т. Уоткінс, Е. Чен, Б. Шиллер та ін.

Економічна безпека, як багатоаспектний об'єкт наукового економічного дослідження, набула широкої популярності у російській економічній думці. Теоретико-методологічні основи економічної безпеки закладені в наукових працях таких сучасних російських учених як Л. Абалкін, С. Глаз'єв, С. Загашвілі, В. Медведєв, Є. Олєйніков, В. Сенчагов. Проблема оцінки стану економічної безпеки національної економіки на основі кількісних показників отримала своє вирішення у роботах А. Ілларіонова, І. Петренка, Т. Ромащенко.

Сучасні дослідження прикладних аспектів економічної безпеки проводяться за наступною проблематикою: фінансова безпека (В. Бурцев, А. Логвіна, Ю. Любімцев, І. Петренко); продовольча безпека (Р. Гумеров,

А. Ємел'янов, М. Корнілов, В. Назаренко, І. Оболенцев, М. Синюк); технологічна безпека (А. Вольський, В. Пресняков, С. Симановський, В. Соколов). Вплив на економічну безпеку "тіньової" економіки досліджували А. Вакурін, С. Глінкіна, Р. Клейнер, А. Нестеров, регіональні аспекти економічної безпеки – А. Куклін, С. Рабкін, О. Романова, А. Скопін, А. Татаркін, В. Яковлев та інші.

Поняття економічної безпеки увійшло до активного використання економічною наукою в другій половині XX століття. Її дослідженням сприяли глобалізація економічних відносин, перехід до інноваційного типу відтворення і накопичення ризиків, загроз, передумов конфліктів в процесі інтенсифікації соціально-економічних перетворень.

Перші статті з проблем економічної безпеки на теренах колишнього СРСР з'явилися наприкінці 1994 р. в Росії. Слід зазначити, що в сфері забезпечення економічної безпеки на підприємствах наукове обґрунтування досить слабке, хоча є ряд праць відомих авторів, а саме: Л.І. Абалкіна, Г. Арбатова, В.А. Богомолова, Н. Гловацької, Г.А. Пастернак-Таранушенка, А. Пороховського, В. Рубанова, В.К. Сенчагова, В.Л. Тамбовцева та ін. Найбільш повно теоретичну сторону даного питання розкрили на сторінках журналу "Вопросы экономики" Л.І. Абалкін, А.К. Архіпов.

Однак, серед російських вчених і фахівців-практиків поки що не склалося єдиної теоретично і методологічно обґрунтованої точки зору щодо сутності економічної безпеки як наукової категорії. Про це, зокрема, свідчить те, що до теперішнього часу запропоновано вже достатню кількість визначень економічної безпеки. Це й "стан економіки і інститутів влади, при якому забезпечуються гарантований захист національних інтересів, соціальна спрямованість політики, достатній оборонний потенціал" [6, с. 12], і "стан, в якому народ може суверенно, без втручання і тиску ззовні, визначати шляхи та форми свого економічного розвитку" [7], а, крім того, ще й "готовність та здатність інститутів влади створювати механізми реалізації і захисту національних інтересів розвитку вітчизняної економіки, підтримку соціально-

6 Экономика и организация безопасности хозяйствующих субъектов: [2-е изд] / В.С. Гусев, В.А. Демин, Б.И. Кузин, М.Д. Медников, А.С. Соколицын, С.В. Степашин, А.В. Федотов, В.Л. Шульц. – СПб.: Питер, 2004. – 288 с.

7 Жандаров А.М. Экономическая безопасность России: определения, гипотеза, расчеты / А.М. Жандаров, А.А. Петров // Безопасность. – 1994. – № 3. – С. 40-48.

політичної стабільності суспільства" [8, с. 12], та "здатність економіки забезпечувати ефективне задоволення суспільних потреб..."[9], а також "рівень розвитку економіки, який забезпечує економічну, соціально-політичну і військову стабільність в умовах дії несприятливих факторів" [10] тощо.

Майже в усіх формулюваннях дивує не лише їх декларативність, але й абсолютне неврахування того, що поняття "безпека" означає відсутність небезпеки або, інакше кажучи, захищеність будь-кого (будь-чого) від будь-кого (будь чого) [11, с. 41]. З цих же формулювань неможливо зрозуміти, від чого і що в економіці слід захищати.

Співставлення всіх цих визначень не лише переконує в тому, що економічна безпека не може бути одночасно станом, здатністю та рівнем розвитку економіки, а, крім того, ще й готовністю та здатністю інститутів влади, а й підтверджує наявність значних розбіжностей в розумінні сутності даної наукової категорії.

З усього кола думок щодо розуміння та вивчення економічної безпеки сьогодні можна виділити два принципово різних концептуальних підходи.

Сутність першого підходу полягає в тому, що економічна безпека є домінанта або, принаймні, найважливіша характеристика економіки, причому характеристика в системному відношенні настільки всеосяжна, що вона, по суті, розглядається як один з проявів самої економіки. Метою розвитку економіки в цьому випадку є забезпечення її безпеки.

Штучність такого підходу очевидна. Крім того, він суперечить основним законам суспільного розвитку. Адже якщо розуміти безпеку як захищеність, то виходить, що розвиток економіки скінчений. Інакше кажучи, при такому підході функціонування будь-якої господарської системи неминуче повинно прийняти збитковий, загасаючий характер. А міжнародні економічні зв'язки або складатимуться на користь тих, хто зумів забезпечити безпеку своєї економіки, або – стійко слабшати до їх повного припинення.

---

[8] Экономика и организация безопасности хозяйствующих субъектов: [2-е изд] / В.С. Гусев, В.А. Демин, Б.И. Кузин, М.Д. Медников, А.С. Соколицын, С.В. Степашин, А.В. Федотов, В.Л. Шульц. – СПб.: Питер, 2004. – 288 с.

[9] Архипов А. Экономическая безопасность: оценки, проблемы, способы обеспечения / А. Архипов, А. Городецкий, Б. Михайлов // Вопросы экономики. – 1994. – № 12. – С. 36-44.

[10] Пискунов А.П. Военно-экономическая безопасность России на современном этапе / А.П. Пискунов // Военная мысль. – 1995. – № 2. – С. 68-71.

[11] Ожегов С.И. Словарь русского языка: [изд. 11-е, стер.] / С.И. Ожегов. – М.: Русский язык, 1975. – 846 с.

Другий підхід зводиться до того, що забезпечення економічної безпеки будь-якої господарської системи є ні чим іншим як однією з найважливіших умов (точніше – мінімально необхідною умовою) стійкого прогресивного розвитку такої системи поруч, наприклад, із її забезпеченістю кадрами або наявністю капіталовкладень. Економічна безпека в цьому випадку стає невід'ємною складовою економічно розвинених країн, а категорії "економічна безпека" і "економічний розвиток" розглядаються як цілком рівноправні.

Практика показує, що розвиток економіки без забезпечення її безпеки якщо і мав місце (Бразилія в 60-ті рр. XX ст., Єгипет і Польща в 70-ті рр. XX ст., Мексика в 80-ті рр. XX ст., Туреччина, Таїланд і Індонезія в 90-ті рр. XX ст.), то, як правило, він носив надто нестійкий характер, а сам період господарського пожвавлення тривав недовго та закінчувався настанням тяжкої економічної кризи.

В своєму дослідженні ми схиляємося до другого підходу. Відповідно, вивчення економічної безпеки як складової національної безпеки пропонуємо розпочати з розгляду тих характеристик господарської діяльності суб'єктів господарювання, які якраз і дозволяють сприймати безпеку економіки як необхідну умову її стійкого позитивного розвитку. В той же час ці характеристики слід розглядати як складові системи економічної безпеки та водночас сприймати як поняття, що мають самостійне теоретичне та методологічне значення, тобто як наукові категорії.

Відповідно до даної точки зору основною науковою категорією виступають життєво важливі інтереси основних об'єктів безпеки. Основними об'єктами економічної безпеки, тобто тими фігурантами, інтереси яких необхідно захищати в економічній сфері, є особа, суспільство (в цілому, а також в особі місцевого самоврядування і різних громадських організацій комерційного та некомерційного характеру) та держава (в цілому, а також в особі різних гілок влади і державних інститутів).

Основними ж суб'єктами економічної безпеки, які можуть та повинні в межах своєї компетенції захищати інтереси згаданих об'єктів, є держава в особі уповноважених на те державних інститутів, органи місцевого самоврядування, інші громадські організації та окремі громадяни. Іншими словами, основні об'єкти економічної безпеки залежно від конкретних обставин можуть виступати як суб'єкти економічної безпеки та навпаки.

Для ефективного забезпечення економічної безпеки необхідним є впровадження цілого комплексу заходів. Перш за все необхідно переглянути нормативно-правову базу економічної безпеки. По завершенні даного етапу необхідно перейти безпосередньо до створення такого середовища, яке б сприяло забезпеченню економічної безпеки. Важливою частиною економічної безпеки є система її фінансування, без якої держава не спроможна реалізувати політику безпеки, з притаманними їй елементами, структурами та відповідними механізмами. Фінансування повинно здійснюватись як на рівні держави, так і на рівні місцевих бюджетів, позабюджетних коштів, коштів суб'єктів господарювання, які впроваджують економічну безпеку.

Реалізація економічної безпеки як держави в цілому, так і окремих суб'єктів господарювання є неможливою за відсутності висококваліфікованих кадрів у даній сфері. Також необхідно мати високий рівень професіоналізму щодо вибору стратегії, законів та алгоритмів здійснення економічної безпеки. При цьому слід враховувати практичні надбання в частині забезпечення економічної безпеки та міжнародний досвід і національні особливості. Одна з особливостей полягає в тому, що Україна в даному напрямі знаходимось на початку шляху. Саме тому досить важливим є вибір правильної, науково обґрунтованої моделі створення та розвитку економічної безпеки. На перше місце потрібно винести загальнодержавні інтереси, оскільки правильна реалізація економічної безпеки є одним з найважливіших шляхів переходу країни до стійкого соціально-економічного розвитку і, в кінцевому результаті, до інформаційного суспільства.

Економічна безпека, будучи однією з основних складових безпеки держави, набуває все більшого значення. Дана тенденція пов'язана з тим, що учасники ринкових відноси прагнуть захистити себе від розголошення комерційної таємниці, що має місце у системі ринкових відносин при створенні більш сприятливих матеріальних умов для заохочення праці підприємствами-конкурентами та зумовлює актуальність проблеми забезпечення економічної безпеки держави та підприємств зокрема в теперішніх умовах. Також одним з основних завдань економічної безпеки є забезпечення стабільного функціонування в даний час, що дає право претендувати на високий рівень розвитку в майбутньому.

Останнім часом зацікавленість проблемою забезпечення економічної безпеки країни викликана двома причинами. Головна причина пов'язана з результатами впровадження нової моделі економічного реформування в пострадянських країнах. Іншою причиною зацікавленості є необхідність в

розвитку економічної безпеки. Це пов'язано з потребою в забезпеченні безперервного режиму захисту інформації підприємства, а зокрема, облікових даних, які складають комерційну таємницю підприємства. Таким чином, метою п.1.1. є розкриття поняття "економічна безпека", а також механізмів її забезпечення.

В суспільних науках поняття "безпека" означає задоволення таких потреб як існування, цілісність, незалежність, спокій та розвиток.

Відповідно до словника В. Даля, безпека – це стан, за якого відсутня загроза будь-кому чи будь-чому або "відсутність небезпеки, збереження, надійність". Цікавим є трактування цього терміну в іспанській мові: "безпека – такий стан речей, який робить їх міцними, визначеними, постійними, впевненими, стійкими, надійними, вільними від усякого ризику й небезпеки" [12].

Сьогодні в економічній науці вчені не можуть дійти до єдиної думки щодо визначення поняття "економічна безпека".

Економічна безпека як наукова категорія має ряд особливостей, які зумовлюють різні підходи до її трактування. Варіанти трактувань поняття "економічна безпека" наведено в таблиці 1.1.

Таблиця 1.1. Визначення поняття "економічна безпека" у різних економічних джерелах

№ з/п	*Джерело*	*Визначення економічної безпеки*
1	*2*	*3*
1	Абалкін Л.І. [13]	"Економічна безпека – це стан економічної системи, який дозволяє їй розвиватися динамічно, ефективно та вирішувати соціальні завдання і при якому держава має можливість розробляти та впроваджувати незалежну економічну політику".
2	Балабанов В.С., Борисенко Е.Н. [14]	"Економічна безпека – головна конструкція, каркас національної безпеки та благоустрій будь-якої держави".
3	Гусєв В.С. [15]	"Економічна безпека – захищеність стану суспільних стосунків, що забезпечують прогресивний розвиток суспільства в конкретних історичних і природних умовах, від небезпек, джерелом виникнення яких служать внутрішні і зовнішні суперечності".

[12] Даль В.И. Толковый словарь живого великорусского языка: в 4 тт. Т. 2 / В.И. Даль. – Спб.: ТОО "Диамант", 1996. – 784 с.

[13] Абалкин Л.И. Экономическая безопасность России: угрозы и их отражение / Л.И. Абалкин // Вопросы экономики. – 1994. – № 12. – С. 4-13.

[14] Балабанов В.С. Продовольственная безопасность: (международные и внутренние аспекты) / В.С. Балабанов, Е.Н. Борисенко; Рос. Акад. предпринимательства. – М.: ЗАО "Издательство "Экономика", 2002. – 544 с.

[15] Экономика и организация безопасности хозяйствующих субъектов: [2-е изд] / В.С. Гусев, В.А. Демин, Б.И. Кузин, М.Д. Медников, А.С. Соколицын, С.В. Степашин, А.В. Федотов, В.Л. Шульц. – СПб.: Питер, 2004. – 288 с.

Продовження Таблиці 1.1

1	*2*	*3*
4	Економічна енциклопедія [16]	"Економічна (науково-інформаційна) безпека – наявність економічного суверенітету держави у сфері науки та інформаційного простору".
5	Капустін Н. [17]	"Економічна безпека – це кількісна та якісна характеристика економічних властивостей системи з погляду її здатності до самовиживання та розвитку в умовах дестабілізуючої дії непередбачуваних та важкопрогнозованих зовнішніх і внутрішніх факторів".
6	Паньков В. [18]	"Економічна безпека – це такий стан національної економіки, який характеризується її стійкістю, "імунітетом" до впливу внутрішніх і зовнішніх факторів, які порушують нормальне функціонування процесу суспільного відтворення, підривають досягнутий рівень життя населення, і тим самим викликають підвищену соціальну напруженість в суспільстві, а також загрози існуванню держави."
7	Пастернак-Таранушенко Г.А. [19]	"Економічна безпека – стан держави, у якому усі потреби населення і країни забезпечені повністю і своєчасно, що дозволяє вести нормальну життєдіяльність та розвиватися системі (держава) і кожному її елементу (людині). Забезпеченням економічної безпеки держави має перейматися комплексна система, що створюється завдяки виконанню визначеної кількості дій. При цьому слід враховувати, що екосестейт* сама по собі теж має багато відгалужень. Усе в існуванні світу, держави та у житті людини має економічне підґрунтя, тому напрямків економічної безпеки багато".
8	Рубанов В. [20]	"Економічна безпека – здатність національної економіки забезпечувати благоустрій нації та стабільність внутрішнього ринку незалежно від дії зовнішніх факторів".
9	Савін В.А. [21]	"Економічна безпека – система захисту життєвих інтересів держави. В якості об'єктів захисту можуть виступати: народне господарство країни в цілому, окремі регіони країни, окремі галузі господарської діяльності, а також юридичні та фізичні особи, які є суб'єктами господарської діяльності".
10	Тамбовцев В.Л. [22]	"Економічна безпека – сукупність властивостей стану її виробничої підсистеми, яка забезпечує можливість досягнення мети всією системою".

[16] Мочерний С. Економічна (валютно-фінансова) безпека. // Економічна енциклопедія: У трьох томах. Т.1 / Ред. кол.: С.В. Мочерний (відп. ред.) та ін. – К.: Видавничий центр "Академія", 2000. – 864 с.

[17] Капустин Н. Экономическая безопасность отрасли и фирмы / Н. Капустин // Бизнес-информ. – 1999. – № 11-12. – С. 45-47.

[18] Паньков В. Экономическая безопасность: мирохозяйственный и внутренний аспект / В. Паньков // Внешнеэкономические связи. – 1992. – № 8. – С. 5-18.

[19] Пастернак-Таранушенко Г.А. Економічна безпека держави. Методологія забезпечення: [монограф.] / Г.А. Пастернак-Таранушенко. – К.: Київський економічний інститут менеджменту, 2003. – 320 с.

* Екосестейт (скорочення англійської назви "economic security of state") – наука про економічну безпеку держави.

[20] Рубанов В. Безопасность – лозунги, теория и политическая практика / В. Рубанов // РЭЖ. – 1991. – № 17. – С. 31-41.

[21] Савин В.А. Некоторые аспекты экономической безопасности России / В.А. Савин // Международный бизнес России. – 1995. – № 9. – С. 14-16.

[22] Тамбовцев В.Л. Экономическая безопасность хозяйственных систем: структура, проблемы / В.Л. Тамбовцев // Вестник МГУ. Сер. 6. Экономика. – 1995. – № 3. – С. 3-9.

Зведені в таблиці 1.1 визначення “економічної безпеки” свідчать про неодностайність думок вчених щодо визначення даного поняття. Це пов’язано перш за все з тим, що науковці розглядають економічну безпеку в різних галузях суспільної діяльності.

Таким чином, узагальнення поглядів науковців щодо напрямів економічної безпеки можна графічно представити в наступному вигляді (рис. 1.1), що дасть змогу удосконалити існуючі визначення “економічної безпеки” та надати власний варіант трактування даного поняття, який міститиме всі суттєві аспекти здійснення економічної безпеки.

Рис. 1.1. Напрями економічної безпеки

Необхідно зауважити, що забезпечення економічної безпеки може здійснюватися за допомогою наведених на рисунку напрямів.

Таким чином, під економічною безпекою слід розуміти важливу характеристику, притаманну економічній системі, яка визначає здатність системи підтримувати нормальні умови діяльності та забезпечення ресурсами господарюючого суб’єкта. Проаналізувавши наведені твердження, можна дійти висновку про те, що економічна безпека є невід’ємною складовою національної безпеки країни.

Забезпечення системи економічної безпеки є гарантом незалежності країни, умовою ефективності та стабільності суспільної діяльності. Це пояснюється тим, що економіка є однією з найважливіших сторін розвитку суспільства, держави та особистості. Поняття національної безпеки не матиме сенсу без оцінки економіки, її міцності при можливих зовнішніх або внутрішніх загрозах, тому забезпечення економічної безпеки належить до числа найважливіших національних пріоритетів.

Сутність економічної безпеки полягає у забезпеченні поступального економічного розвитку суспільства з метою виробництва необхідних благ та послуг, що задовольняють індивідуальні та суспільні потреби. Раніше усі питання, пов'язані із забезпеченням безпеки, покладалися на державні органи. Останніми роками можна спостерігати відтворення системи економічної безпеки, в якій головна роль відводиться саме державі.

Економічна безпека є однією з найважливіших категорій в функціонуванні держави та в існуванні міжнародних відносин, зокрема. Вона є однією з проблем, яку досліджують науковці і якій присвячено велику кількість наукових публікацій. Крім того, аналізом різних проблем безпеки займається ряд інституцій, зокрема Лондонський Інститут стратегічних досліджень (ЛІСД) та Стокгольмський Інститут досліджень безпеки (СІДБ).

Інститутами, які приділяють увагу проблемам економічної безпеки в Україні є: Національний інститут стратегічних досліджень Адміністрації Президента України, Інститут економіки НАН України, Українська академія зовнішньої торгівлі, Рада національної безпеки та оборони України, , Національний інститут проблем міжнародної безпеки, Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка та ряд інших державних наукових установ.

Нині більшість авторів (зокрема, В. Бєлов [23; 24]; С. Гордієнко [25]; М. Косолапов [26]; Є. Кравець, Г. Мурашин [27]; С. Селіванов [28] та ін.) визначають безпеку як певну характеристику стану системи та її основних складових.

---

[23] Белов В.Г. Правовая охрана конфиденциальности коммерческой тайны / В. Белов, А. Полянский // Право и экономика. – 1993. – № 13-14. – С. 12-21.
[24] Белов В.Г. Правовая охрана конфиденциальности коммерческой тайны / В. Белов, А. Полянский // Право и экономика. – 1993. – № 15-16. – С. 8-27.
[25] Гордієнко С.Г. Сутність та зміст поняття "державна безпека" / С.Г. Гордієнко // Стратегічна панорама. – 2003. – № 2. – С. 114-121.
[26] Косолапов Н. Сила, насилие, безопасность: современная диалектика взаимосвязей / Н. Косолапов // МЭиМО. – 1992. – № 11. – С. 45-58.
[27] Мурашин Г. О концепции национальной безопасности / Г. Мурашин, Е. Кравец // Політика і час. – 1992. – № 5. – С. 10-18.
[28] Селіванов В. Національна безпека України та її забезпечення / В. Селіванов // Право України. – 1992. – № 7.

В наш час термін “безпека” існує на всіх етапах суспільного розвитку і є основним елементом забезпечення стабільних умов існування суспільства.

Для забезпечення всебічного розгляду питань щодо безпеки потрібно розглядати її в різних сферах, системах та на різних рівнях людського існування.

Так з економічної точки зору безпеку можна поділити на три рівні (рис. 1.2):

1) глобальний рівень (увесь світ);

2) макрорівень (держава);

3) мікрорівень (підприємство, організація, установа).

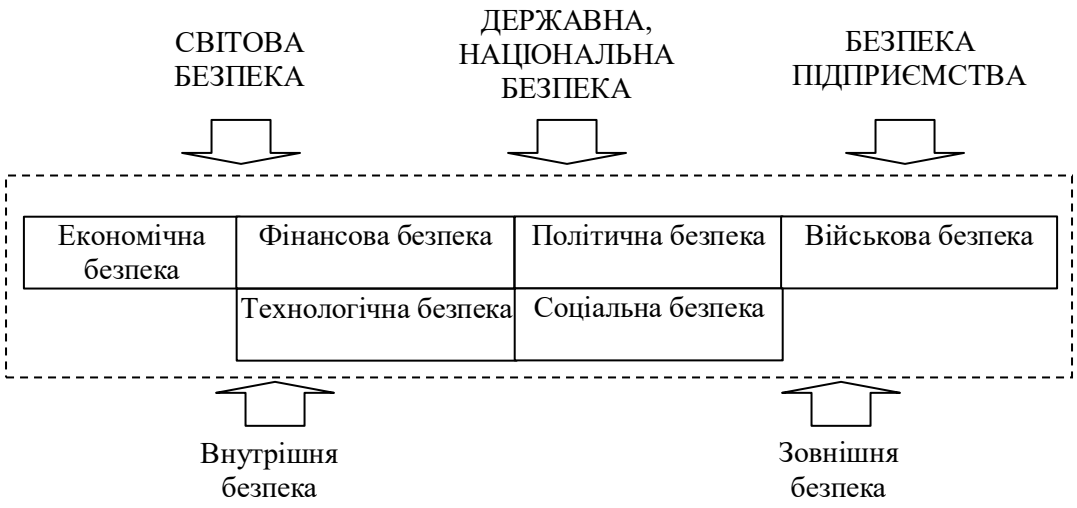


Рис. 1.2. Узагальнена класифікація видів безпеки

На нашу думку, дана класифікація слугує відображенням всього обсягу складових, які наповнюють безпеку та формують повне уявлення щодо її сутності. Вона відображає основні характерні риси безпеки. Незважаючи на те, що наведені вище види безпеки розглядаються окремо, але кожен з них є складовою частиною іншого, тобто вони є взаємопов’язаними.

Перш за все, слід розглянути глобальний рівень або світову безпеку. Нині вона набуває актуальної форми, оскільки світова безпека є запорукою захищеності та забезпечення безперешкодного існування людства. В свою чергу наступною сходинкою є державна безпека, яка залежить від системи політичних відносин, які прямо або опосередковано пов’язані із забезпеченням нормального функціонування державної влади та її інститутів у середині суспільства та в її стосунках з іноземними державами.

Згідно з "Концепцією (основами державної політики) національної безпеки України" (1993 р.), національна безпека – "стан захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз". Подібної точки зору дотримуються М. Косолапов, Г. Мурашин, С. Пирожков, В. Селіванов та інші.

У проекті Концепції Національної безпеки України, що запропонований Апаратом РНБОУ, Українським інститутом досліджень навколишнього середовища та Національним інститутом проблем міжнародної безпеки, визначено, що національна безпека – це стан захищеності національних інтересів громадян, суспільства і держави, за якого забезпечується попередження і нейтралізація потенційних та реальних внутрішніх і зовнішніх загроз.

Національна і державна безпека дещо однорідні поняття, але відрізняються черговістю об'єктів, яким надається захист. Так, безпосередньо об'єктами національної безпеки є: громадянин – його права та свободи; суспільство – його матеріальні й духовні цінності; держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність кордонів. А об'єктами державної безпеки відповідно: держава, суспільство, особа.

Наступним рівнем є підприємницький, який торкається питання безпеки підприємства. Він є основним у формуванні фундаменту для всіх інших рівнів економічної безпеки, оскільки безпека підприємства є однією із складових частин економічної безпеки держави, а отже, і світової безпеки.

1.2. Поняття та значення економічної безпеки підприємств: моніторинг явищ

Перехід економіки до нових умов господарювання вимагає від керівників підприємств не лише розробки стратегії поведінки на ринку товарів та послуг, але й розробку стратегії економічної безпеки, яка полягає в створенні спеціальних програм захисту інтелектуальної власності, облікових даних підприємства та іншої інформації, що може становити комерційну таємницю підприємства. Така тенденція пов'язана з тим, що ринкові умови надають можливість збільшувати прибутки, в результаті чого виникають загрози розкриття комерційної таємниці, що в свою чергу може спричинити негативні наслідки для підприємства.

У зв’язку з трансформацією економічних відносин, що спричинило появу нових для нашої держави форм власності та організаційно-правових форм організації підприємства, для діяльності більшості підприємств суттєво змінився підхід до поняття “безпека”. Зміст цього поняття з виміру, підпорядкованого раніше в основному державним інтересам, переходить у вимір реальної економіки, стосуючись нижчих рівнів: регіону та його підприємницьких структур – підприємств, банків, корпорацій.

У сучасних умовах господарювання підприємство як система відкритого типу функціонує у складному економічному середовищі, яке характеризується постійною динамікою та нестабільністю. Дане середовище змушує управлінський персонал швидко адаптуватися до нових умов, вимагає знання принципів розвитку та впровадження нових методів існування у ринковій економіці, врахування чинників нестійкості та невизначеності економічного середовища.

Оскільки підприємства здійснюють свою діяльність на макро-, мезо- та мікрорівні економічну безпеку підприємств слід розглядати з позиції багаторівневості. Механізм забезпечення економічної безпеки підприємства залежить від економічної безпеки країни, її стану в окремих регіонах. Як відомо, кожен регіон має свою специфіку, у зв’язку з чим необхідним є удосконалення системи економічної безпеки. Також вибір стратегії економічної безпеки залежить від соціально-економічного стану країни та її економічних можливостей.

Найбільш дискусійними залишаються питання, пов’язані з визначенням сутності, загроз та значення економічної безпеки. Ці питання закладено в основу прийняття рішень в сфері забезпечення економічної безпеки.

На мікрорівні ефективність економічної безпеки проявляється у нормальній і стабільній діяльності підприємства, наявності та використанні засобів щодо попередження витоку інформації, яка становить комерційну таємницю. Отже, показник економічної безпеки підприємства визначається як рівень забезпечення захисту усіх існуючих систем підприємства при здійсненні господарської діяльності.

Останнім часом з’являється література з питань безпеки підприємництва. Проте системних та узагальнюючих досліджень в цій специфічній сфері поки що недостатньо, хоча потреба в них є досить очевидною. Передусім за все необхідно сформулювати основні поняття, визначити концептуальні підходи, розробити методи проектування раціональних структур безпеки.

Питання економічної безпеки підприємства розглядаються в працях таких вітчизняних та зарубіжних науковців, як: А.О. Азарова [29], І.О. Александров [30], Г. Андрощук [31; 32], О.В. Ареф'єва [33], Г. Дарнопих [34], В. Забродський [35], Н. Капустін [36], Д. Ковальов [37], В. Коржов [38], В. Кульпінов [39; 40; 41], В.П. Пономарьов [42], А.І. Соловйов [43], Т.Г. Сухорукова [44], В. Шликов [45; 46; 47] та ін.

Складність вирішення організаційних і економічних завдань забезпечення економічної безпеки підприємств зумовлена:

комплексністю виробничо-господарської та фінансової діяльності господарюючих суб'єктів;

відсутністю теоретичних напрацювань з даної проблематики за часів Радянського Союзу.

---

[29] Азарова А.О. Розробка методики визначення економічної безпеки підприємства / А.О. Азарова, О.В. Гаврилова // Економіка: проблеми теорії та практики. Збірник наукових праць. Випуск 191: В 4 т. Том ІІІ. – Дніпрпетровськ: ДНУ, 2004. – 318 с.

[30] Александров І.А. Кластеризація територіальних утворень України за рівнем економічної безпеки / І.А. Александров, О.В. Половян // Економічна кібернетика. – 2000. – № 5-6. – С. 40-47.

[31] Андрощук Г. Правове регулювання ноу-хау / Г. Андрощук // Інтелектуальна власність. – 2004. – № 10. – С. 29-35.

[32] Андрощук Г.А., Крайнев П.П. Экономическая безопасность предприятия: защита коммерческой тайны: [монограф.] / Г.А. Андрощук, П.П. Крайнєв. – К.: Издательский Дом "Ин Юре", 2000. – 400 с.

[33] Ареф'єва О.В. Планування економічної безпеки підприємств / О.В. Ареф'єва, Т.Б. Кузенко. – К: Вид-во Європ. ун-ту, 2004. – 170 с.

[34] Дарнопих Г. Сучасні проблеми економічної безпеки України / Г. Дарнопих // Вісник Академії правових наук України. – 1998. – № 1. – С. 142-150.

[35] Забродский В. Теоретические основы оценки экономической безопасности отрасли и фирмы / В. Забродский, Н. Капустин // Бизнес-информ. – 1999. – № 15-16. – С. 35-37.

[36] Капустин Н. Экономическая безопасность отрасли и фирмы / Н. Капустин // Бизнес-информ. – 1999. – № 11-12. – С. 45-47.

[37] Ковалев Д. Экономическая безопасность предприятия Д. Ковалев, Т. Сухорукова // Экономика Украины. – 1998. – № 10. – С. 48-52.

[38] Коржов В. Сколько стоит безопасность? / В. Коржов // Computerword. – 2004. – № 12: [Електронний ресурс]. – Режим доступу: http://www.outsourcing.ru/content/rus/131/1314-article.asp.

[39] Кульпінов В. Кадри позбавляють усього. Як нейтралізувати штатних шкідників / В. Кульпінов // Контракти. – 2004. – № 41. – С. 54-55.

[40] Кульпінов В. Комерційний смерш / В. Кульпінов // Контракти. – 2004. – № 43. – С. 34-38.

[41] Кульпінов В. Прозріння Феміди / В. Кульпінов // Контракти. – 2004. – № 48. – С. 34-35.

[42] Пономарев В.П. Оценка уровня экономической безопасности предприятия: материалы Международной науч.-практ. конф. [Настоящее и будущее российской экономики: проблемы, подходы, решения] / В.П. Пономарев. – Пермь: Гос. ун-т, 1999. – С. 189-190.

[43] Соловьев А.И. Экономическая безопасность хозяйствующего субъекта А.И. Соловьев // Конфидент. – 2002. – № 3. – С. 46-50.

[44] Сухорукова Т.Г. Концептуальный взгляд на экономическую безопасность предприятия / Т.Г. Сухорукова // Залізничий транспорт України. – 1998. – № 2-3. – С. 9-12.

[45] Шлыков В.В. Экономическая безопасность предприятия (во что обходится хозяйствующим субъектам защита собственности и способы минимизации возможных потерь) / В.В. Шлыков// РИСК. – 1997. – № 6. – С. 61-63.

[46] Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия / В.В. Шлыков. – СПб.: "Алетейя", 1999. – 138 с.

[47] Шлыков В.В. Экономическая безопасность предприятия (факторы влияния, анализ необходимости) / В.В. Шлыков // Машиностроитель. – 1995. – № 1. – С. 31-34.

Поняття “економічна безпека” в сучасних умовах господарювання і з врахуванням факторів, які зумовлюють процеси управління набуває іншого значення. Вперше поняття “економічна безпека” почало застосовуватися на Заході у зв’язку зі зростанням проблеми обмеженості ресурсів та розпадом колоніальної системи, що призвело до порушення традиційних зв’язків між постачальниками ресурсів, життєво необхідних індустріальним суспільствам.

Головна мета системи економічної безпеки суб’єкта господарювання полягає в гарантуванні йому максимально ефективного, а також стабільного функціонування в теперішній час та високий рівень розвитку в майбутньому.

Найбільш важливими факторами, які впливають на економічну безпеку підприємства, є: досконалість законодавчої бази, системи оподаткування, участь суб’єктів господарювання у роботі міжнародних ринків, інвестиційна привабливість певного регіону та держави в цілому. Насамперед економічна безпека підприємства залежить від економічної безпеки держави, регіону, адже вона базується на їх фінансовому, сировинному та виробничому потенціалі, перспективах розвитку. Концепція багаторівневої економічної безпеки підприємства дозволить передбачати та уникнути зовнішніх загроз підприємства.

Економічній безпеці підприємства властивий подвійний характер: по-перше, можливе ії власне функціонування, по-друге – вона може бути складовою економічної безпеки системи більш глобального рівня, що дозволить забезпечити виконання функцій певним регіоном та державою. В сучасних умовах господарювання та розвитку економіки актуальними є дослідження саме макроекономічних аспектів концепції економічної безпеки.

Посилення конкурентної боротьби, а також збільшення кількості випадків використання прийомів недобросовісної конкуренції, активізація шахрайства з боку співробітників підприємства, а інколи й навіть відкритий силовий вплив з боку конкурентів, можуть завдати бізнесу невиправних втрат. Дані обставини вимушують керівників більшості підприємств все частіше ставити питання про забезпечення безпечного функціонування власного підприємства, особливо у сфері прийняття управлінських рішень та протидії негативним проявам з боку персоналу підприємства.

За даними Головного Контрольно-ревізійного управління України протягом 2008 р. виявлено порушення, які призвели до втрат фінансових і матеріальних ресурсів, на загальну суму понад 3,7 млрд. гривень. Внаслідок

неправомірних дій окремих керівників бюджетами усіх рівнів, бюджетними установами та організаціями, підприємствами втрачена можливість отримати належні їм доходи в сумі майже 1,3 млрд. грн., у тому числі бюджетами – 754,9 млн. гривень. Структура таких порушень містить: незаконні витрати ресурсів (55,6 %), недоотримання фінансових ресурсів (34,4 %), витрати проведені не за цільовим призначенням (7,1 %), розкрадання коштів та матеріальних цінностей (2,9 %) (рис. 1.3, 1.4).

Структура порушень, що призвели до втрат фінансових і матеріальних ресурсів, виявлених органами державної контрольно-ревізійної служби за 2008 рік

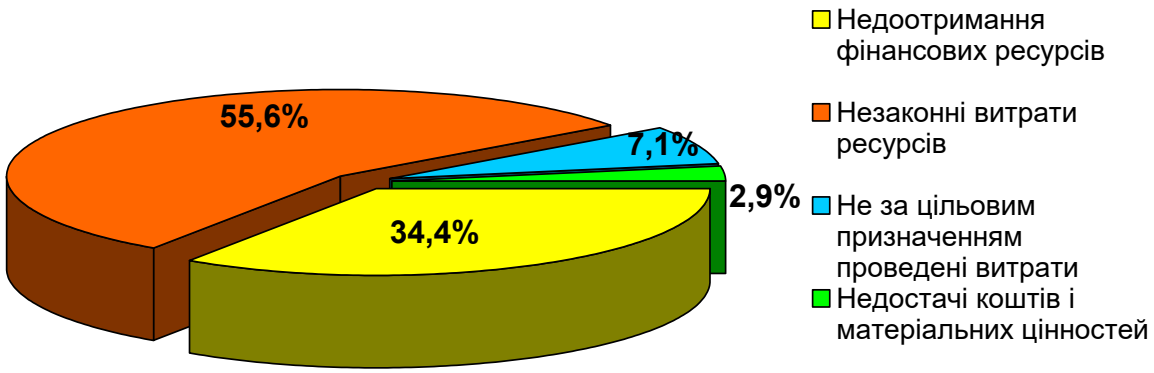


Рис. 1.3. Структура порушень, що призвели до втрат фінансових і матеріальних ресурсів за 2008 рік

Загалом протягом І-го півріччя 2009 року майже у всіх з перевірених підприємств, установ і організацій усіх форм власності виявлено незаконні та не за цільовим призначенням проведені витрати, недостачі коштів та матеріальних цінностей, а також недоотримання фінансових ресурсів на загальну суму понад 1,6 млрд. гривень. З них на 7,2 тис. об'єктів контролю встановлено незаконне і нецільове витрачання коштів і матеріальних цінностей, їх недостачі на загальну суму понад 1 млрд. грн. (або 61,9 % від загальної суми виявлених порушень, що призвели до втрат).

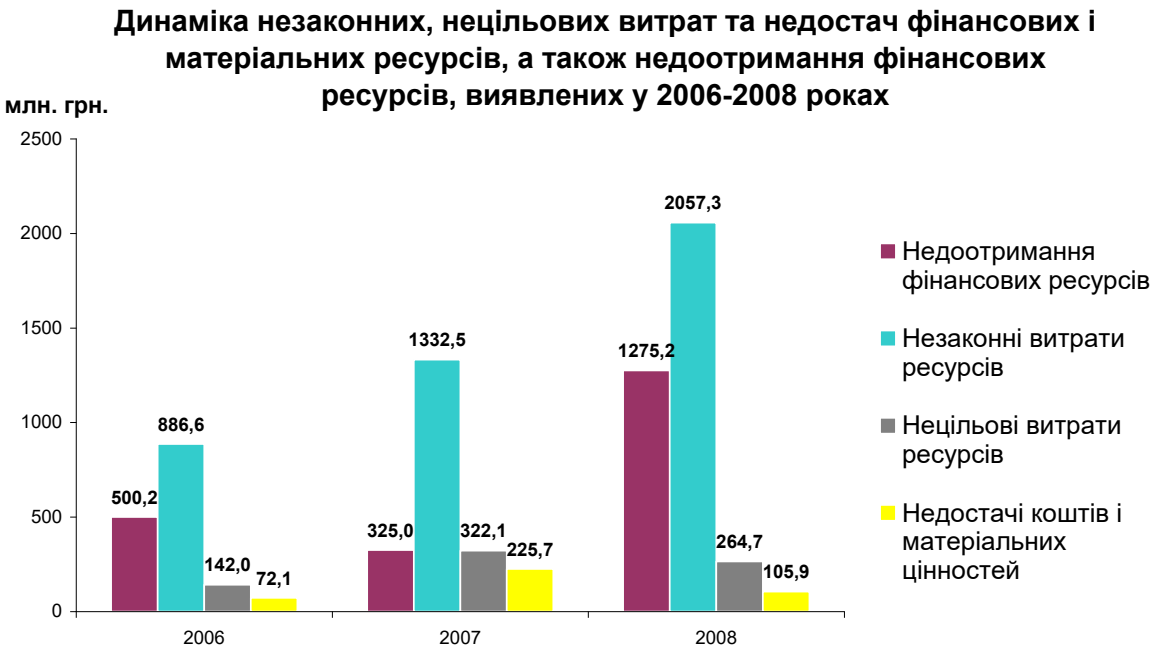


Рис. 1.4. Динаміка незаконних, нецільових витрат та недостач матеріальних ресурсів, виявлених у 2006-2008 рр.

Зміни, які відбуваються у внутрішньому і зовнішньому середовищі функціонування суб'єкта господарювання впливають на формування економічної безпеки підприємства. Цим змінам притаманна раптовість і вони потребують швидкого пристосування суб'єктів господарювання до ринкових умов, з урахуванням невизначеності економічного середовища та його нестійкості. Все це впливає на процес управління підприємством, як суб'єктом господарювання, та вимагає адаптування до змінних ринкових умов. Ефективне вирішення цих питань дозволить реалізувати конкурентні переваги підприємства та створити стабільну базу його подальшої діяльності.

Конкуренте середовище, в якому функціонує підприємство, вимагає постійної роботи управлінського персоналу над удосконаленням рішень щодо забезпечення високого рівня економічної безпеки. Обов'язковою умовою цього процесу є оцінка та здійснення аналізу господарської діяльності підприємства. Обрання методик їх здійснення визначається метою та впливом на елементи зовнішнього та внутрішнього середовища або їх взаємозв'язок.

Безпека може не лише здійснюватись в контексті розвитку бізнесу, але й позитивно впливати на значну кількість бізнес-показників розвитку підприємства. Будучи одним із внутрішніх процесів підприємства, забезпечення безпеки, як і всі інші, повинно бути спрямоване на досягнення

поставлених бізнесом цілей. Впровадження економічної безпеки передбачає проведення тактичного планування діяльності підприємства та його розробку, що дозволить реалізувати певні визначені завдання.

Проф. С.Б. Барнгольц та М.В. Мельник зазначають, що для управління діяльністю суб'єкта господарювання в цілому, окремими її напрямами та діями кожного виконавця перш за все розробляється модель цієї діяльності, яка описується системою узагальнюючих та часткових показників, зафіксованих у бізнес-плані, рівень та взаємозв'язок яких повинні забезпечити досягнення запланованих результатів діяльності [48, с. 143].

Забезпечення безпеки, в першу чергу, це завдання не лише служби економічної безпеки, але й усіх співробітників підприємства. Для того, щоб вони це зрозуміли, вимагається активна взаємодія між службою інформаційної безпеки та іншими підрозділами. Впровадження інформаційної безпеки – це завжди рух в дві сторони. Слід відходити від заборонної практики, розповсюдженої в сфері інформаційної безпеки. Будь-яка заборона викликає негативну реакцію, яка не найкращим чином впливає на ставлення до безпеки в цілому.

При дослідженні поняття "економічна безпека підприємства" встановлено, що зміст економічної безпеки відображає певний стан діяльності підприємства, який дозволяє уникнути впливу внутрішніх і зовнішніх загроз. У зв'язку з цим економічна безпека підприємства розглядається як сукупність заходів із забезпечення його стійкого розвитку, в умовах невизначеності, які існують в зовнішньому середовищі, незалежно від впливу зовнішніх факторів на діяльність суб'єкта господарювання. Сутність поняття "економічна безпека підприємств" наведено в Додатку А.

Поняття економічної безпеки розглядалося як дотримання умов забезпечення захисту комерційної таємниці підприємства. Саме такому тлумаченню економічної безпеки присвячені наукові праці кінця XX століття В. Алєксєєнка [49], В.Г. Бєлова [50; 51], В.А. Гавриша [52],

---

[48] Барнгольц С.Б. Методология экономического анализа деятельности хозяйствующего субъекта: [учеб. пособие] / С.Б. Барнгольц, М.В. Мельник. – М.: Финансы и статистика, 2003. – 240 с.

[49] Алексеенко В. Система защиты коммерческих объектов / В. Алексеенко, Б. Сокольский. – М., 1992. – 195 с.

[50] Белов В.Г. Правовая охрана конфиденциальности коммерческой тайны / В. Белов, А. Полянский // Право и экономика. – 1993. – № 13-14. – С. 12-21.

[51] Белов В.Г. Правовая охрана конфиденциальности коммерческой тайны / В. Белов, А. Полянский // Право и экономика. – 1993. – № 15-16. – С. 8-27.

[52] Гавриш В.А. Практическое пособие по защите коммерческой тайны / В.А. Гавриш. – Симферополь, 1994. – 153 с.

В.А. Деружинского [53], Е.Я. Соловйова [54]. В більшості наукових праць економічна безпека розглядається перш за все як забезпечення захисту інформації, серед яких необхідно назвати роботи А. Шаваєва [55; 56; 57], В. Ярочкіна [58; 59] і ряд інших В.С. Барсукова [60], Ю.М. Батуріна [61], І.В. Василевського [62], В.І. Васильця, В.М. Голованова [63], В.С. Горячева [64], В.І. Кащєєв [65], Г. Раєвського [66]. Проблеми щодо дотримання економічної безпеки підприємства у вказаному напрямі необхідно вирішувати, виходячи з концепції, що рівень надійності системи захисту інформації визначається ступенем захисту її слабкої ділянки, якою є співробітники підприємства.

Система економічної безпеки підприємства може бути представлена у вигляді ієрархічної структури захисту інформації двох рівнів. Перший рівень забезпечує збереження комерційної таємниці підприємства за рахунок діючої служби економічної безпеки. Другий – передбачає створення сприятливої атмосфери в колективі підприємства, що підвищує відповідальність персоналу. Визнаючи, що захист інформації є одним з основних напрямів забезпечення економічної безпеки підприємства, необхідно наголосити, що забезпечення економічної безпеки підприємства лише на рівні захисту складових комерційної таємниці є спрощеним варіантом її вирішення. Цілком

[53]Деружинский В.А. Основы коммерческой тайны: [Практ. пособ. для предпринимателя] / В.А. Деружинский, В.В. Деружинский. – Мн.: ООО “Полирек”, 1994. – 214 с.

[54] Соловьев Э.Я. Коммерческая тайна и ее защита / Э.Я. Соловьев. – М.: Ось-89, 2001. – 112 с.

[55] Шаваев А.Г. Безопасность банковских структур / А.Г. Шаваев // Экономика и жизнь. – 1994. – № 16.– С. 11-12.

[56] Шаваев А.Г. Концептуальные основы обеспечения безопасности негосударственных объектов экономики / А.Г. Шаваев. – М.: Академия экономической безопасности, 1994. – 281 с.

[57] Шаваев А.Г. Криминологическая безопасность негосударственных объектов экономики / А.Г. Шаваев. – М.: Инфра-М, 1995. – 126 с.

[58] Ярочкин В.И. Безопасность информационных систем / В.И. Ярочкин. – М. “Ось-89”, 1996. – 197 с.

[59] Ярочкин В.И. Предприниматель и безопасность. Ч. 2 / В.И. Ярочкин. – М.: Экспертное бюро, 1994. – 132 с.

[60] Барсуков В.С. Обеспечение информационной безопасности / В.С. Барсуков. – М., 1996. – 271 с.

[61] Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жоздишевский. – М., 1999. – 297 с.

[62] Василевский И.В. Найти и обезвредить. Техника защиты информации / И.В. Василевский // Система безопасности. – 1995. – № 6. – С. 11-15.

[63] Василец В.И. Методические основы обеспечения конфиденциальности производственной и коммерческой деятельности акционерного общества / В.И. Василец, В.Н. Голованов // Вопросы защиты информации. – 1994. – № 1. – С. 5-11.

[64] Горячев В.С. Информация и ее защита / В.С. Горячев // Вопросы защиты информации. – 1994. – № 2. – С. 13-18.

[65] Кащеев В.И. Обеспечение информационной безопасности коммерческого объекта / В.И. Кащеев // Системы безопасности. – 1995. – № 5. – С. 8-12.

[66] Раевский Г. Система экономической безопасности предприятия / Г. Раевский // Частный сыск, охрана, безопасность. – 1994. – № 2. – С. 5-11.

очевидно, що таке вузьке розуміння економічної безпеки страждає надмірною "економічністю" і не враховує всього спектру впливу зовнішнього середовища як основного джерела небезпек для діяльності підприємства.

Дещо пізніше запанував інший підхід до трактування поняття економічної безпеки підприємства. Різкий спад виробництва в цілому по країні, а головне – зміна економічних функцій держави, яка вже не була основним інвестором і споживачем продукції, примусили подивитися набагато ширше на проблему економічної безпеки підприємств. Відповідно до цього погляду економічна безпека підприємства обумовлена впливом зовнішнього середовища на діяльність підприємства, яке в ринковій економіці весь час змінюється, ніколи не залишається стабільним та постійним. Саме з цієї позиції захисту підприємств від його негативного впливу і розглядається зміст категорії економічної безпеки підприємства, у тому числі і в публікаціях вітчизняних вчених-економістів.

З часом при трактуванні поняття "економічна безпека" стала переважати думка, що зміст економічної безпеки віддзеркалює стан діяльності підприємства, який дозволяє уникнути впливу несприятливих зовнішніх факторів. В результаті такого бачення економічну безпеку підприємства почали розглядати дещо ширше, а саме як можливість досягнення певного рівня стійкості в несприятливих умовах, які спричиняються розвитком зовнішнього середовища, незалежно від характеру її впливу на господарську діяльність.

На думку Д. Ковальова економічна безпека підприємства визначена як "захищеність його діяльності від негативних впливів зовнішнього середовища, а також як здатність швидко усунути різноваріантні загрози або пристосуватися до існуючих умов, які не позначаються негативно на його діяльності" [67, с. 48]. Такої ж точки зору дотримується В. Забродський, який трактує економічну безпеку як "кількісну і якісну характеристику властивостей фірми, що відображає здатність "самовиживання" і розвитку в умовах виникнення зовнішньої і внутрішньої економічної загрози" [68, с. 35].

---

[67] Ковалев Д. Экономическая безопасность предприятия Д. Ковалев, Т. Сухорукова // Экономика Украины. – 1998. – № 10. – С. 48-52.

[68] Забродский В. Теоретические основы оценки экономической безопасности отрасли и фирмы / В. Забродский, Н. Капустин // Бизнес-информ. – 1999. – № 15-16. – С. 35-37.

Відповідно до точки зору В. Забродського, економічна безпека фірми визначається сукупністю чинників, що відображають незалежність, стійкість, можливості зростання, забезпечення економічних інтересів тощо. В. Шликов розглядає економічну безпеку підприємства як "...стан захищеності життєво важливих інтересів підприємства від реальних і потенційних джерел небезпеки або економічних загроз" [69, с. 33].

Використовуючи термін "загроза", автори найчастіше не дають його визначення, за виключенням, напевно, В. Тамбовцева, який поняття "загроза" розглядає як "такі зміни в зовнішньому або внутрішньому середовищі, які приводять до небажаних змін предмету безпеки (підприємства)" [70, с. 4].

Автори цього підходу економічну безпеку підприємства розглядають як "стан найбільш ефективного використання корпоративних ресурсів для запобігання загроз та забезпеченню стабільного функціонування підприємства в даний час і в майбутньому" [71, с. 38]. З цією метою Є.А. Олєйніков розглядає економічну безпеку як сукупність процесів, що відбуваються на підприємстві, зі всіма їх характерними особливостями і взаємозв'язками, які складають єдину споріднену групу з погляду їх функціональної ролі в забезпеченні економічної безпеки підприємства і, разом узяті, відіграють важливу роль у забезпеченні економічної безпеки підприємства.

У ресурсно-функціональному підході основними напрями економічної безпеки підприємства виділяють сім складових: фінансову, політико-правову, інтелектуально-кадрову, екологічну, техніко-технологічну, інформаційну і силову [72, с. 39].

Детальне вивчення зазначеного вище підходу до тлумачення економічної безпеки підприємства дозволяє виділити його основну перевагу – необмежене, системне значення, так як в межах даного підходу досліджуються чинники, що впливають на рівень цієї складової економічної безпеки підприємства, вивчають основні дії, що впливають на її забезпечення, проводиться аналіз

---

[69] Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия / В.В. Шлыков. – СПб.: "Алетейя", 1999. – 138 с.

[70] Тамбовцев В.Л. Экономическая безопасность хозяйственных систем: структура, проблемы / В.Л. Тамбовцев // Вестник МГУ. Сер. 6. Экономика. – 1995. – № 3. – С. 3-9.

[71] Основы экономической безопасности (Государство, регион, предприятие, личность) / Под ред. Е.А. Олейникова. – М.: ЗАО "Бизнес-школа "Интел-синтез", 1997. – 228 с.

[72] Основы экономической безопасности (Государство, регион, предприятие, личность) / Под ред. Е.А. Олейникова. – М.: ЗАО "Бизнес-школа "Интел-синтез", 1997. – 228 с.

розподілу і використання різних ресурсів підприємства, аналізуються економічні індикатори, що відображають рівень забезпечення функціональної складової економічної безпеки підприємства, і впроваджуються заходи щодо забезпечення максимального рівня зазначеної складової .

Проте ця перевага ресурсно-функціонального підходу одночасно є і його недоліком, оскільки економічна безпека розглядається дуже широко – і в аспекті адаптації до впливу зовнішнього середовища, і в аспекті ресурсозабезпеченості підприємства, і в аспекті якості реалізації функцій управління, таких як планування, облік і аналіз тощо. При використанні такого підходу втрачається сутність економічної безпеки, і відбувається її ототожнення з господарської діяльністю підприємства та ефективністю її функціонування. Такий висновок підтверджує дане Е.А. Олейніковим саме визначення економічної безпеки підприємства – "стан найбільш ефективного використання корпоративних ресурсів" [73, с. 33].

Окрім підходів щодо визначення сутності економічної безпеки підприємства, виходячи з негативного впливу на його діяльність чинників зовнішнього середовища, існують і інші точки зору з даного питання. Так, В. Шликов [74, с. 62] економічну безпеку підприємства розглядає з погляду мінімізації втрат і збереження контролю над власністю. Як способи забезпечення економічної безпеки підприємства пропонується впровадження політики захисту його інтересів, в якому основна увага приділена питанням боротьби з недобросовісною конкуренцією, забезпеченню інформаційної безпеки і правовому захисту інтелектуальної власності [75, с. 48]. Слід зазначити незрозумілість і неузгодженість такого аспекту забезпечення економічної безпеки підприємства, як боротьба з недобросовісною конкуренцією. Зокрема, незрозуміло, в яких формах, яким чином і якими способами суб'єкт господарювання може здійснювати боротьбу з недобросовісною конкуренцією.

---

[73] Основы экономической безопасности (Государство, регион, предприятие, личность) / Под ред. Е.А. Олейникова. – М.: ЗАО "Бизнес-школа "Интел-синтез", 1997. – 228 с.

[74] Шлыков В.В. Экономическая безопасность предприятия (во что обходится хозяйствующим субъектам защита собственности и способы минимизации возможных потерь) / В.В. Шлыков// РИСК. – 1997. – № 6. – С. 61-63.

[75] Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия / В.В. Шлыков. – СПб.: "Алетейя", 1999. – 138 с.

Заслуговує уваги точка зору В.А. Копилова [76, с. 62] та В. Шликова [77, с. 62] про необхідність захисту економічних інтересів суб'єктів господарювання. У цьому питанні важливим є пошук правильного співвідношення між можливими втратами при порушенні економічних інтересів підприємства і допустимою величиною витрат для запобігання або мінімізації втрат. Проте наведена точка зору носить дещо декларативний характер, оскільки захист економічних інтересів автором зводиться до захисту інформації, що містить комерційну таємницю, а проблема виявлення граничного значення рівня витрат, що розділяє витрати на ефективні і неефективні, тільки умовна.

Окрім того, можна сказати про підходи до визначення економічної безпеки підприємства та можна тлумачити їх, як вузькофункціональні. Йдеться про розгляд економічної безпеки підприємства з позиції окремого аспекту його діяльності. Найважливішим напрямом розробки та впровадження системи економічної безпеки, у тому числі і підприємств, є залучення дієвого інструменту – фінансової безпеки. Обґрунтовується, що бухгалтерський облік є однією з основних функцій управління, спрямованою на забезпечення економічної безпеки підприємства, і саме бухгалтерський облік виключає можливість розкрадань майна підприємства без встановлених законом наслідків, створює інформаційні умови для здійснення контролю доцільності і законності використання ресурсів в превентивному, поточному і наступному режимах і сприяє запобіганню реалізації загроз, які знижують економічну стійкість підприємств.

Економічна безпека підприємства є системою понять та пов'язана не лише з його внутрішнім станом, але й із взаємодією суб'єктів зовнішнього середовища, з якими суб'єкт господарювання вступає у взаємовідносини. Також економічну безпеку підприємства можна розглядати як ступінь гармонізації в часі та просторі економічних інтересів цього суб'єкта з інтересами пов'язаних з ним суб'єктів зовнішнього середовища, що діють поза його межами.

---

[76] Копылов В.А. Информационное право: [учеб.] / В.А. Копылов – М.: Юристь, 2004. – 512 с.

[77] Шлыков В.В. Экономическая безопасность предприятия (факторы влияния, анализ необходимости) / В.В. Шлыков // Машиностроитель. – 1995. – № 1. – С. 31-34.

Дослідники А. Городецький та А. Морукова наголошують на тому, що проблеми економічної безпеки підприємства необхідно вирішувати в сукупності на основі загальноекономічних, контрольних і правоохоронних механізмів забезпечення [[78], с. 92].

Отже, розглянувши думки авторів стосовно поняття "економічна безпека підприємства", можна дійти висновку, що вона залежить: від стану та ефективного використання його ресурсів; від внутрішніх та зовнішніх факторів, які певною мірою мають вплив на підприємство.

На підставі проведеного аналізу підходів дослідників щодо визначення економічної безпеки підприємства, нами запропоновано власне визначення економічної безпеки підприємства. Таким чином, під економічною безпекою підприємств будемо розуміти стан збереження майна та інформації підприємства відповідно до обраної стратегії та принципу безперервності діяльності. Вважаємо, що дане визначення повною мірою відображає всі аспекти забезпечення економічної безпеки підприємств.

При впровадженні економічної безпеки на підприємстві необхідно говорити про використання системного підходу до механізмів її забезпечення. Він передбачає тісний взаємозв'язок всіх елементів системи і гарантує комплексний ефект від її забезпечення.

Під забезпеченням економічної стабільності розуміється реалізація комплексу заходів для виявлення, попередження і припинення протиправних дій, здатних негативно відбитися на економічному становищі комерційних структур, їх акціонерів та ділових партнерів.

На формування економічної безпеки підприємства впливає зміна умов господарювання, що характеризуються нестабільністю, мінливістю, невизначеністю та нестійкістю економічного середовища. Це впливає на управління суб'єктом господарювання в умовах ринкових відносин та його можливість адаптуватися до змінних умов ринку. Для того, щоб констатувати наявність економічної безпеки підприємства, необхідно створити необхідні передумови для її забезпечення. Необхідним є використання ефективної системи заходів з певним економічним, юридичним, інформаційним та організаційним забезпеченням. Це передбачає

[78] Городецкий А. Формирование единой системы государственного финансового контроля / А. Городецкий, А. Морукова // Вопросы экономики. – № 1. – 2004. – С. 92.

формування ефективної структури управління з цілісним використанням праці співробітників відділу безпеки; оцінку економічних взаємовідносин, в тому числі з міжнародними партнерами, та ухвалення ефективних управлінських рішень про їх збереження чи подальший розвиток.

Забезпечення економічної безпеки необхідно розглядати як попередження виникнення збитків різного характеру та прояву несприятливих факторів в усіх напрямах діяльності підприємства. Негативно на економічну безпеку підприємства можуть впливати як внутрішні, так і зовнішні фактори. До зовнішніх факторів, що впливають на економічну безпеку, відноситься законодавчо-правова система держави, яка здійснює регулювання економікою та соціальним розвитком країни, її безпекою.

Ідентифікація чинників ризику, небезпек та загроз є найважливішим завданням забезпечення економічної безпеки підприємства.

На думку вітчизняних і зарубіжних авторів найбільш відомих публікацій з проблематики безпеки, успішний захист підприємства від загроз залежить від повноти реалізації принципів системного підходу до вирішення даної проблеми. Системність підходу до структуризації безпеки підприємства можна зобразити у вигляді наступної схеми (рис. 1.5).

У нашій країні сьогодні зростає необхідність у формуванні фундаментальної теорії економічної безпеки на рівні суб’єктів господарювання. Дослідження практики господарювання підприємств молочної промисловості показує, що економічна безпека підприємницької сфери є поєднанням економічних та правових умов, які забезпечують стійке здійснення фактів господарського життя в тривалій перспективі законними і ефективними методами. Процес реалізації економічної безпеки передбачає зниження ризику втрати достовірності, ефективності та законності використання трудових, фінансових, виробничих, земельних та підприємницьких ресурсів.

Основні складові концепції економічної безпеки підприємств наведено в Додатку Б.

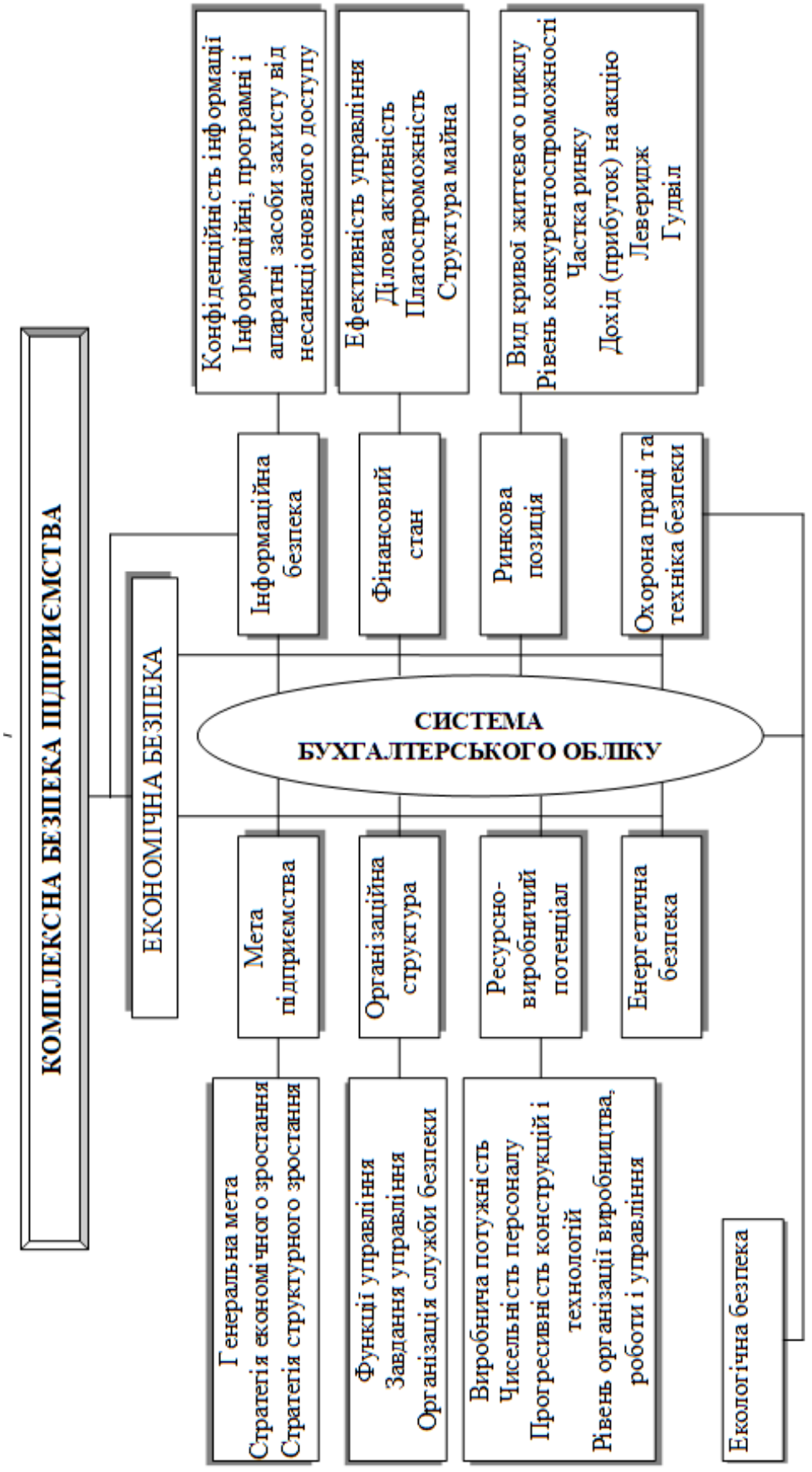


Рис. 1.5. Концепція комплексної безпеки підприємства

Складнощі в застосуванні системного підходу до забезпечення економічної безпеки підприємства полягають в тому, що необхідно давати економічну оцінку альтернативних варіантів проектування і реалізації певної системи заходів. Передбачається, що така система заходів повинна забезпечувати найбільш раціональне вирішення комплексу завдань з дотримання економічної безпеки певного підприємства в умовах невизначеності впливу зовнішніх і внутрішніх загроз як в частині прогнозування загроз, так і можливостях їх усунення.

Позитивно оцінюючи вплив зовнішнього та внутрішнього середовища слід розглядати управлінські та технічні нововведення, які комплексно впливають на господарську діяльність підприємства. Підприємство у своїй господарській діяльності може використовувати ці пропозиції, а може й нехтувати ними, проте необхідність враховувати пропозиції обумовлено низкою об'єктивних причин. При здійсненні інноваційної діяльності виникають особливі засоби та способи виробництва. Це зумовлює необхідність активного приєднання підприємств до інноваційних процесів, критичного аналізу впровадження можливих засобів та способів виготовлення одного і того ж виду продукції. З іншої ж точки зору – це різноманіття шляхів підвищення ефективності виробництва, форм організації виробництва та праці. Необхідність впровадження нововведень у сфері технології виробництва, організації виробництва та управління, зумовлена, двома причинами:

1) можливістю зниження витрат виробництва і в той же час збільшенням прибутку та отриманням конкурентних переваг на ринку;

2) розширенням існуючого сегменту ринку та оволодіння новими ринками збуту.

Зрештою, і перший, і другий напрями призведуть до збільшення фінансового результату підприємства, посиленню його конкурентних переваг на ринку, а також підвищенню існуючого рівня економічної безпеки.

Взаємодія підприємства із зовнішнім середовищем відбувається за допомогою виконання у ньому функціональних видів господарської діяльності. До учасників зовнішнього середовища необхідно перш за все віднести державу, яка здійснює найбільший вплив на діяльність суб'єктів господарювання, внаслідок регулювання всіх напрямів його господарської діяльності. Всі підприємства в ході господарської діяльності обов'язково взаємодіють зі споживачами продукції, яку виготовляють. Також

підприємства взаємодіють і з постачальниками певних ресурсів та сировини для виготовлення продукції. Суб'єкти ринку значною мірою визначаються специфікою господарської діяльності підприємства.

Існуючі підходи до розробки методики оцінки визначення рівня економічної безпеки поділяються на наступні групи, залежно від підходу, що застосовується (рис. 1.6).

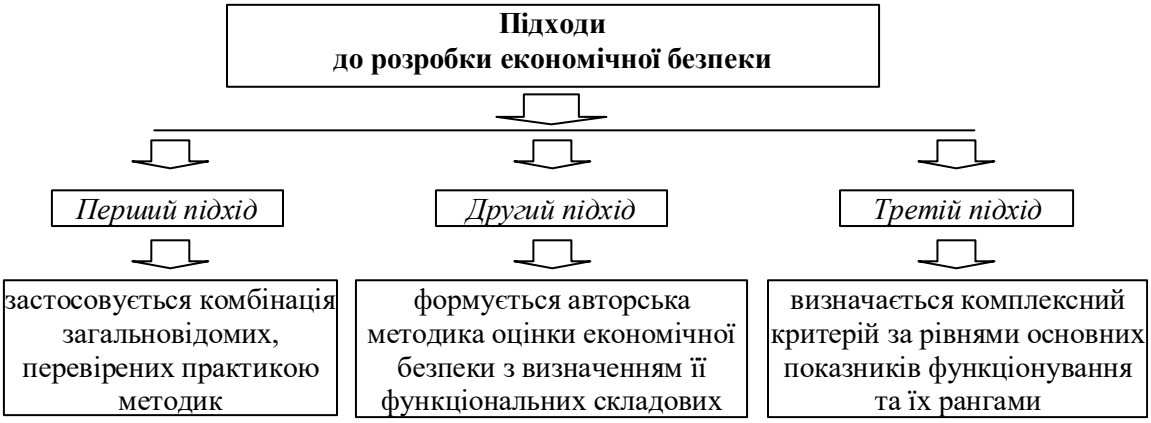


Рис. 1.6. Підходи до розробки економічної безпеки [79, с. 13]

Оцінка рівня економічної безпеки для підприємств є важливою, передусім, тому, що їх потенціал є базовим чинником антикризового управління. Належний рівень економічної безпеки забезпечує сталий економічний розвиток країни, її незалежність та безпеку в цілому.

В процесі розробки економічної безпеки підприємства можна виділити дві основні стадії (рис. 1.7).

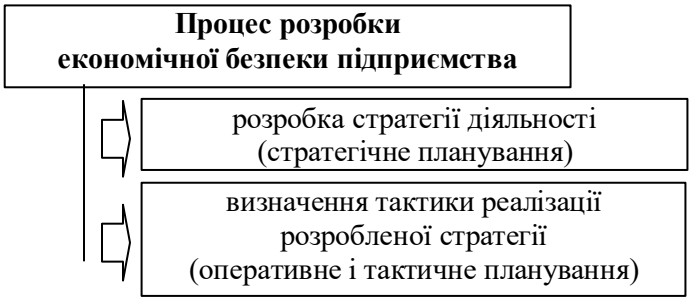


Рис. 1.7. Стадії розробки економічної безпеки підприємства [80, с. 13]

[79] Дикий А.П. Економічна безпека підприємства: сутність та шляхи забезпечення / А.П. Дикий // Materiały II Międzynarodowej naukowe-praktycznej konferencji "Wykształcenie i nauka bez granic – '2005". 19-27 grudnia 2005 roku. Tom 6. Ekonomiczne nauki. – Przemyśl-Praha: Sp. z o.o. "Nauka i studia", 2005. – 130 s. – S. 12-14.

[80] Дикий А.П. Економічна безпека підприємства: сутність та шляхи забезпечення / А.П. Дикий // Materiały II Międzynarodowej naukowe-praktycznej konferencji "Wykształcenie i nauka bez granic – '2005". 19-27 grudnia 2005 roku. Tom 6. Ekonomiczne nauki. – Przemyśl-Praha: Sp. z o.o. "Nauka i studia", 2005. – 130 s. – S. 12-14.

Концепція економічної безпеки повинна включати: визначення зовнішніх і внутрішніх загроз економічній безпеці підприємства; ідентифікацію та моніторинг чинників, які зміцнюють або негативно впливають на рівень його соціального та економічного стану на перспективу; визначення параметрів та критеріїв показників, що обумовлюють інтереси підприємства і відповідають рівню економічної безпеки; впровадження економічної політики, що використовує інструменти обліку, які здійснюють вплив на рівень економічної безпеки; напрями діяльності суб'єкта господарювання відносно реалізації стратегії.

Розробка стратегії є ефективним засобом прогнозування майбутніх загроз та можливостей, дозволяючи управлінському персоналу планувати виробничу діяльність на тривалий період. Стратегія є базисом для ухвалення рішень щодо попередження та виявлення ризиків.

Стратегічне планування в напрямі економічної безпеки дозволяє розробити та впровадити стратегічну політику підприємства, що забезпечує реалізацію усіх стратегічних завдань.

Інформаційні системи управління підприємством, серед яких ключове місце належить системі бухгалтерського обліку, повинні організовуватися таким чином, щоб забезпечувати стратегічне і тактичне планування діяльності та унеможливлювати вихід інформації, не призначеної для зовнішніх суб'єктів, що і служить основою економічної безпеки підприємства.

Доволі точно зазначає В.С. Гусєв, що ефективні структури безпеки підприємства повинні базуватися на узгодженні національних та регіональних інтересів, ресурсних можливостей підприємств і регіонів, моделюванні ризиків можливих загроз і факторів невизначеності в господарській діяльності, оптимізації обраних рішень [[81], с. 6].

Впровадження економічної безпеки підприємства повинне забезпечувати виконання двох основоположних функцій: створення механізмів захисту та управління цими механізмами.

[81] Экономика и организация безопасности хозяйствующих субъектов: [2-е изд] / В.С. Гусев, В.А. Демин, Б.И. Кузин, М.Д. Медников, А.С. Соколицын, С.В. Степашин, А.В. Федотов, В.Л. Шульц. – СПб.: Питер, 2004. – 288 с.

Ефективна система безпеки підприємств може бути побудована на комплексному підході до організації процесу захисту виробничо-господарської і фінансової діяльності від прояву реальних та потенційних, зовнішніх та внутрішніх загроз.

Комплексна безпека підприємства визначається як захищеність його функцій від внутрішніх та зовнішніх загроз за наявності рівноваги між функціями та інтересами держави, суспільства та особистості.

Забезпечення економічної безпеки є досить важливим та складним напрямом в діяльності підприємства, без реалізації якого неможливе функціонування та розвиток підприємства, оскільки захист та безпека даних господарської діяльності є основою для збереження майна підприємства. До складу системи забезпечення економічної безпеки організації входить об'єкт, суб'єкт безпеки та механізм забезпечення економічної безпеки організації.

Об'єктом безпеки може виступати все те, на що спрямовані дії із забезпечення економічної безпеки (бухгалтерська інформація, комерційна таємниця, інформаційні ресурси, майно організації та засоби виробництва).

Суб'єктом безпеки є підрозділи підприємства, які займаються забезпеченням безпеки, а саме:

– зовнішні, до яких належить держава, шляхом реалізації своїх функцій через законодавчі, виконавчі, судові, правоохоронні та інші органи; контрагенти підприємства;

– внутрішні, які входять до складу структури підприємства.

Механізм забезпечення економічної безпеки підприємств є дещо унікальним, тому що залежить від специфіки діяльності підприємства, системи бухгалтерського обліку та ефективності його роботи та ряду інших чинників. Механізмом забезпечення економічної безпеки є теоретичне обґрунтування послідовності дій, які необхідно здійснювати з метою забезпечення економічної безпеки. Вибір найбільш оптимального механізму забезпечення економічної безпеки підприємства сприяє підвищенню рівня безпеки підприємства.

Основними цілями забезпечення економічної безпеки підприємства в частині бухгалтерського обліку є:

– своєчасне виявлення зовнішніх та внутрішніх загроз в системі бухгалтерського обліку;

– збереження та ефективне використання ресурсів підприємства (фінансових, матеріальних, інформаційних, кадрових);

– прогресивний, незалежний розвиток підприємства.

Виходячи з вищенаведених цілей, на підприємстві необхідно вирішувати наступні завдання, серед яких є:

– прогнозування та уникнення виникнення загроз економічній безпеці підприємства в частині бухгалтерського обліку;

– виявлення та захист найбільш слабких, уразливих сторін господарської діяльності підприємства;

– прийняття оптимальних управлінських рішень на підставі аналітичної інформації, що надається системі бухгалтерського обліку;

– організація оперативної взаємодії підприємства з державними органами;

– забезпечення постійного контролю за здійсненням механізму забезпечення економічної безпеки підприємства як в цілому, так і в частині бухгалтерського обліку.

Однак, як зазначає Є.А. Олєйніков, основним завданням системи безпеки підприємства є запобігання виникненню збитків, а зрештою й запобігання загрозі банкрутства підприємства [[82], с. 545]. Тому на кожному підприємстві повинна розроблюватися програма економічної безпеки в частині бухгалтерського обліку, що враховує сучасні загрози та тенденції. Також в програмі передбачається можливість попередження загроз, що можуть виникати в межах підприємства.

Досягнення цілей економічної безпеки підприємств можливе лише при ефективній побудові системи економічної безпеки підприємства в частині бухгалтерського обліку та при її постійному вдосконаленні, а це, в свою чергу, є неможливим без підтримки держави.

Економічна безпека підприємства – це певний стан захищеності підприємства від зовнішніх та внутрішніх загроз, які є факторами негативного впливу. Безпека підприємства нерозривно розглядається з її економічною сутністю. Це зумовлено тим, що основною метою будь-якої підприємницької діяльності є отримання прибутку, який знаходить своє відображення в економічних показниках та бухгалтерській звітності, що є передумовою саме розгляду економічної безпеки підприємства як результату його діяльності.

[82] Экономическая и национальная безопасность: [учеб.] / Под ред. Е.А. Олейникова. – М.: Экзамен, 2005. – 768 с.

Зміст поняття економічної безпеки підприємства включає систему заходів, що забезпечують конкурентоспроможність та економічну стабільність підприємства, а також сприяють підвищенню добробуту працівника.

Співвідношення між рівнями економічної безпеки підприємств та держави є неоднозначним в умовах ринкової економіки, оскільки підприємства, маючи певний рівень економічної свободи та самостійність у здійсненні своєї фінансово-господарської діяльності та прийнятті управлінських рішень, все ж функціонують в рамках державного законодавства.

Висновки до 1-го розділу

1. Дослідженням встановлено неоднозначність підходів до визначення поняття економічної безпеки. В роботі виділено наступні рівні економічної безпеки: мікро- (особа, організація), мезо- (галузь, регіон), макро- (суспільство, держава), а також визначено напрями економічної безпеки, серед яких: науково-технічна безпека; інформаційна безпека; інтелектуальна безпека; енергетична безпека; фінансова безпека; інвестиційна безпека; безпека зовнішньоекономічної діяльності тощо.

2. Економічній безпеці підприємства властивий подвійний характер: по-перше, можливе ії власне функціонування, по-друге – вона може бути складовою економічної безпеки системи більш глобального рівня, що дозволить забезпечити виконання функцій певним регіоном та державою.

3. В результаті аналізу існуючих підходів до визначення економічної безпеки підприємства запропоновано авторське визначення даного поняття, згідно якого під економічною безпекою підприємств слід розуміти стан збереження майна та інформації підприємства відповідно до обраної стратегії та принципу безперервності діяльності. На нашу думку, дане визначення повною мірою відображає сутність економічної безпеки підприємства та відображає її взаємозв'язок з бухгалтерським обліком. При забезпеченні економічної безпеки важливим є визначення співвідношення між рівнем захисту державних інтересів та відкритістю економіки.

РОЗДІЛ 2
БУХГАЛТЕРСЬКИЙ ОБЛІК ЯК ІНФОРМАЦІЙНА МОДЕЛЬ ЕКОНОМІЧНОЇ БЕЗПЕКИ

2.1. Прояв загроз економічній безпеці підприємства в системі бухгалтерського обліку

Як було з'ясовано у ході дослідження, в сучасних умовах економічна безпека є загальнонаціональним комплексом заходів, спрямованих на постійний стабільний розвиток та удосконалення економіки країни, що обов'язково передбачає соціально-політичну стабільність та самостійність держави, усіх її складових, а також використання механізму протидії зовнішнім та внутрішнім загрозам.

Досліджуючи економічну безпеку підприємства, не можна оминати чинники, які здійснюють негативний вплив на безпеку підприємства та економіки в цілому.

Вітчизняна та світова практика забезпечення безпеки свідчать про те, що для ефективної протидії загрозам і створення умов безпечної та стабільної роботи підприємства, необхідно не лише створити систему комплексного захисту, але й забезпечити її раціональне функціонування [83].

Рівень економічної безпеки формують чинники зовнішнього та внутрішнього середовища, які можуть змінюватись відповідно до галузі народного господарства. Так, О.І. Судакова, Д.В. Гречко та А.В. Шкурупій [84] зазначають, що є й загальні типові чинники, які впливають на рівень економічної безпеки підприємства незалежно від форм власності та галузі виробництва, які зображено на рис. 2.1.

Існують також й інші чинники економічної безпеки підприємства, які не пов'язані з безпосередньою виробничою діяльністю, але суттєво впливають. Вони пов'язані з поведінкою окремих людей, їх мораллю, духовністю.

Всі перераховані вище чинники потрібно реалізовувати відповідно до політики економічної безпеки, спрямовувати їх на реалізацію виробничої стратегії, досягнення належного рівня економічної безпеки кожного підприємства.

---

[83] Герасименко В.А. Организация комплексной защиты информации на современных объектах / В.А. Герасименко, М.В. Мецатунян // Вопросы защиты информации. 1995. – № 1. – С. 10-16.

[84] Судакова О.І., Гречко Д.В., Шкурупій А.В. Стратегія забезпечення належної економічної безпеки підприємства [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com4._SVMN_2007Economics18818.doc.htm.

Рис. 2.1. Чинники, які впливають на рівень економічної безпеки підприємства

Слід зазначити, що в деяких публікаціях висвітлений ряд підходів до класифікації та оцінки можливих загроз як на концептуальному рівні В. Гайкович, А. Першин [85], В.А. Герасименко, М.В. Мецатунян [86], так і на прикладі конкретних об'єктів В. Гайкович, А. Першин [87], Є.А. Олєйніков [88], зокрема з використанням математичних методів Е.І. Абалмазов, М.Е. Кротова [89], Е.І. Абалмазов [90], Ю.Б. Клюєв, А.Я. Лавров, В.Р. Окороков [91], Є.Д. Соложенцев, В.В. Карасьов, В.Є. Соложенцев [92].

Вважаємо, що найбільш чітке визначення загрози безпеці підприємництва запропоноване В.І. Ярочкіним : "реально або потенційно можливі дії або умови навмисного або випадкового (ненавмисного) порушення режиму функціонування підприємства шляхом нанесення матеріального (прямого або непрямого) збитку, що приводить до фінансових втрат, включаючи і упущену вигоду" [93].

Негативно впливати на економічну безпеку підприємств можуть:

1) навмисні або ненавмисні дії окремих працівників підприємства та інших суб'єктів господарювання;

2) збіг об'єктивних обставин (стан фінансової кон'юнктури на ринках даного підприємства, наукові відкриття та технологічні розробки, форс мажорні обставини тощо).

"Кадрове питання, – наголошує В. Кульпінов, – вважається ключовою позицією в системі безпеки підприємства. Експерти в галузі безпеки приписують персоналу 70-80 % потенційних загроз мирному процвітанню фірми, залишаючи на частку зовнішніх чинників лише 20-30 %. На перших

---

85 Гайкович В. Безопасность электронных банковских систем / В. Гайкович, А. Першин / Под ред. Ю.В. Гайковича. – М.: Единая Европа, 1994. – 363 с.

86 Герасименко В.А. Организация комплексной защиты информации на современных объектах / В.А. Герасименко, М.В. Мецатунян // Вопросы защиты информации. 1995. – № 1. – С. 10-16.

87 Гайкович В. Безопасность электронных банковских систем / В. Гайкович, А. Першин / Под ред. Ю.В. Гайковича. – М.: Единая Европа, 1994. – 363 с.

88 Основы экономической безопасности (Государство, регион, предприятие, личность) / Под ред. Е.А. Олейникова. – М.: ЗАО "Бизнес-школа "Интел-синтез", 1997. – 228 с.

89 Абалмазов Э.И. Декомпозиция и композиция систем безопасности / Э.И. Абалмазов, М.Э. Кротова // Системы безопасности, связи и телекоммуникаций. – 1995. – № 6. – С. 19-21.

90 Абалмазов Э.И. Концепция безопасности: тактика высокоэффективной защиты / Э.И. Абалмазов // Системы безопасности. – 1995. – № 2.

91 Клюев Ю.Б. Экономико-математическое моделирование производственных систем энергетики / Ю.Б. Клюев, А.Я. Лавров, В.Р. Окороков. – М.: Высшая школа, 1992.

92 Соложенцев Е.Д. Логико-вероятностная оценка банковских рисков и мошенничество в бизнесе / Е.Д. Соложенцев, В.В. Карасев, В.Е. Соложенцев. – СПб.: Политехника, 1996. – 59 с.

93 Ярочкин В.И. Предприниматель и безопасность. Ч. 2 / В.И. Ярочкин. – М.: Экспертное бюро, 1994. – 132 с.

порах розвитку бізнесу зовнішні загрози мінімальні, оскільки молоде підприємство не представляє великого інтересу для зовнішніх недоброзичливців, однак, лише в тому випадку, коли компанія має намір вести конкурентну політику" [94, с. 54].

Проф. Б.І. Холод та доц. Ю.М. Воробйов зазначають, що "будь-яке підприємство взаємодіє із зовнішнім середовищем, тобто з тим оточенням, яке впливає на господарську діяльність конкретного суб'єкта господарювання. Зовнішнє середовище складається з чотирьох основних груп компонентів:

1) державні центральні і місцеві органи влади, їх служби й установи. Цей компонент зовнішнього середовища здійснює суттєвий вплив, особливо в умовах нестійкої економіки, нерозвиненої системи ринкових відносин;

2) постачальники основних елементів виробництва – машин і устаткування, сировини і матеріалів, палива і енергії тощо, а також різні посередники, які надають ті чи інші послуги;

3) споживачі продукції, які визначають кінцеву необхідність господарської діяльності даного підприємства, його економічну і фінансову результативність;

4) населення – головний компонент зовнішнього середовища, тому що саме воно є основним споживачем створених товарів і послуг, а також постачальником робочої сили, тобто персоналу будь-якого підприємства" [95, с. 9].

Всі чинники небезпеки та загроз бухгалтерській інформації можна згрупувати за різними класифікаційними ознаками [96]. Так, залежно від можливості їх прогнозування виділяють наступі загрози (рис. 2.2).

Рис. 2.2. Прогнозовані загрози економічній безпеці

[94] Кульпінов В. Кадри позбавляють усього. Як нейтралізувати штатних шкідників / В. Кульпінов // Контракти. – 2004. – № 41. – С. 54-55.

[95] Управління ресурсами підприємства: [навч. посіб.] / Під ред. к.е.н. Ю.М. Воробйова і д.е.н. Б.І. Холода. – К.: "Центр навчальної літератури", 2004. – 288 с.

[96] Дикий А.П. Економічна безпека суб'єкта господарювання: характеристика загроз / А.П. Дикий // Вісник Житомирського державного технологічного університету. Економічні науки. – 2007. – № 1 (39). – С. 68-71.

Іншими словами, прогнозовані загрози безпосередньо пов'язані з діяльністю підприємства і можуть бути передбачені відповідними службами підприємства. Непередбачувані загрози мають місце в діяльності підприємства в результаті зміни умов зовнішнього середовища (прийняття закону, політична ситуація в країні, зміна валютного курсу).

Існують і інші класифікації загроз економічній безпеці підприємства, які зображено на рис. 2.3.

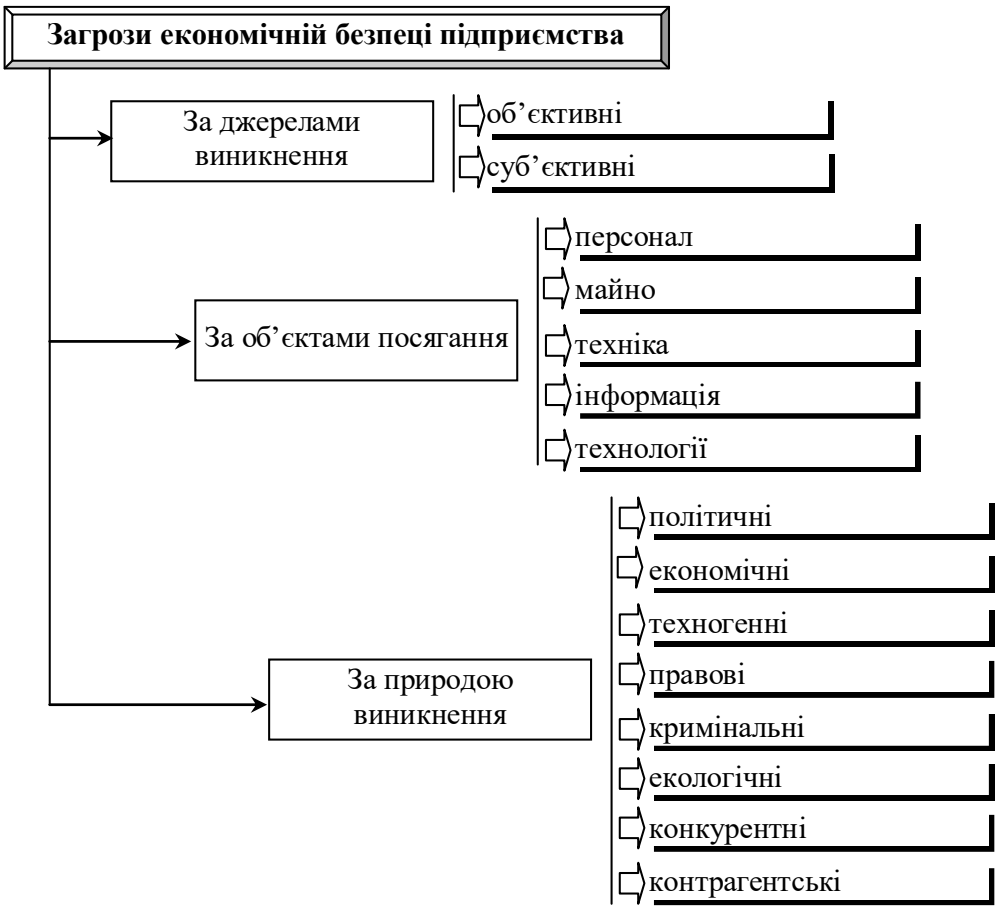


Рис. 2.3. Загрози економічній безпеці підприємства за різними класифікаційними ознаками

Об'єктивні загрози виникають без участі та бажання підприємства або його співробітників, незалежно від ухвалених рішень, дій менеджерів. Суб'єктивні загрози викликані навмисними або ненавмисними діями людей, різних установ та організацій, зокрема державних та міжнародних підприємств конкурентів.

Окрім того, загрози класифікують за об'єктами посягання та за природою виникнення загроз, що дає змогу зрозуміти, який суб'єкт та на що може зазіхати.

Найбільшого поширення в науці отримало виділення небезпек і загроз залежно від сфери їх виникнення. За цією ознакою розрізняють внутрішні і зовнішні загрози.

Отже, розробляючи цілі та визначаючи об'єкти стратегії безпеки облікових даних, необхідно враховувати:

вплив зовнішніх та внутрішніх загроз економічної безпеки підприємства;

впровадження економічної політики, яка включає механізми обліку факторів, що впливають на стан економічної безпеки;

здатність підприємства щодо реалізації даної стратегії.

Існує велика кількість загроз економічній безпеці в системі бухгалтерського обліку. Це пояснюється тим, що підприємство має різноманітні взаємозв'язки з іншими суб'єктами господарської діяльності рис. 2.4.

Рис. 2.4. Зовнішні та внутрішні загрози економічній безпеці підприємства в системі бухгалтерського обліку

Зовнішні загрози виникають за межами підприємства, не пов'язані з його виробничою діяльністю, та можуть завдати значних збитків. Внутрішні загрози пов'язані з діяльністю підприємства та його персоналом. Ці загрози зумовлені процесами, які виникають в господарській діяльності підприємства та можуть впливати на результати господарської діяльності. Найсуттєвішими з них є: протиправні дії співробітників бухгалтерської служби, порушення режиму збереження бухгалтерської інформації, що становить комерційну таємницю, відсутність належної кваліфікації бухгалтерського персоналу, неналежний рівень технічного забезпечення, суттєві прорахунки як в тактичному, так і в стратегічному управлінні, оскільки від дотримання заданих підприємством параметрів залежить ефективність та результативність діяльності підприємства.

Під впливом різних зовнішніх чинників можуть виникнути й різні зовнішні загрози економічній безпеці підприємства, до яких відносять: несприятливі зміни політичної ситуації, зміну законодавства, промислово-економічне шпигунство, недобросовісну конкуренцію, розкрадання матеріальних засобів, зараження програм ЕОМ різного роду комп'ютерними вірусами, протизаконні фінансові операції, крадіжки грошових коштів та матеріальних цінностей, несанкціонований доступ конкурентів до бухгалтерської інформації, що становить комерційну таємницю.

До внутрішніх загроз економічній безпеці підприємства слід відносити: недостатній рівень дисципліни персоналу, недотримання правил збереження конфіденційної інформації, неправильна оцінку кваліфікації кадрів, низький освітній рівень керівників, вибір ненадійних партнерів і інвесторів, вихід з ладу обчислювальної техніки, суттєві прорахунки як в тактичному, так і в стратегічному плануванні.

Проаналізувавши внутрішні загрози, можемо сказати, що здебільшого проблеми всередині підприємства виникають через недостатню кваліфікацію керівників.

Класифікуючи загрози за об'єктами особливого значення набувають загрози обліковій інформації. Вивчення загроз обліковій інформації є дуже важливим для керівництва підприємства, оскільки від її достовірності, повноти та оперативності залежить результат функціонування всієї господарської системи. Тут необхідно використовувати класифікацію навмисних інформаційних загроз, що виникають в комп'ютерній інформаційній системі бухгалтерського (КСБО) (табл. 2.1).

Таблиця 2.1. Класифікація видів економічних загроз в умовах використання КСБО

№ з/п	*Принцип класифікації*	*Види ймовірних загроз*
1	За метою впливу на КСБО	– порушення конфіденційності інформації – порушення цілісності інформації – часткове або повне порушення працездатності КСБО
2	За принципом впливу на КСБО	– з використанням доступу об'єкта системи до об'єкту загрози – використання скритих каналів
3	За характером впливу на КСБО	– активний вплив – пасивний вплив або бездіяльність
4	За причиною появи помилки захисту, що використовується	– невідповідність політики безпеки реаліям КСБО – помилка адміністративного управління – помилка в алгоритмах та програмах – помилка в реалізації алгоритмів та програм
5	За способом впливу на об'єкт загрози	– безпосередній вплив на об'єкт загрози – вплив на систему прийняття рішень – опосередкований вплив через інших користувачів КСБО – присвоєння прав іншого користувача інформаційної системи
6	За способом впливу на КСБО	– в активному режимі – в пакетному режимі
7	За об'єктом загрози	– КСБО в цілому – об'єкти КСБО – суб'єкти КСБО – канали передачі даних, пакети даних
8	За засобами реалізації загрози, що використовуються	– віруси – програмні пастки
9	За станом об'єкта загрози	– зберігання даних – передача даних – обробка даних

Наведена класифікація загроз в умовах використання комп'ютерних систем бухгалтерського обліку може застосовуватись також і для інших об'єктів захисту, оскільки вона дозволяє адекватно диференціювати за цими об'єктами самі загрози та їх джерела.

Виявлення і ідентифікація чинників ризику, небезпек і загроз в частині бухгалтерського обліку – одне з найбільш важливих завдань забезпечення економічної безпеки підприємства.

Зовнішнє середовище може також позитивно впливати на господарську діяльність підприємства, у вигляді впровадження комплексних технологічних та управлінських нововведень, що ефективно відобразяться на його діяльності. Як результат інноваційних процесів є поява нових способів та засобів виробництва.

Взаємодія підприємств із зовнішнім середовищем здійснюється в ринковому середовищі, одним з параметрів стану якої є присутність загальноекономічних ризиків, які пов'язані з рівнем розвитку економіки країни в цілому. Існують наступні види взаємодії підприємств з суб'єктами зовнішнього середовища, до яких відносяться пряма та опосередкована взаємодія.

Пряма взаємодія передбачає безпосередні контакти між підприємствами, які відбуваються тимчасово або постійно та задокументовані. Результат такої взаємодії впливає на розмір прибутку підприємства.

При опосередкованій взаємодії не відбувається безпосереднього контакту між окремим підприємством та суб'єктами зовнішнього середовища, діяльність яких, прямо не впливаючи на оперативну діяльність підприємства, визначає стратегічно важливі рішення, які приймаються управлінським апаратом. Не зважаючи на те, що опосередкована взаємодія не означає безпосередніх контактів між суб'єктами, вона впливає на результат діяльності підприємства, зокрема, на його прибуток.

Внутрішні чинники загроз економічній безпеці підприємства пов'язані з його господарською діяльністю та діями персоналу. Ці загрози зумовлені процесами, які виникають у ході виробництва та реалізації продукції і можуть впливати на результати господарської діяльності. Найсуттєвішими з них є: якість планування та прийняття рішень; дотримання технології виробництва; організація праці та робота з персоналом; фінансова політика підприємства; дисципліна персоналу тощо.

Найважливішою проблемою, яка постає перед керівництвом та службою безпеки підприємства, є проблема лояльності співробітників або проблема внутрішніх загроз бухгалтерській інформаційній, і, в свою чергу, економічній безпеці.

Цілком ймовірно, що працівник, який має доступ до важливої інформації та володіє певними знаннями про структуру корпоративної мережі, може завдати підприємству набагато більше шкоди, ніж будь-яка стороння особа ззовні.

Як зазначають В.С. Гусєв та інші [97, с. 70], система реальних та потенційних загроз економічній безпеці не статична. Загрози можуть з'являтися та зникати, наростати та зменшуватися. До того ж суб'єкти відносин безпеки (людина, суспільство, підприємство, регіон, держава) є досить складними багатоцільовими системами, визначити потребу в безпеці яких досить складно.

Далі автори загрозу безпеці підприємства трактують як будь-який конфлікт цілей функціонування та розвитку підприємства із зовнішнім або внутрішнім середовищем, а якщо цілі збігаються – як неспівпадання шляхів їх досягнення. Іншими словами, загроза безпеки підприємства – сукупність умов та факторів, що створюють небезпеку його життєво важливим інтересам [98, с. 71].

Ми погоджуємося із запропонованим авторами визначенням, яке дозволяє розглядати систему забезпечення безпеки підприємства як комплекс ефективних заходів (управлінських рішень) для локалізації реальних та потенційних внутрішніх і зовнішніх загроз. Цей комплекс заходів має бути обґрунтований оцінкою характеру цих загроз, аналізом кризових ситуацій, інших несприятливих чинників, що перешкоджають досягненню цілей підприємства, і що представляють небезпеку для нього.

Аналізуючи численні загрози підприємству, власник підприємства повинен спрогнозувати найбільш небезпечні з них та розробити систему заходів щодо їх своєчасного попередження або виявлення та послаблення їх впливу. Виявлення наведених вище загроз значною мірою допоможе власникам підприємств захистити їх комерційну таємницю в частині бухгалтерського обліку, і тим самим забезпечити належний рівень її захисту та попередити розголошення.

---

97 Экономика и организация безопасности хозяйствующих субъектов: [2-е изд] / В.С. Гусев, В.А. Демин, Б.И. Кузин, М.Д. Медников, А.С. Соколицын, С.В. Степашин, А.В. Федотов, В.Л. Шульц. – СПб.: Питер, 2004. – 288 с.

98 Экономика и организация безопасности хозяйствующих субъектов: [2-е изд] / В.С. Гусев, В.А. Демин, Б.И. Кузин, М.Д. Медников, А.С. Соколицын, С.В. Степашин, А.В. Федотов, В.Л. Шульц. – СПб.: Питер, 2004. – 288 с.

2.2. Бухгалтерський облік як інструмент збереження комерційної таємниці підприємств

Необхідність захисту комерційної таємниці, що може міститися в даних бухгалтерського обліку, від небажаних зовнішніх впливів та значних внутрішніх змін є, зокрема, однією з базових потреб для кожного окремого підприємства.

В процесі розробки заходів із захисту складових комерційної таємниці підприємств необхідно, передусім, обґрунтувати з економічної точки зору необхідність засекречування певної бухгалтерської інформації. Для надійного захисту складових комерційної таємниці необхідним є також чітке уявлення щодо каналів розповсюдження такої інформації.

Вирішення практичних проблем із забезпечення безпеки бухгалтерської інформації є важливою передумовою, спрямованою на забезпечення безпеки підприємства на всіх етапах його розвитку. Особливого значення набуває проблема визначення місця комерційної таємниці у становленні системи економічної безпеки.

У 1990 році, після тривалої перерви, у Законі "Про підприємства в СРСР" знову з'явилося поняття комерційної таємниці (ст. 33). Даний закон містив правові засади захисту комерційної таємниці в усьому пострадянському просторі, зокрема:

"– під комерційною таємницею підприємства розуміються відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами й іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) яких може заподіяти збиток його інтересам;

склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються керівником підприємства. Види діяльності підприємств, відомості, які не можуть становити комерційної таємниці, визначаються Радою Міністрів СРСР з метою запобігання приховуванню підприємством відомостей про забруднення навколишнього середовища та іншу негативну діяльність, яка може завдати шкоди суспільству;

відповідальність за розголошення відомостей, які становлять комерційну таємницю підприємства, і за порушення порядку охорони таких відомостей встановлюється законодавчими актами СРСР".

Крім того, у 1991 році було прийнято Основи цивільного законодавства Союзу РСР і республік. Стаття 151 Основ була спеціально присвячена "секретам виробництва" та встановлювала загальні ознаки цієї категорії, умови надання правового захисту та окремі особливості правового режиму. В Основах було закріплено умови, за яких власник інформації, яка складала секрет виробництва (ноу-хау), набував права захисту від її незаконного використання третіми особами. Ці умови були запозичені із згаданої Угоди. У свою чергу, відповідне положення Угоди фактично дублювало визначення "комерційної таємниці" із Уніфікованого Закону про комерційну таємницю США.

Ці положення були перенесені і у відповідне законодавство тоді ще Української РСР – Закон УРСР "Про підприємства в Українській РСР" (№ 887-XII від 27.03.1991 р.) та Основи цивільного законодавства УРСР. Так, у Законі "Про підприємства в Українській РСР" (з жовтня 1992 року – Закон України "Про підприємства в Україні") було дослівно відтворено положення аналогічного Закону СРСР. Також з'явилася норма (стаття 32) про відповідальність службових осіб, організацій та органів, що проводять перевірку підприємства, за розголошення комерційної таємниці підприємства. Закон України "Про підприємства в Україні", у тому числі його положення щодо комерційної таємниці, діяли до 1 січня 2004 року, коли набув чинності Господарський кодекс України.

Після проголошення Україною незалежності термін "комерційна таємниця" був введений у правовий оборот Законом України "Про підприємства в Україні" від 27.03.1991 р. Здійснення правової охорони таємної інформації в Україні стало можливим на підставі Закону України "Про інформацію" від 2 жовтня 1992 р., інших законів про інформацію і прийнятого Цивільного кодексу України.

Сучасні підприємства функціонують в умовах нової економіки, що називають нематеріальною чи інтелектуальною економікою. Впровадження інновацій, створення, нагромадження й ефективне використання знань на сьогодні є найважливішою зброєю в конкурентній боротьбі. Існуючі зміни зумовили переорієнтацію управлінських пріоритетів підприємств. Джерелом економічної вартості є вже не виробництво матеріальних благ, а створення, збереження нематеріальних активів підприємства за допомогою системи бухгалтерського обліку, їх ефективне використання та управління ними.

За результатами аналізу діяльності підприємств молочної промисловості Житомирської області за період з 2003 по 2007 рр. виявлено тенденцію зменшення кількості підприємств галузі (рис. 2.5).

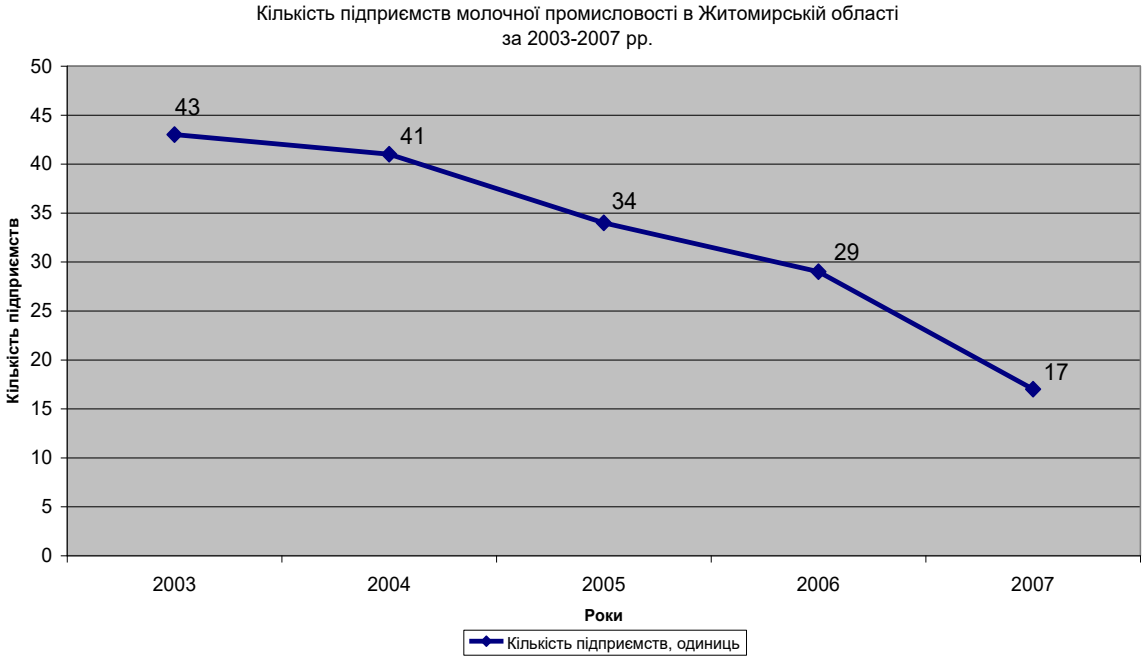


Рис. 2.5. Кількість підприємств молочної промисловості за період з 2003 по 2007 рр.

Це, передусім, пов'язано з тим, що на частині збанкрутілих підприємств молочної промисловості відсутня служба економічної безпеки, що сприяло розголошенню бухгалтерської та іншої економічної інформації, яка становить комерційну таємницю. В умовах конкуренції це є суттєвим прорахунком керівного складу підприємств, адже в такій ситуації у конкурентів з'являється можливість без будь-яких додаткових зусиль отримати інформацію, яка становить комерційну таємницю.

Розвиток молочної промисловості в країні в цілому, а також і в Житомирській області дещо уповільнився порівняно з попередніми роками. Причиною є не лише загальне зниження купівельної спроможності населення, а й недостатній рівень економічної безпеки підприємства в частині бухгалтерського обліку. На графіку (рис. 2.6) узагальнено дані Державного комітету статистики в Житомирській області* відносно індексів обсягу виготовленої продукції та продуктивності праці підприємств молочної промисловості, які функціонують на території Житомирської області.

* Узагальнено на підставі статистичних даних Державного комітету статистики у Житомирській області. Замовлення № 03/1-11-422 від 16.12.2008 р.

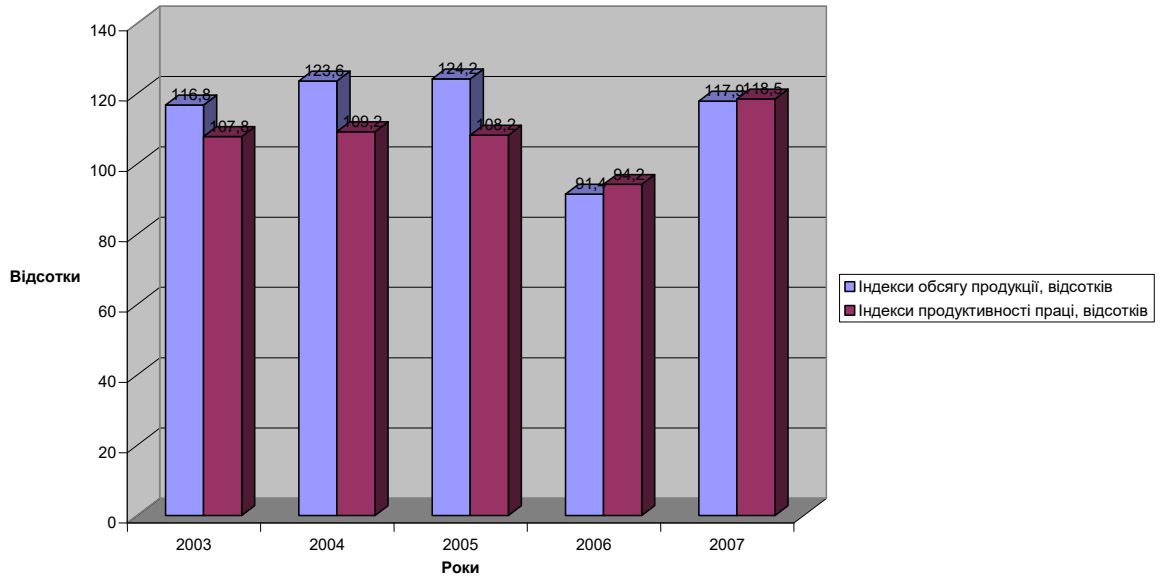


Рис. 2.6. Індекси обсягу виготовленої продукції та продуктивності праці підприємств молочної промисловості Житомирської області за 2003-2007 рр.

Проаналізувавши наведені дані, можна дійти висновку, що не у всі роки на підприємствах молочної промисловості Житомирської області індекси обсягу виготовленої продукції перевищували індекси продуктивності праці. Така тенденція спостерігалася протягом 2003-2005 років, однак, у 2006-2007 рр. ситуація змінилася на протилежну, що є не досить позитивним показником діяльності підприємств. Такі тенденції щодо зміни наведених індексів можуть бути пов'язані з недотриманням належного рівня економічної безпеки підприємства в частині захисту бухгалтерської інформації, що становить комерційну таємницю.

Разом з тим, рівень продуктивності праці впливає на обсяг виготовленої продукції підприємств молочної промисловості, про що свідчать дані, графічно представлені на рис. 2.7.

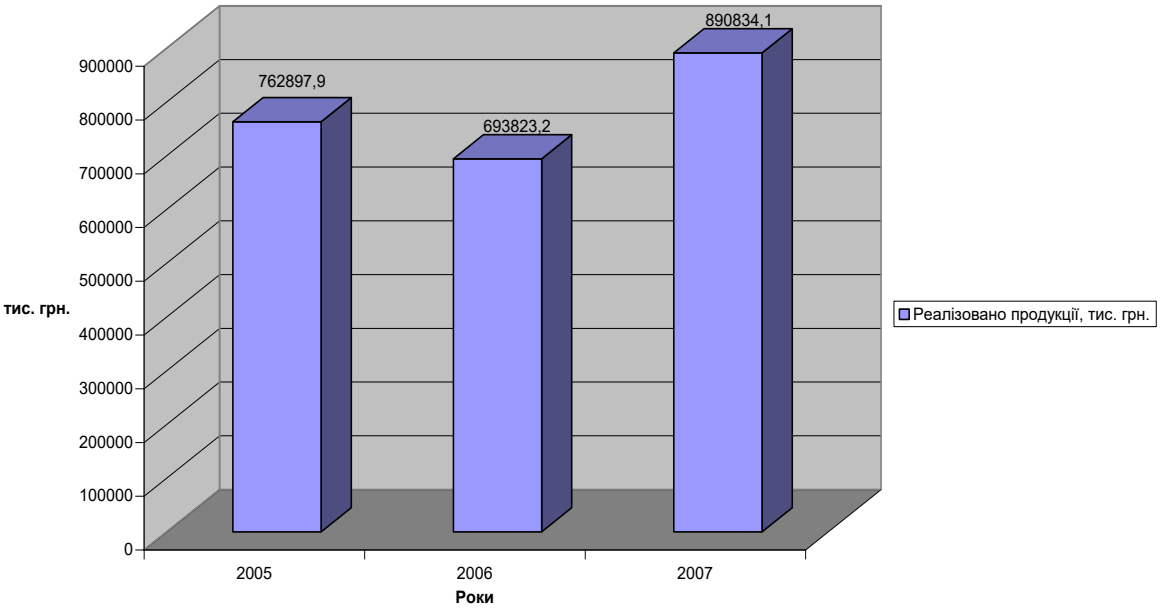


Рис. 2.7. Обсяг реалізованої продукції підприємств молочної промисловості Житомирської області в 2003-2007 рр.

До недавнього часу в Україні не потрібно було охороняти інтелектуальну власність. Результати інтелектуальної праці не розглядалися як самостійна цінність, здатна приносити підприємству економічну вигоду. В силу вказаної причини результати інтелектуальної праці не визнавались самостійними економічними об'єктами і не підлягали відображенню в бухгалтерському обліку як активи. У ринкових умовах господарювання інформація бухгалтерського обліку стала найціннішим ресурсом для здійснення процесу управління поряд з матеріальними, енергетичними, трудовими та фінансовими ресурсами.

Важливе значення для роботи підприємства має інформація:

1) комерційна (приймається рішення про основні пріоритети діяльності підприємства, а саме: асортимент, обсяг та ціна продукції, яка реалізується, витрати на її виробництво та реалізацію;

2) фінансова (визначення розміру виручки та прибутку, що може отримати підприємство; обсяг фінансових засобів, необхідних для здійснення господарської діяльності; спосіб розподілу та використання отриманого прибутку; спосіб здійснення розрахунків з власниками, державою, постачальниками продукції, сировини, матеріалів, послуг тощо);

3) технічна (характеристика продукції, опис технології її виготовлення; визначення необхідних матеріалів для виготовлення певного виду продукції, машин, устаткування та прийомів, необхідних для проведення робіт);

4) оперативна (видача завдання персоналу; здійснення його розміщення на робочих місцях, здійснення контролю, обліку та регулювання ходу виробничого процесу, а також коригування прийнятих управлінських рішень). За допомогою відображення в бухгалтерському обліку вищенаведеної інформації всі зазначені складові елементи поєднуються в єдиний виробничий комплекс в межах підприємства.

Як зазначає Г.А. Пастернак-Таранушенко, інформація – це дуже коштовний товар, а її носії та розповсюджувачі, засоби масової інформації, журналісти, телеведучі, названі в Україні "четвертою владою" [99].

В сучасних умовах розвитку економіки в Україні, як і в інших країнах світу, в процесі підприємницької діяльності при створенні нових технологій та в результаті інтелектуальної праці виникають насичені найрізноманітнішими відомостями інформаційні об'єкти, що мають комерційну цінність. Залежно від того, наскільки підприємства залучаються до комерційної діяльності, все більшого значення набуває необхідність захисту бухгалтерської інформації, що може становити комерційну таємницю підприємства.

Не всі підприємницькі відносини обов'язково є конфіденційними. Не вся інформація, розкрита в конфіденційних відносинах, обов'язково складає комерційну таємницю. Тому важливо встановити, що складає зміст комерційної таємниці.

Комерційна таємниця, яка міститься в бухгалтерській інформації підприємств, має наступні, властиві лише їй відмінні ознаки (рис. 2.8).

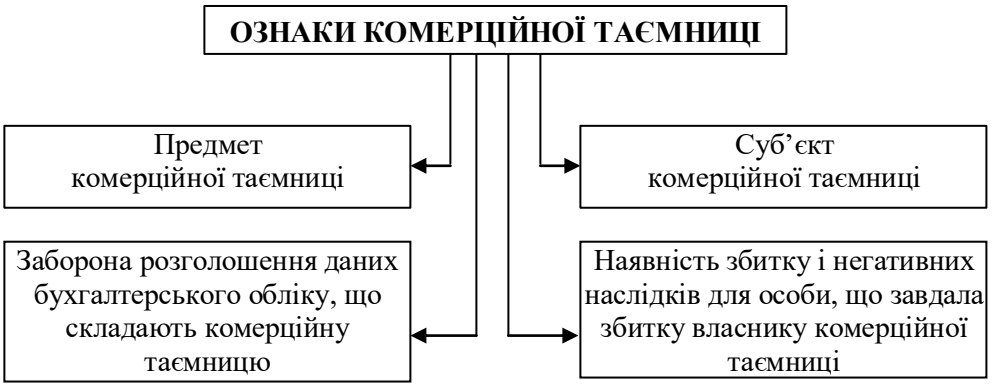


Рис. 2.8. Ознаки комерційної таємниці, що міститься в даних бухгалтерського обліку підприємств

[99] Пастернак-Таранушенко Г.А. Економічна безпека держави. Методологія забезпечення: [монограф.] / Г.А. Пастернак-Таранушенко. – К.: Київський економічний інститут менеджменту, 2003. – 320 с.

Предметом комерційної таємниці є відомості бухгалтерського обліку, пов'язані з господарською діяльністю підприємства, до яких можна віднести виробничу та технологічну інформацію, інформацію про управління, фінанси й іншу діяльність. Також до предмету комерційної таємниці підприємства можуть бути віднесені документи про переговори підприємства з потенційними контрагентами та методи ціноутворення, документи, пов'язані з маркетинговими дослідженнями ринку, відомості про організацію праці і підбір працівників, інформація про умови збереження документів, тобто відомості, які містять комерційну цінність.

Фактично, комерційною таємницею є інформація, яка має комерційну цінність. Іншими словами, це інформація, що має економічну цінність, здатна впливати на фінансовий стан підприємства, розмір одержуваного ним прибутку та призначена лише для певної групи користувачів.

В даний час кожен власник повинен створити систему заходів безпеки, яка б сприяла виявленню ознак можливих правопорушень та злочинних дій на різних стадіях, на етапі формування злого наміру та розробки планів злочинних дій, що дозволило б вчасно попередити та знешкодити злочинні наміри. Це означає, що безпека підприємництва повинна бути превентивною, а захист комерційної таємниці на підприємстві повинен бути на першому місці. Правове забезпечення економічної безпеки та комерційної таємниці, як її прояву, визначається відповідними правовими нормами, до яких належать Господарський кодекс, Кримінальний кодекс, Закон України "Про державну податкову службу" [100], Закон України "Про інформацію" [101], Закон України "Про захист від недобросовісної конкуренції" [102], Постанова КМУ "Про перелік відомостей, що не становлять комерційної таємниці" [103]. Документом, який здійснює регулювання захисту складових комерційної таємниці, є Положення про комерційну таємницю на підприємстві, що регламентує порядок доступу до інформації комерційного характеру та захищає власника від

[100] Закон України "Про державну податкову службу" № 509-XII від 4.12.1990 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=509-12.

[101] Закон України "Про інформацію" № 1703-IV від 11.05.2004 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?page=1&nreg=2657-12.

[102] Закон України "Про захист від недобросовісної конкуренції" № 236/96-ВР від 07.06.1996 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=236%2F96-%E2%F0.

[103] Постанова Кабінету Міністрів України "Про перелік відомостей, що не становлять комерційної таємниці" № 611 від 09.08.1993 р.: [Електронний ресурс]. – Режим доступу: http://www.yurist.kh.ua/index.php?option=com_content&task=view&id=29&Itemid=51.

втрати, несанкціонованого доступу, викривлення, псування або її знищення, а також обмежує коло осіб (навіть серед працівників фірми), які мають до неї доступ, повний або ж обмежений, в залежності від займаної посади.

Статус комерційної таємниці інформація може отримати лише у випадку документального підтвердження відповідного переліку відомостей керівником підприємства або уповноваженого ним органу.

Комерційна таємниця є також необхідною умовою конкуренції, оскільки вона охороняється законодавством країни. З іншого боку, товаровиробники намагаються вивчати і запозичувати методи роботи конкурентів, які мають успіх. Таким чином, в умовах конкуренції виникає необхідність існування комерційної таємниці, продиктованої бажанням товаровиробників приховати від конкурента все те, що дає змогу виробляти товари підвищеного попиту і одержувати високі прибутки.

Кожен підприємець самостійно визначає склад відомостей, які становлять комерційну таємницю. Згідно з Господарським кодексом України (ст. 36), комерційною таємницею можуть бути "відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб'єкта господарювання" [104] (Додаток В).

Відомості, наведені у додатку В, підприємства зобов'язані подавати органам державної виконавчої влади, контролюючим та правоохоронним органам, іншим юридичним особам відповідно до чинного законодавства, за їх вимогою.

Відповідно до Цивільного кодексу України, органи державної влади зобов'язані охороняти від недобросовісного використання інформацію, яка є комерційною таємницею та створення якої потребує значних зусиль і яка надана їм з метою отримання встановленого законом дозволу на діяльність, пов'язану з фармацевтичними, сільськогосподарськими, хімічними продуктами, що містять нові хімічні сполуки. Ця інформація охороняється органами державної влади також від розголошення, крім випадків, коли розголошення необхідне для забезпечення захисту населення або не вжито заходів щодо її охорони від недобросовісного комерційного використання. Органи державної влади

[104] Господарський кодекс України № 436-IV від 16.01.2003 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=436-15

зобов'язані захищати комерційну таємницю також в інших випадках, передбачених законом. Терміном "комерційна таємниця" не охоплюються відомості, що складають банківську таємницю, страхову таємницю, авторські права. Зазначені відомості складають самостійні групи конфіденційної інформації із своїм відмінним від "комерційної таємниці" правовим регулюванням.

Основні категорії суб'єктів комерційної таємниці наведені на рис. 2.9.

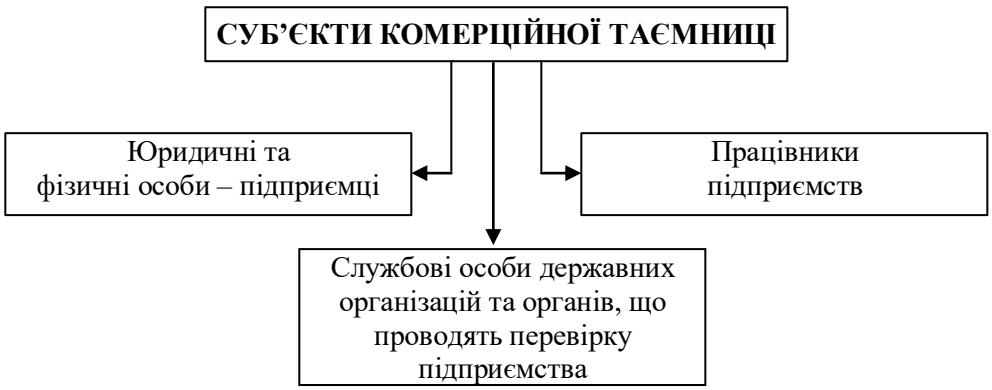


Рис. 2.9. Категорії суб'єктів комерційної таємниці

Працівники мають право користуватися відомостями, які становлять комерційну таємницю, для виконання своїх трудових обов'язків. Ступінь доступу кожного з працівників до такої інформації визначається керівником підприємства самостійно (Додаток Д), а умови користування – документами, затвердженими керівником та угодою (Додаток Ж).

Інформацію про комерційну таємницю підприємства службовці державних організацій одержують у рамках адміністративних правовідносин. Обсяг їх доступу до такої інформації обмежується напрямком перевірки, що повинно бути зазначено в документах на перевірку. За розголошення комерційної таємниці державні службовці та організації несуть відповідальність, встановлену законодавством України. Загальною підставою такої відповідальності є Господарський кодекс України, вимоги якого про нерозголошення комерційної таємниці поширюються на всіх службових осіб державних органів і організацій.

Способи розголошення відомостей, що складають комерційну таємницю, можуть бути різними: передача інформації конкурентам підприємства; ознайомлення з комерційною таємницею службових осіб державних організацій і органів без належних на те прав і основ як з боку розголошувача, так і з боку державного службовця, розголошення відомостей, що складають комерційну таємницю, через засоби масової інформації; використання в особистих цілях – передача родичам, знайомим для заняття власною

підприємницькою діяльністю. Мотиви розголошення так само можуть бути різними (в залежності від інтересів користувача): користь, особисті неприязні відносини, халатне відношення до трудових і службових обов'язків.

Як наголошує В.Г. Бєлов, порушенням зобов'язань із забезпечення конфіденційності визнається не лише розголошення та пряма передача конфіденційних відомостей однієї із сторін іншим зацікавленим користувачам без згоди партнера, але й не вживання заходів для їх охорони, що попереджують вільний доступ до відомостей та можливість їх розголошення. До таких заходів потрібно віднести, зокрема, ознайомлення співробітників, які приймають участь у виконанні договірних робіт та мають доступ до інформації, з правилами дотримання конфіденційності [[105], с. 129].

Дотримання та нерозголошення комерційної таємниці є не лише правом, але й обов'язком суб'єктів, пов'язаних з діяльністю окремого підприємства. Без належного дотримання вимог щодо користування та збереження інформації, що складає комерційну таємницю, неможливо забезпечити необхідну охорону такої інформації як цивільно-правовими заходами, так і державно-примусовими.

До відомостей, що складають комерційну таємницю, можуть бути віднесені тільки ті відомості, розголошення яких може завдати шкоди підприємству, а отже і його власнику. Причому не має значення, який вид збитку може бути заподіяний, збиток майновим або немайновим правам (моральний збиток). Права суб'єкта підприємницької діяльності підлягають захисту, а заподіяна шкода відшкодуванню в обох зазначених випадках.

Найчастіше канали витоку бухгалтерської інформації з'являються там, де є нерегламентований порядок доступу до неї, і, таким чином, створюється реальна можливість для сторонніх осіб одержувати конфіденційну інформацію з ділового листування, службових телефонних переговорів, неврахованих копій документів.

Дані бухгалтерського обліку і пов'язана з ними інформація можуть представляти інтерес для різних її користувачів. Часто інформація має дійсну або потенційну комерційну цінність через її невідомість третім зацікавленим

[105] Белов В.Г. Правовые аспекты оборота непубликуемой научно-технической информации // Электронный документ и документооборот: Правовые аспекты: Сб. науч. тр. / РАН. ИНИОН. Центр социальных науч.-информ. исслед. Отдел правоведения; РАН. ИГП. Центр публичного права. Сектор информационного права; Отв. ред. – Алферова Е.В., Бачило И.Л. – М., 2003. – 208 с.

особам (наприклад конкурентам). Тому власник інформації має право приймати заходи щодо охорони її конфіденційності. Правовідносини, пов'язані із службовою і комерційною таємницею, регулюються Господарським кодексом України та законами України.

Керівництво підприємства може самостійно визначати перелік відомостей, що відносяться до комерційної таємниці, включивши в нього окремі види інформації на свій розсуд з числа не заборонених законодавством. Нами у роботі запропоновано перелік бухгалтерської інформації підприємств, що становить комерційну таємницю, які наведено на рис. 2.10.

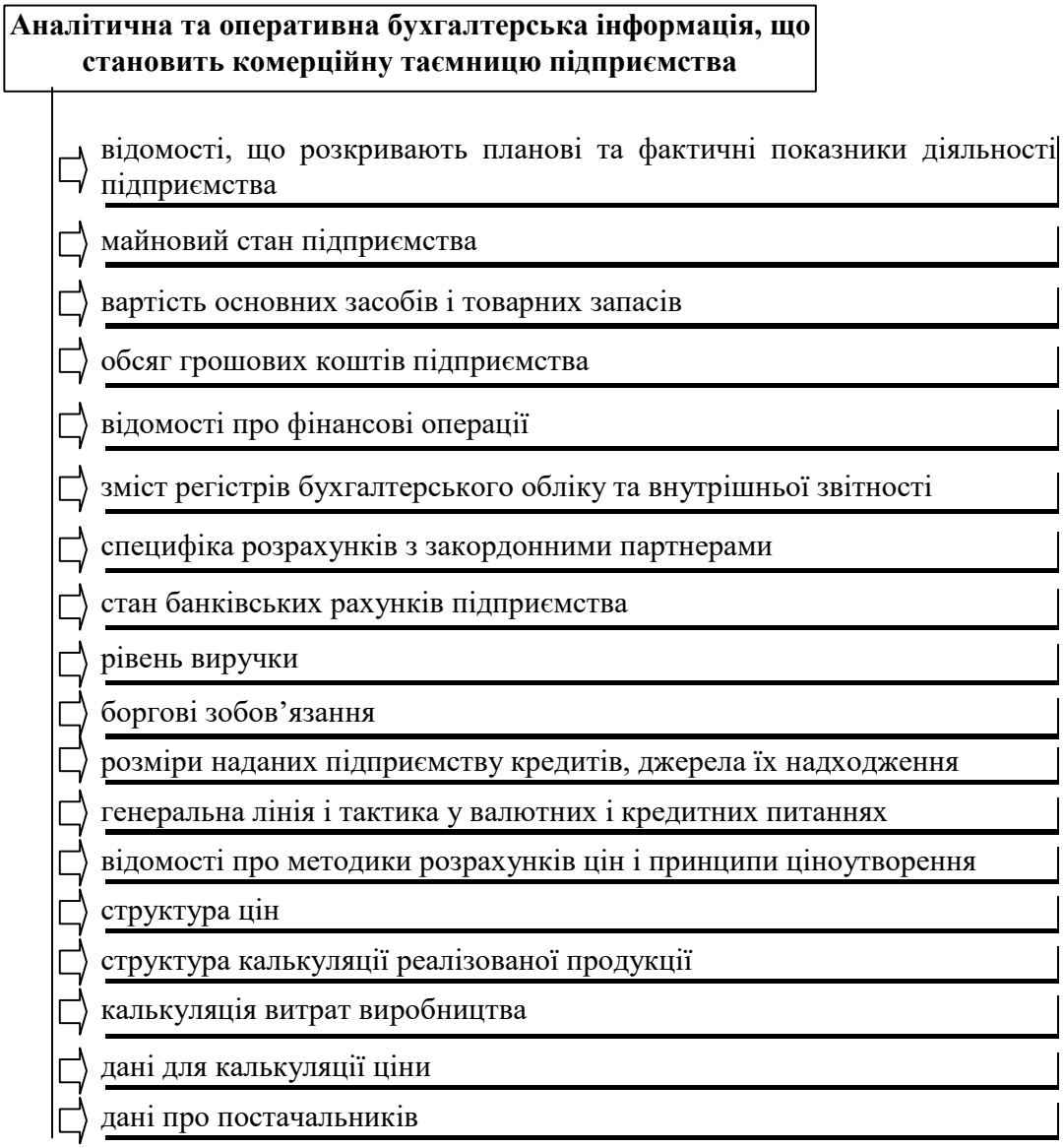


Рис. 2.10. Перелік бухгалтерської інформації, що становить комерційну таємницю

Окрім наведеної вище інформації до складу відомостей, що можуть становити комерційну таємницю підприємства можна віднести дані наведені в Додатку З. Такий перелік доцільно оформити наказом по підприємству (Додаток И) та довести його до відома всіх працівників під підпис.

Відзначимо також, що з моменту ухвалення арбітражним судом рішення про визнання боржника банкротом дані про фінансовий стан боржника перестають відноситися до категорії відомостей, що носять конфіденційний характер або що є комерційною таємницею.

Для забезпечення захисту складових комерційної таємниці підприємства, що міститься в бухгалтерській документації, перш за все, необхідно сформувати команду, відповідальну за виконання програми щодо захисту складових комерційної таємниці підприємства; визначити, яка імовірність розповсюдження такої інформації.

Правовий захист комерційної таємниці може бути забезпечений за умови, якщо її власник вживатиме відповідних заходів для збереження конфіденційності зазначеної інформації. Це є необхідною умовою правового захисту складових комерційної таємниці, адже при розкритті сутності таємниці втрачається будь-яке значення її захисту. Комерційна таємниця за своїм характером може бути найрізноманітнішою, відповідно, й заходи із забезпечення захисту складових комерційної таємниці та документи, що закріплюють статус комерційної таємниця певного суб'єкта, також можуть бути найрізноманітнішими (наприклад, у складних технологіях потрібен письмовий опис нерозкритої інформації, яку можливо зберегти у таємниці шляхом заборони доступу інших осіб до цього опису; у простих технологіях можна зберігати інформацію шляхом її нерозголошення, мовчання).

Нині склад та обсяг інформації, що становить комерційну таємницю та порядок її захисту, визначаються керівництвом підприємства. Ця інформація належить підприємству з повним правом власності. Порядок та ступінь відповідальності за порушення права власності та розпорядження комерційною таємницею встановлюється Кримінальним Кодексом України.

Крім того, підприємство як власник інформації, що містить комерційну таємницю, має право визначити осіб, які можуть володіти, користуватися та розпоряджатися такою інформацією, визначити правила обробки інформації та права доступу до неї, а також встановлювати інші умови щодо комерційної таємниці.

Особам, які не мають відношення до діяльності підприємства, не слід надавати інформацію, яка містить комерційну таємницю підприємства. У випадку, коли уникнути цього неможливо, скажімо, потрібно укласти договір з новим клієнтом, який вимагає надання інформації, яка вважається конфіденційною, необхідно включити в договір (до обов'язків сторін) про використання конфіденційної інформації та зазначити відповідальність сторін за розголошення конфіденційної інформації. До чинних договорів, які не передбачають відповідальності за розголошення конфіденційної інформації, необхідно підписати окремі договори або додаткові угоди про використання конфіденційної інформації.

Угода з працівником, який згідно службових обов'язків має доступ до службової або комерційної таємниці підприємства, може містити в розділі "Обов'язки працівника" вимогу про нерозголошення цих відомостей, або працівником може бути підписано "Зобов'язання про нерозголошення комерційної таємниці" (Додаток К).

Керівництву необхідно чітко визначити, яку інформацію, для чого та від кого необхідно захищати. Зважаючи на складність визначення та класифікації даних, які становлять комерційну таємницю підприємства, зокрема, в частині бухгалтерського обліку, слід зазначити, що зазвичай, предметом ворожих посягань є документи, записи, звіти, калькуляції витрат виробництва, відомості про постачальників та клієнтів, відомості про конфіденційні ділові переговори, огляди ринку інвестицій, відомості про устаткування, яке використовується на підприємстві, результати наукових досліджень, а також інші джерела інформації, які можуть містити комерційну таємницю. Ці завдання повинні покладатись як на службу безпеки, яка є обов'язковим підрозділом на підприємстві, так і на інші підрозділи.

Головною метою безпеки облікової інформації підприємств є забезпечення його максимально ефективного функціонування та високий потенціал розвитку.

Як показують проведені незалежними експертами дослідження [106], більшість українських підприємств не приділяють належної уваги безпеці (збереженню) власної комерційної інформації. Хоча, як показує міжнародний

[106] Уманец А. Вас учили не брать чужое? Нет? Это хорошо / А. Уманец // Бизнес. – 2003. – № 51. – С. 143-145.

досвід, застережні заходи стосовно забезпечення конфіденційності інформації підприємства обійдуться дешевше, аніж втрати, яких може зазнати фірма через розголошення комерційної таємниці.

Захист облікових даних, що складають комерційну таємницю, покладається не лише на службу безпеки, але й на весь управлінський персонал підприємства. Система повинна охоплювати всіх співробітників – від керівника до технічного персоналу. Кваліфікація та кількість працівників, які забезпечують безпеку підприємства, повинні чітко відповідати завданням, поставленим перед службою безпеки. При недотриманні цих умов служба безпеки може бути або тягарем для бюджету підприємства, або – загрозою для діючого керівництва, що є набагато гірше.

Забезпечення захисту інформації на підприємстві повинно покладатися на спеціальний відділ, до складу якого входять:

– служба охорони підприємства;

– служба збору конфіденційної інформації;

– служба захисту промислової та комерційної таємниці;

– служба накопичення та обробки інформації.

Кожна з цих служб має свої специфічні функції та працює відносно автономно. Проте, в сукупності вони утворюють організаційну систему забезпечення безпеки господарюючого суб'єкта. Функції координатора відділу повинен виконувати керівник підрозділу, який в свою чергу безпосередньо підпорядковується керівництву підприємства. Керівник повинен розуміти, що для правильного та ефективного виконання відділом своїх функцій, керівник відділу повинен бути в курсі усіх справ підприємства.

Таким чином, до основних функцій підрозділу безпеки підприємства відносяться:

– забезпечення високого рівня безпеки комерційної та промислової таємниці;

– забезпечення керівництва інформацією про стан справ для прийняття важливих як стратегічних, так і тактичних рішень, які впливають на діяльність господарюючого суб'єкта.

Розглянемо більш детально основні функції служби захисту промислової та комерційної таємниці підприємства, до складу яких входять:

– дії щодо контролю за дотриманням працівниками режимів, що діють на підприємстві;

– дії із забезпечення безпеки території, об'єктів, обладнання та продукції підприємства;

– дії з виявлення підготовки різних акцій відносно підприємства з боку конкурентів та протидія цим акціям;

– розробка та проведення заходів із захисту каналів зв'язку та протидії технічної розвідки конкурентів;

– збір відкритих матеріалів про підприємства-конкуренти;

– збір та передача в інформаційну систему інформації про факти, які мають значення для забезпечення безпеки підприємства.

Для правильної організації забезпечення захисту складових комерційної таємниці на підприємстві повинна постійно діяти ретельно підготовлена програма захисту складових комерційної таємниці. В цілому ця програма є одним із найважливіших елементів системи заходів із забезпечення економічної безпеки підприємства.

Згідно із Законом України "Про захист від недобросовісної конкуренції" розголошенням комерційної таємниці є "ознайомлення іншої особи без згоди особи, уповноваженої на те, з відомостями, що відповідно до чинного законодавства України становлять комерційну таємницю, особою, якій ці відомості були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків, якщо це завдало чи могло завдати шкоди суб'єкту господарювання" [107]. Під розголошенням слід розуміти як незаконне ознайомлення інших осіб з відомостями, що складають комерційну таємницю, так і створення особою, якій ці відомості стали відомі (в зв'язку з професійною або службовою діяльністю і яка повинна зберігати їх у таємниці) умов, сприятливих для ознайомлення із ними сторонніх осіб.

До таких осіб належать працівники правоохоронних органів, банківських установ, податкових органів, органів влади та управління, а також інші особи, які відповідно до законодавства мають право знайомитися із відомостями, що складають комерційну таємницю, або мають доступ до таких відомостей за характером виконуваних ними професійних чи службових обов'язків. Засоби розголошення комерційної таємниці (повідомлення іншим особам, через засоби масової інформації чи в інший спосіб) значення не мають.

[107] Закон України "Про захист від недобросовісної конкуренції" № 236/96-ВР від 07.06.1996 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=236%2F96-%E2%F0.

Держава, в особі законодавця, прагне дати підприємству (власнику) інструменти захисту належної йому документованої інформації, а також передбачає відповідальність за порушення комерційної таємниці.

Посадові особи, які за родом своєї професійної діяльності мають доступ до інформації, що становить комерційну таємницю підприємств, несуть майнову відповідальність за її розголошення.

В даний час за порушення прав власності комерційної таємниці законодавством України встановлені наступні види відповідальності рис. 2.11.

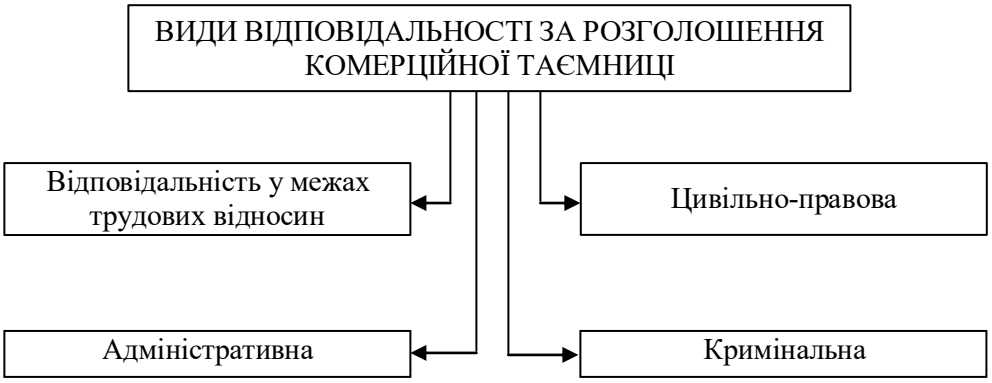


Рис. 2.11. Види відповідальності за розголошення комерційної таємниці

За недотримання режиму роботи у межах трудових відносин з інформацією, що складає комерційну таємницю, до працівників підприємства може бути застосована матеріальна та дисциплінарна відповідальність. Притягнення до матеріальної та дисциплінарної відповідальності здійснюється на загальних підставах, з урахуванням особливостей правового статусу "комерційної таємниці". Для законного застосування санкцій за правопорушення, пов'язаних з комерційною таємницею в рамках трудових відносин, керівнику підприємства необхідно мати деякі документи, а саме:

а) документ, що встановлює перелік відомостей, які складають комерційну таємницю (Додаток З). Це може бути затверджене керівником підприємства Положення про комерційну таємницю, у якому чітко обумовлюється, які відомості є комерційною таємницею, порядок віднесення їх до таких, умови збереження, а також які працівники підприємства можуть передавати закриті відомості представникам державних органів і організацій;

б) посадові інструкції (Додаток Л, Додаток М). У посадових інструкціях визначається коло вповноважених працівників підприємства та відомості, що містять комерційну таємницю, з якими працівник має право працювати,

порядок роботи з ними. В посадових інструкціях співробітників бухгалтерської служби підприємств, які мають справу з бухгалтерським даними, що містять комерційну таємницю, пропонуємо додати пункт, згідно якого особа несе відповідальність за розголошення комерційної таємниці;

в) угода (Додаток Н). В угоді або контракті зазначаються зобов'язання щодо дотримання працівником нерозголошення комерційної таємниці та наслідки недотримання цього обов'язку. Умови матеріальної відповідальності працівника за розголошення комерційної таємниці можуть бути передбачені як даною угодою, так і окремою угодою про матеріальну відповідальність.

З першими двома документами працівник повинен ознайомитися перед початком своєї трудової діяльності на даному підприємстві. Факт ознайомлення повинен фіксуватися письмово, із зазначенням дати ознайомлення.

Підписання документів про нерозголошення комерційної таємниці забороняє співробітникам використовувати отриману інформацію у своїй діяльності без відповідної на те згоди керівництва.

Проведення заходів захисту складових комерційної таємниці передбачає комплекс організаційних, програмно-технічних та криптографічних засобів та заходів захисту інформації в процесі документообороту, при роботі співробітників з таємними документами та відомостями, при обробці інформації в автоматизованих системах різного рівня та призначення, при передачі каналами зв'язку, при веденні конфіденційних переговорів, при використанні зарубіжних технічних засобів від розкрадання, втрати, знищення, розголошення, викривлення, та підробки за рахунок несанкціонованого доступу та спеціального впливу.

Організацію захисту розпочинають зазвичай з підготовки внутрішніх нормативних документів:

– положення про захист комерційної таємниці;

– інструкція щодо роботи з документами, які містять комерційну таємницю;

– правила надання доступу до інформаційних ресурсів;

– правила роботи користувачів в корпоративній мережі;

– правила роботи в мережі Інтернет;

– інструкція із захисту від комп'ютерних вірусів.

Для працівників підприємства передбачаються наступні попереджувальні моменти:

– угода про нерозголошення комерційної таємниці, яку укладають при прийнятті на роботу;

– в трудовій угоді зазначаються вимоги інформаційної безпеки та відповідальність за їх порушення;

– в посадові інструкції додаються положення про відповідальність за недотримання вимог щодо нерозголошення комерційної таємниці підприємства.

Одним із ефективних методів щодо організації захисту інформації вважається спосіб поділу інформації на окремі частини, який передбачає, що співробітник не має доступу до інформації, призначеної для інших співробітників.

Існує дві основні моделі використання принципу поділу інформації на окремі частини: ієрархічна та функціональна. Згідно з ієрархічною моделлю поділ інформації відбувається відповідно службового становища. Якщо співробітник має високу посаду, то відповідно він знає більше. Відповідно до функціональної моделі інформація поділяється за спеціалізацією відділів підприємства.

За порушення режиму комерційної таємниці до працівника можуть бути застосовані наступні дисциплінарні санкції: догана, звільнення. Якщо була укладена угода про матеріальну відповідальність за розголошення відомостей, що складають комерційну таємницю, працівник так само відповідає і матеріально, у розмірах передбачених угодою сторін.

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну та таємну.

Згідно із Законом України "Про інформацію" "конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов" [108].

До конфіденційної інформації відноситься будь-яка інформація професійного, ділового, виробничого, банківського та іншого комерційного характеру. Для підприємства конфіденційною інформацією можуть бути:

дотримання договірної політики;

стан платіжної дисципліни;

---

[108] Закон України "Про інформацію" № 1703-IV від 11.05.2004 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?page=1&nreg=2657-12.

дані про розмір доходів працівників, відомості про авторські винагороди та гонорари;

корпоративні вечірки, порядок прийому ділових партнерів;

ділове листування;

кадровий склад і порядок його підбору;

взаємодія структурних підрозділів.

Згідно із Законом України "Про інформацію" "до таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої може завдати шкоди особі, суспільству і державі. Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до законодавства" [109].

Наведене вище також підтверджує думка В.Г. Бєлова про те, що "інформація, яка становить службову або комерційну таємницю має дійсну та потенційну комерційну цінність в силу невідомості її третім особам, до неї немає вільного доступу на законних підставах, власник інформації вживає заходів щодо охорони її конфіденційності" [110, с. 128].

Комерційна або службова таємниця, в якості об'єкта цивільного права, повинні мати три ознаки: відповідна інформація невідома третім особам, до неї немає доступу на законних підставах, власник інформації вживав заходи для захисту її конфіденційності. Дійсно, лише в силу невідомості третім особам результати науково-технічної діяльності зберігають свій інноваційний потенціал як предмети промислового впровадження, що надають певні конкурентні переваги їх законному власнику.

У разі дотримання необхідних заходів безпеки власник матиме право на юридичний захист від заподіяної йому шкоди внаслідок неправомірних дій, з метою заволодіння комерційною таємницею.

Проблеми економічної та облікової безпеки інформації необхідно вирішувати із застосуванням системного підходу: в поєднанні з загальноекономічними, контрольними та правоохоронними механізмами.

---

[109] Закон України "Про інформацію" № 1703-IV від 11.05.2004 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?page=1&nreg=2657-12.

[110] Белов В.Г. Правовые аспекты оборота непубликуемой научно-технической информации // Электронный документ и документооборот: Правовые аспекты: Сб. науч. тр. / РАН. ИНИОН. Центр социальных науч.-информ. исслед. Отдел правоведения; РАН. ИГП. Центр публичного права. Сектор информационного права; Отв. ред. – Алферова Е.В., Бачило И.Л. – М., 2003. – 208 с.

На даному етапі недостатньо розробленими є підходи відносно питань стратегічного удосконалення економічної безпеки, спроможної забезпечити цілковите використання існуючого потенціалу, перешкоджати виникненню загроз, підтримувати належний рівень економічної безпеки. Це досить часто не враховують керівники підприємств, які не лише не використовують існуючі наукові розробки в цій сфері, але й забувають про організацію та забезпечення захисту складових комерційної таємниці і конфіденційної інформації на підприємстві, – однієї з основних і визначаючих ланок забезпечення економічної безпеки підприємства.

Однак дедалі актуальнішими постають питання поширення, отримання, використання і збереження інформації оскільки користувачі вимагають від підприємства різної за змістом і рівнем деталізації інформації. Таким чином, організація бухгалтерського обліку повинна забезпечити захист бухгалтерської інформації шляхом обмеження доступу до неї, тобто попередження несанкціонованого її використання.

Робота бухгалтера в багатьох аспектах пов'язана з конфіденційними даними, оскільки виконуючи покладені на нього обов'язки, бухгалтер працює з великою кількістю особистих даних працівників підприємства, з даними про їх доходи тощо. Крім того, бухгалтер має доступ до умов договорів з контрагентами, даних про структуру собівартості й цін та багато іншого. Проте, цю інформацію бухгалтер не повинен розголошувати не лише працюючи на підприємстві, а й після звільнення.

Висновки до 2-го розділу

1. Забезпечення економічної безпеки необхідно розглядати як попередження виникнення збитків різного характеру та прояву несприятливих факторів в усіх напрямах діяльності підприємства. Негативно на економічну безпеку підприємства впливають як внутрішні, так і зовнішні загрози. До зовнішніх загроз в системі бухгалтерського обліку, що впливають на економічну безпеку, слід віднести: негативний вплив конкурентів, партнерів та інвесторів, несанкціонований доступ конкурентів до конфіденційної інформації, промислово-економічне шпигунство тощо.

2. До внутрішніх загроз відносяться: неналежна кваліфікація бухгалтерського персоналу, протиправні дії бухгалтерів, неефективна політика підприємства щодо організації бухгалтерського апарату, порушення режиму збереження бухгалтерської інформації, що становить комерційну таємницю підприємства тощо. Виявлення наведених вище загроз значною мірою допоможе захистити інформацію, яка містить комерційну таємницю підприємства, і таким чином попередити її розголошення.

3. Оскільки інформація, яка використовується в управлінні підприємством, формується в системі бухгалтерського обліку, постає необхідність впровадження комплексу заходів щодо її збереження. Для досягнення даної мети визначено перелік бухгалтерської інформації, що становить комерційну таємницю підприємства, а також розроблено та удосконалено змістовне наповнення внутрішніх розпорядчих документів в частині захисту бухгалтерської інформації, серед яких виділено: посадові інструкції бухгалтерів, угоду про нерозголошення інформації, що становлять комерційну таємницю, наказ про захист інформації, що становить комерційну таємницю. Застосування зазначених документів дозволить забезпечити дотримання економічної безпеки підприємства та впровадити на підприємстві систему комерційної таємниці, що містить в собі механізм захисту бухгалтерської інформації.

РОЗДІЛ 3
ОРГАНІЗАЦІЯ БУХГАЛТРЕЬСКОГО ОБЛІКУ У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

3.1. Принципи організації бухгалтерського обліку як передумова збереження майна підприємств

Захист інформації є першою життєвою необхідністю будь-якої системи, що не може не зацікавити керівників, які розуміють цінність комерційної таємниці підприємств. Занепокоєння відносно захисту облікових даних або збереження комерційної таємниці є досить актуальним питанням для бізнесу, а ринок систем і засобів переповнений пропозиціями різних технічних рішень.

Важливе значення для ефективної діяльності підприємств має те, на скільки воно може забезпечити захист своєї інформації. Добробут підприємства напряму залежить від того, наскільки вдало забезпечується конфіденційність даних, які складають комерційну таємницю.

Основою інформації, яка використовується в управлінні економічним комплексом, є інформація, що міститься в бухгалтерському обліку, який є на сьогодні однією із головних умов, що визначає ефективність управління підприємства та досягнення успіху. Бухгалтерський облік є інструментом управління господарською діяльністю будь-якої ланки економічного комплексу держави.

Інформацію бухгалтерського обліку використовують не лише менеджери, економісти, юристи, працівники інших галузей з метою планування, управління, аналізу та контролю за господарською діяльністю підприємства та індивідуальних підприємців, але й інвестори, банки, фінансові та податкові органи.

На інформації, яка знаходиться в документах бухгалтерського обліку, базується розробка та планування концепції економічної безпеки держави. Відповідно, оцінка та використання інформації бухгалтерського обліку дозволяють управляти економікою країни, планувати та контролювати господарську діяльність підприємства.

Забезпечення економічної безпеки управління економікою, попередження незаконного збагачення є кінцевою метою бухгалтерського обліку. Тому в законодавчих актах, спрямованих на організацію господарської діяльності, регулювання економічних відносин, бухгалтерські вимоги повинні займати відповідне місце.

В сучасних умовах одним із факторів забезпечення ефективної діяльності підприємства є безпека захисту даних бухгалтерського обліку. Будь-який керівник розуміє, що він не зможе контролювати ситуацію в тих місцях, де його в даний час немає. Саме тому, необхідно поміркувати над попередженням ситуацій, які можуть спричинити витік конфіденційної інформації, для забезпечення подальшого розвитку та нормального функціонування підприємства. Виникає необхідність створення системи захисту облікових даних, а також визначення імовірності виникнення загроз для діяльності підприємства.

Захист облікових даних, що складають комерційну таємницю покладається не лише на службу безпеки, але й на весь управлінський персонал підприємства. Система повинна охоплювати всіх співробітників – від керівника, до технічного персоналу. Кваліфікація та кількість працівників, які забезпечують безпеку господарюючого суб'єкта, повинні чітко відповідати завданням, поставленим перед службою безпеки. При недотриманні цих умов служба безпеки може бути або "тягарем" для бюджету підприємства, або – загрозою для діючого керівництва, що є набагато гірше.

У Законі України "Про бухгалтерський облік та фінансову звітність в Україні" [111] наведено основні принципи бухгалтерського обліку та фінансової звітності, до складу яких входять:

– "обачність – застосування в бухгалтерському обліку методів оцінки, які повинні запобігати заниженню оцінки зобов'язань та витрат і завищенню оцінки активів і доходів підприємства";

– "повне висвітлення – фінансова звітність повинна містити всю інформацію про фактичні та потенційні наслідки господарських операцій та подій, здатних вплинути на рішення, що приймаються на її основі";

[111] Закон України "Про бухгалтерський облік та фінансову звітність в Україні" № 996-XIV від 16.07.1999 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=996-14&test=4/UMfPEGznhhgnE.Ziv6CI8tHdlFIsFggkRbI1c.

– "автономність – кожне підприємство розглядається як юридична особа, відокремлена від її власників, у зв'язку з чим особисте майно та зобов'язання власників не повинні відображатися у фінансовій звітності підприємства";

– "послідовність – постійне (із року в рік) застосування підприємством обраної облікової політики. Зміна облікової політики можлива лише у випадках, передбачених національними положеннями (стандартами) бухгалтерського обліку, і повинна бути обгрунтована та розкрита у фінансовій звітності";

– "безперервність – оцінка активів та зобов'язань підприємства здійснюється виходячи з припущення, що його діяльність буде тривати далі";

– "нарахування та відповідність доходів і витрат – для визначення фінансового результату звітного періоду необхідно порівняти доходи звітного періоду з витратами, що були здійснені для отримання цих доходів. При цьому доходи і витрати відображаються в бухгалтерському обліку та фінансовій звітності в момент їх виникнення, незалежно від дати надходження або сплати грошових коштів";

– "превалювання сутності над формою – операції обліковуються відповідно до їх сутності, а не лише виходячи з юридичної форми";

– "історична (фактична) собівартість – пріоритетною є оцінка активів підприємства, виходячи з витрат на їх виробництво та придбання";

– "єдиний грошовий вимірник – вимірювання та узагальнення всіх господарських операцій підприємства у його фінансовій звітності здійснюються в єдиній грошовій одиниці";

– "періодичність – можливість розподілу діяльності підприємства на певні періоди часу з метою складання фінансової звітності".

Однак, організацію бухгалтерського обліку слід здійснювати із застосуванням певних принципів, що забезпечують злагодженість та ефективність роботи підприємства.

Як зазначає в своїй праці проф. Н.М. Малюга [112, с. 28], "принцип – це те, що завжди, за будь-яких умов, без будь-якого винятку властиве певному явищу. Принцип виступає основою, початком, керівною ідеєю у будь-яких відносинах".

[112] Малюга Н.М. Наукові дослідження в бухгалтерському обліку: [навч. посіб. для студентів вищих навчальних закладів] / Н.М. Малюга / За ред. проф. Ф.Ф. Бутинця. – Житомир: ПП "Рута", 2003. – 476 с.

Дане питання у своїх наукових працях розглядали Д.І. Пільменштейн, П.В. Мєзєнцев, Ю.А. Литвин, В.А. Полторадня, Е.А. Смирнов, Я.В. Соколов, А.М. Кузьмінський, Л.Н. Зудін, В.В. Сопко, Л.В. Вербицька. Слід зазначити, що визначення принципів організації бухгалтерського обліку розглянуто не всіма вченими. Найбільш поширеними серед виділених науковцями принципів є: принцип безперервності, пропорційності, ритмічності, стабільності.

Також доцільно виділити принципи побудови бухгалтерського обліку, запропоновані засновником Української бухгалтерської школи проф. П.П. Німчиновим [[113], с. 3]:

– "відображення на бухгалтерських рахунках процесу створення суспільного продукту, його наявності, руху та невиробничого споживання";

– "побудова рахунків бухгалтерського обліку відповідно до їх економічного змісту й призначення";

– "побудова форм бухгалтерського обліку, звітності й організації облікової роботи".

Як бачимо, в процесі розвитку бухгалтерського обліку принципи залишаються такими ж, змінюються лише назви на більш сучасні.

На сьогодні питання визначення та пояснення принципів організації бухгалтерського обліку є досить суперечливим. Серед великої кількості підходів вчених до даного питання відсутня одностайність думок, оскільки немає єдиної системи класифікації принципів організації бухгалтерського обліку.

В умовах становлення ринкових відносин принципи організації бухгалтерського обліку набувають нового значення. Адже саме вони є основою формування обліку та забезпечення його подальшої провідної ролі в діяльності підприємства.

Здійснивши аналіз існуючих принципів організації бухгалтерського обліку можемо зробити висновок про те, що організація бухгалтерського обліку в сучасних умовах господарювання має базуватися на наступних принципах:

– принцип автономності, передбачає відокремлення майна власника від майна підприємства;

– принцип адаптивності, передбачає пристосування будови та функцій бухгалтерського обліку до певних умов управління;

[113] Нимчинов П.П. Общая теория бухгалтерского учета / П.П. Нимчинов. – К.: Вища школа, 1977. – 240 с.

– принцип ритмічності в організації бухгалтерського обліку означає рівномірне надходження даних та показників, а також надання вихідної інформації;

– принцип послідовності, передбачає постійне застосування обраної підприємством облікової політики;

– принцип застосування комп'ютерної техніки, що застосовується при організації бухгалтерського обліку в умовах комп'ютеризації суспільства;

– принцип зниження витрат на ведення бухгалтерського обліку, при тому, що достовірність, оперативність та своєчасність бухгалтерської інформації підвищуватиметься;

– принцип постійного удосконалення організації облікового процесу, який в свою чергу включає принципи економії часу та праці, а також їх пропорційності.

До складу існуючих принципів організації бухгалтерського обліку доцільно включити також запропоновані нами принципи, що наведені за допомогою наступної схеми (рис. 3.1).

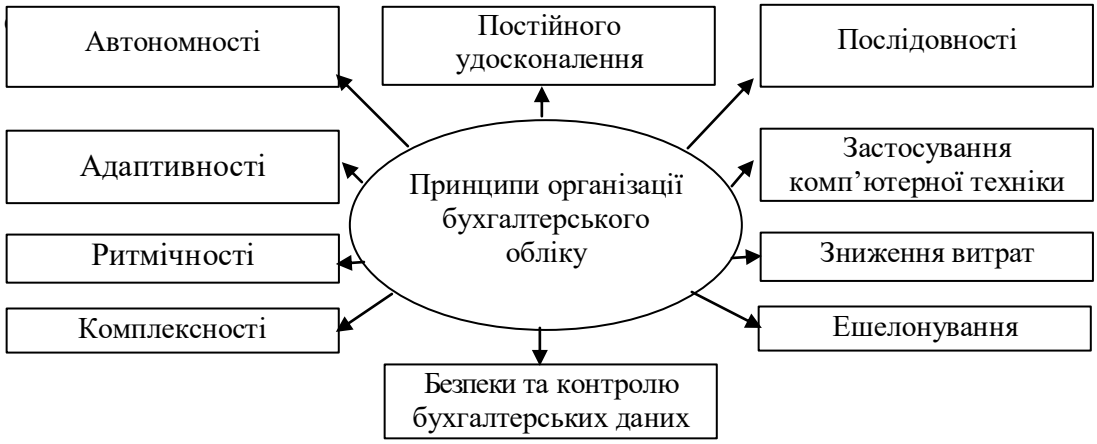


Рис. 3.1. Принципи організації бухгалтерського обліку

На нашу думку, до складу принципів організації бухгалтерського обліку є доречним залучення нових принципів, серед яких можна виділити наступні:

– принцип комплексності, згідно з яким при побудові системи захисту облікових даних необхідно передбачати прояв усіх видів можливих загроз для підприємства, включаючи канали несанкціонованого доступу до бухгалтерської інформації, та всі можливі для нього засоби захисту. Застосування цих засобів потрібно порівнювати з можливими видами загроз, а засоби захисту облікової інформації повинні функціонувати в межах єдиного комплексу захисту конфіденційної інформації підприємства, взаємно доповнюючи один одного у функціональному і технічному аспектах;

– принцип безпеки та контролю даних, який передбачає захист цінної облікової інформації, шляхом встановлення обмеження користувачів, віднесення її до інформації конфіденційного характеру та запровадження обмежень при роботі з нею;

– принцип ешелонування бухгалтерських даних (рис. 3.2) полягає в створенні декількох послідовних зон захисту облікової інформації. Таким чином, найбільш важлива інформація бухгалтерської служби повинна розташовуватись всередині інших зон захисту бухгалтерської інформації.

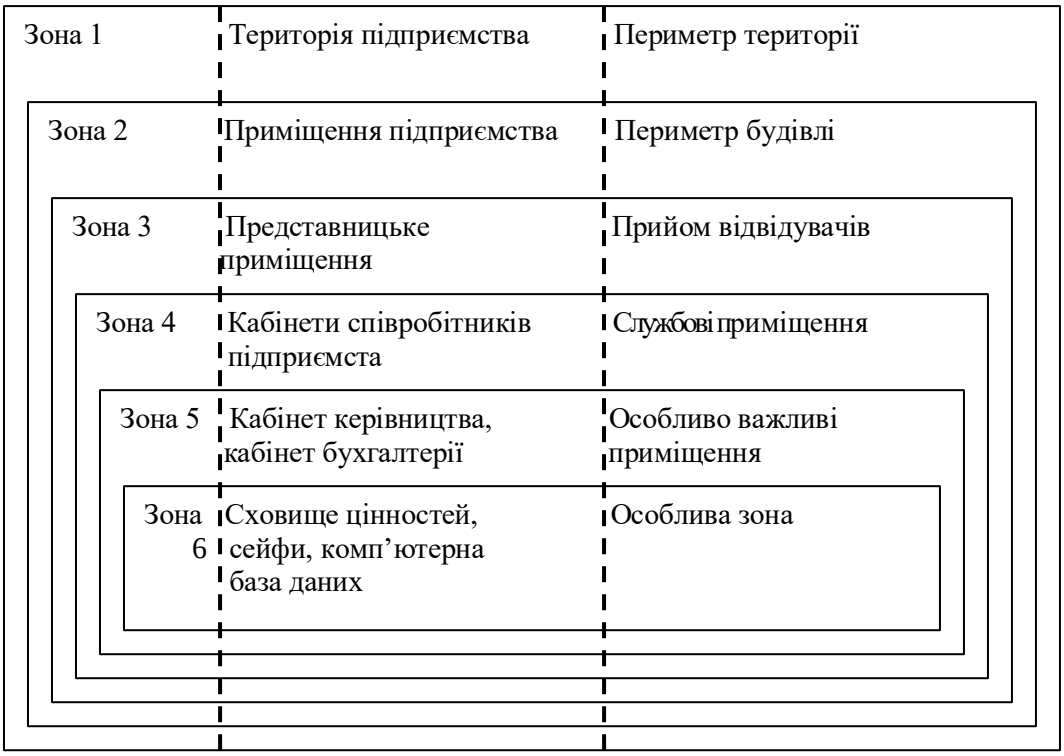


Рис. 3.2. Системна реалізація принципу ешелонування в системі безпеки підприємства

В наш час, коли прояви недосконалої конкуренції все більше і більше почали турбувати керівників підприємств, актуальним є використання поняття безпеки на всіх рівнях господарської діяльності підприємства. В зв'язку з цим, при організації бухгалтерського обліку на підприємстві, необхідно більше уваги приділяти дотриманню принципу безпеки та контролю даних. Адже впровадження даного принципу дозволить керівництву підприємства здійснювати належний контроль відносно ефективного використанням активів і пасивів підприємства, що дозволить зберегти кошти та майно підприємства шляхом ведення бухгалтерського обліку.

Останнім часом занепокоєння відносно захисту облікових даних або збереження комерційної таємниці є досить актуальними питаннями для бізнесу, а ринок систем і засобів переповнений пропозиціями різних технічних рішень. Саме тому принцип безпеки та контролю даних є ключовим при організації бухгалтерському обліку на підприємстві. В зв'язку з цим, для підприємств особливо актуальним є питання відносно того, хто повинен виконувати функції зі збору, обробки та аналізу даних для забезпечення захисту та накопичення пропозицій відносно запровадження системи безпеки на підприємстві.

Нині найоптимальнішим структурним підрозділом підприємства, який може забезпечити збереження конфіденційної інформації та безпеку її зберігання є бухгалтерська служба. Бухгалтерська служба є одним з найважливіших структурних підрозділів підприємства, який займається не лише веденням бухгалтерського обліку і складанням звітності, а й забезпечує внутрішніх та зовнішніх користувачів достовірною та своєчасною інформацією про господарську діяльність підприємства, яка необхідна для прийняття відповідних рішень. Дана інформація є також стратегічно важливим елементом для конкурентів, які прагнуть зміцнення власного становища за рахунок передбачення дій сусідів. На основі цього значущість бухгалтерської служби набуває зовсім іншого значення. До її обов'язків доповнюється необхідність захисту інформації, яка становить певну цінність для підприємства.

Отже, підґрунтям, на якому має базуватися організація бухгалтерського обліку, є принципи. І від того, на основі яких принципів буде базуватися організація бухгалтерського обліку, залежить подальше ефективне ведення бухгалтерського обліку, та відповідно й успішне функціонування самого підприємства.

Необхідним атрибутом захисту облікової інформації є кадрова робота з персоналом бухгалтерії. Вона полягає у забезпеченні фізичної безпеки бухгалтерів, охороні приміщення та документів, роз'яснювальній роботі, а також у забезпеченні суворого нагляду за діями бухгалтерів. Інформація, що накопичується підсистемою управлінського обліку, зазвичай, є основним об'єктом промислового шпигунства.

Головним пріоритетом захисту бухгалтерської інформації на підприємстві є розробка заходів спрямованих на збереження інформації, що

міститься в інформаційній базі підприємства при використанні комп'ютерних технологій. Це, передусім, пов'язано з тим, що в теперішніх умовах господарювання використовується комп'ютерна форма обліку, яка передбачає застосування різних програмних продуктів для ведення бухгалтерського обліку. Інформація системи бухгалтерського обліку містить усі дані про господарську діяльність підприємства, і відповідно є об'єктом зацікавленості конкурентів. В результаті чого Інформація системи бухгалтерського обліку повинна бути захищена на підприємстві в першу чергу.

Для будь-якого підприємства при побудові системи безпеки облікової інформації необхідно розробити концепцію забезпечення інформаційної безпеки, можливо у формі внутрішнього документу, в якій на основі аналізу сучасного рівня та динаміки розвитку інформаційних технологій розглядається систематизоване викладення цілей, завдань та принципів досягнення потрібного рівня захисту бухгалтерської інформації.

Успішна діяльність підприємств багато в чому залежить від якісної характеристики інформації, що відображає сутність усіх процесів, які відбуваються при здійсненні господарської діяльності. Зміни, що відбуваються в економіці також впливають і на бухгалтерський облік, чим розширюють коло його завдань. На початковій стадії завдання бухгалтерського обліку полягало у збереженні майна власника, дещо пізніше до нього додалося визначення та розподіл фінансового результату діяльності підприємства. Ці завдання досить тісно взаємодіють з управлінням, однак в нинішніх умовах господарювання надання інформації для потреб управління стало новим завданням бухгалтерського обліку.

Бухгалтерський облік є інформаційною системою, яка обслуговує процес прийняття управлінських рішень (рис. 3.3).

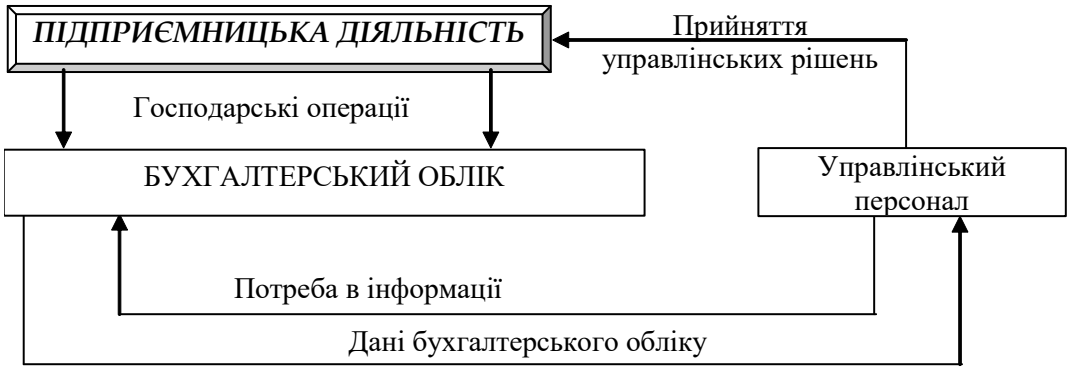


Рис. 3.3. Бухгалтерський облік як базис економічної безпеки підприємства

Проаналізувавши рис. 3.3, можна дійти висновку, що бухгалтерський облік є частиною загальної інформаційної системи, за допомогою якої дані з первинних документів перетворюються в оброблену інформацію для управління.

Звідси витікає, що найважливішим напрямом формування системи економічної безпеки, у тому числі і підприємства, є створення дієвого механізму безпеки, яким є бухгалтерський облік. Все це пояснюється тим, що бухгалтерський облік є однією з основних функцій управління, спрямованою на забезпечення економічної безпеки підприємства, і саме бухгалтерський облік виключає можливість прямих розкрадань без встановлених законом наслідків, створює інформаційні умови для здійснення контролю доцільності і законності використання ресурсів в превентивному, поточному і наступному режимах та сприяє запобіганню реалізації загроз, які знижують економічну стійкість підприємств.

Для будь-якої системи захисту даних підприємства джерелом небезпеки є персонал. Система економічної безпеки створюється та впроваджується фахівцями, через це працівники повинні досить чітко, не задумуючись виконувати поставлені перед ними вимоги. Такий підхід може вберегти підприємство від неочікуваних наслідків з боку осіб, які бажають заволодіти комерційною таємницею. Недостатній контроль за діями своїх співробітників досить часто переростає в значні збитки для підприємств. В сучасній практиці мають місце випадки, при яких інсайдери домовляються один з одним, торгують конфіденційною інформацією або здійснюють фінансові шахрайства в межах компанії. Наслідки таких інцидентів є досить серйозними: прямі збитки та зниження кількості клієнтів супроводжуються штрафами та судовими переслідуваннями з боку регулюючого органу. Таким чином, за усіма операціями з суттєвими даними повинен встановлюватись прозорий, але жорсткий контроль.

Розголошення конфіденційної інформації може досить дорого коштувати підприємству.

Основою збереження комерційної таємниці є створення облікового апарату, який в процесі своєї діяльності здійснює контроль не тільки за правомірністю господарських операцій на підприємстві, а й за охороною конфіденційної інформації.

Як зазначають С.Б. Барнгольц та М.В. Мельник, зміни в економіці, створення великої кількості комерційних організацій, їх значна диверсифікація, вимоги орієнтуватись на потреби клієнтів, облік дій конкурентів призвели до суттєвої зміни процесу управління виробництвом, потребуючи якомога більшої гнучкості та адаптивності організацій до нових умов [[114], с. 168].

Позитивно оцінюючи вплив зовнішнього та внутрішнього середовища слід розглядати управлінські та технічні нововведення, які комплексно впливають на господарську діяльність підприємства. Підприємство у своїй господарській діяльності може використовувати ці пропозиції, а може й нехтувати ними, проте необхідність враховувати пропозиції обумовлено низкою об'єктивних причин. При здійсненні інноваційної діяльності виникають особливі засоби та способи виробництва. Це об'єктивно зумовлює необхідність активного долучення підприємств до інноваційних процесів, критичного аналізу можливих засобів та способів виготовлення одного й того ж виду продукції. Необхідність впровадження нововведень у сфері технології виробництва, організації виробництва та управління, зумовлена, двома причинами: 1) можливістю зниження витрат виробництва і в той же час збільшенням прибутку та отриманням конкурентних переваг на ринку; 2) розширенням існуючого сегменту ринку та оволодіння новими ринками збуту.

Наведене вище повинно призвести до зростання прибутку підприємства, зміцненню його конкурентних позицій на ринку та підвищенню рівня економічної безпеки, що в свою чергу забезпечить збереження майна підприємства.

Проаналізувавши викладений вище матеріал, можна сказати, що на підприємстві діє ефективна система економічної безпеки, в тому випадку коли економічні інтереси підприємства узгоджені з інтересами постачальників, споживачів, інвесторів, конкурентів, суспільства та держави. Узгодження інтересів суб'єкта господарювання з суб'єктами зовнішнього середовища можливе при інтеграції їх інтересів.

[114] Барнгольц С.Б. Методология экономического анализа деятельности хозяйствующего субъекта: [учеб. пособие] / С.Б. Барнгольц, М.В. Мельник. – М.: Финансы и статистика, 2003. – 240 с.

Необхідність захисту майна підприємства підтверджує також А.Е. Тарас в своїй праці [115], зазначаючи про те, що серед всіх видів злочинів в СНД майже 70 % складають крадіжки майна громадян (включаючи, звичайно, бізнесменів), власності підприємств та фірм. Кожен третій серед цих майнових злочинів був буквально спровокований безпечністю власників або недостатньою захищеністю місць зберігання матеріальних цінностей.

У зв'язку з цим необхідним є виділення суб'єктів інтересів підприємства. При розробці ієрархії суб'єктів інтересів підприємства домінуючі позиції повинні належати власнику засобів виробництва та керівництву підприємства. Реальний контроль над діяльністю підприємства може здійснюватися сторонніми структурами, наприклад, кредиторами. Присутність такого суб'єкта контролю над діяльністю підприємства можна визначити за наслідками аналізу його фінансового стану за допомогою показників питомої ваги довгострокових та короткострокових кредитів в структурі капіталу і оцінки структури кредиторів підприємства. Використання позикових коштів у великому обсязі може привести до того, що реально діяльність підприємства протягом певного періоду контролюють власники позикових засобів. Крім того, реальна політика підприємства може формуватися і реалізовуватися поза сферою його управління, наприклад, через різного роду консультативні і дорадчі органи.

Вимоги, які висуваються користувачами до інформації, що формується в системі бухгалтерського обліку, постійно підвищуються. Розвиток економічних відносин, зростання інвестицій, глобалізація економіки, а також суттєві зміни в засобах комунікації змушують учасників економічних процесів віддавати перевагу достовірній та надійно захищеній інформації. У зв'язку з цим постає проблема захисту облікової інформації підприємства, як така, що потребує першочергового вирішення. Значущість даної проблеми підвищується тим, що інформаційний простір, який містить значні обсяги загальнодоступної інформації, є не лише джерелом даних для прийняття користувачами певних рішень, але й може бути джерелом для несанкціонованого розповсюдження конфіденційної інформації. Передусім, захист облікової інформації з метою збереження активів і пасивів повинен стати центральною ланкою економічної, а

[115] Тарас А.Е. Безопасность бизнесмена и бизнеса: [практ. пособ.] / А.Е. Тарас. – Мн.: "Сэкай", 1996. – 180 с.

також важливою частиною й інформаційної безпеки, спрямованої на задоволення потреб користувачів інформації.

Основна мета захисту бухгалтерської інформації полягає в тому, щоб запобігти її розголошенню та оволодінню нею конкурентами.

Захист бухгалтерської інформації з метою збереження майна підприємства є збалансованим станом здійснення фактів підприємницької діяльності при ефективному та законному використанні економічних ресурсів, на базі обліку, аналізу та контролю.

Такий підхід до забезпечення стійкої та довгострокової діяльності підприємства вимагає розробки концепції економічної безпеки підприємницької в частині бухгалтерського обліку, спрямованої на усунення загрози настання неспроможності, в основу якої покладені:

– бухгалтерський фінансовий, управлінський, податковий облік фактів господарської діяльності;

– комплексний економічний аналіз підприємницьких планів та фактів господарської діяльності;

– внутрішній контроль законності підприємництва та обліку фактів підприємницької діяльності.

Для підтримки збалансованого та стійкого стану в підприємницькій діяльності необхідно враховувати факти господарського життя, проводити їх комплексний економічний аналіз та здійснювати внутрішній контроль. Місцем взаємодії елементів даної системи є поле економічної безпеки підприємницької діяльності.

Формування концепції економічної безпеки підприємницької діяльності підприємств визначило необхідність нового концептуального підходу, до бухгалтерського фінансового, управлінського та податкового обліку, комплексного економічного аналізу, внутрішнього контролю.

Подальший розвиток підприємств зумовив необхідність проведення досліджень та розробки теорії і методології формування ефективної системи контролю за діяльністю суб’єктів господарювання.

Вдосконалення обліку та контролю забезпечує створення інформаційного забезпечення управління підприємницькою діяльністю підприємств.

Забезпечення безпеки облікових даних є однією з найважливіших проблем, що постає перед кожним підприємством. В загальній системі управління підсистема забезпечення безпеки має тісний зв’язок з підсистемою

управління персоналом. Завдання підсистеми управління персоналом в системі економічної безпеки підприємства можна визначити як мінімізацію ризику і загроз з боку співробітників. Співробітники повинні бути надійними та лояльними. При прийомі людей на відповідальні посади необхідно покладатися не лише на професійне чуття працівника відділу кадрів, але й на спеціальне обладнання. Прикладом такого обладнання може слугувати пристрій, який дасть можливість визначити справжні наміри майбутнього співробітника. Звісно, особа може не погоджуватися на такий тест. Але, якщо вона зацікавлена в отриманні місця та дійсно має намір працювати на користь підприємства, то погодиться на проведення обстеження.

Для обмеження доступу користувачів до різного роду конфіденційної інформації підприємства, яка міститься в бухгалтерській документації, можна застосовувати засобами, які спрямовані на зазначення обов'язкового місцезнаходження певного працівників в певний проміжок часу на підприємстві. Тобто, з метою уникнення випадкового або навмисного розголошення конфіденційної інформації, яке може виникнути у випадку, коли один із співробітників проходячи за спиною у свого колеги мав можливість заглянути у його файли, бачити які йому не потрібно.

Заходи щодо захисту облікової інформації повинні структурувати та максимально формалізувати відносини між підрозділами, документальні потоки між ними, правила спілкування відділів, правила передачі інформації між ними. Таким чином, основне завдання захисту облікової інформації з метою захисту майна підприємства полягає у необхідності визначення:

– обмеженого кола осіб, які мають доступ до певного виду як електронної інформації, так і інформації на паперових носіях;

– осіб, які мають право доступу до цієї інформації;

– місця зберігання цієї інформації;

– правил поведінки з конфіденційними документами.

До структурованої таким чином системи вже не складно застосувати захисні механізми.

Вважаємо, що для боротьби з шахрайством у відношенні майна підприємства, яке здійснюється шляхом знищення раніше введених проводок або внесення змін до них, необхідно дозволяти доступ для введення бухгалтерських проводок лише бухгалтеру, який відповідає за виконання роботи на цій ділянці обліку.

Для досягнення необхідного рівня інформаційної безпеки доцільно підходити до цієї проблеми комплексно, тобто витрачати кошти не на придбання засобів захисту, а приймати комплексні рішення, які можуть бути інтегровані з інформаційними технологіями.

Важливим моментом інформаційної безпеки облікової інформації є те, що керівництво підприємства повинно забезпечити необхідний для підприємства ступінь захисту інформації, яка використовується при складанні різного роду звітності. Хоча ця проблема і виходить за межі бухгалтерського обліку, не слід забувати про те, що вона існує та вимагає адекватного вирішення. Бухгалтерська інформація є найціннішою інформацією, яка характеризує всі сторони діяльності підприємства, тому питання забезпечення інформаційної безпеки необхідно вирішувати ще на етапі її формування.

Також доцільним є формування інфраструктури сприйняття облікової інформації, тобто системи організаційних форм структуризації відносин щодо формування, захисту, передачі та сприйняття облікової інформації. Необхідність формування розвиненої інфраструктури, спрямованої на пріоритетний розвиток та підвищення якості процесів сприйняття інформації, викликана специфічними особливостями процесів сприйняття саме облікової інформації.

Сучасний підхід до забезпечення безпеки облікової інформації потребує створення цілісної системи інформаційної безпеки, яка б містила комплекс організаційних, правових, інженерно-технічних та програмно-апаратних заходів захисту та використовувала б сучасні методи прогнозування, аналізу та моделювання змінних ситуацій.

3.2. Формування бухгалтерської служби підприємства з метою забезпечення економічної безпеки підприємств

Розвиток ринкової економіки змінює відношення до проблем забезпечення безпеки економічної інформації, оскільки власник, підприємець та бухгалтер є зацікавленими у захисті своїх громадських та економічних прав. Причому зацікавленість останнього спричинена його доступом практично до всієї основної фінансової інформації підприємства при веденні бухгалтерського обліку. Виходячи з цього виникає об’єктивна необхідність захисту економічних та фінансово-господарських показників діяльності підприємства, тобто бухгалтерської інформації. На сучасному етапі розвитку

економіки великого значення набуває впровадження системи заходів, спрямованих на захист цінної інформації суб'єкта господарювання від зазіхань конкурентів. Основним елементом, що спроможним стати на заваді втрати цієї інформації, є бухгалтерський облік, а саме його організація. Тобто, при організації бухгалтерського обліку на підприємстві, беззаперечно повинна приймати участь бухгалтерська служба, працівники якої матимуть змогу організувати бухгалтерський облік таким чином, щоб уникнути витоку цінної інформації завдяки роботі бухгалтерів.

Бухгалтерська інформація є основною складовою економічної та інформаційної безпеки підприємства. Оскільки інформаційна безпека передбачає захист переважно бухгалтерської інформації і є організаційно-правовим заходом безпеки, невід'ємною його складовою, основним елементом захисту складових комерційної таємниці від впливу негативних факторів слід вважати бухгалтерський облік, який є передумовою порядку та безпеки суб'єкта господарювання. Тобто, організація бухгалтерського обліку на підприємстві є досить важливим етапом в роботі підприємства, оскільки від неї в подальшому залежатиме ефективне функціонування суб'єкта господарювання та його безпека.

Будь-який керівник повинен розуміти, що він не зможе контролювати ситуації в тих місцях, де його в даний час немає. Захист відомостей, що містять комерційну таємницю, регулюється чинним законодавством. Однак не всі відомості комерційного характеру, наприклад, інформація про клієнтів, організацію виробництва, методи управління підприємством можуть бути захищені як об'єкти інтелектуальної власності. Саме тому в подібних ситуаціях необхідно поміркувати над попередженням ситуацій, які можуть спричинити розголошення конфіденційної інформації, для забезпечення подальшого розвитку та нормального функціонування підприємства.

Забезпечення стабільного функціонування суб'єкта господарювання потребує реалізації комплексу спеціальних заходів економічної безпеки та засобів захисту, заснованих на внутрішньофірмовій стратегії та політиці безпеки, аналізі ризиків загроз, можливих для даного підприємства в певний період.

Важливою умовою ефективного управління суб'єктом господарювання є високий рівень організації бухгалтерського обліку, основним завданням якого є забезпечення управлінського персоналу достовірною інформацією для прийняття ефективних управлінських рішень.

Дослідженням питань організації бухгалтерського обліку займалися такі вчені як П.С. Безруких [116], Ф.Ф. Бутинець [117], О.М. Галаган [118], Н.М. Грабова [119], А.Н. Кашаєв [120], П.А. Костюк [121] та ін.

Актуальним питанням є визначення сутності поняття "організація бухгалтерського обліку", завдань, які висуваються перед організацією бухгалтерського обліку, дослідження принципів організації бухгалтерського обліку, сформульованих вченими, адже спеціалізація будь-якої галузі науки чи наукової дисципліни безпосередньо пов'язана з чітким визначенням її поняття, завдань і принципів. Дані моменти є досить важливими для подальшого функціонування підприємства, оскільки визначають основні організаційні та методичні засади ведення бухгалтерського обліку та запобігають витоку інформації, яка становить комерційну таємницю підприємства та міститься в даних бухгалтерського обліку. У зв'язку з цим з'ясуємо сутність поняття "організація бухгалтерського обліку".

Поняття "організація" походить від давньогрецького слова "орган", яке позначає знаряддя або інструмент. Термін "організація" має різне значення. В найбільш загальному вигляді – це упорядкування, налагодження, приведення до визначеного порядку (системи) будь-чого. [122, с. 5].

Варто відмітити, що вже протягом багатьох років здійснюються спроби визначити сутність поняття "організація", сформулювати основні його характеристики, та цілий ряд питань залишається дискусійним і потребує подальшого дослідження. Для цього терміну характерне вираження цілеспрямованого функціонування взаємопов'язаних елементів системи та розвитку.

---

116 Безруких П.С. Организация бухгалтерского учета на предприятии / П.С. Безруких. – М.: "Финансы", 1966. – 204 с.

117 Бутинець Ф.Ф. Організація бухгалтерського обліку: [Підр. для студентів спеціальності 7.050106 "Облік і аудит" вищих навчальних закладів, 4-е вид., доп. і перероб.] / Ф.Ф. Бутинець, О.П. Войналович, І.Л. Томашевська / За редакцією д.е.н., проф., Заслуженого діяча науки і техніки України Ф.Ф. Бутинця. – Житомир: ПП "Рута", 2005. – 528 с.

118 Галаган А. История предпринимательства российского. От купца до банкира / А. Галаган. – М.: Ось-89, 1997. – 160 с.

119 Грабова Н.Н. Теория бухгалтерского учета [учеб. пособие для сред. с.-х. заведений] / Н.Н. Грабова. – М.: "Финансы", 1972. – 223 с.

120 Кашаев А.Н. Организация бухгалтерского учета в производственных объединениях / А.Н. Кашаев. – М.: Финансы и статистика, 1986. – 192 с.

121 Костюк П.А. Бухгалтерский словарь / П.А. Костюк. – Минск: "Вышэйшая школа", 1971. – 160 с.

122 Кузьминский А.Н., Сопко В.В. Организация бухгалтерского учета и анализа хозяйственной деятельности. – К.: Вища школа, 1986. – 256 с.

Організація бухгалтерського обліку в широкому розумінні є упорядкуванням всіх елементів системи бухгалтерського обліку, налагодженням і удосконаленням його процесу. Детальніше визначення поняття "організація бухгалтерського обліку" наведено в Додатку П.

Проф. Ф.Ф. Бутинець визначає "організацію бухгалтерського обліку як цілеспрямовану діяльність керівників підприємства по створенню, постійному впорядкуванню та удосконаленню системи бухгалтерського обліку з метою забезпечення інформацією внутрішніх та зовнішніх користувачів" [123, с. 41].

"Поняття "організація бухгалтерського обліку" можна визначити як науково обґрунтовану сукупність умов, при яких найбільш економно і раціонально здійснюється збір, обробка і зберігання бухгалтерської інформації з метою оперативного контролю за правильним використанням майна підприємства та надання користувачам неупередженої інформації щодо показників фінансової звітності" [124, с. 41].

"Під організацією бухгалтерського обліку також розуміють систему умов та елементів побудови облікового процесу з метою отримання достовірної та своєчасної інформації про господарську діяльність підприємства і здійснення контролю за раціональним використанням виробничих ресурсів і готової продукції" [125, с. 40].

Ми вважаємо, що найбільш вдале тлумачення поняття "організація бухгалтерського обліку" дав проф. Ф.Ф. Бутинець, оскільки він показує, що бухгалтерський облік – це динамічний процес, на який постійно впливають зміни як внутрішнього так і зовнішнього середовища підприємства. Отже, можемо стверджувати, що організація бухгалтерського обліку є основою функціонування інформаційної системи підприємства.

Лівертовський Д.С. під організацією бухгалтерського обліку на підприємстві розуміє стійку систему реєстрації операцій та групування даних на рахунках аналітичного і синтетичного обліку, що забезпечує високу якість обліку

---

123 Організація бухгалтерського обліку: [навч. посіб. для студентів вузів спеціальності 7.050106 "Облік і аудит", 2-е вид., доп. і перероб.] / Ф.Ф. Бутинець, О.В. Олійник, М.М. Шигун, С.М. Шулепова. – Житомир: ЖІТІ, 2001. – 576 с.

124 Організація бухгалтерського обліку: [навч. посіб. для студентів вузів спеціальності 7.050106 "Облік і аудит", 2-е вид., доп. і перероб.] / Ф.Ф. Бутинець, О.В. Олійник, М.М. Шигун, С.М. Шулепова. – Житомир: ЖІТІ, 2001. – 576 с.

125 Організація бухгалтерського обліку: [навч. посіб. для студентів вузів спеціальності 7.050106 "Облік і аудит", 2-е вид., доп. і перероб.] / Ф.Ф. Бутинець, О.В. Олійник, М.М. Шигун, С.М. Шулепова. – Житомир: ЖІТІ, 2001. – 576 с.

і контролю при найменших витратах праці. При організації бухгалтерського обліку потрібно мати на увазі задачі всього господарського обліку, важливою частиною якого є бухгалтерія кожного окремого підприємства. Раціонально організований бухгалтерський облік у багатьох випадках позбавляє від паралельного ведення оперативно-статистичного обліку, тобто поточного нагляду за окремими сторонами процесу діяльності підприємства, яке необхідне для управління підприємством. Добре продумана система групування даних господарської діяльності підприємства повинна давати в бухгалтерському обліку насичений змістом матеріал для статистичних узагальнень, для глибокого аналізу господарських процесів, що відбуваються [[126], с. 2].

Ми не погоджуємось з даним Д.С. Лівертовським визначенням, оскільки він говорить лише про рахунки синтетичного та аналітичного обліку, а саме про реєстрацію на них даних, і зовсім не звертає увагу, наприклад, на складання звітності.

Проф. А.М. Кузьмінський та проф. В.В. Сопко зазначають, що приведення у визначений порядок усіх вузлів систем бухгалтерського обліку і аналізу характеризує їх організацію в широкому змісті. Організація бухгалтерського обліку представляє собою систему методів і засобів, що забезпечують оптимальне її функціонування і подальший розвиток [[127], с. 5]. Визначення, дане А.М. Кузьмінським та В.В. Сопком, є досить загальним і на практиці досить складно зрозуміти, що саме включає організація бухгалтерського обліку.

Заслуговує на увагу визначення, що наводить І.С. Кумок [[128], с. 15], який під організацією бухгалтерського обліку розуміє систему умов і елементів облікового процесу, що включає первинний облік і документування операцій, план рахунків бухгалтерського обліку, форми організації обліково-обчислювальних робіт, обсяг та зміст звітності.

На підставі проведеного дослідження можна зробити висновок, що погляди науковців стосовно визначення сутності “організації бухгалтерського обліку” різняться, але їх умовно можна поділити на три групи.

---

[126] Ливертовский Д.С. Вопросы организации бухгалтерского учета / Д.С. Ливертовский. – М.: “Госстатиздат”, 1953. – 152 с.

[127] Кузьминский А.Н., Сопко В.В. Организация бухгалтерского учета и анализа хозяйственной деятельности. – К.: Вища школа, 1986. – 256 с.

[128] Настольная книга бухгалтера – профессионала / Под общ. ред. И.С. Кумка. – М.: АОЗТ “Московское Финансовое Объединение”, 1995. – 304 с.

Перша група дослідників зосереджувала увагу на складових організації бухгалтерського обліку. За основу вчені брали той факт, що організація бухгалтерського обліку повинна включати цілі, завдання, функції обліку і передбачати побудову елементів системи бухгалтерського обліку. Такої позиції дотримувалися більшість авторів досліджених джерел, зокрема О.М. Кашаєв [129], П.А. Костюк [130], А.М. Кузьмінський, В.В. Сопко [131], І.С. Кумок [132], Я.В. Соколов [133].

Друга група представлена такими науковцями, як Р.Я. Вейцман [134], О.М. Галаган [135], О.М. Островський, Т.А. Шнайдерман [136] та інші, які акцентують увагу на тому, що організація бухгалтерського обліку повинна зосереджуватися, головним чином, на управлінні обліковим персоналом.

Безруких П.С. [137], Гальперін Я.М. [138], Грабова Н.М. [139], Литвин Ю.Я., Олійник В.М., Палюх М.С., Семчишин М.В. [140] дотримувались позиції, що організація бухгалтерського обліку – це певний раціональний процес, тобто досягнення максимальних результатів при мінімальних затратах.

Слід відмітити, що при організації бухгалтерського обліку необхідно синтезувати всі три підходи. Також недоліком всіх вищенаведених визначень є те, що ніхто з вчених не звертає увагу на захист облікової інформації, проте саме вона акумулює всі дані господарської діяльності.

---

129 Кашаев А.Н. Организация бухгалтерского учета в производственных объединениях / А.Н. Кашаев. – М.: Финансы и статистика, 1986. – 192 с.

130 Костюк П.А. Бухгалтерский словарь / П.А. Костюк. – Минск: "Вышэйшая школа", 1971. – 160 с.

131 Кузьминский А.Н., Сопко В.В. Организация бухгалтерского учета и анализа хозяйственной деятельности. – К.: Вища школа, 1986. – 256 с.

132 Настольная книга бухгалтера – профессионала / Под общ. ред. И.С. Кумка. – М.: АОЗТ "Московское Финансовое Объединение", 1995. – 304 с.

133 Ковалев В.В. Организация бухгалтерского учета на совместных предприятиях / В.В. Ковалев, Е.Н. Евстигнеев, Я.В. Соколов. – М.: Финансы и статистика, 1991. – 160 с.

134 Вейцман Р.Я. Курс счетоводства. Двойная бухгалтерия и ее применение к различным видам хозяйств: [Одиннадцатое изд., перераб. и доп.] / Р.Я. Вейцман. – М.: Центрсоюз, 1926. – 447 с.

135 Галаган А. История предпринимательства российского. От купца до банкира / А. Галаган. – М.: Ось-89, 1997. – 160 с.

136 Островский О.Н. Типовые элементы организации бухгалтерского учета / О.Н. Островский, Т.А. Шнайдерман. – М.: Финансы и статистика, 1988. – 207 с.

137 Безруких П.С. Организация бухгалтерского учета на предприятии / П.С. Безруких. – М.: "Финансы", 1966. – 204 с.

138 Гальперин Я.М. Основы бухгалтерского учета: [Четвертое изд.] / Я.М. Гальперин. – М.-Л., 1970. – 370 с.

139 Грабова Н.Н. Теория бухгалтерского учета [учеб. пособие для сред. с.-х. заведений] / Н.Н. Грабова. – М.: "Финансы", 1972. – 223 с.

140 Організація обліку, контролю і аналізу в сільському господарстві / Ю.Я. Литвин, В.М. Олійник, М.С. Палюх, М.В. Семчишин. – Тернопіль: "Тернопіль", 1998. – 376 с.

Перед організацією бухгалтерського обліку постають завдання, виконання яких забезпечує ефективність ведення бухгалтерського обліку:

– відображення фактів господарського життя та дотримання вимог повноти, достовірності, своєчасності, безперервності при формуванні облікової інформації на підприємстві;

– обробка бухгалтерських даних у відповідності до існуючих процедур, правил, прийомів та способів;

– формування на підставі отриманої бухгалтерської інформації фінансової звітності та використання її певними користувачами;

– визначення меж застосування фінансового та управлінського обліку;

– вибір методики ведення бухгалтерського обліку;

– вибір технології і техніки ведення бухгалтерського обліку;

– підбір облікового персоналу та забезпечення їх роботи;

– обмеженість кола користувачів облікової інформації.

Від вирішення цих завдань залежить ступінь оперативності та якості обліку, задоволеності інтересів користувачів бухгалтерської інформації.

Погоджуємося з думкою Грабової Н.М., яка відмічає, що правильна організація бухгалтерського обліку залежить від таких найбільш важливих передумов:

– встановлення оперативної взаємодії бухгалтерії з оперативно відокремленими підрозділами підприємства;

– визначення обсягу і характеру облікової роботи [141].

Захист облікових даних та контроль потоків бухгалтерської інформації, що складають комерційну таємницю, має покладатися не лише на службу безпеки, але й на весь управлінський персонал підприємства.

Інформаційна система підприємства створюється для певного об’єкта, а в даному випадку – для підприємства та його бухгалтерії. Ефективна інформаційна система враховує різницю між ланками управління, сферами дій, а також зовнішніми обставинами та надає будь-якій ланці управління лише таку інформацію, яка необхідна їй для ефективної реалізації функцій управління.

[141] Грабова Н.Н. Теория бухгалтерского учета [учеб. пособие для сред. с.-х. заведений] / Н.Н. Грабова. – М.: “Финансы”, 1972. – 223 с.

Передумовою зменшення витоку життєво необхідної інформації багато в чому залежить від того, наскільки раціонально організовано бухгалтерську службу на підприємстві, правильно визначено її форму організації та структуру, що зумовлюються особливостями кожного підприємства та можуть коригуватися відповідно до його власних потреб.

Проте, питання організації бухгалтерської служби на підприємстві є досить проблематичним. Як в науковій, так і практичній сферах йому приділяється незначна увага. Про це свідчить, насамперед, відсутність праць рекомендаційного характеру з організації бухгалтерської служби та незначна кількість навчальних посібників з організації бухгалтерського обліку в цілому. Ще однією проблемою, що заважає раціонально організувати роботу бухгалтерської служби, є небажання самих бухгалтерів проводити зміни в організаційній структурі бухгалтерської служби та діяльності, що нею здійснюється.

Таким чином, бухгалтерська служба підприємства є одним з провідних самостійних підрозділів управлінської структури підприємства, який, крім ведення бухгалтерського обліку і складання бухгалтерської звітності, виконує складну і відповідальну роботу з організації своєчасного і достовірного бухгалтерського обліку, формування повної та достовірної інформації про його діяльність та майновий стан, необхідної також для контролю за дотриманням діючого законодавства, за раціональним та економним використанням матеріальних, трудових і фінансових ресурсів, попередженням негативних явищ в діяльності організації, здійснення суворого режиму економії та ін.

Отже, з метою забезпечення належного рівня економічної безпеки на підприємстві необхідною є розробка комплексної системи заходів з організації бухгалтерського обліку. Заходи щодо впровадження комплексної системи з організації бухгалтерського обліку наведено на рис. 3.4.

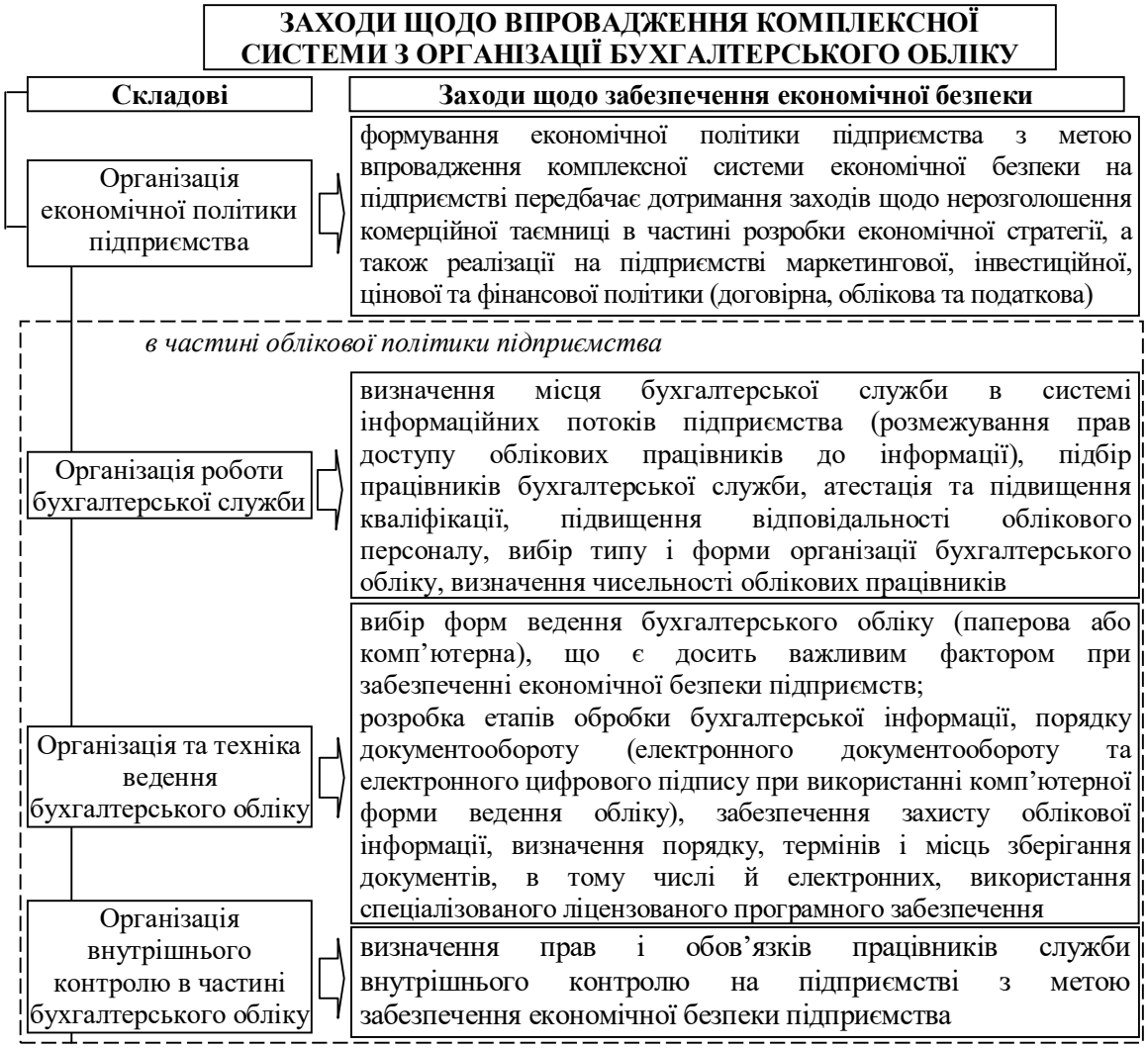


Рис. 3.4. Заходи щодо впровадження комплексної системи з організації бухгалтерського обліку

Застосування на практиці описаних на рис. 3.4 заходів щодо впровадження комплексної системи з організації бухгалтерського обліку підприємств дозволить вирішити основні питання, пов'язані із забезпеченням економічної безпеки підприємства.

Актуальність впровадження комплексної системи заходів з організації бухгалтерського обліку зумовлена необхідністю правильної організації облікового процесу, що здійснюється з метою збереження облікових даних для забезпечення економічної безпеки підприємства.

Оскільки близько 80 % інформації про господарську діяльність підприємства міститься в системі бухгалтерського обліку, то з'являється необхідність її організації з метою збереження бухгалтерських даних, які

становлять комерційну таємницю, від сторонніх осіб та працівників підприємства, які не мають права доступу до неї. Таким чином, забезпечення економічної безпеки в частині бухгалтерського обліку можливо досягти при його належній організації.

У вузькому розумінні, організація бухгалтерського обліку – це застосування елементів облікового процесу з метою досягнення цілі ведення бухгалтерського обліку на підприємстві.

На підприємствах організація облікового процесу зводиться до формування облікової політики підприємства, а також підписанні керівництвом розпорядчих документів, які стосуються діяльності облікового апарату: положення про бухгалтерську службу (Додаток Р), посадових інструкцій співробітників бухгалтерської служби (Додаток Л, Додаток М).

Слід зазначити, що в частині облікової політики підприємства оптимізація облікового процесу відбувається за трьома складовими:

організація роботи бухгалтерської служби;

організація та техніка ведення бухгалтерського обліку;

організація внутрішнього контролю.

Зазначені складові організації бухгалтерського обліку відображають процес ведення бухгалтерського обліку поетапно: від створення бухгалтерської служби до здійснення контролю за її діяльністю. Це досить важливо при веденні бухгалтерського обліку, оскільки:

– на першому етапі власником або керівником підприємства визначається суб'єкт ведення бухгалтерського обліку. На вибір суб'єкту впливають фактори як мікро-, так і макро- середовища.

– другий етап організації бухгалтерського обліку передбачає аналіз всіх можливих варіантів ведення бухгалтерського обліку та вибір найоптимальнішого для конкретного підприємства з огляду на те, при якому з них система обліку буде найефективніше виконувати свої функції для досягнення своєї мети.

– третій етап організації бухгалтерського обліку полягає виборі форми контролю за діяльністю облікового персоналу для забезпечення економічної безпеки.

Таким чином, впровадження комплексної системи заходів організації бухгалтерського обліку забезпечить якісне виконання обліковим персоналом

своїх обов'язків та підвищить їх відповідальність при виконанні поставлених завдань з метою дотримання економічної безпеки та збереження майна підприємства.

Підприємство як власник бухгалтерської інформації, що містить комерційну таємницю, має право визначити перелік осіб, які можуть володіти, розпоряджатися, користуватися такою інформацією, визначити правила обробки інформації та права доступу до неї, а також встановлювати інші умови щодо збереження комерційної таємниці. За умови дотримання необхідних заходів щодо організації бухгалтерського обліку власник матиме право на юридичний захист даних, що дозволи підвищити відповідальність облікового персоналу та зберегти майно підприємства, яке йому належить.

Проф. Ф.Ф. Бутинець наголошує, що необхідність створення бухгалтерської служби як відокремленого підрозділу підприємства, з правової точки зору, зумовлена наступним:

– по-перше, без ведення бухгалтерського обліку від моменту реєстрації до офіційної ліквідації, підприємство не має права на існування;

– по-друге, бухгалтерська служба є тим підрозділом, який повинен слідкувати за дотриманням чинного законодавства: господарського, податкового, трудового та ін., оскільки лише законні господарські операції підлягають відображенню у бухгалтерському обліку. Причому контроль повинен здійснюватися як щодо рішень і дій всіх працівників підприємства, так і щодо операцій, які здійснюються з контрагентами підприємства [142, с. 128].

Слід зазначити, що основними завданнями та функціями бухгалтерської служби на підприємстві є:

– формування облікової політики відповідно до законодавства про бухгалтерський облік виходячи з особливостей діяльності підприємства;

– забезпечення законності, своєчасності і правильності оформлення первинних документів;

– організація та ведення достовірного бухгалтерського обліку на підприємстві;

---

[142] Організація бухгалтерського обліку: [навч. посіб. для студентів вузів спеціальності 7.050106 "Облік і аудит", 2-е вид., доп. і перероб.] / Ф.Ф. Бутинець, О.В. Олійник, М.М. Шигун, С.М. Шулепова. – Житомир: ЖІТІ, 2001. – 576 с.

– складання податкової і бухгалтерської звітності на основі достовірних первинних документів і відповідних бухгалтерських записів, своєчасне подання її відповідним органам;

– забезпечення своєчасності платежів за зобов'язаннями підприємства, зокрема перед державним бюджетом;

– здійснення (спільно з іншими службами) економічного аналізу фінансово-господарської діяльності підприємства за даними бухгалтерського обліку та звітності з метою виявлення внутрішньогосподарських резервів, ліквідації втрат і непродуктивних витрат;

– здійснення контролю за збереженням власності підприємства, правильним витрачанням коштів і матеріальних цінностей, дотриманням найсуворішого режиму економії і своєчасності господарських розрахунків;

– своєчасне проведення інвентаризації коштів, товарно-матеріальних цінностей і розрахунків підприємства;

– вжиття заходів щодо попередження нестач, розтрат та інших порушень і зловживань, забезпечення своєчасності оформлення матеріалів за нестачами, розтратами, розкраданнями та іншими зловживаннями;

– впровадження передових форм і методів бухгалтерського обліку на основі широкого застосування обчислювальної техніки та ін.

Як правило, очолює бухгалтерську службу головний бухгалтер, який є штатним працівником підприємства.

Головному бухгалтеру підприємства безпосередньо підпорядковуються працівники бухгалтерської служби. Їх кількість та посади, що вони обіймають, залежать від характеру, складу і обсягу облікових робіт на підприємстві.

Обов'язки головного бухгалтера на різних підприємствах суттєво відрізняються. Так, на великому підприємстві, де бухгалтерська служба має в своєму складі декілька відділів (груп, секторів) зі значною кількістю облікових працівників до основних завдань головного бухгалтера належать: організація роботи бухгалтерської служби та керівництво її діяльністю, розподіл обов'язків між її структурними підрозділами та працівниками в середині самого підрозділу, контроль за виконанням покладених на них завдань та ін.

Якщо ж підприємство мале, то головний бухгалтер не лише забезпечує організацію бухгалтерського обліку, а й безпосередньо відображає здійснені господарські операції підприємства на рахунках бухгалтерського обліку.

Отже, одним із основних завдань, яке в першу чергу постає перед керівництвом будь-якого підприємства, є чітка побудова організаційної структури бухгалтерської служби. Це дасть змогу забезпечити формування необхідної інформації в зручний для використання час, в зрозумілій та достатній для прийняття рішень формі не тільки для всього управлінського персоналу, а й для системи управління в цілому.

Розглянемо підходи до організаційної побудови бухгалтерської служби, і наведемо переваги та недоліки їх використання в практичній діяльності підприємств, а також охарактеризуємо основні етапи формування структури бухгалтерської служби.

Успішне виконання завдань, поставлених перед бухгалтерською службою, багато в чому залежить від встановлення такої її форми побудови та структури, яка б найбільшою мірою відповідала конкретним умовам роботи підприємства.

Як зазначає проф. Ф.Ф. Бутинець, насамперед необхідно зазначити, що на організацію бухгалтерської служби, в тому числі і на вибір підприємством її форми організаційної побудови та типу організаційної структури, впливають наступні фактори:

– вид діяльності підприємства (виробництво, послуги, комерційна діяльність);

– обсяг виробництва, тобто чи є це підприємство мале, середнє чи велике;

– загальна чисельність працівників;

– кількість структурних підрозділів;

– характер організації технології виробництва;

– кількість філій (дочірніх підприємств);

– обсяг та рівень автоматизації облікових робіт та ін. [143, с. 137].

Створюючи бухгалтерську службу, керівництво підприємства, в першу чергу повинно визначити форму її організаційної побудови, яка є формою розподілу і кооперування праці та передбачає розподіл всього комплексу облікових робіт між виконавцями.

Бухгалтерська служба є таким же підрозділом підприємства, як і всі інші адміністративні служби. Більшість науковців та вчених (П.С. Безруких [144],

[143] Організація бухгалтерського обліку: [навч. посіб. для студентів вузів спеціальності 7.050106 "Облік і аудит", 2-е вид., доп. і перероб.] / Ф.Ф. Бутинець, О.В. Олійник, М.М. Шигун, С.М. Шулепова. – Житомир: ЖІТІ, 2001. – 576 с.

Н.М. Грабова [145], А.Г. Загородній [146], О.М. Кашаєв [147], М.С. Пушкар [148], Я.В. Соколов [149]), вважають, що залежно від форми організації роботи бухгалтерської служби її структура на середніх та великих підприємствах може бути централізованою або децентралізованою.

При централізованій структурі всі облікові роботи (обробка документів, аналітичний та синтетичний облік, складання зведеного балансу і звітності) здійснюються в центральній бухгалтерській службі. В окремих підрозділах підприємства складаються лише первинні документи (виписуються накладні, прибуткові та видаткові касові ордери та ін.), які разом зі звітами матеріально-відповідальних осіб передається до централізованої бухгалтерської служби.

За даної структури увесь обліковий персонал зосереджується в центральній бухгалтерській службі і підпорядкований головному бухгалтеру в адміністративному та методологічному відношенні.

Децентралізована структура передбачає, що в окремих виробничих підрозділах підприємства є власні бухгалтерські служби або облікові працівники, які в адміністративному відношенні підпорядковані керівникові даного структурного підрозділу (начальнику цеху, виробництва тощо), а в методологічному – головному бухгалтеру. Така бухгалтерська служба здійснює синтетичний і аналітичний облік, складає звітність. В головній бухгалтерській службі, на підставі звітів підрозділів, складається зведений баланс і звітність, а також здійснює контроль за постановкою обліку в окремих частинах підприємства.

Залежно від форми організації роботи бухгалтерської служби залежить і чисельність облікових працівників та витрати на утримання. Чим більша чисельність працівників бухгалтерської служби, тим більші витрати на

---

144 Безруких П.С. Организация бухгалтерского учета на предприятии / П.С. Безруких. – М.: "Финансы", 1966. – 204 с.

145 Грабова Н.Н. Теория бухгалтерского учета [учеб. пособие для сред. с.-х. заведений] / Н.Н. Грабова. – М.: "Финансы", 1972. – 223 с.

146 Загородній А.Г. Облік і аудит: [Термінологічний словник] / А.Г. Загородній, Г.Л. Вознюк, Г.О. Партин. – Львів: "Центр Європи", 2002. – 671 с.

147 Кашаев А.Н. Организация бухгалтерского учета в производственных объединениях / А.Н. Кашаев. – М.: Финансы и статистика, 1986. – 192 с.

148 Пушкар М.С. Теоретичні основи бухгалтерського обліку: [підр. для вузів, вид. 2-ге, перероб. і доп.] / М.С. Пушкар, Г.П. Журавель, Ю.Я. Литвин, В.Г. Мельник. – Тернопіль:ТАНГ, 1998. – 269 с.

149 Соколов Я.В. Бухгалтерский учет: от истоков до наших дней: [Учебн. пособие для вузов] / Я.В. Соколов. – М.: Аудит, ЮНИТИ, 1996. – 638 с.

оплату праці, утримання приміщень (оренду, нарахування амортизації, освітлення, опалення, поточний та капітальний ремонт тощо), організацію робочих міст бухгалтерів, телефонні та інші витрати.

При використанні централізованої форми організації бухгалтерського обліку чисельність працівників бухгалтерської служби менша, ніж при децентралізації обліку, так як знижується чисельність адміністративного апарату (головний бухгалтер, заступник), з'являється можливість більшого завантаження працівників за рахунок збільшення обсягів виконуваних ними робіт. А основною перевагою є шляхом зменшення працівників, зменшується ймовірність витоку цінної інформації.

"Разом з тим, – зазначає А.Н. Сушкевич, – децентралізація обліку дозволяє краще організовувати контроль раціонального використання трудових та матеріальних ресурсів в місцях виникнення витрат, підвищити оперативність обліку, а значить, і прийняття управлінських рішень, що сприяють зниженню собівартості продукції та зростанню прибутку" [[150], с. 74].

За цих обставин ймовірність втрати інформації збільшується. Все залежить від того, яким чином було організовано облік. Перевагою даної структури є те, що кожному працівнику бухгалтерської служби надається окрема частка роботи, за яку він в подальшому несе відповідальність. Тобто інформація міститься у розпорядженні обмеженої кількості працівників, що є передумовою її збереження. На думку проф. О.М. Кашаєва [[151], с. 21], встановлення оптимального співвідношення між централізацією та децентралізацією при побудові структури бухгалтерської служби є найважливішим шляхом удосконалення управління підприємством та підвищення ефективності обліку.

Обравши форму організації бухгалтерської служби, головний бухгалтер повинен визначити її внутрішню структуру.

Організаційна структура бухгалтерської служби представляє собою склад і підпорядкованість її взаємопов'язаних організаційних одиниць і ланок, що виконують різні функції. Іншими словами, під структурою бухгалтерської служби розуміють її поділ на складові частини на основі

[150] Сушкевич А.Н. Организация бухгалтерского учета в субъектах хозяйствования / А.Н. Сушкевич. – Мн.: Ред. журн. "Пром.-торговое право", 2004. – 252 с.

[151] Кашаев А.Н. Организация бухгалтерского учета в производственных объединениях / А.Н. Кашаев. – М.: Финансы и статистика, 1986. – 192 с.

принципів розподілу праці, тобто спеціалізації працівників бухгалтерської служби і кооперації їх спільних зусиль.

Варто зазначити, що при розвитку організаційних структур бухгалтерської служби відбуваються значні зміни, про що свідчать тенденції, відмічені в наш час. Зокрема, старі організаційні структури бухгалтерської служби в багатьох випадках не відповідають вимогам ринкових відносин, оскільки не дозволяють врахувати специфіку основних завдань, які поставлені для вирішення перед бухгалтерською службою. Створюючи організаційну структуру, слід враховувати не лише власний досвід та досвід діючих підприємств, але й наукові методичні підходи та нові розробки. Крім того, в переважній більшості випадків останнім часом на підприємствах віддають перевагу комп'ютерній формі ведення обліку, що не може не відобразитися на особливостях побудови їх організаційної структури.

Досить важливими залишаються проблеми визначення оптимального співвідношення лінійного та функціонального управління, а також встановлення горизонтальних та вертикальних зв'язків. Однак, навіть за умови формування потрібного співвідношення в управлінні не можна гарантувати повної безпеки при збереженні облікових даних на підприємстві. Нерідко самі працівники підприємства, які з корисливих мотивів, злого наміру чи просто через необачність передають зацікавленим особам таємну інформацію, стають джерелом витоку цінної інформації за межі підприємства. З огляду на це, потрібно створити умови для задоволення працівниками потреб у реалізації їхніх здібностей і потенціалу, у суспільному визнанні значущості їх успіхів.

Підсумовуючи викладений вище матеріал, можна дійти висновку, що існують певні етапи формування організаційної структури бухгалтерської служби з метою забезпечення економічної безпеки підприємства (рис. 3.5).

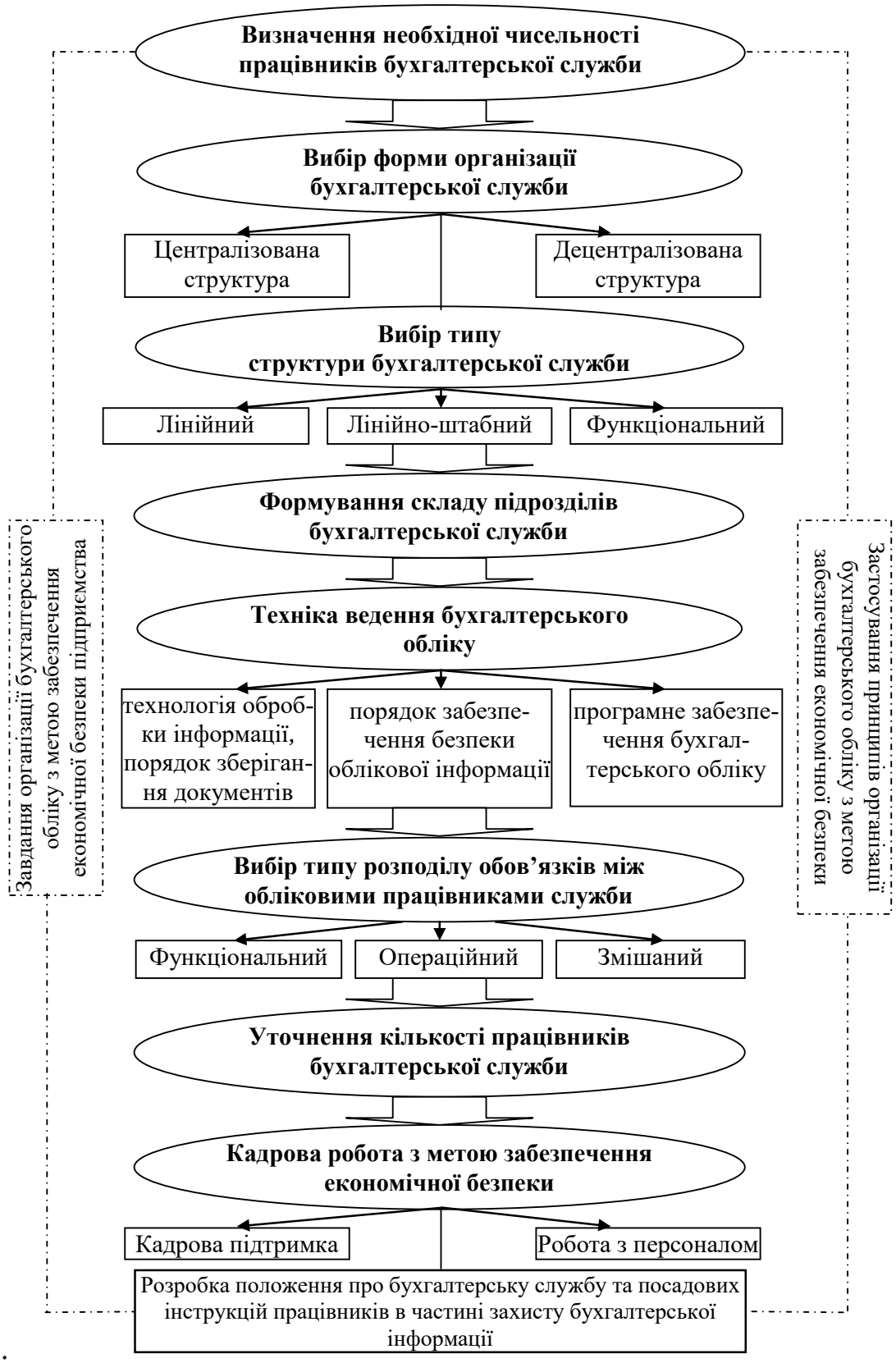


Рис. 3.5. Модель організації бухгалтерського обліку та побудови облікового апарату з метою забезпечення економічної безпеки підприємства

Таким чином, вибір певної форми організації та структури бухгалтерської служби зумовлює рівень захисту бухгалтерської інформації. Інформація, що накопичується підсистемою управлінського обліку, зазвичай, є основним об'єктом промислового шпигунства.

"Система безпеки ефективна лише тоді, – зазначає А.П. Градов, – коли відбувається її належне управління, здійснюється підтримка її стабільного функціонування на всіх рівнях. Реалізація цих вимог щодо системи безпеки дозволяє попередити витік конфіденційної економічної інформації з підприємства, порушення комерційної таємниці, економічні диверсії" [152].

Схожі принципи наведені в праці В. Гайковича та А. Першина [153], в якій автори систему безпеки підприємства розглядають як комплексну систему захисту інформації – організовану та керовану сукупність органів, засобів і методів, призначених для реалізації на регулярній основі функцій захисту інформації. Під функцією захисту автори розуміють сукупність однорідних у функціональному відношенні заходів, здійснюваних на об'єкті з метою створення, підтримки та забезпечення умов, об'єктивно необхідних для надійного захисту інформації. Основна базова вимога, яка повинна задовольняти ряд функцій, полягає в системному забезпеченні захисту інформації при раціональному використанні ресурсів, які потребують захисту.

Для будь-якої системи захисту даних підприємства джерелом небезпеки є люди. Система економічної безпеки створюється та впроваджується фахівцями, через це працівники повинні досить чітко, виконувати поставлені перед ними вимоги. Такий підхід може вберегти підприємство від неочікуваних наслідків з боку осіб, які бажають заволодіти комерційною таємницею. "Недостатній контроль за діями своїх співробітників, – наголошує керівник відділу системного програмного забезпечення компанії "Геліос Комп'ютер" В. Лупанов, – досить часто переростає в значні збитки для підприємств. В сучасній практиці мають місце випадки, при яких інсайдери* домовляються один з одним, торгують конфіденційною інформацією або здійснюють фінансові шахрайства в межах компанії. Наслідки таких інцидентів досить плачевні: прямі збитки та зниження кількості клієнтів

[152] Градов А.П. Национальная экономика: [2-е изд.] / А.П. Градов. – СПб.: Питер, 2005. – 240 с.
[153] Гайкович В. Безопасность электронных банковских систем / В. Гайкович, А. Першин / Под ред. Ю.В. Гайковича. – М.: Единая Европа, 1994. – 363 с.
* Інсайдер – співробітник компанії або міністерства, який має доступ до конфіденційної інформації в зв'язку зі службовими обов'язками *(прим. автора)*.

супроводжуються штрафами та судовими переслідуваннями з боку регулюючого органу. Таким чином, за усіма операціями з суттєвими даними повинен встановлюватись прозорий, але жорсткий контроль" [154].

Узагальнюючи міжнародний досвід щодо поділу співробітників за ступенем небезпеки, яка від них виходить, та яку необхідно оцінити ще на стадії розгляду певної кандидатури при прийнятті на роботу, персонал можна умовно розподілити за групами низького, допустимого та високого ризику.

Робота з групою низького ризику не потребує особливих затрат, тому що вони навряд чи вдадуться до компрометації своєї честі та гідності незалежно від стану навколишнього середовища та створених заходів безпеки та контролю.

До групи високого ризику належить категорія людей, яку в переважній більшості випадків не допускають в лави співробітників фірми ще на стадії відбору, так як витрати на реалізацію необхідних заходів безпеки, спрямованих на попередження деструктивних дій з їх сторони, можуть перевищити розмір потенційної користі, яку вони можуть принести фірмі. Крім того, кропітка робота з контингентом високого ризику в умовах обмеженого фінансування служби по роботі з персоналом, може викликати недостаток сил, засобів та уваги до інших категорій співробітників та, як наслідок, збільшить імовірність деструктивних дій групи допустимого ризику.

Перебуваючи в підконтрольних умовах, співробітники групи допустимого ризику, які мають певні права, повноваження та ліміт відповідальності будуть досить лояльними до компанії, в тому числі при зміні стану внутрішнього та зовнішнього середовища. Саме тому вони і є об'єктом особливої уваги осіб, які відповідають за управління персоналом та забезпечення безпеки підприємства.

Такий підхід, в першу чергу, передбачає діяльність спеціалістів служби персоналу та безпеки в напрямі виявлення на етапі відбору та первинної перевірки осіб, які схильні за своїми морально-етичними установками здійснювати протиправні дії незалежно від встановлених заходів безпеки. Такі кандидати під час відбору повинні виключатися зі списків претендентів на посаду. В процесі повсякденної діяльності вимагається досить жорстка регламентація усіх бізнес-процесів в поєднанні з системою контролю. В

[154] 12 самых громких случаев ИТ-воровства в России: [Електронний ресурс]. – Режим доступу: http://www.cnews.ru/reviews/?2005/12/02/192675.

цьому випадку передбачається виявлення та локалізація шахрайств, які можуть готуватися, а також кримінальних та інших дій деструктивного характеру відносно підприємства з боку свого персоналу. При цьому особливу увагу необхідно приділяти закриттю можливих каналів витоку конфіденційної інформації, попередженню розкрадань матеріальних цінностей, зловживанням службовим становищем, злочинами проти особистості, діям, які завдають збитків репутації. Посилення конкуренції, прагнення до лідерства спонукають керівників підприємств по-новому розглядати проблему безпеки, особливо її кадровий аспект.

За даними міжнародної статистики "приблизно у половині випадків розкриття інформації підприємства (промислового шпигунства) винні самі співробітники, яких вербують конкуренти або спеціальні агенти, що спеціалізуються на такого роду замовленнях" [155, с. 14].

Шкоду, завдану працівниками, можна умовно поділити на навмисну і ненавмисну, причому кожен підвид може бути прихованим або явним. Зазвичай кадрові проблеми починаються на тих підприємствах, де кількість працівників нижчої ланки різко зросла, а наявна система менеджменту зберегла колишню чисельність та структуру. Для запобігання внутрішній небезпеці розшарування кадрів потрібно вжити наступних заходів:

– зміна структури управління;

– правильний добір персоналу до формованої ієрархії;

– залучення професійних психологів.

Якщо на підприємстві використовується обробка бухгалтерської інформації за допомогою комп'ютерних технологій, то передбачається, що всі основні канали витоку інформації знаходяться безпосередньо в комп'ютерних мережах.

Але існує й ряд інших каналів витоку інформації, які також важливі і потребують кваліфікованого захисту. Так, в кабінеті керівництва постійно циркулює інформація, що становить цінність або комерційну таємницю підприємства (телефонні переговори, обговорення, редагування інформації на персональному комп'ютері тощо).

[155] Аглицкий И. Защита информации в бизнесе: секретные диски / И. Аглицкий // Финансовая газета. – 1999. – № 23 (391) – С. 14.

Розголошення такої інформації може завдати збитків підприємству. Тому важливо визначити всі основні канали витоку, виділити найбільш небезпечні і адекватно застосовувати відповідні заходи захисту.

У сучасних умовах діяльністю щодо отримання відомостей, які становлять комерційну таємницю підприємства, можуть займатися: державні та приватні підприємства, банки, вітчизняні фірми-конкуренти, аудиторські та консалтингові компанії, підрозділи безпеки інших підприємств та інші особи. Найбільш негативна ситуація для підприємства складається у випадках, коли до витоку інформації причетні його співробітники. Це пов'язано з тим, що співробітник може викрадати службові документи, знімати з них невраховані копії, здобувати зразки нової продукції, а інколи навіть і встановлювати різного роду технічні пристрої для отримання конфіденційної інформації.

Висновки до 3-го розділу

1. З метою забезпечення економічної безпеки підприємства запропоновано до складу принципів організації бухгалтерського обліку включити наступні принципи: безпеки та контролю бухгалтерських даних, комплексності, ешелонування. Застосування даних принципів значною мірою сприятиме впровадженню комплексної системи заходів організації бухгалтерського обліку, метою якого буде посилення функції збереження власності та забезпечення безперервності діяльності підприємства.

2. Економічна політика підприємства, робота бухгалтерської служби, організація та техніка ведення бухгалтерського обліку, а також організація внутрішнього контролю є важливими складовими розробленої комплексної системи заходів щодо організації бухгалтерського обліку. Це пояснюється тим, що застосування всіх складових комплексної системи заходів організації бухгалтерського обліку забезпечує виконання бухгалтерським обліком в майбутньому його основних завдань та функцій. Необхідність впровадження комплексної системи заходів організації бухгалтерського обліку пов'язана з потребою підвищити відповідальність облікового персоналу на вимогу внутрішніх розпорядчих документів, які передбачають захист бухгалтерської інформації, що становить комерційну таємницю підприємства.

Дотримання вимог щодо захисту облікової інформації підприємства гарантує його стабільне максимально ефективне функціонування та високий потенціал розвитку в майбутньому.

РОЗДІЛ 4
РОЗВИТОК ОРГАНІЗАЦІЇ БУХГАЛТЕРСЬКОГО ОБЛІКУ В УМОВАХ ЗАСТОСУВАННЯ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

4.1. Модель організації бухгалтерського обліку в умовах застосування комп'ютерних технологій у забезпеченні економічної безпеки підприємств

В Україні, як і в інших країнах світу, в процесі підприємницької діяльності, при створенні нових технологій, в результаті інтелектуальної праці, виникають нові, насичені найрізноманітнішими відомостями інформаційні об'єкти, що мають комерційну цінність. Це можуть бути методики робіт, перспективні технічні рішення, результати маркетингових досліджень тощо, націлені на досягнення підприємницького успіху. Обмін інформацією охоплює всі сфери діяльності суспільства. В сучасних умовах інформація стає одним з найважливіших чинників розвитку ринкової економіки, найважливішою умовою формування інформаційної інфраструктури держави, продуктом взаємного обміну між державами, підприємствами, фізичними особами тощо [156, с. 45].

Інформація, інформаційні системи, інформаційна взаємодія, інформаційне середовище є сферою інтересів вчених, фахівців в сфері економіки, політики та техніки, відповідних державних служб, керівників компаній. Вивчення різних аспектів інформації проводиться за різними напрямами та пов'язане, передусім, з вирішенням завдань побудови єдиного інформаційного простору.

Як зазначає П. Чеботар, інформація компанії – це вся інформація, яка зберігається та підлягає обробці в компанії. Інформація може зберігатися в електронних сховищах, в архівах на фізичних носіях та у головах співробітників компанії. Інформаційна система включає в себе засоби зберігання, обробки та передачі інформації компанії [157, с. 52].

---

156 Дикий А.П. Значение коммерческой тайны при формировании экономической безопасности предприятия // Securitatea informationala 2006 / Conferinta internationala (editia a III-a) 14-15 aprrilie 2006. Editura ASEM – Chisinau, 2006. – 54 s. – S. 16-18

157 Чеботарь П. Концепция построения АИС на основе конфликта интересов: Conferinta internationala (editia a III-a) 14-15 aprrilie 2006 [Securitatea informationala 2006]. – Editura ASEM Chisinau 2006. – S. 52-54.

В умовах глобалізації інформаційних процесів захист інформації від несанкціонованого доступу, який викликає викривлення інформації та завдає тим самим відчутних збитків державі, її структурам, підприємствам та громадянам, є на сьогодні однією із складових національної та інформаційної безпеки в цілому.

У Законі України "Про електронні документи та електронний документообіг" [158] визначено основні організаційно-правові засади електронного документообороту та використання електронних документів. "Електронний документ може бути створений, переданий, збережений та переведений електронними засобами у візуальну форму. Електронний документообіг є сукупністю процесів із створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів".

Використання електронного документообороту має ряд переваг над звичайною формою документообороту. Основні переваги наведено на рис. 4.1.

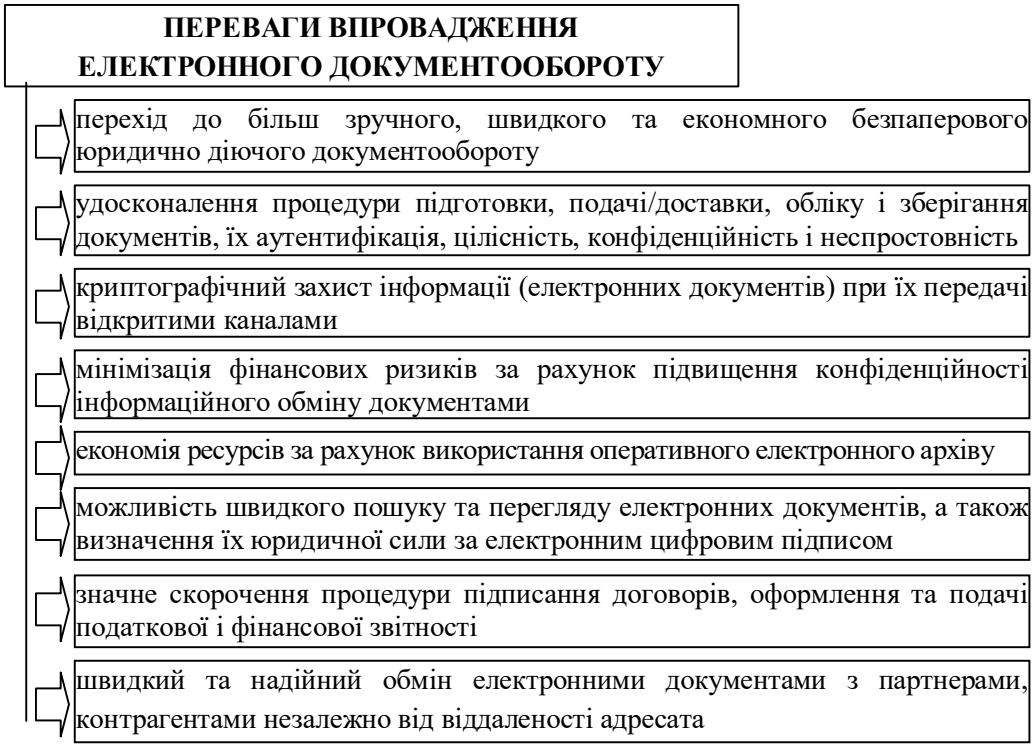


Рис. 4.1. Переваги електронного документообороту

При використанні на підприємстві системи електронного документообороту повинні вирішуватися основні завдання, наведені на рис. 4.2.

158 Закон України "Про електронні документи та електронний документообіг" № 851-IV від 22.05.2003 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=851-15.

ЗАВДАННЯ,
які вирішуються при використанні електронного документообороту

- автоматизація роботи спеціалістів за визначеним регламентом обробки документів, пошук та відбір необхідної інформації, розсилка опрацьованих документів для подальшої обробки
- уніфікація технологічних процедур проходження, передачі та опрацювання документів, збирання, реєстрація, накопичення, обробка та аналіз інформації, що надходить до кожного з вузлів, забезпечення постійного зв'язку та обміну інформацією між вузлами
- автоматизація функцій управління процесами на основі повідомлень спеціалістів про надходження документів для обробки, про закінчення нормативних строків обробки, синхронізація робіт спеціалістів
- автоматизація контролю виконання документів на основі оперативного відображення поточного стану процесів діловодства, відхилень від планових строків, визначення нових термінів завершення робіт та "критичних шляхів" в маршрутних схемах, заповнення переліків виконавців, ознак документів тощо
- автоматизація процесів реєстрації документів, заповнення кодованих реквізитів реєстраційних та контрольних карток з використанням класифікаторів і довідників, забезпечення механізмів анотованого опису документів та збору резолюцій, доставка звітів про виконання доручень
- автоматизація збирання даних про результати виконання технологічних процесів та формування на їх основі аналітичних і статистичних звітів та довідок щодо документообігу та контролю за виконанням документів, формування довільних аналітичних довідок
- розсилка, зберігання та використання вхідних, вихідних і внутрішніх документів за єдиною нумерацією з початку року
- відправлення, приймання та опрацювання електронної пошти
- оперативний пошук інформації про вхідні, вихідні та внутрішньо-розпорядчі документи за комбінацією умов з будь-яких реквізитів реєстраційних карток або за контекстом документа
- наскрізний контроль (група контролю, керівник установи, безпосередній виконавець) за проходженням і виконанням документів
- ведення, системи класифікаторів та довідників
- постійне оновлення та адміністрування головної бази даних, забезпечення достовірності, можливість оперативного доступу та збереження інформаційного фонду
- забезпечення надійного зберігання всіх версій документів та інших інформаційних об'єктів, максимально зручна систематизація сховища документів
- організація служб копіювання-відновлення інформації, що зберігається, забезпечення її захисту від несанкціонованого доступу
- формалізація технологічних процесів обробки інформації, визначення типових маршрутних технологічних схем для їх виконання
- визначення кола осіб, що за посадовими обов'язками здійснюють підготовку та обробку документів та призначення рівнів їх доступу до інформації, повноважень та прав
- підготовка друкованих належним чином ілюстрованих зведень, аналітичних довідок тощо, друкування реєстраційних карток, журналів реєстрації, реєстрів розсилки, статистичних та аналітичних довідок про стан виконання документів та документообороту

Рис. 4.2. Основні завдання, які вирішуються при використанні електронного документообороту

Про необхідність захисту інформації в комп'ютерному середовищі та про серйозність цього питання говорить в своїй праці В.Н. Носевич [159,с. 140]. Автор наголошує, що наш час характеризується стрімким розвитком інформаційних технологій. Все більша частина інформації переводиться з паперових на електронні носії або одразу створюється в цифровій формі, не маючи паперових аналогів. Але, на жаль, досвід історії не раз показував, що прогрес не приводить до усунення проблем: він просто заміняє одні процеси іншими. Повною мірою це відноситься й до новітніх комп'ютерних технологій. З їх впровадженням виникають не лише нові перспективи, але й нові перепони, додаткові джерела потенційного ризику.

З'являються нові можливості для несанкціонованого доступу до конфіденційної інформації, а також ймовірність втрати великих масивів цінної інформації через відмову обладнання, вірусні атаки або некваліфіковані дії користувача. Перспективи довгострокової доступності інформації в цифровій формі, поки що досить нечіткі, тобто існує потенційна загроза втратити всю таку інформацію, накопичену протягом десятиліть.

Як зазначає Н.В. Пошерстник, автоматизація бухгалтерського обліку є об'єктивною необхідністю. Далі автор продовжує, що робота бухгалтера все більше стає творчою, і впровадження комп'ютерних технологій підвищує ефективність, беручи на себе, окрім всього іншого, всю рутинну роботу. Але автоматизація викликає необхідність побудови технології вирішення бухгалтерських завдань з урахуванням ряду наступних питань:

– обмеження доступу до первинної та систематизованої інформації шляхом введення паролів (ключів секретності) та недопущення несанкціонованого доступу;

– збереження облікової інформації на необхідний термін;

– діалогового режиму роботи користувачів з засобами обчислювальної техніки [160, с. 99-100].

Як стверджує А. Лукацький, інформаційна безпека є одним із найважливіших завдань будь-якого підприємства, але до того ж і одним із самих незрозумілих, "неринкових" та не рекламованих [161, с. 65-72].

---

159 Носевич В.Н. Электронные документы и меры по обеспечению их сохранности (Опыт Республики Беларусь) // Электронный документ и документооборот: Правовые аспекты: Сб. науч. тр. / РАН. ИНИОН. Центр социальных науч.-информ. исслед. Отдел правоведения; РАН. ИГП. Центр публичного права. Сектор информационного права; Отв. ред. – Алферова Е.В., Бачило И.Л. – М., 2003. – 2008 с.

160 Пошерстник Н.В. Бухгалтерский учет на современном предприятии: [учеб.-практ. пособие] / Н.В. Пошерстник. – М.: ТК Велби, изд-во Проспект, 2006. – 552 с.

161 Лукацкий А. Как связать безопасность компании с ее бизнесом / А. Лукацкий // Корпоративные системы. – 2008. – № 1. – С. 65-72.

Розголошення конфіденційної інформації може досить дорого коштувати підприємству [162]. Згідно спільного дослідження ФБР та Інституту комп'ютерної безпеки (див. "CSI/FBI Computer Crime Security Survey 2005"), в якому взяли участь 700 представників американського бізнесу, середній збиток кожній компанії, яка зареєструвала крадіжку конфіденційних даних в 2005 році, склав 355,5 тис. доларів. Звичайно, не є фактом те, що абсолютно всі компанії стикаються з крадіжками конфіденційних даних щорічно. Тим не менше, на широке розповсюдження внутрішніх загроз IT-безпеці зазначають одразу декілька авторитетних досліджень. Так, наприклад, організація CERT (див. "2005 E-Crime Watch Survey"), яка провела опитування більше 800 компаній, з'ясувала, що кожна друга компанія хоча б раз протягом року постраждала від витоку суттєвих відомостей. Також за даними PricewaterhouseCoopers и CXO Media (див. "Global State of Information Security 2005"), які опитали більше 13 тис. компаній в 63 країнах світу (в тому числі й Росії та Україні), підраховано, що 33 % та 20 % інцидентів розголошення комерційної таємниці викликані теперішніми та колишніми співробітниками відповідно, 11 % приходиться на частку клієнтів компанії, 8 % відбуваються з вини партнерів, 7 % зумовлені тимчасовими працівниками (рис. 4.3).

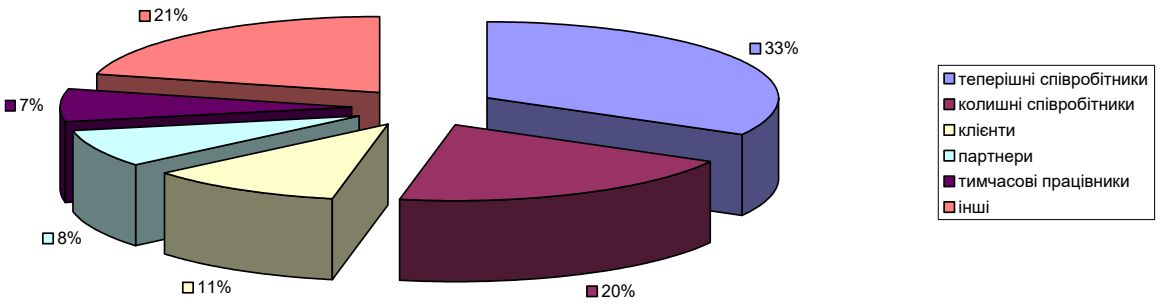


Рис. 4.3. Шляхи розголошення бухгалтерської інформації, що містить комерційну таємницю

Якщо не враховувати клієнтів та партнерів, то за 60 % усіх інцидентів несуть відповідальність колишні, теперішні та тимчасові співробітники компанії, що з урахуванням середньорічного збитку кожній організації (355 тис. доларів) піднімає проблему внутрішньої інформаційної безпеки на перше місце у списку пріоритетів керівництва компанії.

[162] 12 самых громких случаев ИТ-воровства в России: [Електронний ресурс]. – Режим доступу: http://www.cnews.ru/reviews/?2005/12/02/192675.

Вищенаведене підтверджує те, що ситуації, пов'язані з витоком конфіденційної інформації, можуть створювати співробітники підприємства, які в силу своїх обов'язків мають до неї доступ.

Одним з компонентів економічного інформаційного простору виступає бухгалтерська інформація. Вона може розглядатися як невід'ємний елемент не лише економічного інформаційного простору, але і єдиного інформаційного простору. Бухгалтерська інформація, взаємодіючи з іншими частинами єдиного інформаційного простору, поступово розширює межі своєї присутності в єдиному інформаційному просторі.

Поняття інформаційної безпеки є дещо ширшим, ніж комп'ютерна безпека. Інформаційна безпека бухгалтерських даних – це стан захищеності інформаційного середовища підприємства, що забезпечує його формування, використання та розвиток з метою отримання прибутку.

Захист інформації є першою життєвою необхідністю будь-якої системи, що не може не зацікавити керівників, які розуміють цінність комерційної таємниці підприємств. Занепокоєння відносно захисту облікових даних або збереження комерційної таємниці стало досить актуальним питанням для бізнесу, а ринок систем і засобів переповнений пропозиціями різних технічних рішень.

В якості стандартної моделі інформаційної безпеки підприємства часто наводять так звану "модель CIA" (рис. 4.4).

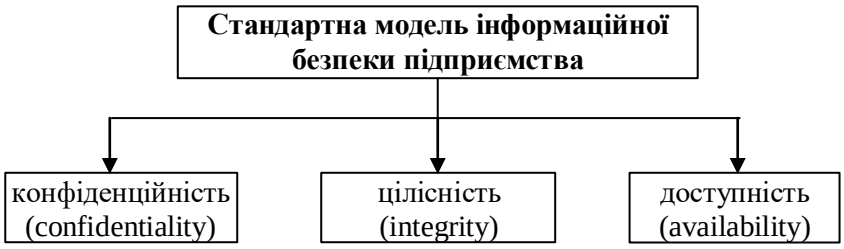


Рис. 4.4. Стандартна модель інформаційної безпеки облікових даних підприємства

Під конфіденційністю розуміється доступність бухгалтерської інформації лише певному колу осіб, під цілісністю – гарантія існування бухгалтерської інформації в початковому вигляді, під доступністю – можливість отримання бухгалтерської інформації в комп'ютерному середовищі авторизованим користувачем в потрібний для нього час.

Також до складу складових стандартної моделі інформаційної безпеки облікових даних підприємства можна додати наступні категорії:

– аутентичність – можливість встановлення власника (автора) бухгалтерської інформації;

– апельованість – можливість довести, що автором є саме заявлена особа, і ніхто інший.

Для будь-якого підприємства при побудові системи безпеки облікових даних необхідно розробити концепцію забезпечення інформаційної безпеки, в якій на основі аналізу сучасного рівня та динаміки розвитку інформаційних технологій розглядається систематизоване викладення цілей, завдань та принципів досягнення потрібного рівня безпеки інформації.

Якщо ж на підприємстві існує система безпеки облікової інформації, то з часом настає необхідність її подальшого розвитку та модернізації, тому що з розвитком новітніх технологій також розвиваються й засоби та методи спрямовані на отримання таємної інформації.

В зв'язку з цим, для підприємств особливо актуальним є питання відносно того, хто повинен виконувати функції зі збору, обробки та аналізу даних для забезпечення захисту та накопичення пропозицій відносно впровадження систем безпеки.

Економічний інформаційний простір підприємства включає інформаційні ресурси, що містять дані, знання, зафіксовані на відповідних носіях інформації. Інфраструктуру економічного інформаційного простору складають відповідні організаційні структури, що забезпечують збір, обробку, зберігання, розповсюдження і передачу інформації; засоби інформаційної взаємодії, які регламентують доступ до інформації та базуються на діючих інформаційних технологіях.

Інформаційна система створюється для певного об'єкта, в даному випадку – для підприємства та його бухгалтерії. Ефективна інформаційна система враховує різницю між ланками управління, сферами дій, а також зовнішніми обставинами та надає будь-якій ланці управління лише таку інформацію, яка необхідна їй для ефективної реалізації функцій управління.

Великі обсяги та динамічність облікової інформації об'єктивно обумовлює необхідність використання для її обробки нових інформаційних технологій. Виходячи з того, що значна частина облікової інформації формується в межах бухгалтерського обліку, важливо здійснювати комп'ютеризацію облікового

процесу. Для цього використовується сучасна комп'ютерна техніка, засоби комунікацій та спеціалізоване програмне забезпечення.

Питанню забезпечення захисту облікової інформації в інформаційному середовищі надається все більше значення, оскільки інформація стає важливим ресурсом будь-якого підприємства. Автоматизована обробка обліково-аналітичної інформації своєчасно забезпечує керівництво підприємства достовірними відомостями про використовування матеріальних, трудових і грошових ресурсів, про фактичну собівартість і фінансових результатах. На підставі цих даних здійснюється економічний аналіз господарської діяльності підприємства та приймаються оптимальні управлінські рішення. У зв'язку з цим значно зростають вимоги до збереження і захисту обліково-аналітичної інформації, одержуваної за допомогою використання новітніх комп'ютерних технологій. Проте поширення інформаційних технологій має і негативний аспект, який відкриває шлях до так званої злочинної поведінки. Комп'ютерні системи містять у собі нові, досить досконалі можливості для вчинення невідомих раніше порушень щодо несанкціонованого доступу до конфіденційної інформації та безперешкодного заволодіння цією інформацією.

Окрім злочинів, які здійснюються з використанням новітніх комп'ютерних технологій, що завдають великих економічних збитків, суспільство стає все більш залежним від роботи комп'ютерних інформаційних систем у різноманітних галузях людської діяльності починаючи від управління підприємствами і закінчуючи розробкою національної безпеки держави. Іноді навіть незначний збій у функціонуванні таких систем може призвести до реальної загрози несанкціонованого витоку конфіденційної інформації підприємства. Крім того, стрімке зростання глобальних комп'ютерних та телекомунікаційних мереж, а також можливість підключення до них через звичайні телефонні лінії посилюють можливості їх використання для здійснення несанкціонованого доступу до інформації, яка має обмежений доступ.

У такому випадку необхідно здійснювати заходи, що сприяють збереженню інформації в комп'ютерній інформаційній системі. Під безпекою автоматизованої інформаційної системи необхідно розуміти її захищеність від випадкового і навмисного втручання в нормальний процес її функціонування, а також від спроб руйнування або модифікації її компонент.

Не виникає сумнівів, що найбільше від комп'ютерних злочинів потерпають розвинуті у технічному відношенні країни, однак і в інших країнах, з початком процесу комп'ютеризації створюються сприятливі умови для здійснення таких злочинів. Зокрема, глобальна комп'ютерна мережа Internet надає можливість увійти до будь-якої світової відомчої комп'ютерної системи. Крім того, це можна зробити майже з будь-якої точки світу. Інформаційна безпека українських підприємств, на відміну від розвинених країн, поки що значно менше залежить від комп'ютерних мереж: комп'ютерних злочинів в основному зазнає у нас фінансово-кредитна сфера.

Сідней Дж. Грей та Белверд Е. Нідлз наголошують на тому, що при сучасному широкому розповсюдженні комп'ютерів багато інформаційних потреб бізнесу систематизуються в управлінські інформаційні системи. Управлінська інформаційна система складається з взаємопов'язаних підсистем, які надають інформацію, необхідну для ведення бізнесу. Бухгалтерська інформаційна система є найважливішою підсистемою, тому що вона відіграє провідну роль в управлінні потоком економічної інформації у всі підрозділи бізнесу, а також зацікавленим особам поза бізнесом [[163], с. 6].

В сучасних умовах ефективно сконструйована система захисту облікової інформації підприємства забороняє несанкціонований доступ користувачів, які не мають певних прав на входження в інформаційну систему підприємства, до конфіденційної інформації. Досягнення такої мети дозволяє забезпечити підприємству збереження комерційної таємниці, що в свою чергу сприяє стабілізації фінансового стану підприємства.

Облікова інформація містить усі відомості про господарську діяльність суб'єкта господарювання, і тому досить часто привертає увагу конкурентів. Проте програмне забезпечення бухгалтерського обліку, яке сьогодні існує на ринку, має різноманітні можливості щодо забезпечення захисту даних. У програмах "Финансы без проблем" та "Инфин-бухгалтерия" взагалі відсутня система розмежування прав доступу. У програмах "Парус-Предприятие", "1С: Предприятие" така система має вигляд розмежування прав доступу за ділянками обліку для певних осіб, які мають свої паролі. Це дозволяє захистити інформаційну базу від несанкціонованого доступу до інформації, та зберегти її від незаконного використання персоналом, що має відношення

[163] Грэй, Сидней Дж. Финансовый учет: Глобальный подход: [учеб.-метод. пособие: пер. с англ] / Сидней Дж. Грэй, Белверд Е. Нидлз. – М.: Волтерс Клувер, 2006. – 614 с.

до роботи бухгалтерської служби. Проте самі файли інформаційних баз часто незахищені і їх може використати будь-яка особа з мінімальними знаннями у сфері інформаційних технологій.

На великих підприємствах із розвинутими комп'ютерними інформаційними системами повинні бути власні внутрішні стандарти з організації безпеки та захисту бухгалтерської інформації, яка міститься в комп'ютерному середовищі. Загалом у таких документах повинні міститись вимоги до внутрішніх розпорядчих документів, до систем розподілу прав доступу, до процедури шифрування даних, а також до інструментів забезпечення фізичного захисту складових інформаційної системи. Крім того, стандарт має охоплювати вимоги із забезпечення безперервності захисту, вимоги до порядку і періодичності перегляду прав доступу користувачів інформаційної системи.

Завдання організації забезпечення безпеки та захисту даних в бухгалтерській службі підприємства передбачає виконання комплексу технічно-організаційних, режимних заходів та роботи з персоналом, спрямованих на захист комерційної таємниці і відповідного контролю за роботою працівників бухгалтерської служби. На підприємстві необхідно розробити модель організації бухгалтерського обліку в умовах використання комп'ютерної системи бухгалтерського обліку з метою забезпечення економічної безпеки підприємства (рис. 4.5).

Нами розроблено та впроваджено в діяльність Дочірнього підприємства "Молочний завод" Товариства з обмеженою відповідальністю "Молочна фабрика "Рейнфорд" модель організації бухгалтерського обліку в умовах використання КСБО з метою забезпечення економічної безпеки підприємства.

Для запобігання несанкціонованого доступу до бухгалтерської інформації, що зберігається в комп'ютерній базі даних, кожен із співробітників підприємства повинен мати особистий код, що дозволяє користуватися лише тією інформацією, яка стосується його службових обов'язків. Наявність подібних кодів є досить надійним захистом бухгалтерської інформації від осіб, які прагнуть отримати дані, що становлять комерційну таємницю підприємства.

Будь-яке підприємство має різноманітні технічні засоби, призначені для прийому, передачі, обробки та зберігання бухгалтерської інформації. В процесі обробки бухгалтерської інформації за допомогою технічних засобів можуть виникати технічні канали витоку інформації.

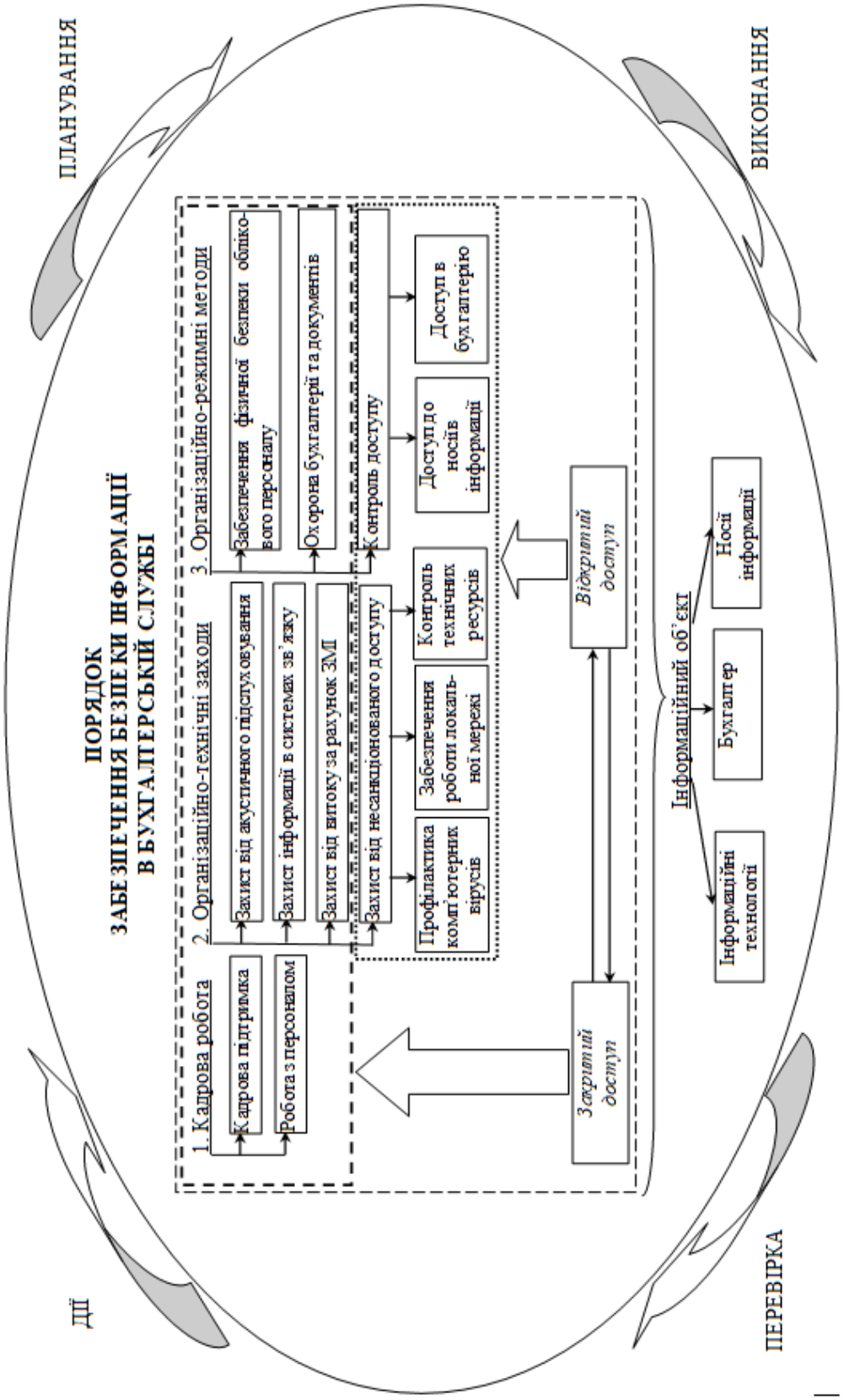


Рис. 4.5. Модель організації бухгалтерського обліку в умовах використання КСБО з метою забезпечення економічної безпеки підприємства

Технічні канали витоку бухгалтерської інформації, що зберігається в комп'ютерних базах даних, поділяються на:

– радіоканали (електромагнітні випромінювання радіодіапазону);

– акустичні (розповсюдження звукових коливань в будь-якому звукопровідному матеріалі);

– оптичні (електромагнітні випромінювання у видимій, інфрачервоній і ультрафіолетовій частинах спектру).

Якщо персональна ЕОМ використовується лише одним користувачем, то важливо, по-перше, попередити несанкціонований доступ до комп'ютера інших осіб в той час, коли в ньому міститься бухгалтерська інформація, що потребує захисту, та, по-друге, забезпечити захист даних на зовнішніх носіях від витоку. Якщо ж персональна ЕОМ використовується групою осіб, то, окрім вказаних моментів захисту бухгалтерської інформації, може виникнути необхідність запобігти несанкціонованому доступу цих користувачів до інформації один одного.

Крім того, у всіх випадках необхідно захищати бухгалтерську інформацію від псування унаслідок помилок програм та обладнання, зараження комп'ютерними вірусами. Однак, проведення перестрахувальних заходів є обов'язковим для всіх без винятку користувачів ЕОМ та не відноситься лише безпосередньо до проблеми захисту бухгалтерської інформації від конкурентів.

Для забезпечення безпеки бухгалтерської інформації в комп'ютерному середовищі використовуються наступні методи:

– засоби захисту обчислювальних ресурсів, що використовують парольну ідентифікацію, та що обмежують доступ несанкціонованого користувача;

– застосування різних шифрів, які не залежать від контексту інформації.

У персональних ЕОМ важливим також є захист вбудованих накопичувачів. Існують декілька типів програмних засобів, за допомогою яких можна вирішувати ці завдання:

– захист диска від запису та читання;

– контроль за зверненнями до диска;

– засоби видалення залишків секретної інформації.

Як зазначає Г.В Бєлов, у зв'язку із становленням та розвитком ринкових відносин виникає необхідність законодавчого регулювання інформаційних відносин, зокрема, пов'язаних з охороною результатів науково-технічної діяльності, що можуть містити предмети, які охороняються авторським правом, ноу-хау або складати державну чи комерційну таємницю. Організація заходів з їх захисту є необхідною умовою формування у суспільстві традицій добросовісної конкуренції та правового простору сприятливого для розвитку творчої діяльності у всіх сферах соціально-економічного життя [[164], с. 122].

Захист облікової інформації на підприємстві може проходити два етапи. Першим етапом є підбір надійного персоналу. На другому етапі визначаються та розподіляються права доступу користувачів та правила поведінки з конфіденційною інформацією.

Для обмеження доступу користувачів до різного роду конфіденційної інформації підприємства, можна застосовувати засоби, які спрямовані на зазначення обов'язкового місцезнаходження певного працівника в певний проміжок часу на підприємстві. Тобто, з метою уникнення випадкового або навмисного розголошення конфіденційної інформації, яке може виникнути у випадку, коли один із співробітників, проходячи за спиною у свого колеги, мав можливість заглянути у його файли, бачити які йому не потрібно.

Заходи щодо захисту облікової інформації повинні структурувати та максимально формалізувати відносини між підрозділами, документальні потоки між ними, правила спілкування відділів, правила передачі інформації між ними. Таким чином, основне завдання захисту облікової інформації полягає у необхідності визначення:

– обмеженого кола осіб, які мають доступ до певного виду як електронної, так і інформації на паперових носіях;

– осіб, які мають право доступу до цієї інформації;

– місця зберігання цієї інформації;

– правил поведінки з конфіденційними документами.

[164] Белов В.Г. Правовые аспекты оборота непубликуемой научно-технической информации // Электронный документ и документооборот: Правовые аспекты: Сб. науч. тр. / РАН. ИНИОН. Центр социальных науч.-информ. исслед. Отдел правоведения; РАН. ИГП. Центр публичного права. Сектор информационного права; Отв. ред. – Алферова Е.В., Бачило И.Л. – М., 2003. – 208 с.

До структурованої таким чином системи вже не складно застосувати захисні механізми.

Найважливішою організаційною формою представлення бухгалтерської інформації є документ. З появою та розвитком електронно-обчислювальної техніки, комп'ютерів та інформаційних цифрових технологій з'явилася нова група документів – електронні цифрові документи.

Масове впровадження сучасних інформаційних та телекомунікаційних технологій, розширення економічних зв'язків як всередині країни, так і за її межами, що здійснюється шляхом дистанційного обміну електронними документами (в тому числі і за допомогою мережі Інтернет), загострило необхідність правового вирішення питань, пов'язаних з легалізацією облікових документів. В основу такої легалізації спочатку було закладено загальний принцип, згідно з яким інформація, що міститься в електронних документах, може прирівнюватися до паперової форми, якщо вона є доступною для її сприйняття та придатною для використання в цивільному обігу. В якості аналогу власноручного підпису застосовується електронно-цифровий підпис.

Одним із надійніших методів захисту бухгалтерської інформації, що міститься в комп'ютерному середовищі, є, безумовно, шифрування, оскільки в цьому випадку охороняється безпосередньо сама інформація, а не доступ до неї. Таким чином, зашифрований файл не можна прочитати навіть у разі його викрадення разом з носієм інформації. Більшість засобів захисту реалізуються у вигляді програм або пакетів програм, що розширюють можливості стандартних операційних систем, а також систем керування базами даних.

Існує безліч альтернативних методів шифрування даних, в більшості випадків вони мають наступний принцип дії (рис. 4.6).

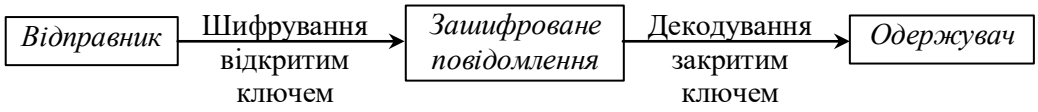


Рис. 4.6. Принцип дії шифрування даних

Щоб відправляти та отримувати повідомлення, кореспонденти спочатку створюють окремі пари закритих і відкритих ключів. Відкритий ключ зберігається в комп'ютерній директорії, а секретний – в максимально захищеному місці. Відправник зашифровує повідомлення за допомогою відкритого ключа одержувача. Одержавши лист, отримувач використовує свій закритий ключ для його декодування. Окрім нього, цей ключ нікому не відомий, тому можна бути упевненим, що листування залишиться в таємниці.

Кодування дає можливість захистити бухгалтерські дані, які становлять комерційну таємницю та вирішує проблеми з достовірністю і цілісністю повідомлень. Аутентифікація дозволяє переконатися одному з учасників операції в достовірності інших партнерів. В звичайній господарській діяльності з цією метою використовується власний підпис. Перевірка цілісності повідомлення визначає, чи не піддалося воно в процесі передачі змінам та чи повністю дійшло.

Одним з таких напрямів є поява об'єктивної необхідності в надійному захисті бухгалтерської інформації, яка оброблюється за допомогою засобів обчислювальної техніки, від її навмисного викривлення, витоку, підробки та інших неправомірних дій, що викликають втрату одного із показників юридичної значущості облікових документів, – достовірності документів, які містять цю інформацію.

Електронний цифровий підпис може використовуватися юридичними і фізичними особами як аналог власноручного підпису для надання електронним бухгалтерським документам юридичної сили. Юридична сила електронного документа, підписаного за допомогою електронного цифрового підпису, є еквівалентною юридичній силі документа на паперовому носії, підписаного власноручним підписом певної особи та скріпленого печаткою.

З метою підвищення і удосконалення рівня послуг, а також міжнародного визнання цифрового підпису, законом передбачені механізми добровільної акредитації центрів сертифікації ключів, а також створення системи, яка здійснює процедуру акредитації і нагляд за роботою акредитованих центрів сертифікації ключів.

Електронний цифровий підпис є функціонально аналогічним звичайному рукописному підпису на папері і володіє всіма його основними перевагами:

– засвідчує те, що отриманий документ надійшов від особи, яка його підписала;

– гарантує цілісність та захист від викривлення, виправлення підписаного документа;

– не дає можливості особі, яка підписала документ, відмовитися від зобов'язань, що виникли в результаті підписання цього електронного документа.

Електронний цифровий підпис, як аналог власноручного підпису, має цілий ряд переваг, обумовлених його електронною природою (рис. 4.7).

Застосування електронного цифрового підпису дозволяє значно скоротити час руху бухгалтерських документів в процесі оформлення звітів та обміну документацією. Документи, підписані при використанні електронного цифрового підпису, передаються через Інтернет або локальну мережу за декілька секунд. Всі учасники електронного обміну документами отримують рівні можливості, незалежно від їх віддаленості між собою.

Відповідно до Закону України "Про електронний цифровий підпис" від 22.05.2003 р. [165] та Закону України "Про електронні документи та електронний документообіг" від 22.05.2003 р. [166] електронний цифровий підпис використовується для подання всіх видів електронної звітності, а саме:

– до Державної податкової інспекції;

– до Пенсійного фонду України;

– до Державного комітету фінансового моніторингу України;

– інформаційного обміну з ТОВ "Перше всеукраїнське бюро кредитних історій";

– митного електронного декларування.

[165] Закон України "Про електронний цифровий підпис" № 852-IV від 22.05.2003 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=852-15.

[166] Закон України "Про електронні документи та електронний документообіг" № 851-IV від 22.05.2003 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=851-15.

Рис. 4.7. Переваги електронного цифрового підпису

Цифровий підпис надає користувачам можливість забезпечити достовірність та цілісність електронного документа, а також засвідчити авторство власника, який завіряє таким способом документ. Сьогодні існує достатня кількість програмних продуктів, реалізованих у вигляді доповнень до стандартних програм. Ці програми надають весь спектр послуг з використання цифрового підпису. При цьому процедури накладення і перевірки підпису абсолютно зрозумілі для пересічних користувачів і, як правило, не викликають жодних труднощів, хоча переважній більшості з них незнайомий механізм електронного цифрового підпису. Іншими словами, можна з впевненістю заявити, що рівень розвитку суспільства впритул підійшов до необхідності використання в електронному документообороті цифрового підпису як способу посвідчення достовірності та автентичності електронних даних.

Для бухгалтерської служби підписання документів за допомогою електронного цифрового підпису дозволить спростити оформлення фінансових документів, рахунків та платіжних доручень, спростити візування документів, забезпечити швидкість та зручність обміну документами, а також спростити роботу при передачі звітів до контролюючих органів. Це пов'язано з тим, що з електронним цифровим підписом працюють Державна податкова інспекція, Пенсійний фонд, Управління статистики, Фонд загальнообов'язкового державного соціального страхування на випадок безробіття, Фонд соціального страхування від нещасних випадків на виробництві та професійних захворювань, Фонд соціального страхування на випадок тимчасової втрати працездатності. Нами в роботі розроблено схему електронного документообороту з використанням електронного цифрового підпису, що дозволило забезпечити захист бухгалтерської інформації від негативного впливу внутрішніх і зовнішніх загроз (рис. 4.8).

Специфіка використання комп'ютерної техніки передбачає особливі методи забезпечення захисту облікової інформації.

Як зазначають С.М. Бичкова та С.В. Івахненков, обчислювальна техніка суттєво підвищує якість обробки облікової інформації. При цьому застосування комп'ютерів змінює зміст та організацію роботи облікового персоналу: зменшується кількість ручних операцій з обробки первинних документів, систематизації облікових показників, заповненню регістрів та звітних форм. Облікова робота стає творчою, спрямованою на організацію та удосконалення обліку [[167], с. 3].

[167] Бычкова С.М. Информационные технологии в бухгалтерском учете и аудите: [учеб. пособие] / С.М. Бычкова, С.В. Ивахненков / Под ред. С.М. Бычковой. – М.: ТК Велби, Изд-во Проспект, 2005. – 216 с

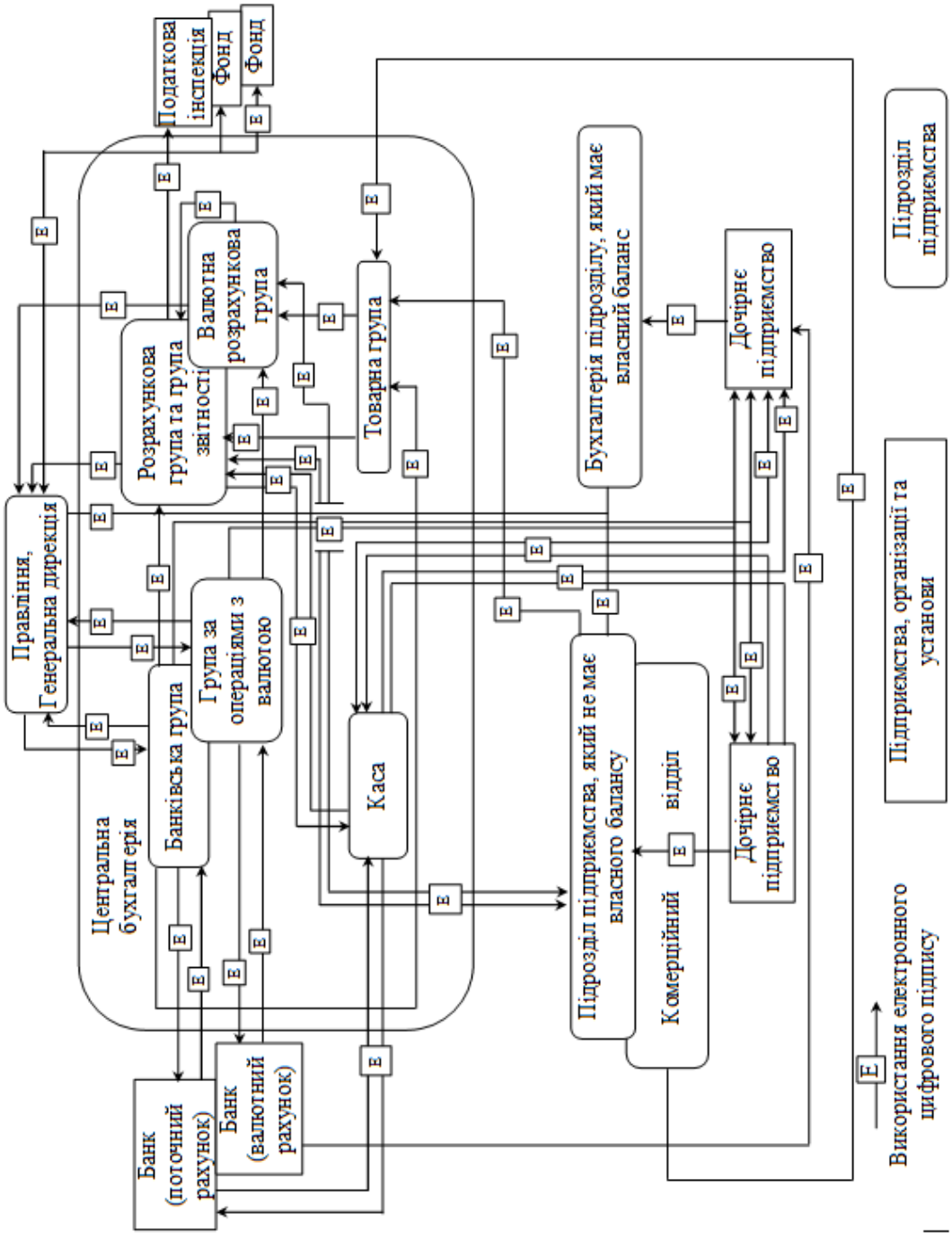


Рис. 4.8. Схема електронного документообороту підприємства

В процесі господарської діяльності або під час налагодження комп'ютерних систем частина облікової інформації стає доступною для сторонніх осіб. Тому слід за допомогою особливих внутрішніх положень (наказів, інструкцій) обмежити доступ сторонніх осіб до інформації, яка є комерційною таємницею підприємства, а також встановити або передбачити механізм перевірки звітної інформації, що виходить за межі підприємства. Наприклад, інформація з фінансової звітності, що оприлюднюється, не повинна містити зайвих деталей, які не передбачені законодавством або угодою з користувачами звітності. Необхідною є також кадрова робота з персоналом бухгалтерії. Вона полягає, з одного боку, в забезпеченні фізичної безпеки бухгалтерів, охороні приміщення та документів, роз'яснювальній роботі, а з іншого боку – у забезпеченні постійного нагляду за діями бухгалтерів суб'єктами внутрішнього контролю підприємства. Інформація, що накопичується підсистемою управлінського обліку, зазвичай, є основним об'єктом промислового шпигунства.

Служба безпеки підприємства повинна слідкувати за можливістю акустичного прослуховування приміщення бухгалтерії, відсутністю пристроїв підслуховування в комп'ютерах, комп'ютерних мережах, телефонах, копіювальній техніці тощо.

Особи, що працюють в адміністрації підприємства, можуть здійснювати викрадення інформації шляхом викривлення звітності підприємства, встановлення знижок на ціну товару, маніпуляцій з переоцінкою товарно-матеріальних цінностей та іншими діями.

Значною проблемою яка постає перед підприємством є забезпечення захисту облікової інформації, а також створення резервних копій електронних документів та створення паперових копій документів на випадок навмисного або випадкового пошкодження технічного та програмного забезпечення. Для вирішення даної проблеми необхідним є створення паралельних потоків інформації і збереження них на різних носіях накопичення даних. Архівні копії бази даних повинні зберігатися визначений час, який залежить від терміну використання даної інформації. Необхідно постійно зберігати декілька архівних копій бази даних за різні проміжки часу. У випадку появи нового архіву бази даних - перший архів знищується. Архівні копії бази даних зберігаються протягом одного звітного року та можуть використовуватися для відновлення інформації у разі виникнення такої потреби. Такі копії зазвичай зберігають на зовнішніх носіях накопичення інформації.

В даний час кожен власник повинен створити систему заходів безпеки, яка б сприяла виявленню ознак можливих правопорушень та злочинних дій на різних стадіях, на етапі формування злого наміру та розробки планів злочинних дій, що дозволило б вчасно попередити та знешкодити злочинні наміри. Це означає, що захист інформації на підприємстві, в тому числі й облікової, повинен бути на першому місці. В свою чергу, це змушує учасників ринку створювати більш вдосконалені засоби забезпечення обліково-інформаційної безпеки, доповнювати засоби фізичної безпеки більш цивілізованими різновидами, включаючи технічні та юридичні засоби.

Головним пріоритетом захисту конфіденційної інформації на підприємстві є розробка заходів, спрямованих на збереження комп'ютерної інформації. Це, передусім, пов'язано з тим, що в сучасних умовах господарювання використовується комп'ютерна форма обліку, яка передбачає застосування різних програмних продуктів для ведення бухгалтерського обліку. На більшості підприємств створюється єдина інформаційна система, до складу якої входять різні програми, які використовуються для здійснення управління підприємством, включаючи безпосередньо керівництво виробничим процесом, а також ведення бухгалтерського обліку. При створенні такої системи збільшується ризик витоку облікових даних по мережі, через те, що інформація може бути доступною не лише співробітникам одного структурного підрозділу підприємства, в даному випадку – бухгалтерії, але й співробітникам інших підрозділів, а в окремих випадках, якщо підприємство має доступ до регіональної або глобальної мережі – користувачам поза межами підприємства. Також при використанні комп'ютерних мереж виникає імовірність проникнення комп'ютерного вірусу або несанкціонованого доступу сторонньої особи, що може спричинити знищення інформації, що в свою чергу може призвести до зупинки виробництва та розвалу підприємства.

Інформаційні системи управління підприємством, серед яких ключове місце належить системі бухгалтерського обліку, повинні організовуватися таким чином, щоб забезпечувати стратегічне і тактичне планування діяльності та унеможливлювати вихід інформації не за призначенням, що і служить основою економічної безпеки підприємства.

Вимоги, які пред'являються користувачами до інформації, що формується в системі бухгалтерського обліку, постійно зростають. Розвиток економічних відносин, зростання інвестицій, глобалізація економіки, а також суттєві зміни в засобах комунікації змушують учасників економічних процесів віддавати перевагу достовірній та надійно захищеній інформації. У зв'язку з цим постає проблема захисту облікової інформації підприємства, як така, що потребує першочергового вирішення. Значущість даної проблеми підвищується тим, що інформаційний простір, який містить значні обсяги загальнодоступної інформації, є не лише джерелом даних для прийняття користувачами певних рішень, але й може бути джерелом для несанкціонованого розповсюдження конфіденційної інформації. Передусім захист облікової інформації повинен стати центральною ланкою економічної, а також важливою частиною й інформаційної безпеки, спрямованої на задоволення потреб користувачів інформації.

Важливим моментом інформаційної безпеки облікової інформації є те, що керівництво підприємства повинно забезпечити необхідний для підприємства ступінь захисту інформації, яка використовується при складанні різного роду звітності. Хоча ця проблема і виходить за межі бухгалтерського обліку, не слід забувати про те, що вона існує та вимагає адекватного вирішення. Бухгалтерська інформація є найціннішою інформацією, яка характеризує всі сторони діяльності підприємства, тому питання забезпечення інформаційної безпеки необхідно вирішувати ще на етапі її формування.

Також доцільним є формування інфраструктури сприйняття облікової інформації – системи організаційних форм структуризації відносин щодо формування, захисту, передачі та сприйняття облікової інформації. Необхідність формування розвиненої інфраструктури, спрямованої на пріоритетний розвиток та підвищення якості процесів сприйняття інформації викликана специфічними особливостями процесів сприйняття саме облікової інформації.

В умовах конкуренції економічна безпека бухгалтерської інформації набуває життєво важливого значення. На ВАТ "Житомирський маслозавод" нами розроблено та впроваджено ряд розробок (політику захисту

бухгалтерської інформації; порядок доступу до бухгалтерських даних, що становлять комерційну таємницю; схему робіт з певними відомостями, які знаходяться на різних носіях інформації; встановлено терміни, впродовж яких певні відомості є таємними; визначено категорії носіїв таємної та закритої інформації; визначено місце, час та форму збереження конфіденційної інформації), які визначають порядок роботи з обліковою інформацією, що становить комерційну таємницю підприємства в комп'ютерному середовищі. Інтенсивний розвиток комп'ютерних систем, які охопили всі види підприємницько-господарської діяльності, впровадження автоматизації документообороту, послідовий перехід до безпаперової технології, забезпечення безпечного ведення бізнесу з використанням інформаційних технологій зумовили нові підвищені вимоги до захисту облікової інформації, яка є найважливішою складовою економічної безпеки підприємства.

Слід зазначити, що побудова системи захисту облікової інформації в сучасних умовах є необхідною передумовою організації ефективної роботи підприємства.

Головною метою безпеки облікової інформації підприємства є гарантування його стабільного максимально ефективного функціонування та високий потенціал розвитку.

В сучасних умовах ефективно сконструйована система захисту облікової інформації підприємства забороняє несанкціонований доступ користувачів, які не мають певних прав на входження в інформаційну систему підприємства, до конфіденційної інформації. Досягнення такої мети дозволяє забезпечити підприємству збереження комерційної таємниці, що сприяє стабілізації фінансового стану підприємства.

Система, що проектується, повинна сприяти захисту інформації підприємства і забезпечувати надійність та безпеку інформації в системі. Якісна інформаційна система повинна виконувати наступні функції щодо безпеки даних: 1) поділ доступу до функцій і даних системи шляхом авторизації користувачів за паролем; 2) шифрування даних; 3) наявність контролю за входом до системи і ведення журналу робочого часу; 4) контроль за періодичністю створення резервних (архівних) копій інформації.

Майже в усіх підприємствах існують спеціальні підрозділи, які займаються захистом конфіденційної інформації від несанкціонованого доступу. Їх головним завданням є формування програми роботи в сфері інформаційної безпеки та забезпечення її виконання шляхом виділення необхідних ресурсів та постійного контролю стану справ.

Основними завданнями співробітників, які забезпечують інформаційну безпеку, є:

– розробка та впровадження політики інформаційної безпеки підприємства;

– проведення організаційних заходів для підтримки політики безпеки;

– застосування необхідних механізмів захисту (технічних засобів);

– модернізація системи інформаційної безпеки тощо.

Співробітники, які працюють у напрямі комп'ютерної безпеки, повинні володіти такими ж знаннями, як і системні адміністратори, тобто бути ознайомленим з операційними системами та різними прикладними продуктами, що використовуються на підприємстві повинні бути не гіршими, ніж у адміністратора мережі.

Основною програмою захисту інформації є багаторівнева політика безпеки, яка відображає підхід певного підприємства до захисту своїх інформаційних активів. Політика безпеки є сукупністю умов, за яких користувачі обчислювальної системи можуть отримати доступ до інформації та ресурсів, не порушуючи при цьому її цілісності та не сприяючи її витоку. Таким чином, політика безпеки визначає організаційно-технічні і програмно-апаратних вимоги, які повинні бути виконані при реалізації певної системи захисту інформації.

Політика безпеки включає правила та норми поведінки при обробці, захисті, а також розповсюдженні конфіденційної облікової інформації. Зокрема, правила визначають, в яких випадках користувач має право працювати з певними наборами даних. Від надійності комп'ютерної системи залежить суворість та різноманітність правила, які забезпечують політику безпеки.

4.2. Внутрішній контроль за дотриманням економічної безпеки з метою захисту бухгалтерської інформації на підприємстві

В даний час внутрішній контроль за дотриманням економічної безпеки підприємства є одним з найбільш актуальних напрямів стратегічного та оперативного менеджменту, що динамічно розвиваються, в галузі безпеки інформації. Його основне завдання – об'єктивно оцінити поточний стан економічної безпеки підприємства, а також її адекватність поставленим цілям та завданням бізнесу з метою збільшення ефективності і рентабельності економічної діяльності.

Під контролем економічної безпеки підприємства необхідно розуміти системний процес отримання об'єктивних, якісних та кількісних оцінок про поточний стан економічної безпеки підприємства відповідно до певних критеріїв і показників безпеки. Результати контролю безпеки дозволяють побудувати оптимальну з точки зору ефективності та витрат корпоративну систему захисту бухгалтерської інформації, адекватну поточним завданням та цілям підприємницької діяльності.

Важливим компонентом надійності системи є політика економічної безпеки бухгалтерської інформації на підприємстві. Вона включає правила та норми поведінки при обробці, захисті, а також розповсюдженні конфіденційної облікової інформації. Зокрема, правила визначають, в яких випадках користувач має право працювати з певними даними бухгалтерського обліку. Від надійності комп'ютерної системи залежить суворість та різноманітність правил, які забезпечують політику економічної безпеки.

Політика економічної безпеки підприємства в частині захисту бухгалтерської інформації включає комплекс принципів, правил, процедур та практичних прийомів щодо захисту конфіденційних даних та інформаційних процесів на підприємстві. Політика економічної безпеки підприємства включає вимоги до управлінського персоналу, працівників технічних служб.

Політика економічної безпеки підприємства в частині захисту бухгалтерської інформації залежить:

– від конкретної технології обробки бухгалтерської інформації;

– від використовуваних технічних та програмних засобів обробки бухгалтерської інформації.

Політика економічної безпеки підприємства в частині захисту бухгалтерської інформації повинна містити систему заходів на достатньо високому рівні. Політика описує загальний підхід до інформаційної безпеки без специфічних деталей. Типова політика економічної безпеки підприємства в частині захисту бухгалтерської інформації має містити наступні розділи (табл. 4.1).

Таблиця 4.1. Розділи політики економічної безпеки підприємства в частині захисту бухгалтерської інформації

Назва розділу	*Характеристика розділу*
Терміни і визначення	Основні терміни та визначення, які містяться в політиці економічної безпеки підприємства
Вступ	Необхідність появи даного документа
Мета політики	Цілі створення документу
Сфера застосування	Об'єкти та суб'єкти, які повинні виконувати вимоги даної політики. Політика застосовується до всіх співробітників, що мають будь-яку форму доступу до бухгалтерської інформації в комп'ютерному середовищі підприємства
Політика	Основні рівні захисту щодо забезпечення економічної безпеки підприємства
Відповідальність	Відповідальність за порушення зазначених у попередньому розділі вимог
Історія змін даної політики	Дає можливість відстежити всі зміни, що вносяться до документу

Така структура дозволяє лаконічно описати всі основні моменти, пов'язані з предметом політики економічної безпеки в частині захисту бухгалтерської інформації. Основними напрями розробки політики економічної безпеки підприємства в частині захисту бухгалтерської інформації є визначення даних, які необхідно захищати, визначення осіб та якої шкоди вони можуть заподіяти підприємству в інформаційному аспекті, а також виявлення ризиків та визначення схеми їх зменшення до допустимої величини (Додаток С).

Політика економічної безпеки підприємства в частині захисту бухгалтерської інформації встановлює жорсткі вимоги для запобігання незаконному використанню бухгалтерських даних, що є власністю підприємства та його партнерів. В основу системи безпеки бухгалтерської інформації підприємства повинні бути закладені наступні принципи рис. 4.9.

Рис. 4.9. Принципи безпеки системи бухгалтерської інформації підприємства

Всі співробітники підприємства, що мають доступ до бухгалтерської інформації, яка має відношення до третьої сторони та довіреної підприємству в межах ділової співпраці (дані, документація тощо), зобов'язані дотримуватися її конфіденційності.

Положення, що забезпечують захист бухгалтерської інформації, повинні бути внесені до посадових інструкцій співробітників, міститися у відповідних правилах із забезпечення безпеки бухгалтерської інформації та угоді про нерозголошення комерційної таємниці підприємства, яка підписується кожним співробітником при прийнятті його на роботу. Відповідно до цих вимог співробітники підприємства забезпечують конфіденційність бухгалтерської інформації, даних, документація та зобов'язуються здати роботодавцю всі подібні матеріали після закінчення роботи.

Цікавим є той факт, що згідно з результатами досліджень рівня безпеки інформації, проведених компанією Делойтт (Deloitte) у 2006 році, підприємства, які мають політику інформаційної безпеки, значно рідше піддаються "зламуванню". Це свідчить про те, що наявність політики є ознакою зрілості підприємства в питаннях інформаційної безпеки. Те, що підприємство чітко сформулювало свої принципи та підходи до забезпечення інформаційної безпеки означає, що в цьому напрямі було виконано серйозну роботу.

Доповненням політики економічної безпеки підприємства в частині захисту бухгалтерської інформації є механізм підзвітності, який дозволяє визначати, хто працює в системі та, що робить в певний момент часу. Засоби підзвітності можна розділити на наступні категорії, зображені на рис. 4.10.

Рис. 4.10. Механізм підзвітності безпеки підприємства

Ідентифікація та аутентифікація полягає в тому, що кожен користувач, перш ніж одержати право на здійснення будь-яких дій в комп'ютерній системі бухгалтерського обліку, повинен ідентифікувати себе. Звичайний спосіб ідентифікації – введення імені користувача при вході в систему. У свою чергу система повинна перевірити аутентичність особи користувача, тобто що саме він є тим, за кого себе видає. Стандартний засіб перевірки аутентифікації – пароль, хоча можуть використовуватися також різного роду особисті картки, біометричні пристрої, такі як, наприклад, сканування сітківки ока або відбитків пальців, або ж їх комбінація.

Надання надійного шляху пов'язує користувача безпосередньо з надійною обчислювальною базою, обійшовши інші, потенційно небезпечні компоненти системи. Мета надання надійного шляху полягає в можливості надати користувачу можливість переконатися в аутентичності обслуговуючої його системи.

Аналіз реєстраційної інформації передбачає наявність засобів вибіркового протоколювання відносно користувачів (здійснюється стеження як за підозрілими особами, так і за подіями, зокрема, вхід та вихід із комп'ютерної інформаційної системи, звернення до видаленої системи, операції з файлами, зміна прав доступу користувачів бухгалтерської інформації).

Протоколювання допомагає стежити за користувачами комп'ютерної системи бухгалтерського обліку та відтворювати здійснені події. Відтворення подій дозволяє проаналізувати випадки порушень, зрозуміти, чому вони стали можливі, оцінити розміри збитку та вжити необхідних заходів щодо уникнення подібних порушень в майбутньому. При здійсненні протоколювання події, що відбулася в комп'ютерній системі бухгалтерського обліку, фіксуються наступні дані (рис. 4.11).

Рис. 4.11. Протоколювання події, що відбувалася в комп'ютерній інформаційній системі бухгалтерського обліку

Додаткові труднощі для забезпечення інформаційної безпеки виникають, якщо підприємство в своїй діяльності використовує комп'ютерні мережі. При розробці системи захисту облікової інформації в комп'ютерному середовищі необхідно пам'ятати, що складна інформаційна система є менш захищеною і розробка її захисту є досить нелегкою справою. Складні системи не завжди можна налагодити належним чином, а різні неточності, які виникають у процесі цього налагодження, можуть призвести до виникнення проблем безпеки.

В сучасних умовах стрімкого використання інформаційних технологій завданням контролю за дотриманням економічної безпеки є перевірка дієвості та ефективності використання систем захисту бухгалтерської інформації на підприємстві.

Для забезпечення економічної безпеки та встановлення контролю за її дотриманням на підприємстві необхідним є створення служби економічної безпеки. В своїй діяльності дана структура повинна:

– керуватися відповідною нормативною базою;

– діяти відповідно до встановлених заходів, тобто виконувати прийняту на підприємстві політику економічної безпеки;

– мати у своєму розпорядженні відповідні засоби, тобто технічне обладнання.

При цьому, даний структурний підрозділ підприємства повинен вирішувати завдання забезпечення безпеки облікової інформації на всіх

етапах її накопичення, обробки, використання та зберігання, а також в усіх напрямках господарської діяльності підприємства.

Служба економічної безпеки повинна бути підпорядкована безпосередньо керівнику підприємства, який несе відповідальність за дотримання правил збереження інформації. В деяких випадках керівником даного структурного підрозділу підприємства може бути безпосередньо і сам директор або його заступник.

За участю представників служби економічної безпеки підприємства повинно відбуватись створення корпоративної інформаційної системи підприємства з початку її проектування до моменту введення в експлуатацію. Разом з тим, уже працюючу систему необхідно періодично обстежувати на предмет виявлення нових слабких місць і ризиків, та здійснювати постійний внутрішній контроль над нею. Нехтування щодо безпеки корпоративних систем приводить до великих фінансових втрат у результаті появи та реалізації внутрішніх або зовнішніх загроз.

На початковому етапі створення, основним завдання служби економічної безпеки є визначення напрямку розвитку та підтримки намірів підприємства, спрямованих на захист інформації в тому числі й бухгалтерської від несанкціонованого ознайомлення, зміни або знищення. Це досягається шляхом упровадження відповідних правил, інструкцій та вказівок.

Служба економічної безпеки відповідає за розробку, виконання та здійснення контролю планів із забезпечення інформаційної безпеки підприємства в наступних напрямах (рис. 4.12).

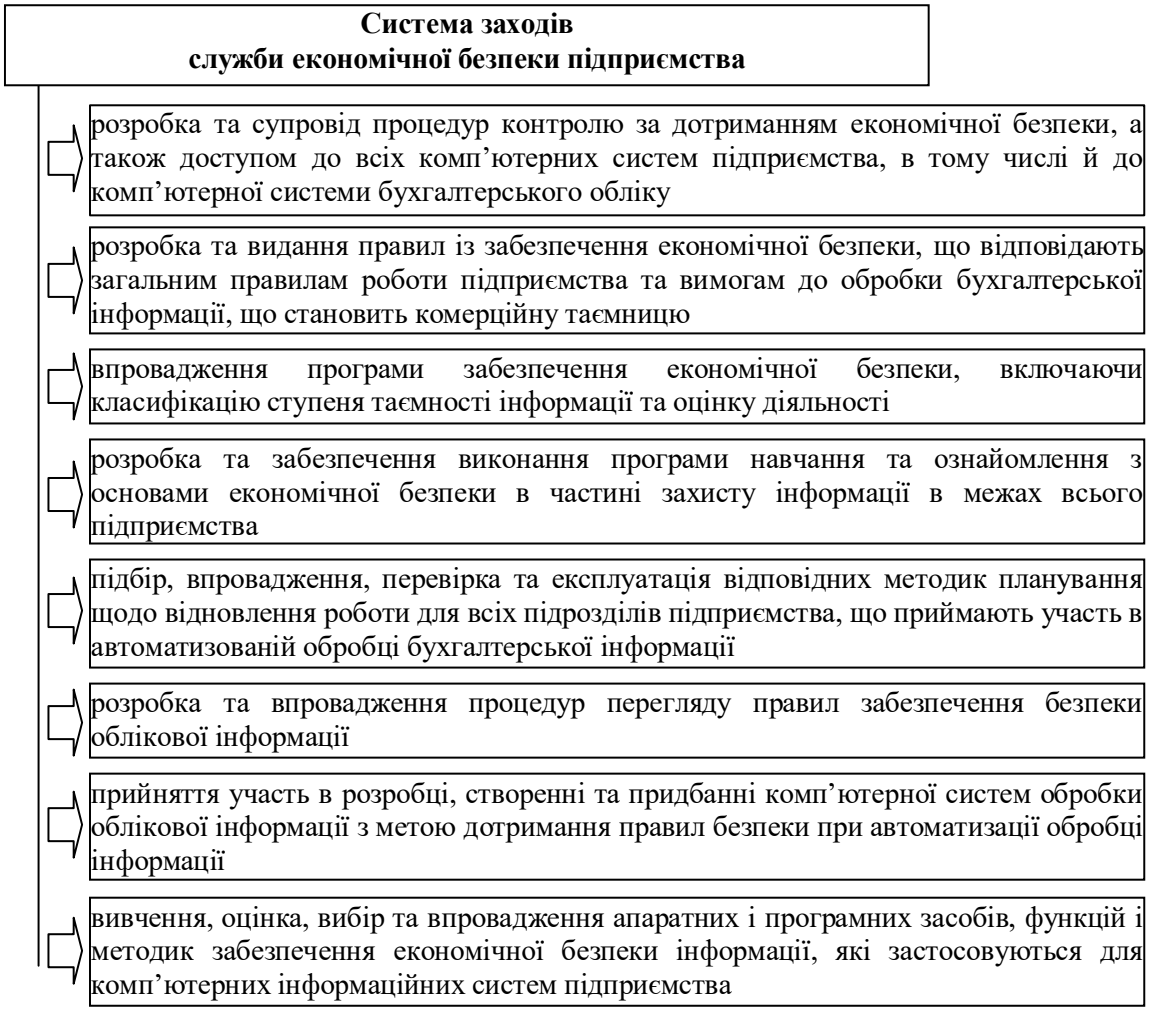


Рис. 4.12. Система заходів щодо виконання та здійснення контролю службою економічної безпеки підприємства

В разі необхідності на службу економічної безпеки можуть покладатися й інші обов'язки в частині контролю захисту інформації, серед яких можна виділити наступні (рис. 4.13).

Створення служби економічної безпеки підприємства потребує значних витрат. Однак не кожному підприємству під силу нести витрати на забезпечення ефективної системи безпеки інформації, тому, насамперед, необхідно провести економічне обґрунтування її створення. Як показують дослідження, у розвинених країнах світу на функціонування служб безпеки виділяється до 20 % чистого прибутку підприємства на рік [168]. Практика діяльності деяких підприємств у цій сфері показує, що на утримання фізичної охорони витрачається до 50 %, на технічне оснащення до 30 %, на

[168] Структура та завдання служби інформаційної безпеки // Безопасность информационных технологий [Електронний ресурс]. – Режим доступу: http://www.security.ukrnet.net/modules/news/article.php?storyid=15

інші складові служби безпеки до 20 % засобів, що витрачаються підприємством для забезпечення своєї безпеки. Оцінивши всі витрати, які пов'язані з функціонуванням служби економічної безпеки, керівництво може зробити відповідні висновки про доцільність її створення на підприємстві.

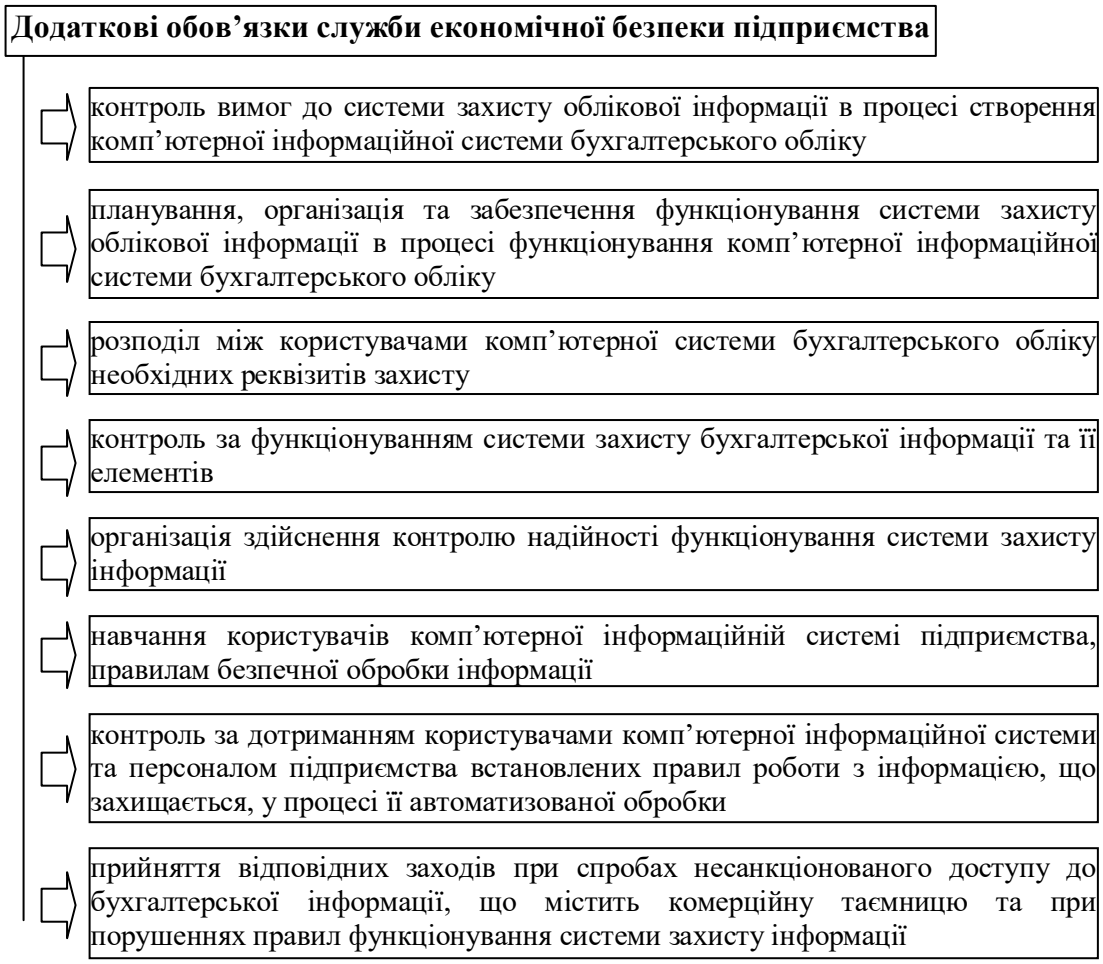


Рис. 4.13. Додаткові обов'язки служби економічної безпеки підприємства в частині контролю захисту інформації

Об'єктивність контролю економічної безпеки забезпечується ступенем його незалежності. Мета здійснення контролю економічної безпеки полягає в наданні допомоги співробітникам підприємства ефективно виконувати свої функції в частині захисту інформації в інформаційному середовищі від вірогідного прояву зовнішніх і внутрішніх загроз. Після проведення перевірки керівництву підприємства надаються відповідні дані аналізу та оцінки, рекомендації та іншу необхідну інформацію, яка є результатом перевірок стану безпеки.

При здійсненні контролю економічної безпеки підприємства, як правило, виконуються наступні функції (рис. 4.14).

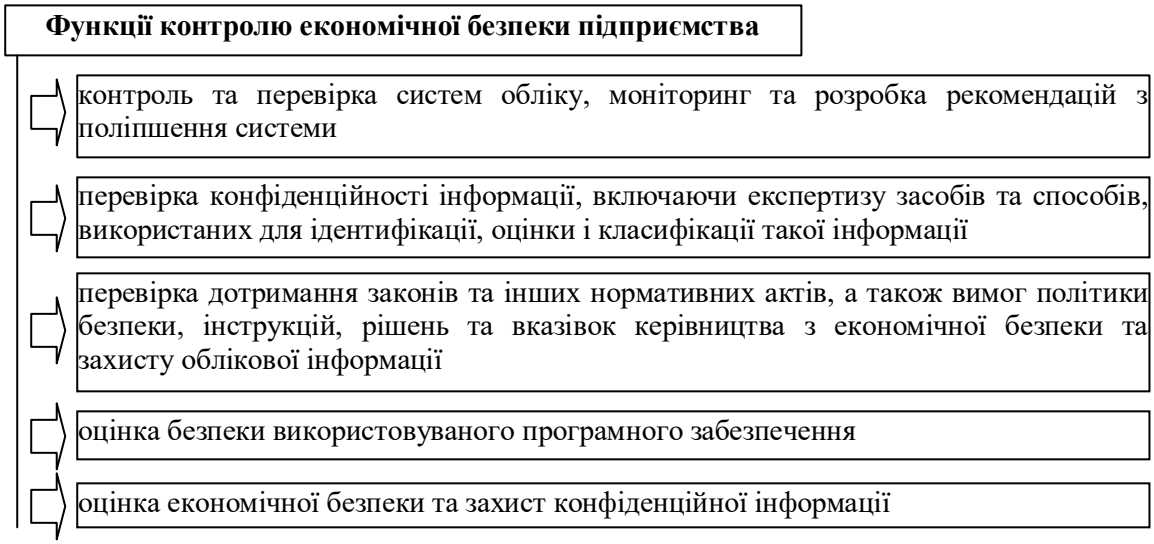


Рис. 4.14. Функції контролю економічної безпеки підприємства

Внутрішній контроль за діями облікового персоналу та системою бухгалтерського обліку дозволяє виявити причини виникнення помилок в звітній документації. Серед співробітників бухгалтерії можуть бути шахраї. Бухгалтери, касири та інші особи, що мають право вести бухгалтерські записи, як правило, здійснюють розкрадання шляхом знищення раніше виконаних проводок або внесенням змін до них. Для боротьби з шахрайством слід дозволити доступ до здійснення бухгалтерських проводок тільки бухгалтеру, що виконує цю роботу і відповідає за неї. З метою контролю слід в кінці кожного робочого дня одержувати роздруковані та завірені підписами двох незалежних за службовими обов'язками працівників підприємства журнал господарських операцій та оборотну відомість.

Слід також мати в друкованому вигляді перелік показників або програмних констант, які використовуються програмою для обчислення сум операцій, набір довідників (картотек), первинних документів і бібліотеку алгоритмів обробки інформації (роздруковувати кожного разу після суттєвих змін). Після закінчення електронної обробки інформації пачки паперових первинних облікових документів повинні передаватися в бухгалтерію підприємства, а електронні документи у відповідний підрозділ відділу комп'ютеризації для підготовки до збереження в архіві. Передача здійснюється з обов'язковою реєстрацією пачок документів. При цьому повинні бути передбачені заходи, які б виключали повторне використання первинної документації, що передається на зберігання.

Внутрішній контроль за дотриманням економічної безпеки підприємства можна розподілити за наступними напрямами:

– контроль об'єктної спрямованості. Здійснюється контроль всієї системи економічної безпеки або певних підрозділів системи;

– контроль проблемної спрямованості. Здійснюється контроль окремих складових забезпечення безпеки підприємства (облікова, інформаційна сфери);

– контроль функціональної спрямованості. Здійснюється контроль функціональних підрозділів підприємства з питань забезпечення безпеки (охорона, кадри, документи).

Оскільки проблеми економічної безпеки підприємств безпосередньо пов'язані з їх виробничими процесами, контроль за дотриманням економічної безпеки можна трактувати як спостереження служби безпеки за оцінкою ступеня відповідності реального стану безпеки підприємства вимогам обстановки та критеріям відповідних нормативних і законодавчих актів, підкреслюючи тим самим, що зміст контролю безпеки визначається специфікою господарської діяльності підприємства. Це визначення містить основні характеристики загального контролю, які розповсюджуються і на контроль економічної безпеки:

– вимір поточних характеристик;

– порівняльний аналіз відповідності законодавчим та нормативним вимогам;

– контроль та оцінка ступеня безпеки.

Внутрішній контроль за дотриманням економічної безпеки підприємства необхідно розглядати як виключно внутрішній інструментарій управління, що виключає, з метою конспірації, неможливість надання інформації про його результати стороннім особам. Внутрішній контроль безпеки є, насамперед, інструментом оцінки діючої системи безпеки підприємства та управління можливими ризиками. Усунення загроз економічній безпеці передбачає, в тому числі, й захист економічних, соціальних і інформаційних інтересів підприємства. Таким чином, можна з впевненістю стверджувати, що контроль за дотриманням безпеки стає інструментом економічного управління підприємством.

Проведення внутрішнього контролю економічної безпеки підприємства дозволяє:

– оцінити дотримання всіх законодавчих вимог із забезпечення економічної безпеки підприємства;

– оцінити дотримання корпоративних заходів щодо забезпечення економічної безпеки;

– виявити та проаналізувати слабкі місця в системі економічної безпеки та спланувати роботу з їх усунення;

– підвищити рівень свідомості співробітників у сфері забезпечення економічної безпеки підприємства;

– запобігти економічним втратам та нанесенню збитку в будь-яких сферах діяльності підприємства.

Ефективне здійснення внутрішнього контролю за дотриманням функціональних обов'язків працівників бухгалтерської служби дозволяє уникнути негативних наслідків, які можуть призвести до появи помилок при реєстрації фактів господарського життя підприємства. До таких причин відносяться: завчасно сплановане викривлення показників звітності, а також навмисна підміна первинних документів; ненавмисне викривлення показників внаслідок незнання або неуважності; недосконаліть організації бухгалтерського обліку через неврахування особливостей підприємства. Серед працівників підприємства також можуть бути шахраї, яких можна умовно розділити на дві групи:

– особи, уповноважені складати бухгалтерські записи можуть вчиняти розкрадання матеріальних цінностей підприємства шляхом внесення завідомо неправдивих даних до регістрів бухгалтерського обліку;

– адміністративний персонал підприємства, який, здійснюючи "коригування" (перекручування) звітних даних, а також проводячи махінації шляхом переоцінки майна підприємства у власних цілях.

В результаті комп'ютеризації бухгалтерського обліку змінився перелік контрольних процедур, які виконувались обліковим персоналом вручну. Комп'ютерна система бухгалтерського обліку сприяє здійсненню поточного контролю за правильністю реєстрації господарських операцій. Правильно розроблена та впроваджена на підприємстві комп'ютерна система бухгалтерського обліку сприяє забезпеченню дотримання обліковими

працівниками правил ведення обліку та порядку документообороту. Корисність для підприємства забезпечується зменшенням вірогідності виникнення помилок, як навмисних, так і випадкових.

При використанні комп'ютерної форми ведення обліку зростає інтеграція контрольних дій, за рахунок чого забезпечується поєднання об'єктів контролю в ході перевірки господарської діяльності підприємства.

Внутрішній контроль щодо належного використання комп'ютерної системи бухгалтерського обліку передбачає здійснення комплексу заходів за дотриманням правил авторизації користувачів системи та своєчасності й правильності відображення ними в обліку господарських операцій.

Забезпечення внутрішнього контролю економічної безпеки в комп'ютерному середовищі має бути складовою частиною процесу її створення.

Управління комп'ютерними системами здійснюється за допомогою комбінації із засобів загального контролю і засобів контролю додатків. Загальний контроль відстежує процеси проектування, забезпечення безпеки, використання програмних продуктів та даних в межах існуючої інформаційної інфраструктури. В цілому він застосовується до всіх комп'ютерних програм і є поєднанням апаратних, програмних та ручних процедур, які разом створюють загальне контрольоване середовище.

Внутрішній контроль додатків програмних продуктів є специфічним для кожної окремої програми. Він включає інструменти контролю, специфічні для певної сфери застосування комп'ютерної системи.

Засоби загального контролю комп'ютерних систем бухгалтерського обліку є інструментами загального управління, що впливають на всю систему економічної безпеки підприємства. Загальний контроль комп'ютерних систем бухгалтерського обліку включає наступні елементи (рис. 4.15).

Рис. 4.15. Елементи внутрішнього контролю комп'ютерних систем бухгалтерського обліку з метою забезпечення економічної безпеки підприємства

Суб'єкти внутрішнього контролю здійснюють контроль за процесом розробки системи та забезпечують управління ним на різних стадіях. Контроль процесу розробки встановлює контрольні точки, кожна з яких повинна відповідати певним вимогам, виконання яких є основою для ухвалення рішення про впровадження готової системи. Контроль процесу розробки також припускає визначення рівня залучення користувачів на кожній із стадій розробки та перевіряє співвідношення витрат і вигод від використання нових технологій.

Внутрішній контроль програмних засобів важливий для всіх типів програм, що використовуються в комп'ютерних інформаційних системах підприємств. Він призначений для спостереження за роботою системного програмного забезпечення і запобігання несанкціонованому доступу до нього. Це одна з найважливіших складових контролю за дотриманням економічної безпеки підприємства, оскільки системні програми виконують всі основні функції з обробки бухгалтерської інформації та файлів даних.

Внутрішній контроль устаткування забезпечує безпеку устаткування на фізичному рівні та відповідає за пошук несправностей. Доступ до устаткування дозволяється лише авторизованому персоналу. Крім того, обчислювальна техніка має бути захищена від пожеж, перепадів температури та вогкості. Підприємства, в діяльності яких використовується комп'ютерна

обробка облікової інформації, з метою забезпечення контролю економічної безпеки, повинні приймати додаткові заходи щодо резервного копіюванню даних та дублювання пристроїв зберігання бухгалтерської інформації.

Контроль комп'ютерних операцій знаходиться у підпорядкуванні фахівців служби економічної безпеки підприємства, які забезпечують узгоджену та коректну обробку бухгалтерських даних в комп'ютерному середовищі та їх зберігання. До контролю комп'ютерних операцій також входять процедури встановлення програм, контроль їх роботи, операції резервного копіювання бухгалтерської інформації та її відновлення. Фахівці служби економічної безпеки можуть розробляти спеціальні інструкції на випадок непередбачених ситуацій, збоїв в роботі комп'ютерних програм для ведення бухгалтерського обліку та обчислювальної техніки.

Внутрішній контроль безпеки даних з метою дотримання економічної безпеки підприємства попереджує несанкціонований доступу до бухгалтерської інформації, її зміни або знищення. Він необхідний як для контролю даних, які обробляються в комп'ютерній інформаційній системи підприємства, так і для забезпечення безпеки носіїв інформації. При введенні бухгалтерських даних за допомогою комп'ютерів в різних підрозділах підприємства, потрібно приділяти особливу увагу процедурам авторизації користувачів. З метою забезпечення дотримання економічної безпеки у подібних ситуаціях необхідно використовувати декілька рівнів захисту бухгалтерської інформації:

– доступ до комп'ютерів може бути фізично обмежений (робота на них дозволяється тільки авторизованому персоналу);

– програмне забезпечення може бути захищене паролями, які вводяться при запуску певних додатків програмного забезпечення. Для реєстрації користувача в системі також необхідним є введення паролю;

– для окремих систем та додатків програмних продуктів можуть бути створені додаткові набори паролів та обмежень. Також можна розмежувати права доступу таким чином, щоб не кожен користувач комп'ютерної інформаційної системи підприємства мав можливість змінювати бухгалтерські дані в певних файлах. Певна частина користувачів зможе лише проглядати бухгалтерську інформацію, якщо це необхідно. У випадку, якщо бухгалтерська інформація не повинна надаватися користувачам, доступ до неї взагалі закривається для певних користувачів.

Адміністративний контроль за впровадженням комп'ютерної системи бухгалтерського обліку включає формалізовані стандарти, правила та процедури з метою загального контролю програмного забезпечення, виконання яких є обов'язковим. Найбільш важливими серед них є: розподіл функцій; процедур; спостереження та контроль за діяльністю співробітників.

Розподіл функцій в комп'ютерній системі бухгалтерського обліку передбачає планування функцій співробітників, що дозволяє звести до мінімуму ризик помилок або неправомірних маніпуляцій з бухгалтерськими даними. Співробітники служби економічної безпеки підприємства, відповідальні за роботу комп'ютерної системи, повинні також проводити всі необхідні дії із зміни та оновлення інформації, що зберігається в ній.

Процедури встановлюють формальні стандарти для засобів управління комп'ютерними системами бухгалтерського обліку. Всі процедури мають бути задокументовані та затверджені керівництвом. Відповідно й обов'язки співробітників та користувачів комп'ютерної системи мають бути чітко визначені.

Спостереження та контроль за діяльністю співробітників забезпечує правильне та своєчасне виконання останніми всіх контрольних процедур. Інакше кажучи, навіть найвитонченіші процедури контролю можуть існувати лише на папері, а на підприємстві не застосовуватися.

Слід зауважити, що не всі інструменти контролю, наведені нами вище, можуть бути наявними в комп'ютерних інформаційних системах підприємств. Деякі комп'ютерні інформаційні системи вимагають більшого контролю, що залежить від важливості даних, що містяться в них та типу програмного забезпечення. З метою дотримання економічної безпеки підприємства контроль комп'ютерних систем бухгалтерського обліку може бути роздільний на три основні групи:

– контроль введення даних;

– контроль обробки даних;

– контроль виведення даних.

Контроль введення даних призначений для перевірки точності та повноти даних перед введенням їх в комп'ютерну систему бухгалтерського обліку. Введені дані мають бути правильно конвертовані для подальшої обробки в системі. Помилки на цьому етапі можуть бути мінімізовані

шляхом проведення основних операцій прямо з комп'ютерного терміналу або використання технології автоматичного формування первинних даних.

Контроль обробки даних забезпечує повноту та точність оновлення даних. На цьому етапі обробки даних необхідно застосовувати методики підрахунку контрольних сум, узгодження та контролю редагування.

Методика підрахунку контрольних сум полягає в порівнянні обсягу введених та оброблених даних бухгалтерського обліку. Оновлення даних може контролюватися за допомогою генерації контрольних сум під час процесу обчислень. Контрольні суми, такі як загальна кількість господарських операцій або обороти за звітний період, можуть порівнюватися вручну або за допомогою комп'ютера. У разі виявлення невідповідностей необхідно ретельно перевірити причини такої ситуації. При комп'ютерному порівнянні дані бухгалтерського обліку, що вводяться, порівнюються з інформацією, що зберігається в комп'ютерній системі бухгалтерського обліку. Більшість помилок виявляються на етапі введення бухгалтерської інформації, але іноді виникає необхідність перевірки повноти оновлення інформації.

Контроль редагування, як правило, виконується під час введення даних в комп'ютерну систему. Проте деякі програми вимагають перевірки коректності даних під час їх оновлення.

Контроль виведення даних призначений для забезпечення точності та повноти результатів комп'ютерних розрахунків. Вони включають наступні інструменти:

– порівняння кінцевих контрольних сум з початковими та сумами, отриманими в процесі підрахунків;

– формальні процедури та документація, в якій перераховані користувачі бухгалтерської інформації.

Від того, наскільки підприємство покладається на комп'ютерні інформаційні системи при здійсненні документування господарських операцій, залежить рівень економічної безпеки інформації. Впровадження та дотримання наведених вище видів контролю на підприємствах допоможе значною мірою посилити контроль за дотриманням економічної безпеки.

Здійснення перерахованих видів контролю покладається на фахівців служби економічної безпеки підприємства.

Контроль за дотриманням економічної безпеки дозволяє отримати якнайповнішу та об'єктивнішу оцінку захищеності підприємства, локалізувати наявні проблеми та розробити ефективну систему забезпечення економічної безпеки підприємства.

Внутрішній контроль економічної безпеки також включає аналіз політики безпеки підприємства та організаційно-технічних заходів із забезпечення режиму безпеки, оцінку їх відповідності вимогам та адекватності існуючим ризикам. Результати здійснення контролю є основою для формування подальшої стратегії забезпечення економічної безпеки підприємства. В процесі контролю здійснюється також перевірка ефективності існуючих організаційно-технічних заходів протидії загрозам економічній безпеці підприємства.

Обов'язковою складовою забезпечення контролю економічної безпеки підприємства виступає визначення її критерію. Під критерієм економічної безпеки підприємства розуміються ознака або певна кількість ознак, на підставі яких може бути зроблений висновок про те, чи знаходиться підприємство в економічній безпеці чи ні. Метою використання даного критерію є оцінка рівня економічної безпеки підприємства. Слід зазначити, що показники для визначення стану економічної безпеки повинні ґрунтуватись на планових та облікових даних господарської діяльності суб'єкта господарювання, що є важливим фактором при використанні даної оцінки в практиці.

Для цього доцільно досліджувати показники фінансової стійкості, беззбиткової та ліквідності підприємства. У економічній літературі вже робилися спроби кількісної оцінки рівня економічної безпеки підприємства, що призвело до появи декількох підходів до оцінки рівня економічної безпеки підприємства. Як зазначає В.Л. Тамбовцев, для оцінки рівня економічної безпеки доцільно використовувати індикаторний підхід, в основу якого покладено застосування так званих індикаторів [169]. Відповідно до цього підходу індикатори є пороговими значеннями показників, які характеризують суб'єктів господарювання в різних сферах господарської діяльності та відповідають певному рівню забезпечення економічної безпеки.

[169] Тамбовцев В.Л. Экономическая безопасность хозяйственных систем: структура, проблемы / В.Л. Тамбовцев // Вестник МГУ. Сер. 6. Экономика. – 1995. – № 3. – С. 3-9.

Визначення рівня економічної безпеки суб'єкта господарювання необхідно здійснювати шляхом співставлення (абсолютного або відносного) фактичних показників господарської діяльності з існуючими індикаторами.

Існує й інший підхід до оцінки рівня економічної безпеки підприємства, який може бути названий ресурсно-функціональним. Відповідно до цього підходу оцінка рівня економічної безпеки підприємства здійснюється на основі оцінки стану використання корпоративних ресурсів за спеціальними критеріями [170]. При цьому як корпоративні ресурси розглядаються чинники підприємницької діяльності, використовувані керівниками та менеджерами підприємства для виконання цілей бізнесу.

Ресурсно-функціональний підхід до оцінки рівня економічної безпеки підприємства є досить обширним. Спроба охопити всі функціональні сфери діяльності підприємства приводить до розмивання поняття економічної безпеки, а оцінка її рівня за допомогою сукупного критерію економічної безпеки, що розраховується на підставі поглядів кваліфікованих експертів з економічної безпеки підприємства, схильна до значного впливу суб'єктивної думки експертів. Як пропонує Є.А. Олєйніков [171], об'єднання показників із застосуванням різних підходів, включаючи також і питому вагу важливості показників, передбачає зниження достовірності та точності оцінки.

Так, В. Забродським та Н. Капустіним запропоновано використовувати для оцінки економічної безпеки підприємства підхід, що відображає принципи та умови програмно-цільового управління і розвитку [172]. Відповідно до цього підходу оцінка економічної безпеки підприємства ґрунтується на інтеграції сукупності показників, що визначають економічну безпеку. Такий підхід відрізняється високим ступенем складності аналізу, що проводиться, з використанням методів математичного аналізу. До того ж, запропонований автором підхід дозволяє оцінити рівень економічної безпеки підприємства, але, швидше, з позиції математика, а не менеджера.

---

[170] Основы экономической безопасности (Государство, регион, предприятие, личность) / Под ред. Е.А. Олейникова. – М.: ЗАО "Бизнес-школа "Интел-синтез", 1997. – 228 с.

[171] Экономическая и национальная безопасность: [учеб.] / Под ред. Е.А. Олейникова. – М.: Экзамен, 2005. – 768 с.

[172] Забродский В. Теоретические основы оценки экономической безопасности отрасли и фирмы / В. Забродский, Н. Капустин // Бизнес-информ. – 1999. – № 15-16. – С. 35-37.

Виходячи з результатів аналізу найбільш відомих підходів до оцінки рівня економічної безпеки підприємства, можна зробити висновок, що ці підходи досить складно використовувати для оцінки та контролю рівня економічної безпеки підприємства.

З метою дотримання високого рівня економічної безпеки на підприємствах необхідно систематично здійснювати її ретельний контроль. Контроль за дотриманням економічної безпеки полягає в ідентифікації всіх засобів контролю та оцінці їх ефективності. Фахівці служби економічної безпеки підприємства повинні володіти повною інформацією про всі бізнес-процеси, обладнання, системи комунікації, правила безпеки, системи контролю, організаційну структуру, співробітників, ручні процедури та окремі програмні продукти. З метою вирішення, які засоби управління необхідно використовувати, фахівці служби економічної безпеки повинні досліджувати всі доступні технології та порівняти їх економічну ефективність. недостатній контроль в одному місці може бути компенсований посиленням контролю в іншому.

Якість економічної безпеки може бути підвищена шляхом виправлення помилок щодо захисту даних, які містяться в комп'ютерній інформаційній системі, тому їх пошук є одним із завдань служби економічної безпеки.

Регулярне проведення контролю якості даних є єдиним способом отримання уявлення про те, наскільки точні, повні та достовірні дані зберігаються в комп'ютерній інформаційній системі підприємства.

Ретельний та систематичний контроль за дотриманням належного рівня економічної безпеки в комп'ютерному середовищі дозволить підприємству визначити ефективність управління інформаційними системами. Регулярний контроль якості даних дозволяє підприємству забезпечити належний рівень повноти та точності бухгалтерської інформації, що зберігається в комп'ютерних системах.

Висновки до 4-го розділу

1. Проведені дослідження дають змогу констатувати, що забезпечення захисту бухгалтерської інформації на підприємстві та дотримання економічної безпеки можливе лише за умови комплексного застосування засобів та методів захисту інформації. Головною метою системи забезпечення економічної безпеки є створення надійних умов функціонування підприємства, запобігання загрозам його безпеки, захист інтересів підприємства від протиправних посягань, недопущення крадіжок фінансових та матеріальних ресурсів, розголошення, втрати, витоку, викривлення або знищення службової інформації.

2. Розроблена модель організації бухгалтерського обліку в умовах застосування сучасних комп'ютерних технологій передбачає впровадження організаційно-технічних засобів та організаційно-режимних методів, а також проведення кадрової роботи з метою забезпечення належного рівня захисту бухгалтерської інформації. Особливе місце у забезпеченні захисту облікової інформації посідає використання електронного цифрового підпису, оскільки його застосування в системі електронного документообороту забезпечує підтвердження підпису документу зазначеною в ньому особою, а також гарантує неможливість внесення змін до документу сторонніми особами після його підписання. В результаті дослідження розроблено схему електронного документообороту з використанням електронного цифрового підпису, що дозволяє здійснювати обмін інформацією, яка становить комерційну таємницю, в досить короткий час та гарантувати її нерозголошення.

3. Внутрішній контроль економічної безпеки підприємства передбачає здійснення процесу отримання об'єктивних, якісних та кількісних оцінок про поточний стан економічної безпеки підприємства відповідно до певних критеріїв і показників безпеки. В роботі запропоновано заходи контролю, які дозволять перевіряти ступінь дотримання економічної безпеки підприємства. Результати контролю безпеки дозволяють побудувати оптимальну з точки зору ефективності та витрат систему захисту бухгалтерської інформації, адекватну поточним завданням та цілям підприємницької діяльності.

4. Для здійснення внутрішнього контролю за дотриманням економічної безпеки на підприємстві доцільним є створення спеціальної служби, що є підрозділом, призначеним для організації робіт зі створення системи захисту інформації та наступного забезпечення її контролю та функціонування. Проте, створення служби економічної безпеки потребує значних витрат, що може бути не під силу підприємству забезпечувати її функціонування. Тому, забезпечення даних функцій, може покладатися на службу внутрішнього контролю підприємства, бухгалтерську службу або окремого працівника, що працює в складі даних підрозділів або займається супроводом комп'ютерної інформаційної системи підприємства.

5. Для будь-якого підприємства при побудові системи безпеки облікових даних необхідним є розробка політики економічної безпеки підприємства, у формі внутрішнього документу, в якій на основі аналізу сучасного рівня та динаміки розвитку інформаційних технологій розглядається систематизоване викладення цілей, завдань та принципів досягнення потрібного рівня економічної безпеки.

ВИСНОВКИ

У монографії теоретично узагальнено та запропоновано нове вирішення наукового завдання, що полягає у теоретичному обґрунтуванні та практичних рекомендаціях з удосконалення організації бухгалтерського обліку як інструмента забезпечення економічної безпеки підприємств. Відповідно до мети автором отримані такі наукові результати.

1. При аналізі існуючих підходів до визначення методичного забезпечення напрямів формування економічної безпеки на мікро-, мезо- та макрорівнях та оцінки її значення для ефективного соціально-економічного розвитку виявлено, що існують фактори, які стримують розвиток економіки, одним з яких є відсутність ефективної стратегії економічної безпеки. В результаті проведеного дослідження виділено суб'єкти, складові, та інформаційне забезпечення економічної безпеки, що впливають на впровадження системи економічної безпеки підприємств.

2. Проведений аналіз існуючих підходів до визначення категорійно-понятійного апарату системного дослідження питань економічної безпеки дозволив розглянути дану економічну категорію у взаємозв'язку з системою бухгалтерського обліку, в результаті чого запропоновано авторське визначення "економічної безпеки підприємств". Під економічною безпекою підприємства розуміють збереження майна та інформації підприємства відповідно до обраної стратегії та принципу безперервності діяльності.

3. Аналізуючи зовнішні та внутрішні загрози, управлінський персонал підприємства повинен спрогнозувати найбільш небезпечні з них та розробити систему заходів щодо своєчасного виявлення, попередження або послаблення їх впливу на систему бухгалтерського обліку. Запропонована класифікація загроз економічній безпеці в системі бухгалтерського обліку дозволяє захистити бухгалтерську інформацію, що становить комерційну таємницю та попередити її розголошення. Для вирішення даного питання необхідним є удосконалення законодавчої бази відносно захисту бухгалтерської інформації та впровадження розроблених заходів з виявлення та уникнення різного роду загроз економічній безпеці підприємства.

4. Запропоновано перелік бухгалтерської інформації, що становить комерційну таємницю та удосконалено внутрішні організаційно-розпорядчі документи (посадові інструкції бухгалтерів, трудова угода, наказ про захист інформації, що становить комерційну таємницю), в частині захисту бухгалтерської інформації, яка дозволить забезпечити сталий розвиток підприємств в конкурентному середовищі. Обґрунтування змісту та структури економічної безпеки підприємства в частині бухгалтерського обліку показало, що інформаційні системи управління підприємством, серед яких ключове місце належить системі бухгалтерського обліку, повинні організовуватися таким чином, щоб забезпечувати стратегічне і тактичне планування діяльності та унеможливлювати використання інформації не за призначенням, що і служитиме основою концепції економічної безпеки підприємства.

5. За результатами дослідження удосконалено принципи організації бухгалтерського обліку, як передумови збереження майна підприємств за допомогою системи бухгалтерського обліку. Запропоновано використовувати розроблені принципи: безпеки та контролю бухгалтерських даних, комплексності та ешелонування з метою удосконалення процесу впровадження комплексної системи заходів організації бухгалтерського обліку та забезпечення економічної безпеки підприємства. Це дозволить впровадити на підприємстві розроблену систему заходів захисту бухгалтерської інформації, що сприятиме збереженню майна підприємства на різних стадіях господарської діяльності. Захисту бухгалтерської інформації на підприємстві повинна приділятися значна увага, що змусить учасників ринку використовувати вдосконалені засоби забезпечення обліково-інформаційної безпеки, доповнюючи засоби фізичної безпеки іншими різновидами, включаючи юридичні та технічні засоби.

6. Розроблено комплексну систему заходів організації бухгалтерського обліку з метою забезпечення економічної безпеки в частині розробки заходів щодо організації економічної політики підприємства, роботи бухгалтерської служби, організації та техніки ведення бухгалтерського обліку та організації внутрішнього контролю. Визначено, що збереження бухгалтерської інформації, що становить комерційну таємницю, передбачає ряд заходів щодо захисту майна підприємства; нерозголошення інформації, яка становить комерційну таємницю підприємства, що є досить важливим в сучасному конкурентному середовищі. Впровадження даної системи дозволяє підвищити

відповідальність працівників бухгалтерської служби завдяки удосконаленню посадових інструкцій бухгалтерів в частині економічної безпеки підприємства; закріплення інформаційних потоків за певними особами, які несуть відповідальність у разі розголошення комерційної таємниці; поділ документації на таємну (з грифом таємності) та нетаємну.

7. Розроблено модель організації бухгалтерського обліку в умовах використання комп'ютерних технологій та схему електронного докоментообороту з використанням електронного цифрового підпису, що враховує принцип системного підходу стосовно забезпечення захисту облікової інформації. Дана модель передбачає створення цілісної системи інформаційної безпеки, яка містить комплекс організаційних, правових, інженерно-технічних, програмно-апаратних заходів захисту та використовує сучасні методи прогнозування, аналізу і моделювання змінних ситуацій. Визначено послідовність дій при впровадженні та використанні запропонованої моделі, що дозволило забезпечити захист бухгалтерської інформації від впливу внутрішніх і зовнішніх загроз в комп'ютерному середовищі підприємства.

8. Внутрішній контроль за дотриманням інформаційної безпеки на підприємстві повинна забезпечувати спеціальна служба, що є підрозділом, призначеним для організації робіт зі створення системи захисту інформації та наступного забезпечення її контролю та функціонування. Розроблено політику економічної безпеки підприємства в частині захисту бухгалтерської інформації у вигляді внутрішнього документу, що містить систему заходів внутрішнього контролю за дотриманням економічної безпеки підприємств з метою захисту облікової інформації при експлуатації комп'ютерної інформаційної системи підприємства. У запропонованій політиці економічної безпеки підприємства розглядається систематизоване викладення цілей, завдань та принципів досягнення потрібного рівня захисту бухгалтерської інформації.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. 12 самых громких случаев ИТ-воровства в России: [Електронний ресурс]. – Режим доступу: http://www.cnews.ru/reviews/?2005/12/02/192675.

2. Абалкин Л.И. Экономическая безопасность России: угрозы и их отражение / Л.И. Абалкин // Вопросы экономики. – 1994. – № 12. – С. 4-13.

3. Абалмазов Э.И. Декомпозиция и композиция систем безопасности / Э.И. Абалмазов, М.Э. Кротова // Системы безопасности, связи и телекоммуникаций. – 1995. – № 6. – С. 19-21.

4. Абалмазов Э.И. Концепция безопасности: тактика высокоэффективной защиты / Э.И. Абалмазов // Системы безопасности. – 1995. – № 2.

5. Аверченков В.И. Аудит информационной безопасности: [учеб. пособ. для вузов] / В.И. Аверченков. – Брянск: БГТУ, 2005. – 268 с.

6. Аглицкий И. Защита информации в бизнесе: секретные диски / И. Аглицкий // Финансовая газета. – 1999. – № 23 (391) – С. 14.

7. Азарова А.О. Розробка методики визначення економічної безпеки підприємства / А.О. Азарова, О.В. Гаврилова // Економіка: проблеми теорії та практики. Збірник наукових праць. Випуск 191: В 4 т. Том III. – Дніпрпетровськ: ДНУ, 2004. – 318 с.

8. Александров І.А. Кластеризація територіальних утворень України за рівнем економічної безпеки / І.А. Александров, О.В. Половян // Економічна кібернетика. – 2000. – № 5-6. – С. 40-47.

9. Алексеенко В. Система защиты коммерческих объектов / В. Алексеенко, Б. Сокольский. – М., 1992. – 195 с.

10. Андрощук Г. Правове регулювання ноу-хау / Г. Андрощук // Інтелектуальна власність. – 2004. – № 10. – С. 29-35.

11. Андрощук Г.А., Крайнев П.П. Экономическая безопасность предприятия: защита коммерческой тайны: [монограф.] / Г.А. Андрощук, П.П. Крайнєв. – К.: Издательский Дом "Ин Юре", 2000. – 400 с.

12. Ареф'єва О.В. Планування економічної безпеки підприємств / О.В. Ареф'єва, Т.Б. Кузенко. – К: Вид-во Європ. ун-ту, 2004. – 170 с.

13. Архипов А. Экономическая безопасность: оценки, проблемы, способы обеспечения / А. Архипов, А. Городецкий, Б. Михайлов // Вопросы экономики. – 1994. – № 12. – С. 36-44.

14. Аудит информационной безопасности / А.П. Курило, С.Л. Зефиров, В.Б. Голованов и др. – М.: Издательская группа “БДЦ-пресс”, 2006. – 304 с.

15. Балабанов В.С. Продовольственная безопасность: (международные и внутренние аспекты) / В.С. Балабанов, Е.Н. Борисенко; Рос. Акад. предпринимательства. – М.: ЗАО “Издательство “Экономика”, 2002. – 544 с.

16. Барнгольц С.Б. Методология экономического анализа деятельности хозяйствующего субъекта: [учеб. пособие] / С.Б. Барнгольц, М.В. Мельник. – М.: Финансы и статистика, 2003. – 240 с.

17. Барсуков В.С. Обеспечение информационной безопасности / В.С. Барсуков. – М., 1996. – 271 с.

18. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жоздишевский. – М., 1999. – 297 с.

19. Безруких П.С. Организация бухгалтерского учета на предприятии / П.С. Безруких. – М.: “Финансы”, 1966. – 204 с.

20. Белов В.Г. Правовая охрана конфиденциальности коммерческой тайны / В. Белов, А. Полянский // Право и экономика. – 1993. – № 13-14. – С. 12-21.

21. Белов В.Г. Правовая охрана конфиденциальности коммерческой тайны / В. Белов, А. Полянский // Право и экономика. – 1993. – № 15-16. – С. 8-27.

22. Белов В.Г. Правовые аспекты оборота непубликуемой научно-технической информации // Электронный документ и документооборот: Правовые аспекты: Сб. науч. тр. / РАН. ИНИОН. Центр социальных науч.-информ. исслед. Отдел правоведения; РАН. ИГП. Центр публичного права. Сектор информационного права; Отв. ред. – Алферова Е.В., Бачило И.Л. – М., 2003. – 208 с.

23. Богомолов В.А. Экономическая безопасность: [учеб. пособ. для студентов вузов, обучающихся по специальностям экономики и управления] / В.А. Богомолов. – М.: ЮНИТИ-ДАНА, 2006. – 303 с.

24. Бутинець Ф.Ф. Організація бухгалтерського обліку: [Підр. для студентів спеціальності 7.050106 “Облік і аудит” вищих навчальних закладів, 4-е вид., доп. і перероб.] / Ф.Ф. Бутинець, О.П. Войналович, І.Л. Томашевська / За редакцією д.е.н., проф., Заслуженого діяча науки і техніки України Ф.Ф. Бутинця. – Житомир: ПП “Рута”, 2005. – 528 с.

25. Бухгалтерский словар: [2-е изд., доп]. – М.: Финансы и статистика, 1996. – 208 с.

26. Бычкова С.М. Информационные технологии в бухгалтерском учете и аудите: [учеб. пособие] / С.М. Бычкова, С.В. Ивахненков / Под ред. С.М. Бычковой. – М.: ТК Велби, Изд-во Проспект, 2005. – 216 с.

27. Валуев Б.И. Возможность углубления интеграции данных оперативного и бухгалтерского учета в основных центрах угроз экономической безопасности предприятия / Б.И. Валуев, А.И. Паламарчук. – Одесса, 2000. – С. 218-221.

28. Василевский И.В. Найти и обезвредить. Техника защиты информации / И.В. Василевский // Система безопасности. – 1995. – № 6. – С. 11-15.

29. Василец В.И. Методические основы обеспечения конфиденциальности производственной и коммерческой деятельности акционерного общества / В.И. Василец, В.Н. Голованов // Вопросы защиты информации. – 1994. – № 1. – С. 5-11.

30. Вейцман Р.Я. Курс счетоводства. Двойная бухгалтерия и ее применение к различным видам хозяйств: [Одиннадцатое изд., перераб. и доп.] / Р.Я. Вейцман. – М.: Центрсоюз, 1926. – 447 с.

31. Власенко М. Кадровая составляющая системы экономической безопасности в предпринимательской деятельности / М. Власенко // Финансовая газета. – 2007. – № 2 (108). – С. 22-24.

32. Вовк В. Інформації теорія // Економічна енциклопедія: У трьох томах. Т. 1: [Ред. кол.: С.В. Мочерний (відп. ред.) та ін.]. – К.: Видавничий центр "Академія", 2002. – 864 с.

33. Вовк В. Кібернетика // Економічна енциклопедія: У трьох томах. Т.1: [Ред. кол.: С.В. Мочерний (відп. ред.) та ін.]. – К.: Видавничий центр "Академія", 2002. – 864 с.

34. Воронко Р.М. Аудит в умовах розвитку сучасних інформаційних технологій: забезпечення конфіденційності та інформаційної безпеки підприємства / Р.М. Воронко // Вісник Львівської комерційної академії. – 2004. – № 16. – С. 147-153.

35. Гавриш В.А. Практическое пособие по защите коммерческой тайны / В.А. Гавриш. – Симферополь, 1994. – 153 с.

36. Гайкович В. Безопасность электронных банковских систем / В. Гайкович, А. Першин / Под ред. Ю.В. Гайковича. – М.: Единая Европа, 1994. – 363 с.

37. Галаган А. История предпринимательства российского. От купца до банкира / А. Галаган. – М.: Ось-89, 1997. – 160 с.

38. Гальперин Я.М. Основы бухгалтерского учета: [Четвертое изд.] / Я.М. Гальперин. – М.-Л., 1970. – 370 с.

39. Герасименко В.А. Организация комплексной защиты информации на современных объектах / В.А. Герасименко, М.В. Мецатунян // Вопросы защиты информации. 1995. – № 1. – С. 10-16.

40. Гордієнко С.Г. Сутність та зміст поняття "державна безпека" / С.Г. Гордієнко // Стратегічна панорама. – 2003. – № 2. – С. 114-121.

41. Городецкий А. Формирование единой системы государственного финансового контроля / А. Городецкий, А. Морукова // Вопросы экономики. – № 1. – 2004. – С. 92.

42. Горячев В.С. Информация и ее защита / В.С. Горячев // Вопросы защиты информации. – 1994. – № 2. – С. 13-18.

43. Господарський кодекс України № 436-IV від 16.01.2003 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=436-15

44. Грабова Н.Н. Теория бухгалтерского учета [учеб. пособие для сред. с.-х. заведений] / Н.Н. Грабова. – М.: "Финансы", 1972. – 223 с.

45. Градов А.П. Национальная экономика: [2-е изд.] / А.П. Градов. – СПб.: Питер, 2005. – 240 с.

46. Грунин О.А. Экономическая безопасность организации / О.А. Грунин, С.О. Грунин. – СПб.: Издательский дом "Питер", 2002. – 160 с.

47. Грэй, Сидней Дж. Финансовый учет: Глобальный подход: [учеб.-метод. пособие: пер. с англ] / Сидней Дж. Грэй, Белверд Е. Нидлз. – М.: Волтерс Клувер, 2006. – 614 с.

48. Губський Б.В. Економічна безпека України: методологія виміру, стан і стратегія забезпечення / Б.В. Губський. – К.: ДП "Укрархбудінформ", 2001. – 122 с.

49. Даль В.И. Толковый словарь живого великорусского языка: в 4 тт. Т. 2 / В.И. Даль. – Спб.: ТОО "Диамант", 1996. – 784 с.

50. Дарнопих Г. Сучасні проблеми економічної безпеки України / Г. Дарнопих // Вісник Академії правових наук України. – 1998. – № 1. – С. 142-150.

51. Деружинский В.А. Основы коммерческой тайны: [Практ. пособ. для предпринимателя] / В.А. Деружинский, В.В. Деружинский. – Мн.: ООО "Полирек", 1994. – 214 с.

52. Дикий А.П. Бухгалтерський облік як інформаційна система / А.П. Дикий // Вісник Житомирського державного технологічного університету. Серія: Економічні науки. – 2005. – № 3 (33). – С. 67-80.

53. Дикий А.П. Економічна безпека підприємства: сутність та шляхи забезпечення / А.П. Дикий // Materiały II Międzynarodowej naukowe-praktycznej konferencji "Wykształcenie i nauka bez granic – '2005". 19-27 grudnia 2005 roku. Tom 6. Ekonomiczne nauki. – Przemyśl-Praha: Sp. z o.o. "Nauka i studia", 2005. – 130 s. – S. 12-14.

54. Дикий А.П. Економічна безпека суб'єкта господарювання: характеристика загроз / А.П. Дикий // Вісник Житомирського державного технологічного університету. Економічні науки. – 2007. – № 1 (39). – С. 68-71.

55. Дикий А.П. Захист бухгалтерської інформації за допомогою електронного цифрового підпису / А.П. Дикий // Економіка: проблеми теорії та практики: Збірник наукових праць. – Випуск 245: В 5 т. – Т. III. – Дніпропетровськ: ДНУ, 2008. – 284 с. – С. 738-744.

56. Дикий А.П. Захист облікової інформації від несанкціонованого доступу при застосуванні інформаційних технологій: тезисы и тексты выступлений на V-ой Международной научной конференции ["Концепции развития бухгалтерской профессии: теория и практика"] / А.П. Дикий / М-во освіти і науки України, Житомир. держ. технолог. ун-т. – Житомир: ЖГТУ, 2006. – 136 с. – С. 45-47.

57. Дикий А.П. Значение коммерческой тайны при формировании экономической безопасности предприятия // Securitatea informationala 2006 / Conferinta internationala (editia a III-a) 14-15 aprrilie 2006. Editura ASEM – Chisinau, 2006. – 54 s. – S. 16-18

58. Дикий А.П. Ідентифікація загроз економічній безпеці господарюючого суб'єкта як передумова збереження комерційної таємниці: зб. тез та текстів виступів на П'ятій всеукраїнській науковій конференції, присвяченій видатним

вченим в галузі бухгалтерського обліку д.е.н., проф. І.В. Малишеву, д.е.н., проф. П.П. Німчинову. Ч. І. [Зимові читання, присвячені ідеям П.П. Німчинова та І.В. Малишева] / А.П. Дикий /. М-во освіти і науки України, Житомир. держ. технолог. ун-т. – Житомир: ЖДТУ, 2007. – 76 с. – С. 27-28.

59. Дикий А.П. Комерційна таємниця як складова економічної безпеки підприємства / А.П. Дикий, М.В. Семенчук // Вісник Житомирського державного технологічного університету. Економічні науки. – 2005. – № 4 (34). – С. 75-82.

60. Дикий А.П. Організація забезпечення захисту комерційної таємниці господарюючого суб'єкта: тези та тексти виступів VI-ої Міжнародної наукової конференції ["Наукові дослідження в сфері бухгалтерського обліку, контролю та аналізу: теоретико-практичне значення та напрями подальшого розвитку"] / А.П. Дикий / М-во освіти і науки України, Житомир. держ. технолог. ун-т. – Житомир: ЖДТУ, 2007. – 336 с. – С. 71-73.

61. Дикий А.П. Основні напрями захисту бухгалтерської інформації з метою збереження комерційної таємниці: тези та тексти виступів VII-ої Міжнародної наукової конференції ["Наукові бухгалтерські школи світу: еволюція, сучасний стан, перспективи розвитку"] /А.П. Дикий/ М-во освіти і науки України, Житомир. держ. технолог. ун-т. – Житомир: ЖДТУ, 2008. – 208 с. – С. 91-93.

62. Дикий А.П. Особливості вибору програмного забезпечення для комп'ютеризації бухгалтерського обліку великих підприємств /А.П. Дикий, Ю.Д. Довгаль // Вісник Житомирського державного технологічного університету. Економічні науки. – 2008. – № 4 (46). – С. 61-70.

63. Дикий А.П. Особливості захисту комерційної таємниці на підприємстві: обліковий аспект / А.П. Дикий // Вісник Житомирського державного технологічного університету. Економічні науки. – 2006. – № 4 (38). – С. 66-70.

64. Дикий А.П. Порядок забезпечення безпеки бухгалтерської інформації в умовах застосування сучасних комп'ютерних технологій / А.П. Дикий // Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. Міжнародний збірник наукових праць. / Серія: Бухгалтерський облік, контроль і аналіз. Випуск 3(12). / Відп. ред. д.е.н., проф. Ф.Ф. Бутинець. – Житомир: ЖДТУ, 2008. – С. 208-214.

65. Дикий А.П. Розробка заходів щодо безпеки облікової інформації: матеріали Міжнародної науково-практичної конференції. Ч. 1. ["Обліково-аналітичні системи: глобальний і національний аспекти"] / А.П. Дикий / М-во освіти і науки України, Укоопспілка, Полтав. у-т спожив. кооперації України. – Полтава: РВЦ ПУСКУ, 2006. – 296 с. – С. 30-32.

66. Дикий А.П. Шляхи захисту облікової інформації на підприємстві: зб. тез та текстів виступів на Четвертій всеукраїнській науковій конференції, присвяченій видатним вченим в галузі бухгалтерського обліку д.е.н., проф. І.В. Малишеву, д.е.н., проф. П.П. Німчинову [Зимові читання, присвячені ідеям П.П. Німчинова та І.В. Малишева] / А.П. Дикий / М-во освіти і науки України, Житомир. держ. технолог. ун-т. – Житомир: ЖДТУ, 2006. – 116 с. – С. 21-23.

67. Дикий А.П. Нормативно-правове регулювання захисту комерційної таємниці в Україні: материали за 4-а международна научна практична конференція Т. 19 ["Динамика изследования", – 2008] / А.П. Дикий /. – София: "Бял ГРАД-БГ" ООД. – 112 с. – С. 24-25.

68. Димитриади Г.Г. Безопасность России и ее экономическая политика / Г.Г. Димитриади. – М.: ЛЕНАНД, 2005. – 24 с.

69. Друри К. Введение в управленческий и производственный учет: [Пер. с англ.] / К. Друри / Под ред. С.А. Табалиной. – М.: Аудит, ЮНИТИ, 1997. – 560 с.

70. Євдокимов В.В. Захист бухгалтерської інформації з метою збереження майна підприємства: зб. тез та текстів виступів на Шостій всеукраїнській науковій конференції, присвяченій видатним вченим в галузі бухгалтерського обліку д.е.н., проф. І.В. Малишеву, д.е.н., проф. П.П. Німчинову [Зимові читання, присвячені ідеям П.П. Німчинова та І.В. Малишева] / А.П. Дикий, В.В. Євдокимов / М-во освіти і науки України, Житомир. держ. технолог. ун-т. – Житомир: ЖДТУ, 2008. – 148 с. – С. 31-33.

71. Євдокимов В.В. Особливості організації бухгалтерського обліку при забезпеченні економічної безпеки підприємства / В.В. Євдокимов, А.П. Дикий // Проблеми і перспективи розвитку банківської системи України. Збірник наукових праць Української академії банківської справи НБУ. – Випуск 24. – Суми: ДВНЗ "УАБС НБУ", 2009. – С. 255-264.

72. Євдокимов В.В. Теоретичні основи економічної безпеки в працях науковців / В.В. Євдокимов, А.П. Дикий // Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. Міжнародний збірник наукових праць. / Серія: Бухгалтерський облік, контроль і аналіз. Випуск 2(8). / Відп. ред. д.е.н., проф. Ф.Ф. Бутинець. – Житомир: ЖДТУ, 2007. – 276 с. – С. 51-57.

73. Жандаров А.М. Экономическая безопасность России: определения, гипотеза, расчеты / А.М. Жандаров, А.А. Петров // Безопасность. – 1994. – № 3. – С. 40-48.

74. Забродский В. Теоретические основы оценки экономической безопасности отрасли и фирмы / В. Забродский, Н. Капустин // Бизнес-информ. – 1999. – № 15-16. – С. 35-37.

75. Загородній А.Г. Облік і аудит: [Термінологічний словник] / А.Г. Загородній, Г.Л. Вознюк, Г.О. Партин. – Львів: "Центр Європи", 2002. – 671 с.

76. Закон України "Про бухгалтерський облік та фінансову звітність в Україні" № 996-XIV від 16.07.1999 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=996-14&test=4/UMfPEGznhhgnE.Ziv6CI8tHdlFIsFggkRbI1c.

77. Закон України "Про державну податкову службу" № 509-XII від 4.12.1990 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=509-12.

78. Закон України "Про державну таємницю" № 887-XII від 21.01.1994 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3855-12.

79. Закон України "Про електронний цифровий підпис" № 852-IV від 22.05.2003 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=852-15.

80. Закон України "Про електронні документи та електронний документообіг" № 851-IV від 22.05.2003 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=851-15.

81. Закон України "Про захист від недобросовісної конкуренції" № 236/96-ВР від 07.06.1996 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=236%2F96-%E2%F0.

82. Закон України "Про інформацію" № 1703-IV від 11.05.2004 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?page=1&nreg=2657-12.

83. Иванов А. Экономическая безопасность предприятия / А. Иванов, В. Шлыков. – М., 1995. – 265 с.

84. Ивашкевич В.Б. Бухгалтерский учет в условиях совершенствования хозяйственного механизма / В.Б. Ивашкевич. – М.: Финансы и статистика, 1982. – 176 с.

85. Ивченко И.С. Управление информационными рисками в системах автоматизации банков / И.С. Ивченко // Корпоративные системы. – 2003. – № 1. – С. 73-78.

86. Інформаційне забезпечення // Економічна енциклопедія: У трьох томах. Т. 1: [Ред. кол.: С.В. Мочерний (відп. ред.) та ін.]. – К.: Видавничий центр "Академія", 2002. – 864 с.

87. Інформаційні системи і технології в обліку: [Підр. для студентів вищих навчальних закладів, 3-є вид., перероб. і доп.] / [Ф.Ф. Бутинець, Т.В. Давидюк, В.В. Євдокимов, С.Ф. Легенчук] / За ред. д.е.н., проф., Заслуженого діяча науки і техніки України Ф.Ф. Бутинця. – Житомир: ПП "Рута", 2007. – 468 с.

88. Каллас К.Э. Организация автоматизированной информационной системы бухгалтерского учета / К.Э. Каллас. – М.: Финансы и статистика, 1990. – 176 с.

89. Капустин Н. Экономическая безопасность отрасли и фирмы / Н. Капустин // Бизнес-информ. – 1999. – № 11-12. – С. 45-47.

90. Кашаев А.Н. Организация бухгалтерского учета в производственных объединениях / А.Н. Кашаев. – М.: Финансы и статистика, 1986. – 192 с.

91. Кащеев В.И. Обеспечение информационной безопасности коммерческого объекта / В.И. Кащеев // Системы безопасности. – 1995. – № 5. – С. 8-12.

92. Кейнс Дж.М. Избранные произведения / Дж.М. Кейнс. – М.: Прогресс, 1993. – 544 с.

93. Кирьянова З.В. Теория бухгалтерского учета: [учеб.] / З.В. Кирьянова. – М.: Финансы и статистика, 1995. – 192 с.

94. Клівець П.Г. Стратегія підприємства: [навч. посіб.] / П.Г. Клівець. – К.: Академвидав, 2007. – 320 с.

95. Клюев Ю.Б. Экономико-математическое моделирование производственных систем энергетики / Ю.Б. Клюев, А.Я. Лавров, В.Р. Окороков. – М.: Высшая школа, 1992.

96. Князєв С. Комерційна таємниця в Україні: особливості організаційно-пра-вового впровадження / С. Князєв // Юридичний журнал. – 2006. – № 6. – С. 93-96.

97. Ковалев Д. Экономическая безопасность предприятия Д. Ковалев, Т. Сухорукова // Экономика Украины. – 1998. – № 10. – С. 48-52.

98. Ковалев В.В. Организация бухгалтерского учета на совместных предприятиях / В.В. Ковалев, Е.Н. Евстигнеев, Я.В. Соколов. – М.: Финансы и статистика, 1991. – 160 с.

99. Колодницький М.М. Основи теорії математичного моделювання систем: [Навч.-довід. посіб., Том 1] / М.М. Колодницький. – Житомир: ЖІТІ, 2001. – 718 с.

100. Концепция обеспечения защиты информации кредитно-финансового учреждения. – М.: Изд-во Центробанка РФ, 1996.

101. Копылов В.А. Информационное право: [учеб.] / В.А. Копылов – М.: Юристь, 2004. – 512 с.

102. Коржов В. Сколько стоит безопасность? / В. Коржов // Computerword. – 2004. – № 12: [Електронний ресурс]. – Режим доступу: http://www.outsourcing.ru/content/rus/131/1314-article.asp.

103. Косолапов Н. Сила, насилие, безопасность: современная диалектика взаимосвязей / Н. Косолапов // МЭиМО. – 1992. – № 11. – С. 45-58.

104. Костюк П.А. Бухгалтерский словарь / П.А. Костюк. – Минск: “Вышэйшая школа”, 1971. – 160 с.

105. Котляр Д. Правова природа та підходи до регулювання комерційної таємниці / Д. Котляр // Часопис Парламент. – 2004. – № 3: [Електронний ресурс]. – Режим доступу: http://www.parliament.org.ua/index.php?action=magazine&id=9&ar_id=572&iar_id=605&as=2.

106. Кримінальний кодекс № 2341-III від 05.04.2001 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14.

107. Крупка Я.Д. Облікові системи та їх інтеграція в умовах повністю автоматизованої обробки інформації / Я.Д. Крупка // Вестник национального технического университета "ХПИ", № 54(1). – Харків, 2008. – С. 48-52.

108. Крупка Я.Д. Про масштаби та способи розкриття інформації у примітках до фінансової звітності / Я.Д. Крупка // Науковий вісник Волинського національного університету ім. Лесі Українки. – Луцьк, 2009. – № 7. – С. 144-149.

109. Крупка Я.Д. Теоретичні основи та принципи формування аудиторського висновку / Я.Д. Крупка // Науковий вісник Ужгородського університету: Серія "Економіка". Вип. 22. Ч. 2. – Ужгород, 2007. – С. 28-33.

110. Кузнецов В. Великий бухгалтерський словник: [2-ге вид., перероб. і доп.] / В. Кузнєцов, О. Михайленко. – Х.: Фактор, 2005. – 532 с.

111. Кузьминский А.Н., Сопко В.В. Организация бухгалтерского учета и анализа хозяйственной деятельности. – К.: Вища школа, 1986. – 256 с.

112. Кульпінов В. Кадри позбавляють усього. Як нейтралізувати штатних шкідників / В. Кульпінов // Контракти. – 2004. – № 41. – С. 54-55.

113. Кульпінов В. Комерційний смерш / В. Кульпінов // Контракти. – 2004. – № 43. – С. 34-38.

114. Кульпінов В. Прозріння Феміди / В. Кульпінов // Контракти. – 2004. – № 48. – С. 34-35.

115. Кульчицький Б.В. Сучасні економічні системи: [навч. посіб.] / Б.В. Кульчицький. – Львів: Афіша, 2004. – 279 с.

116. Левковский А.И. Социальная структура развивающихся стран: проблемы многоукладности переходного общества / А.И. Левковский. – М.: Мысль, 1978. – С. 78-81.

117. Леоненко П.М., Черепніна О.І. Сучасні економічні системи: [навч. посіб.]. – К.: Знання, 2006. – 429 с.

118. Ливертовский Д.С. Вопросы организации бухгалтерского учета / Д.С. Ливертовский. – М.: "Госстатиздат", 1953. – 152 с.

119. Литвин Ю.Я. Організація бухгалтерського обліку, контролю і аналізу в сільському господарстві / Ю.Я. Литвин, В.А. Полторадня. – Тернопіль: "Тернопіль", 1998. – 375 с.

120. Луговець Л. Комерційна таємниця: поняття, проблеми захисту, порядок розкриття та відповідальність / Л. Луговець // Дебет-Кредит. – 2003. – № 23. – С. 26.

121. Лукацкий А. Как связать безопасность компании с ее бизнесом / А. Лукацкий // Корпоративные системы. – 2008. – № 1. – С. 65-72.

122. Ляпунов А.А. Проблемы теоретической и прикладной кибернетики / А.А. Ляпунов. – М.: Наука, 1980. – 335 с.

123. Мак-Мак В.П. Служба безопасности предприятия. Организационно-управленческие и правовые аспекты деятельности / В.П. Мак-Мак. – М.: Мир безопасности, 1999.

124. Малюга Н.М. Наукові дослідження в бухгалтерському обліку: [навч. посіб. для студентів вищих навчальних закладів] / Н.М. Малюга / За ред. проф. Ф.Ф. Бутинця. – Житомир: ПП "Рута", 2003. – 476 с.

125. Маршалл А. Принципы экономической науки: [пер. с англ, Т.1] / А. Маршалл. – М.: "Прогресс", 1993. – 415 с.

126. Медвідь Ф. Економічна безпека: небезпеки і загрози національним та національно-державним інтересам України / Ф. Медвідь // Юридичний вісник України. – 2007. – № 9-10. – С. 23.

127. Михалкевич А.П. Бухгалтерский учет на предприятиях зарубежных стран / А.П. Михалкевич. – Минск: ООО "Мисанта", 1998. – 109 с.

128. Михеев Ф. Об охране "коммерческой тайны" капиталистическими предприятиями / Бутынец Ф.Ф. Бухгалтерский учет в зарубежных странах: [В 2-х частях. Ч. 1: учеб. пособ.]. – Житомир: ЧП "Рута", 2005. – 640 с. – С. 567-572.

129. Мокров Г.Г. Международная торговля, экономическая безопасность и таможенные преступления: [учеб.-практ. пособ.] / Г.Г. Мокров, Р.И. Дронов. – М.: ЮРКНИГА, 2004. – 256 с.

130. Мочерний С. Економічна (валютно-фінансова) безпека. // Економічна енциклопедія: У трьох томах. Т.1 / Ред. кол.: С.В. Мочерний (відп. ред.) та ін. – К.: Видавничий центр "Академія", 2000. – 864 с.

131. Мочерний С. Економічна (науково-інформаційна) безпека // Економічна енциклопедія: У трьох томах. Т.1: [Ред. кол.: С.В. Мочерний (відп. ред.) та ін.]. – К.: Видавничий центр "Академія", 2000. – 864 с.

132. Мочерний С. Система // Економічна енциклопедія: У трьох томах. Т. 3: [Ред. кол.: С.В. Мочерний (відп. ред.) та ін.]. – К.: Видавничий центр "Академія", 2002. – 952 с.

133. Мочерний С. Системно-структурний підхід в економічному дослідженні // Економічна енциклопедія: У трьох томах. Т.3: [Ред. кол.: С.В. Мочерний (відп. ред.) та ін.]. – К.: Видавничий центр "Академія", 2002. – 952 с.

134. Мочерний С. Теорія систем загальна // Економічна енциклопедія: У трьох томах. Т.3: [Ред. кол.: С.В. Мочерний (відп. ред.) та ін.]. – К.: Видавничий центр "Академія", 2002. – 952 с.

135. Мурашин Г. О концепции национальной безопасности / Г. Мурашин, Е. Кравец // Політика і час. – 1992. – № 5. – С. 10-18.

136. Мюрдаль Г. Современные проблемы "третьего мира" (Asian Drama) / Г. Мюрдаль. – М.: Прогресс, 1972. – 767 с.

137. Настольная книга бухгалтера – профессионала / Под общ. ред. И.С. Кумка. – М.: АОЗТ "Московское Финансовое Объединение", 1995. – 304 с.

138. Нидлз Б. Принципы бухгалтерского учета / Б. Нидлз, Х. Андерсон, Д. Колдуэлл: [Пер. с англ.] / Под ред. Я.В.Соколова. – М.: Финансы и статистика, 1997. – 496 с.

139. Нимчинов П.П. Общая теория бухгалтерского учета / П.П. Нимчинов. – К.: Вища школа, 1977. – 240 с.

140. Новак В.О., Макаренко Л.Г., Луцький М.Г. Інформаційне забезпечення менеджменту: [навч. посіб.] / В.О. Новак, Л.Г. Макаренко, М.Г. Луцький. – К.: Кондор, 2006. – 462 с.

141. Норт Д. Институциональные изменения: рамки анализа / Д. Норт // Вопросы экономики. – 1997. – № 3. – С. 11-13.

142. Носевич В.Н. Электронные документы и меры по обеспечению их сохранности (Опыт Республики Беларусь) // Электронный документ и документооборот: Правовые аспекты: Сб. науч. тр. / РАН. ИНИОН. Центр социальных науч.-информ. исслед. Отдел правоведения; РАН. ИГП. Центр публичного права. Сектор информационного права; Отв. ред. – Алферова Е.В., Бачило И.Л. – М., 2003. – 2008 с.

143. Обучающие машины, системы и комплексы: [Справочник] / К.Г. Самофалов, В.Г. Слипченко, В.А. Новиков, В.И. Корнейчук, В.Н. Сороко / Под общей ред. д-ра тех. наук, проф. А.Я. Савельева. – К.: Вища школа, Головное изд-во, 1986. – 303 с.

144. Общая теория национальной безопасности: Учебник / Под общ. ред. А.А. Прохожева. – М.: Изд-во РАГС, 2005. – 344 с.

145. Ожегов С.И. Словарь русского языка: [изд. 11-е, стер.] / С.И. Ожегов. – М.: Русский язык, 1975. – 846 с.

146. Ожегов С.И. Словарь русского языка / С.И. Ожегов. – М.: Советская энциклопедия, 1968. – 990 с.

147. Організація бухгалтерського обліку: [навч. посіб. для студентів вузів спеціальності 7.050106 "Облік і аудит", 2-е вид., доп. і перероб.] / Ф.Ф. Бутинець, О.В. Олійник, М.М. Шигун, С.М. Шулепова. – Житомир: ЖІТІ, 2001. – 576 с.

148. Організація обліку, контролю і аналізу в сільському господарстві / Ю.Я. Литвин, В.М. Олійник, М.С. Палюх, М.В. Семчишин. – Тернопіль: "Тернопіль", 1998. – 376 с.

149. Осмятченко В.О. Дефініції в трактуванні інформаційних систем бухгалтерського обліку / В.О. Осмятченко // Вісник Криворізького економічного інституту. Збірник наукових праць. – Випуск 1 (9). – Кривий Ріг, 2007. – С. 86-89.

150. Осмятченко В.О. Критична оцінка принципів бухгалтерського обліку в умовах функціонування комп'ютеризованих систем / В.О. Осмятченко // Вісник Національного університету водного господарства та природокористування / Економіка. Збірник наукових праць. – Частина 2. – Випуск 4 (44). – Рівне, 2008. – С. 357-363.

151. Осмятченко В.О. Поетапна модель впровадження програмного забезпечення в систему бухгалтерського обліку / В.О. Осмятченко // Вісник Національного університету водного господарства та природокористування / Економіка. Збірник наукових праць. – Випуск 2 (46). – Рівне, 2009. – С. 247-255.

152. Осмятченко В.О. Стан та розвиток комп'ютерних технологій бухгалтерського обліку / В.О. Осмятченко // Вісник Луцького національного технічного університету. Збірник наукових праць. – Випуск 33 (70). – Луцьк, 2009. – С. 184-189.

153. Основные угрозы в сфере информационной безопасности банковской деятельности // Материалы Центробанка РФ. – М., 1996.

154. Основы экономической безопасности (Государство, регион, предприятие, личность) / Под ред. Е.А. Олейникова. – М.: ЗАО "Бизнес-школа "Интел-синтез", 1997. – 228 с.

155. Островский О.Н. Типовые элементы организации бухгалтерского учета / О.Н. Островский, Т.А. Шнайдерман. – М.: Финансы и статистика, 1988. – 207 с.

156. Палий В.Ф. АСУ и проблемы теории бухгалтерского учёта / В.Ф. Палий, Я.В. Соколов. – М: Финансы и статистика, 1981. – 224 с.

157. Палий В.Ф. Теория бухгалтерского учета / В.Ф. Палий, Я.В. Соколов. – М.: Финансы и статистика, 1988. – 279 с.

158. Панченко Є. Інформаційна система // Економічна енциклопедія: У трьох томах. Т.1: [Ред. кол.: С.В. Мочерний (відп. ред.) та ін.]. – К.: Видавничий центр "Академія", 2002. – 864 с.

159. Паньков В. Экономическая безопасность: мирохозяйственный и внутренний аспект / В. Паньков // Внешнеэкономические связи. – 1992. – № 8. – С. 5-18.

160. Парсонс Т. Система современных обществ: [Пер. с англ. Л.А. Седова и А.Д. Ковалева / под ред. М.С. Ковалевой] / Т. Парсонс. – М.: Аспект-Пресс, 1998. – 270 с.

161. Пастернак-Таранушенко Г.А. Економічна безпека держави. Методологія забезпечення: [монограф.] / Г.А. Пастернак-Таранушенко. – К.: Київський економічний інститут менеджменту, 2003. – 320 с.

162. Пискунов А.П. Военно-экономическая безопасность России на современном этапе / А.П. Пискунов // Военная мысль. – 1995. – № 2. – С. 68-71.

163. Плетникова И.П. Определение уровня и планирование ЭБП / И.П. Плетникова // Вісник Технологічного університету Поділля. – 2000. – № 4 (Ч.2). – С. 100-108.

164. Полтерович В.М. Институциональные ловушки и экономические реформы / В.М. Полтерович // Экономика и математические методы. – 1999. – Т. 35. – Вып. 2.

165. Полянська О.А. Організація управлінського обліку на підприємствах гуртової торгівлі як визначальний фактор ефективного функціонування усієї системи управління підприємством / О.А. Полянська // Економіка: проблеми теорії та практики. Збірник наукових праць. Випуск 125. – Дніпропетровськ: ДНУ, 2002. – 200 с.

166. Пономарев В.П. Оценка уровня экономической безопасности предприятия: материалы Международной науч.-практ. конф. [Настоящее и будущее российской экономики: проблемы, подходы, решения] / В.П. Пономарев. – Пермь: Гос. ун-т, 1999. – С. 189-190.

167. Попов Н.У. Математический метод бухгалтерии / Н.У. Попов. – Красноярск, 1906. – 188 с.

168. Постанова Кабінету Міністрів України “Про перелік відомостей, що не становлять комерційної таємниці” № 611 від 09.08.1993 р.: [Електронний ресурс]. – Режим доступу: http://www.yurist.kh.ua/index.php?option=com_content&task=view&id=29&Itemid=51.

169. Постанова КМУ “Про затвердження Порядку акредитації центру сертифікації ключів” № 903 від 13.07.2004 р.: [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/control/uk/publish/article%3FshowHidden=1&art_id=7952553&cat_id=2251550&ctime=1092757517060.

170. Постанова КМУ “Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності” № 1452 від 28.10.2004 р.: [Електронний ресурс]. – Режим доступу: http://www.uazakon.com/document/fpart60/idx60254.htm.

171. Постанова КМУ “Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади” № 1453 від 28.10.2004 р.: [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=38932&cat_id=38834.

172. Пошерстник Н.В. Бухгалтерский учет на современном предприятии: [учеб.-практ. пособие] / Н.В. Пошерстник. – М.: ТК Велби, изд-во Проспект, 2006. – 552 с.

173. Прескотт Джон Е. Конкурентная разведка: Уроки из окопов / Дж.Е. Прескотт, Стивен.Х. Миллер. – М.: Альпина Паблишер, 2003. – 336 с.

174. Пригожин И.С. Порядок из хаоса / И.С. Пригожин, И. Стенгерс. – М.: Прогресс, 1986. – 432 с.

175. Пушкар М.С. Розробка систем обліку: [навч. посіб.] / М.С. Пушкар. – Тернопіль: Карт-бланш, 2003. – 198 с.

176. Пушкар М.С. Тенденції та закономірності розвитку бухгалтерського обліку в Україні (теоретико-методологічний аспект): [Монограф.] / М.С. Пушкар. – Тернопіль: Економічна думка, 1999. – 424 с.

177. Пушкар М.С. Теоретичні основи бухгалтерського обліку: [підр. для вузів, вид. 2-ге, перероб. і доп.] / М.С. Пушкар, Г.П. Журавель, Ю.Я. Литвин, В.Г. Мельник. – Тернопіль:ТАНГ, 1998. – 269 с.

178. Раевский Г. Система экономической безопасности предприятия / Г. Раевский // Частный сыск, охрана, безопасность. – 1994. – № 2. – С. 5-11.

179. Райзберг Б.А. Современный экономический словарь / Б.А. Райзберг, Л.Ш. Лозовский, Е.Б. Стародубцева. – М.: ИНФРА, 1996. – 496 с.

180. Речмен Д.Дж. и др. Современный бизнес: [учеб.: в 2 Т. – Т.1: пер. с англ.] / Д.Дж. Речмен, М.Х. Мескон, К.Л. Боуви, Дж.В. Тилл. – М.: Республика, 1995. – 431 с.

181. Рожнова О.В. Финансовый учет. Теоретические основы, методологический апарат: [2-е изд., перераб. и доп.] / О.В. Рожнова – М: Издательство "Экзамен", 2003. – 192 с.

182. Ромащенко Т.Д. Экономическая безопасность национального хозяйства: теория, методология, формирование в России: [монограф.] / Т.Д. Ромащенко. – Воронеж: Изд-во ВГУ, 2003.

183. Ротару А.Х., Сидорко А.Л. Инновационная экономика – основа национальной безопасности и устойчивого развития государства: conf. int. (2003; Chişinău). Rolul ştiinţei şi învăţământului economic în realizarea reformelor economice din Republica Moldova: Materialele conf. int., 25-26 sept. 2003./ col. red. Grigore Belostecinic, preşed ["Rolul ştiinţei şi învăţământului economic în realizarea reformelor economice din Republica Moldova"]. – Ch.: Dep. Ed.-Poligr. al ASEM, 2003 – 613 p.

184. Рубанов В. Безопасность – лозунги, теория и политическая практика / В. Рубанов // РЭЖ. – 1991. – № 17. – С. 31-41.

185. Савин В.А. Некоторые аспекты экономической безопасности России / В.А. Савин // Международный бизнес России. – 1995. – № 9. – С. 14-16.

186. Селіванов В. Національна безпека України та її забезпечення / В. Селіванов // Право України. – 1992. – № 7.

187. Семенова Н. Охорона комерційної таємниці в Україні / Н. Семенова // Бухгалтерія. – 2002. – № 15/2 (482). – С. 71-72.

188. Смит А. Исследование о природе и принципах богатства народов / А. Смит. – М.: Соц-экгиз, 1962. – 654 с.

189. Соколов Я.В. Бухгалтерский учет: от истоков до наших дней: [Учебн. пособие для вузов] / Я.В. Соколов. – М.: Аудит, ЮНИТИ, 1996. – 638 с.

190. Соловьев Э.Я. Коммерческая тайна и ее защита / Э.Я. Соловьев. – М.: Ось-89, 2001. – 112 с.

191. Соловьев А.И. Экономическая безопасность хозяйствующего субъекта А.И. Соловьев // Конфидент. – 2002. – № 3. – С. 46-50.

192. Соложенцев Е.Д. Логико-вероятностная оценка банковских рисков и мошенничество в бизнесе / Е.Д. Соложенцев, В.В. Карасев, В.Е. Соложенцев. – СПб.: Политехника, 1996. – 59 с.

193. Структура та завдання служби інформаційної безпеки // Безопасность информационных технологий [Електронний ресурс]. – Режим доступу: http://www.security.ukrnet.net/modules/news/article.php?storyid=15

194. Судакова О.І., Гречко Д.В., Шкурупій А.В. Стратегія забезпечення належної економічної безпеки підприємства [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com4._SVMN_2007Economics18818.doc.htm.

195. Сухорукова Т.Г. Концептуальный взгляд на экономическую безопасность предприятия / Т.Г. Сухорукова // Залізничий транспорт України. – 1998. – № 2-3. – С. 9-12.

196. Сушкевич А.Н. Организация бухгалтерского учета в субъектах хозяйствования / А.Н. Сушкевич. – Мн.: Ред. журн. “Пром.-торговое право”, 2004. – 252 с.

197. Тамбовцев В.Л. Объекты экономической безопасности России / В.Л. Тамбовцев // Вопросы экономики. – 1994. – № 12. – С. 45-54.

198. Тамбовцев В.Л. Экономическая безопасность хозяйственных систем: структура, проблемы / В.Л. Тамбовцев // Вестник МГУ. Сер. 6. Экономика. – 1995. – № 3. – С. 3-9.

199. Тарас А.Е. Безопасность бизнесмена и бизнеса: [практ. пособ.] / А.Е. Тарас. – Мн.: “Сэкай”, 1996. – 180 с.

200. Уманец А. Вас учили не брать чужое? Нет? Это хорошо / А. Уманец // Бизнес. – 2003. – № 51. – С. 143-145.

201. Управління ресурсами підприємства: [навч. посіб.] / Під ред. к.е.н. Ю.М. Воробйова і д.е.н. Б.І. Холода. – К.: “Центр навчальної літератури”, 2004. – 288 с.

202. Цивільний кодекс України № 435-IV від 16.01.2003 р.: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=435-15.

203. Чеботарев И. Сокрытие информации / И. Чеботарев, В. Невзоров // Компьютер. – 2006. – № 5-6. – С. 50-52.

204. Чеботарь П. Концепция построения АИС на основе конфликта интересов: Conferinta internationala (editia a III-a) 14-15 aprrilie 2006 [Securitatea informationala 2006]. – Editura ASEM Chisinau 2006. – S. 52-54.

205. Шаваев А.Г. Безопасность банковских структур / А.Г. Шаваев // Экономика и жизнь. – 1994. – № 16.– С. 11-12.

206. Шаваев А.Г. Концептуальные основы обеспечения безопасности негосударственных объектов экономики / А.Г. Шаваев. – М.: Академия экономической безопасности, 1994. – 281 с.

207. Шаваев А.Г. Криминологическая безопасность негосударственных объектов экономики / А.Г. Шаваев. – М.: Инфра-М, 1995. – 126 с.

208. Шипка О. Комерційна таємниця: аспект захисту бізнесу / О. Шипка, О. Руденко, О. Солодухін // Все про бухгалтерський облік. – 1998. – № 64 (246). – С. 28-31.

209. Шлыков В.В. Экономическая безопасность предприятия (во что обходится хозяйствующим субъектам защита собственности и способы минимизации возможных потерь) / В.В. Шлыков// РИСК. – 1997. – № 6. – С. 61-63.

210. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия / В.В. Шлыков. – СПб.: "Алетейя", 1999. – 138 с.

211. Шлыков В.В. Экономическая безопасность предприятия (факторы влияния, анализ необходимости) / В.В. Шлыков // Машиностроитель. – 1995. – № 1. – С. 31-34.

212. Экономика и организация безопасности хозяйствующих субъектов: [2-е изд] / В.С. Гусев, В.А. Демин, Б.И. Кузин, М.Д. Медников, А.С. Соколицын, С.В. Степашин, А.В. Федотов, В.Л. Шульц. – СПб.: Питер, 2004. – 288 с.

213. Экономическая безопасность. Производство, финансы, банки. – М.: ЗАО "Финстатинформ", 1998. – 621 с.

214. Экономическая и национальная безопасность: [учеб.] / Под ред. Е.А. Олейникова. – М.: Экзамен, 2005. – 768 с.

215. Ярочкин В.И. Аудит безопасности фирмы: теория и практика: [учеб. пособ. для студентов высших учебных заведений] / В.И. Ярочкин, Я.В. Бузанова. – М.: Академический Проект; Королев: Парадигма, 2005. – 352 с.

216. Ярочкин В.И. Безопасность информационных систем / В.И. Ярочкин. – М. “Ось-89”, 1996. – 197 с.

217. Ярочкин В.И. Предприниматель и безопасность. Ч. 2 / В.И. Ярочкин. – М.: Экспертное бюро, 1994. – 132 с.

218. Ярочкин В.И. Система безопасности фирмы / В.И. Ярочкин. – М., 1997. – 185 с.

219. Arrow K. Essays in the theory of risk bearing / K. Arrow. – Chicago, 1971. – 278 p.

220. Idzikiewicz Z.A. Ochrona informacji w procesie przetwarzania. PWE / Z.A. Idzikiewicz. – Warszawa 1979.

221. Rapoport A. Mathematical Aspects of General Systems Analysis / A. Rapoport // General Systems. – 1966. – № 1. – p. 3-11.

222. Sokolowski A. Ochrona informacji komputerowych. Wyd. MON / A. Sokolowski. – Warszawa 1987.

Додаток А

Дефініції поняття "економічна безпека підприємства"

№ з/п	*Автор (джерело)*	*Визначення*
1	*2*	*3*
1	Азарова А.О., Гаврилова О.В. [173]	Економічна безпека підприємства – система заходів, що забезпечують конкурентоспроможність і економічну стабільність підприємства, а також сприяють підвищенню рівня добробуту працівника.
2	Алексеенко В., Сокольський Б. [174]	Економічна безпека підприємства – забезпечення умов збереження комерційної таємниці і інших секретів підприємства
3	Белов В., Полянский А. [175]	Економічна безпека підприємства – забезпечення умов збереження комерційної таємниці і інших секретів підприємства
4	Гавриш В.А. [176]	Економічна безпека підприємства – забезпечення умов збереження комерційної таємниці і інших секретів підприємства
5	Дарнопих Г. [177]	Економічна безпека підприємства – це стан, який забезпечує економічний суверенітет, економічне зростання, підвищення добробуту в умовах економічної залежності
6	Деружинский В.А., Деружинский В.В. [178]	Економічна безпека підприємства – забезпечення умов збереження комерційної таємниці і інших секретів підприємства
7	Забродський В., Капустін Н. [179]	Економічна безпека підприємства – це кількісна і якісна характеристика властивостей фірми, що відображає здатність "самовиживання" і розвитку в умовах виникнення зовнішньої і внутрішньої економічної загрози; економічна безпека фірми визначається, як сукупність чинників, які забезпечують незалежність, стійкість, здатність до прогресу в умовах дестабілізуючих факторів, забезпечення економічних інтересів і т.д.
8	Капустін Н. [180]	Економічна безпека підприємства – це кількісна та якісна характеристика економічних властивостей системи з точки зору її здатності до самовиживання та розвитку в умовах дестабілізуючої дії непередбачуваних та важкопрогнозованих зовнішніх та внутрішніх факторів

[173] Азарова А.О. Розробка методики визначення економічної безпеки підприємства / А.О. Азарова, О.В. Гаврилова // Економіка: проблеми теорії та практики. Збірник наукових праць. Випуск 191: В 4 т. Том III. – Дніпрпетровськ: ДНУ, 2004. – 318 с.

[174] Алексеенко В. Система защиты коммерческих объектов / В. Алексеенко, Б. Сокольский. – М., 1992. – 195 с.

[175] Белов В.Г. Правовая охрана конфиденциальности коммерческой тайны / В. Белов, А. Полянский // Право и экономика. – 1993. – № 13-14. – С. 12-21.

[176] Гавриш В.А. Практическое пособие по защите коммерческой тайны / В.А. Гавриш. – Симферополь, 1994. – 153 с.

[177] Дарнопих Г. Сучасні проблеми економічної безпеки України / Г. Дарнопих // Вісник Академії правових наук України. – 1998. – № 1. – С. 142-150.

[178] Деружинский В.А. Основы коммерческой тайны: [Практ. пособ. для предпринимателя] / В.А. Деружинский, В.В. Деружинский. – Мн.: ООО "Полирек", 1994. – 214 с.

[179] Забродский В. Теоретические основы оценки экономической безопасности отрасли и фирмы / В. Забродский, Н. Капустин // Бизнес-информ. – 1999. – № 15-16. – С. 35-37.

[180] Капустин Н. Экономическая безопасность отрасли и фирмы / Н. Капустин // Бизнес-информ. – 1999. – № 11-12. – С. 45-47.

Продовження Додатку А

1	*2*	*3*
9	Ковальов Д., Сухорукова Т. [181]	Економічна безпека підприємства – це захищеність його діяльності від негативного впливу зовнішнього оточення, а також здатність своєчасно усунути різноманітні загрози або пристосуватися до існуючих умов, які не відбиваються негативно на його діяльності
10	Олейніков Е. [182]	Економічна безпека підприємства – стан найбільш ефективного використання корпоративних ресурсів для запобігання загрозам і забезпеченню стабільного функціонування підприємства в даний час і в майбутньому
11	Плетнікова І.П. [183]	Економічна безпека підприємства – стан найефективнішого використання корпоративних ресурсів для уникнення загроз та забезпечення стабільного функціонування підприємства як в даний час, так і в майбутньому
12	Соколов Я.В. [184]	Економічна безпека підприємства – забезпечення умов збереження комерційної таємниці і інших секретів підприємства
13	Тамбовцев В.Л. [185]	Економічна безпека підприємства – це стан підприємства, яке означає, що ймовірність небажаної зміни яких-небудь якостей, параметрів майна, що належить йому, і що зачіпає його зовнішнього середовища невелика (менше певної межі)
14	Шликов В.В. [186]	Економічна безпека підприємства – стан захищеності життєво важливих інтересів підприємства від реальних і потенційних джерел небезпеки або економічних погроз

[181] Ковалев Д. Экономическая безопасность предприятия Д. Ковалев, Т. Сухорукова // Экономика Украины. – 1998. – № 10. – С. 48-52.

[182] Основы экономической безопасности (Государство, регион, предприятие, личность) / Под ред. Е.А. Олейникова. – М.: ЗАО "Бизнес-школа "Интел-синтез", 1997. – 228 с.

[183] Плетникова И.П. Определение уровня и планирование ЭБП / И.П. Плетникова // Вісник Технологічного університету Поділля. – 2000. – № 4 (Ч.2). – С. 100-108.

[184] Соколов Я.В. Бухгалтерский учет: от истоков до наших дней: [Учебн. пособие для вузов] / Я.В. Соколов. – М.: Аудит, ЮНИТИ, 1996. – 638 с.

[185] Тамбовцев В.Л. Объекты экономической безопасности России / В.Л. Тамбовцев // Вопросы экономики. – 1994. – № 12. – С. 45-54.

[186] Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия / В.В. Шлыков. – СПб.: "Алетейя", 1999. – 138 с.

Додаток Б

Складові концепції економічної безпеки підприємств

№ з/п	*Складові концепції*	*Характеристика складових концепції*
1	*2*	*3*
1	Поняття економічної безпеки	Економічна безпека підприємницької сфери – це поєднання економічних та правових умов, які забезпечують стійке здійснення фактів господарської діяльності в тривалій перспективі законними та ефективними методами
2	Зміст економічної безпеки	Процес, що визначає відсутність загрози достовірності, ефективності та законності використання трудових, фінансових, виробничих, земельних та підприємницьких ресурсів
3	Суть економічної безпеки	Суть економічної безпеки підприємницької сфери полягає в збалансованому протіканні фактів господарської діяльності при ефективному та законному використанні економічних ресурсів, із здійсненням обліку, аналізу і контролю з метою запобігання загрозам і забезпеченню стабільного функціонування підприємств молочної промисловості
4	Мета та завдання економічної безпеки	Встановлюються керівниками та власниками підприємств. Мета полягає у забезпеченні збалансованого стану здійснення фактів господарської діяльності при ефективному та законному використанні економічних ресурсів, на рівні системи управління, яке досягається вирішенням завдань. Завдання економічної безпеки підприємств молочної промисловості: 1) розробка внутрішніх регламентів підприємствами молочної промисловості в частині забезпечення економічної безпеки; 2) складання реєстру нормативно-правового регулювання в сфері господарської діяльності підприємств молочної промисловості; 3) визначення загроз здійснення актів незаконного втручання; 4) оцінка вразливості підприємницької діяльності; 5) розробка та реалізація вимог із забезпечення економічної безпеки підприємств молочної промисловості; 6) розробка та реалізація заходів із забезпечення економічної безпеки підприємств молочної промисловості; 7) здійснення обліку (бухгалтерського, податкового, управлінського); 8) проведення комплексного економічного аналізу; 9) здійснення внутрішнього контролю та нагляду в сфері забезпечення економічної безпеки підприємств молочної промисловості; 10) інформаційне, матеріально-технічне та науково-технічне забезпечення економічної безпеки підприємств молочної промисловості

Продовження Додатку Б

1	*2*	*3*
5	Принципи економічної безпеки	1. Пильність. 2. Законність фактів підприємницького діяльності. 3. Дотримання балансу життєво важливих циклів здійснення підприємницької діяльності (облік, аналіз, контроль). 4. Взаємна відповідальність учасників підприємницької діяльності 5. Безперервність здійснення заходів із забезпечення економічної безпеки підприємств молочної промисловості. 6. Ефективність заходів із забезпечення економічної безпеки підприємств молочної промисловості
6	Система економічної безпеки	Вплив в межах одного будь-якого явища або ситуації призводить до впливу на пов'язані з ними явища або ситуації. 1. Суб'єкт економічної безпеки – підприємці, власники бізнесу, управлінський персонал. 2. Об'єкт економічної безпеки – певний суб'єкт господарювання. 3. Предмет – факти господарської діяльності життя (підприємницькі зобов'язання). 4. Облік (бухгалтерський (фінансовий), податковий, управлінський) фактів господарської діяльності. 5. Комплексний економічний аналіз підприємницького задуму та фактів господарського життя. 6. Внутрішній контроль фактів господарської діяльності. 7. Поле підприємницької діяльності підприємств молочної промисловості: факти господарської діяльності; облік; комплексний економічний аналіз; внутрішній контроль
7	Функції системи економічної безпеки	1. Забезпечення економічної безпеки в підприємницькій сфері підприємств молочної промисловості. 2. Вживання заходів із захисту підприємницьких інтересів від актів незаконного втручання; 3. Оцінка законності фактів господарської діяльності підприємств. 4. Безперервність та достовірність ведення бухгалтерського обліку (фінансового, податкового, управлінського). 5. Проведення комплексного економічного аналізу. 6. Організація ефективної системи внутрішнього контролю
8	Оцінка надійності та ефективності системи економічної безпеки	1. Визначення структури негативного впливу на економічну безпеку підприємств молочної промисловості, поділ об'єктивного та суб'єктивного впливу. 2. Формування переліку заходів для усунення впливу негативних дій та оцінка їх ефективності. 3. Визначення причин недостатньої ефективності заходів. 6. Вироблення рекомендацій із усунення та попередження можливого негативного впливу. 8. Оцінка вартості заходів із усунення негативного впливу та визначення виконавців, відповідальних за реалізацію пропонованих заходів

Додаток В

ПЕРЕЛІК
відомостей, що не становлять комерційної таємниці

1. Установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами.
2. Інформація за всіма встановленими формами державної звітності.
3. Дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів.
4. Відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць.
5. Документи про сплату податків і обов'язкових платежів.
6. Інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків.
7. Документи про платоспроможність.
8. Відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю.
9. Відомості, що відповідно до чинного законодавства підлягають оголошенню.

Додаток Д

Організація доступу до відомостей, які складають комерційну таємницю підприємства

№ з/п	*Посада*	*Перелік інформації, до якої дозволяється надавати допуск*	*Категорії користувачів*	*Підстава допуску*
1	*2*	*3*	*4*	*5*
1.	Генеральний директор, голова правління	До всіх відомостей, які складають комерційну таємницю підприємства	1. Заступник генерального директора, головний інженер заводу, директор виробництв, начальник управлінь	1. Наказ про призначення на посаду; 2. “Дозвіл на надання допуску…”
			2. Відряджені спеціалісти інших підприємств	Згода (договір) на проведення спільних робіт
2.	Заступник генерального директора з економічних питань, Керівник експертної комісії із захисту інформації	До всіх відомостей, які складають комерційну таємницю підприємства	1. Заступники генерального директора, директора виробництв, начальники управлінь, цехів та відділів	1. Наказ про призначення на посаду (для керівників структурних підрозділів); 2. “Дозвіл на надання допуску…”
			2. Відряджені спеціалісти інших підприємств	Згода (договір)на проведення спільних робіт
3.	Головний інженер, власник бізнес-процесів: “1.1. Створення нових видів продукції, управління інвестиціями в НДВКР, післяпродажне обслуговування”, “1.2. Технічна підготовка виробництва”, “2.1. Управління якістю”, “2.2. Управління техпереоснащенням”; “3.8. Забезпечення охорони праці та навколишнього середовища”	До всіх відомостей, які складають комерційну таємницю підприємства та відносяться до бізнес-процесів: “1.1. Створення нових видів продукції, управління інвестиціями в НДВКР, післяпродажне обслуговування” “1.2. Технічна підготовка виробництва”, “2.1. Управління якістю”; “2.2. Управління техпереоснащенням”; “3.8. Забезпечення охорони праці та навколишнього середовища”	Всі працівники підприємства	1. Наказ про призначення на посаду (для керівників структурних підрозділів); 2. “Дозвіл на надання допуску…”

Продовження Додатку Д

1	*2*	*3*	*4*	*5*
4	Заст. генерального директора з виробництва, власник бізнес-процесу "Виробництво продукції"	До всіх відомостей, які складають комерційну таємницю підприємства та відносяться до бізнес-процесу "1.3. Виробництво продукції"	Всі працівники виробництва	1. Наказ про призначення на посаду (для керівників структурних підрозділів); 2. "Дозвіл на надання допуску…"
5	Заст. генерального директора з фінансів та збуту – власник бізнес-процесів "2.6. Управління маркетингом, фінансами, поставками", "2.9. Управління персоналом", "3.1. Забезпечення матеріальними ресурсами, комерційна діяльність", "3.2. Забезпечення економічної безпеки"	До всіх відомостей, які складають комерційну таємницю та відносяться до бізнес-процесів: "2.6. Управління маркетингом, фінансами, поставками"; "2.9. Управління персоналом"; "3.1. Забезпечення матеріальними ресурсами, комерційна діяльність"; "3.2. Забезпечення економічної безпеки"	Всі працівники підприємства	1. Наказ про призначення на посаду (для керівників структурних підрозділів); 2. "Дозвіл на надання допуску…"
6.	Заст. генерального директора з комерційних питань – власник бізнес-процесу "3.1. Забезпечення матеріальними ресурсами, комерційна діяльність"	До всіх відомостей, які складають комерційну таємницю підприємства та відносяться до бізнес-процесу "3.1. Забезпечення матеріальними ресурсами, комерційна діяльність"	Всі працівники підприємства	1. Наказ про призначення на посаду (для керівників структурних підрозділів); 2. "Дозвіл на надання допуску…"
7.	Заст. генерального директора з реконструкції та кап. будівництва – Власник бізнес-процесу "2.2. Управління техпереоснащенням"	До всіх відомостей, які складають комерційну таємницю підприємства та відносяться до бізнес-процесу "2.2. Управління техпереоснащенням"	Всі працівники підприємства	1. Наказ про призначення на посаду (для керівників структурних підрозділів); 2. "Дозвіл на надання допуску…"
8.	Головний бухгалтер – власник бізнес-процесів "2.7. Бухгалтерський, податковий облік", "2.8. Управлінський облік"	До всіх відомостей, які складають комерційну таємницю та відносяться до бізнес-процесів: "2.7. Бухгалтерський, податковий облік", "2.8. Управлінський облік"	Всі працівники підприємства	1. Наказ про призначення на посаду (для керівників структурних підрозділів); 2. "Дозвіл на надання допуску…"

Продовження Додатку Д

1	*2*	*3*	*4*	*5*
9.	Заст. головного інженера з АСУ – власник бізнес-процесу “3.3. Формування та обслуговування інфраструктури інформаційного забезпечення”	До всіх відомостей, які складають комерційну таємницю підприємства та відносяться до бізнес-процесу “3.3. Формування та обслуговування інфраструктури інформаційного забезпечення”	Всі працівники підприємства	1. Наказ про призначення на посаду (для керівників структурних підрозділів); 2. “Дозвіл на надання допуску…”
10.	Заст. головного інженера з підготовки виробництва – власник бізнес-процесу “3.6. Забезпечення інструментами”	До всіх відомостей, які складають комерційну таємницю підприємства та відносяться до бізнес-процесу “3.6. Забезпечення інструментами”	Всі працівники підприємства	1. Наказ про призначення на посаду (для керівників структурних підрозділів); 2. “Дозвіл на надання допуску…”
11.	Заст. головного інженера з обладнання, власник бізнес-процесів “3.4. Забезпечення енергоресурсами”, “3.6. Обслуговування і ремонт обладнання”	До всіх відомостей, які складають комерційну таємницю підприємства та відносяться до бізнес-процесу “3.6. Забезпечення і ремонт обладнання”	Всі працівники підприємства	1. Наказ про призначення на посаду (для керівників структурних підрозділів); 2. “Дозвіл на надання допуску…”

Додаток Ж

ПІДПРИЄМСТВО
"_____"

ДОГОВІРНЕ ЗОБОВ'ЯЗАННЯ

про нерозголошення відомостей, які складають комерційну таємницю підприємства

Я, _____ особистий № _____, що
(прізвище, ім'я, по батькові)

працюю в підрозділі _____ на посаді _____
(цех, відділ) ***(посада)***

зобов'язуюсь:

1. Не розголошувати інформацію, яка складає комерційну таємницю _____, яка буде мені довірена або стане відомою при
(назва підприємства)
виконанні службових обов'язків.

2. Не передавати третім особам і не розкривати публічно інформацію, яка становить комерційну таємницю _____, без письмової вказівки
(назва підприємства)
керівника підрозділу.

3. Виконувати вимоги наказів, що стосуються мене, розпоряджень, положень і інструкцій із забезпечення збереження відомостей, які складають комерційну таємницю підприємства.

4. Виконувати роботу на ПК і в корпоративній мережі в рамках встановлених прав доступу.

5. В разі спроб сторонніх осіб отримати від мене відомості, які складають комерційну таємницю підприємства, негайно повідомити керівникові підрозділи і в службу захисту інформації.

6. Не використовувати знання відомостей, які складають комерційну таємницю підприємства, для заняття будь-якою діяльністю, яка як конкурентна дія може завдати збитку _____.
(назва підприємства)

7. На випадок мого звільнення всі носії відомостей, які складають комерційну таємницю підприємства (рукописи, креслення, чернетки,

дискети, роздруківки, моделі тощо), які знаходилися в моєму розпорядженні у зв'язку з виконанням мною службових обов'язків, здати співробітникові відповідальному за облік і зберігання матеріальних носіїв відомостей, які складають комерційну таємницю.

8. Про витік, порушення цілісності (спотворення, модифікація, руйнування, знищення) відомостей, які складають комерційну таємницю підприємства, негайно повідомити керівникові підрозділу і в службу захисту інформації.

До мого відома доведені вимоги нормативних документів з нерозголошення відомостей, які складають комерційну таємницю підприємства.

Мені відомо, що порушення цих положень передбачає дисциплінарну, кримінальну відповідальність відповідно до чинного законодавства України.

_____

"_____" _____ 200_ р. (підпис)

Адміністрація підприємства підтверджує, що дане Вами зобов'язання не обмежує Ваших прав на інтелектуальну власність.

Начальник відділу кадрів _____ _____

(підпис) (ПІБ)

ВИПИСКА

із законів і нормативних актів України
зі зберігання відомостей, які складають комерційну таємницю.

1. З Цивільного кодексу України

Стаття 505. Поняття комерційної таємниці

1. Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

2. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

2. З Кримінального Кодексу України

Стаття 231. "Незаконне збирання з метою використання відомостей, що становлять комерційну таємницю"

"Умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, – карається штрафом від 200 до 1000 неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до п'яти років, або позбавленням волі на строк до трьох років".

Стаття 232. "Розголошення комерційної таємниці"

"Умисне розголошення комерційної таємниці без згоди її власника, особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдавало істотної шкоди суб'єкту господарської діяльності, – карається штрафом від 200 до 500 неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3-х років, або виправними роботами на строк до 2-х років, або позбавленням волі на той самий термін".

Додаток З

ПЕРЕЛІК

відомостей, що становлять комерційну таємницю підприємств

Управління:

– відомості про перспективні методи управління виробництвом.

Виробництво:

– організаційна структура підприємства;
– характер виробництва;
– організація праці на підприємстві;
– відомості про виробничі можливості підприємства;
– характеристика виробництва: дані про резерви сировини на підприємстві; відомості про фонди окремих товарів, у тому числі тих, що виділяються для поставок на експорт.

Плани:

– плани розвитку підприємства;
– відомості про плани підприємства з розширення виробництва;
– інвестиційні програми, техніко-економічні обґрунтування, плани інвестицій;
– планово-аналітичні матеріали за поточний період;
– обсяг майбутніх закупок за строками, асортиментом, цінами, країнами, фірмами;
– зведені відомості про ефективність експорту або імпорту товарів в цілому по зовнішньоекономічній діяльності.

Фінанси:

– бюджет;
– обороти;
– банківські операції;
– банківські зв'язки;
– планові та звітні дані по валютних операціях;
– рівень доходів;
– розміри і умови банківських і інших кредитів;
– відомості про розміри запланованого кредитування.

Партнери:

– характеристика клієнтури;
– дані представників, посередників, дилерів і партнерів;
– дані про покупців і споживачів (оптових і роздрібних);
– відомості про склад торгових та інших клієнтів, представників і посередників;
– негласні компаньйони товариств;
– комерційні зв'язки;
– місця закупки товарів;
– відомості щодо іноземних комерційних партнерах;
– зведення і характеристика підприємств – торгових партнерів (основні виробничі фонди, кредити, товарообіг);
– дані на клієнтів у торгівлі й рекламі;
– відомості про фінансовий стан, репутацію та інші дані, що характеризують ступінь надійності фірми або її представників.

Контракти:

– умови за контрактами, угодами – як укладеними, так і плановаными (строки, обсяги, номенклатура, умови поставки);
– особливі умови контрактів (знижки, доплати, розстрочення платежів, опціони);
– умови платежів за контрактами (ціни, знижки, доплати, розстрочення платежів, опціони);
– особливі угоди і умови компенсаційних угод;
– відомості про виконання контрактів;
– відомості про номенклатуру і кількість товарів за взаємними зобов'язаннями, передбаченими угодами, протоколами, а також про товарообіг;
– відомості про авторські договори.

Оплата праці:

– умови укладень контрактів між адміністрацією підприємства і працівниками;
– відомості про авторські винагороди і гонорари

Додаток И

ПІДПРИЄМСТВО

"_____"

Н А К А З

"__" _____ 200_ р. № _____

Про захист інформації, що становить комерційну таємницю підприємства

Комп'ютеризація бізнес-процесів і розвиток телекомунікацій надали фахівцям підприємства можливості автоматизованого доступу до різної інформації, у тому числі й до відомостей, які складають комерційну таємницю (КТ) підприємства.

Для забезпечення захисту інформації, яка складає КТ підприємства, розроблена і поетапно впроваджена система доступу / допуску, що передбачає обмеження права користування інформацією і носіями інформації; сформований і підтримується в актуальному стані Перелік відомостей, які складають КТ підприємства, допуск до яких здійснюється власниками бізнес-процесів лише на підставі оформлених дозволів і договірних зобов'язань про нерозголошення даних, які є об'єктами комерційної таємниці і стали доступними користувачам; організація роботи з документарними ресурсами, які складають КТ, в структурних підрозділах покладена на спеціально призначених співробітників і адміністраторів комп'ютерних систем. Для забезпечення збереження документів з грифом "Комерційна таємниця", запобігання їх розкраданню або знищенню запроваджений спеціальний порядок їх обліку, зберігання, використання і знищення.

Приміщення із встановленою обчислювальною і розмножувальною технікою в обов'язковому порядку обладналися охоронно-пожежними системами. Процес навчання співробітників підприємства правилам захисту інформації здійснюється у міру регулярного оновлення і видозміни форм і методів захисту інформації.

Контроль виконання норм і вимог захисту інформації, який проводиться заводською експертною комісією, показує, що в структурних підрозділах в основному виконуються встановлені режимні заходи зі збереження відомостей, які складають комерційну таємницю підприємства.

З метою дотримання економічної безпеки, неухильного виконання вимог партнерів з дотримання конфіденційності, підвищення персональної відповідальності працівників підприємства за збереження інформації, яка складає комерційну таємницю підприємства.

НАКАЗУЮ:

1. Затвердити і ввести в дію з дати підписання даного наказу “Перелік відомостей, які складають комерційну таємницю підприємства”, “Політику економічної безпеки підприємства”.

2. Директорам виробництв, начальникам управлінь, цехів, відділів прийняти до відома та неухильного виконання затверджені нормативні документи з економічної безпеки підприємства.

3. В термін до _____ 20__ р. експертній комісії підприємства із захисту інформації направити в структурні підрозділи виписки з “Переліку відомостей, які складають комерційну таємницю підприємства”.

4. Керівникам структурних підрозділів ознайомити під розпис всіх співробітників, які мають доступ до інформації, яка складає комерційну таємницю підприємства, з вимогами “Політики економічної безпеки підприємства”. Реєстр ознайомлення співробітників в термін до _____ 20_ р. надати до експертної комісії із захисту інформації.

5. Контроль за виконанням даного наказу покласти на заступників генерального директора та голову експертної комісії підприємства із захисту інформації.

Голова правління _____ _____
(підпис) (ПІБ)

Генеральний директор_____ _____
(підпис) (ПІБ)

Додаток К

ЗОБОВ'ЯЗАННЯ
про нерозголошення комерційної таємниці підприємства

01.01.20__ р.

Я, _____

(прізвище, ім'я, по батькові)

як працівник _____

(найменування підприємства)

в період трудових (службових) відносин з підприємством (його правонаступником) та протягом _____ після їх закінчення зобов'язуюся:

– не розголошувати дані, що становлять комерційну таємницю підприємства, які мені будуть довірені або стануть відомі в роботі (службі);

– не передавати третім особам та не розкривати публічно відомості, що становлять комерційну таємницю підприємства, без згоди підприємства;

– виконувати вимоги наказів та інструкцій, що стосуються мене щодо забезпечення збереження комерційної таємниці підприємства;

– у разі спроби сторонніх осіб одержувати від мене відомості про комерційну таємницю підприємства негайно повідомити про це _____

(посадова особа або підрозділ підприємства)

– зберігати комерційну таємницю тих підприємств, з якими є ділові відносини підприємства;

– не використовувати знання комерційної таємниці підприємства для занять будь-якою діяльністю, яка як конкурентна дія може завдати збитку підприємству;

– у разі мого звільнення всі носії комерційної таємниці підприємства (рукописи, чернетки, креслення, дискети, роздруки на принтерах, кіно-, фото- аудіо-, відео- матеріали, моделі, вироби тощо), які знаходилися в моєму розпорядженні у зв'язку з виконанням мною службових обов'язків під час роботи на підприємстві, передати _____;

(посадова особа або підрозділ підприємства)

– про втрату або недостачу носіїв комерційної таємниці, посвідчень, пропусків, ключів від режимних приміщень, сховищ, сейфів (металевих шаф), особистого печаток та про інші факти, які можуть призвести до розголошення комерційної таємниці підприємства, а також про причини та умови можливого витоку відомостей, негайно повідомляти

_____

(посадова особа або підрозділ підприємства)

До мого відома доведено з роз'ясненнями відповідні положення щодо забезпечення збереження комерційної таємниці підприємства.

Мені відомо, що порушення цих положень може спричинити кримінальну, адміністративну, цивільно-правову або іншу відповідальність відповідно до законодавства у вигляді позбавлення волі, грошового штрафу, зобов'язання щодо відшкодування збитку підприємству (збитків, упущеної вигоди та моральної шкоди) та інших покарань.

_____	_____	_____
Посада	Підпис	ПІБ

Додаток Л

ПОСАДОВА ІНСТРУКЦІЯ ГОЛОВНОГО БУХГАЛТЕРА

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Дана інструкція розроблена згідно наказу керівника підприємства від "__" _____ 20__ р. № _____.

1.2. Начальник бухгалтерської групи – головний бухгалтер (далі – начальник групи) відноситься до категорії керівників підрозділів фінансового відділу.

1.3. Кваліфікаційні вимоги: вища професійна (економічна) освіта і стаж роботи на посаді бухгалтера I категорії не менше 3 років.

1.4. Начальник групи призначається на посаду і звільняється з посади розпорядженням головного бухгалтера за наявністю атестаційної комісії підприємства.

1.5. У своїй роботі начальник групи повинен керуватися:

1.5.1. Даною посадовою інструкцією.

1.5.2. Інструкцією про фінансове забезпечення діяльності підприємства.

1.5.3. Положенням про фінансовий відділ.

1.5.4. Регламентом роботи групи.

1.6. Начальник групи повинен знати:

1.6.1. Законодавчі та нормативні правові акти, постанови, накази та рішення регіональних і місцевих органів державної влади та управління, а також нормативно-методичні документи інших органів управління (влади), що регламентують організацію фінансової роботи на підприємстві, здійснення ним фінансово-економічної та виробничо-господарської діяльності (за напрямом роботи групи).

1.6.2. Цілі, стратегію розвитку і бізнес-план підприємства.

1.6.3. Профіль, спеціалізацію та організаційну структуру підприємства.

1.6.4. Теоретичні основи фінансового менеджменту.

1.6.5. Фінансову політику підприємства та стратегії її реалізації.

1.6.6. Технологію управління фінансовими ресурсами, систему фінансових методів, що забезпечують найбільш ефективне управління фінансовими потоками.

1.6.7. План і кореспонденцію рахунків.

1.6.8. Організацію документообігу за ділянками бухгалтерського обліку.

1.6.9. Порядок документального оформлення і відображення на рахунках бухгалтерського обліку операцій, пов'язаних з рухом основних засобів, товарно-матеріальних цінностей і грошових коштів.

1.6.10. Методи економічного аналізу господарсько-фінансової діяльності підприємства.

1.6.11. Порядок складання фінансових планів, прогнозних балансів і бюджетів грошових коштів, планів реалізації продукції (робіт, послуг), планів з прибутку (за напрямом групи).

1.6.12. Стандарти фінансового обліку і звітності, бухгалтерський облік.

1.6.13. Засоби обчислювальної техніки, комунікацій і зв'язки, які використовуються у фінансовій роботі.

1.6.14. Правила і норми охорони праці.

1.7. Начальник групи повинен мати уміння і навики, достатні для ефективного виконання посадових обов'язків, зокрема: _____.

(зазначити найбільш важливі)

1.8. Начальник групи підпорядковується начальнику фінансового відділу.

1.9. Начальникові групи підпорядковуються всі працівники даної групи.

1.10. На час відсутності начальника групи його замінює бухгалтер.

2. ОБОВ'ЯЗКИ

2.1. Начальник групи зобов'язаний:

2.1.1. Керувати відповідно до чинного законодавства і внутрішніх актів підприємства роботою групи, несучи відповідальність за наслідки ухвалених рішень.

2.1.2. Організовувати роботу групи, спрямовувати її зусилля на розвиток і вдосконалення фінансової роботи (за відповідним напрямом), повне і якісне виконання відділом завдань за призначенням.

2.1.3. Забезпечувати дієвий контроль за дотриманням працівниками групи законодавчих і інших нормативних правових актів, локальних актів підприємства, наказів директора і розпоряджень головного бухгалтера з питань фінансової роботи.

2.1.4. Організовувати роботу групи на основі широкого використання новітньої техніки і технології, прогресивних методів і прийомів її здійснення, науково обґрунтованих нормативів матеріальних, фінансових і трудових витрат, передового досвіду в галузі фінансового менеджменту.

2.1.5. За вказівці начальника відділу брати участь в підготовці матеріалів, необхідних для розробки і подальшого уточнення програми

перспективного розвитку підприємства, а також в розробці фінансової політики підприємства і визначенні (уточненні) його фінансової стратегії на майбутній період.

2.1.6. Проводити щомісячний аналіз стану роботи групи, на основі результатів аналізу готувати пропозиції з її вдосконаленню, надавати пропозиції на розгляд начальника відділу.

2.1.7. Брати участь в розробці проектів планів роботи відділу, керувати розробкою проекту плану роботи групи, своєчасно надавати його на розгляд начальника відділу.

2.1.8.Приймати вичерпні заходи, спрямовані на підготовку обґрунтованих рішень з питань роботи групи.

2.1.9. Самостійно, в межах наданих йому головним бухгалтером повноважень і у взаємодії з начальниками інших підрозділів відділу вирішувати питання фінансової роботи, покладені на групу.

2.1.10. Керувати роботою з ведення бухгалтерського обліку майна, зобов'язань і господарських операцій (облік основних засобів, товарно-матеріальних цінностей, витрат на виробництво, реалізації продукції, результатів господарсько-фінансової діяльності, розрахунки з постачальниками і замовниками, а також за надані послуги тощо).

2.1.11.Організовувати розробку і здійснення працівниками групи заходів, спрямованих на дотримання фінансової дисципліни і раціональне використання ресурсів.

2.1.12. Здійснювати контроль за розробкою первинної документації (за напрямом групи) і її підготовкою до облікової обробки.

2.1.13. Забезпечувати належне відображення на рахунках бухгалтерського обліку операцій руху основних засобів (товарно-матеріальних цінностей, грошових коштів і ін.).

2.1.14. Перевіряти звітні калькуляції собівартості продукції (робіт, послуг), виявляти джерела утворення втрат і непродуктивних витрат, готувати пропозиції з їх попередження.

2.1.15. Забезпечувати своєчасне і повне нарахування і перерахунок податків і зборів до федерального, регіонального і місцевого бюджетів, страхових внесків до державних позабюджетних соціальних фондів, платежів до банківських установ, засобів на фінансування капітальних вкладень, заробітної плати працівників і службовців, інших виплат і платежів, а також відрахування засобів на матеріальне стимулювання працівників підприємства.

2.1.16. Брати участь в розробці робочого плану рахунків, форм первинних документів, які використовуються для оформлення

господарських операцій, по яких не передбачені типові форми, форм документів для внутрішньої бухгалтерської звітності, а також у визначенні змісту основних прийомів і методів ведення обліку і технології обробки бухгалтерської інформації.

2.1.17. Організовувати проведення працівниками групи економічного аналізу господарсько-фінансової діяльності підприємства за даними бухгалтерського обліку і звітності з метою виявлення внутрішньогосподарських резервів, здійснення режиму економії і заходів щодо вдосконалення документообігу, розробки і впровадження прогресивних форм і методів бухгалтерського обліку.

2.1.18. Збирати дані (за напрямом групи) для складання звітності, стежити за збереженням бухгалтерських документів, забезпечувати їх оформлення відповідно до встановленого порядку для передачі в архів.

2.1.19. Здійснювати контроль за виконанням працівниками групи робіт з формування, ведення і зберігання бази даних бухгалтерської інформації.

2.1.20. Підтримувати взаємодію з колегами по відділу на користь забезпечення максимальної ефективності його діяльності.

2.1.21. Створювати підлеглим умови для високоефективної роботи.

2.1.22. Постійно підвищувати свій професійний рівень в системі корпоративного тренінгу.

2.1.23. Консультувати начальника відділу з питань фінансової роботи (за напрямом роботи групи).

2.1.24. Забезпечувати якісну підготовку і своєчасне надання начальнику відділу довідкових і звітних матеріалів з питань роботи групи.

3. ПРАВА

3.1. Начальник групи має право:

3.1.1. Ухвалювати обґрунтовані рішення з питань роботи групи – в межах компетенції, наданої відповідно до розпорядження головного бухгалтера.

3.1.2. Давати працівникам групи вказівки і доручення з питань фінансової роботи, вимагати їх своєчасного, повного і якісного виконання.

3.1.3. Брати участь в підготовці проектів розпоряджень (наказів) з питань фінансової роботи.

3.1.4. Підписувати службові (ділові) документи з питань роботи групи.

3.1.5. Звертатися до начальника відділу з пропозиціями, спрямованими на вдосконалення роботи групи і діяльності фінансового відділу.

3.1.6. Брати участь в протокольних заходах, на яких розглядаються питання його роботи, а також питання роботи групи.

3.1.7. Вимагати від працівників групи своєчасного, повного і якісного надання достовірній інформації, зокрема документованою.

3.1.8. Забезпечувати надання зацікавленим особам (органам) інформації про стан роботи групи, зокрема документованою, в порядку, передбаченому законодавством і локальними актами підприємства.

3.1.9. Надавати начальникові відділу свої пропозиції із застосування відносно працівників групи заходів заохочення і покарання, передбачених законодавством і локальними актами підприємства, у зв'язку з належним (неналежним) виконанням ними вимог і правил фінансової роботи.

4. ВЗАЄМОДІЯ ЗА ПОСАДОЮ

4.1. Начальник групи здійснює організаційно-інформаційну взаємодію:

4.1.1. З начальником відділу – з питань роботи відділу.

4.1.2. З начальниками підрозділів (груп) фінансового відділу – з питань взаємодії з відповідними групами.

4.1.3. З посадовими особами (підрозділами) фінансових відділів (інших аналогічних структур) інших підприємств, організацій і установ – з питань, які представляють взаємний інтерес для підприємства і сторонніх підприємств (організацій, установ).

5. ВІДПОВІДАЛЬНІСТЬ

5.1. Начальник групи несе відповідальність за:

5.1.1. Порушення положень керівних документів з питань фінансової роботи.

5.1.2. Невиконання наказів директора, рішень начальника фінансового відділу.

5.1.3. Розголошення відомостей, які складають комерційну таємницю підприємства.

5.1.4. Неправомірне використання наданих повноважень, а також використання їх в особистих цілях.

Додаток М

ПОСАДОВА ІНСТРУКЦІЯ БУХГАЛТЕРА

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Дана інструкція розроблена згідно наказу керівника підприємства від “__” _____ 20__ р. № _____.

1.2. Бухгалтер відноситься до категорії фахівців.

1.3. Кваліфікаційні вимоги:

1.3.1. Бухгалтер I категорії: вища професійна (економічне) освіта і стаж роботи на посаді бухгалтера II категорії не менше 3 років.

1.3.2. Бухгалтер II категорії: вища професійна (економічне) освіта без пред’явлення вимог до стажу роботи або середня професійна (економічне) освіта і стаж роботи на посаді бухгалтера не менше 3 років.

1.3.3. Бухгалтер: середня професійна (економічне) освіта без пред’явлення вимог до стажу роботи або спеціальна підготовка за встановленою програмою і стаж роботи з обліку і контролю не менше 3 років.

1.4. Бухгалтер призначається на посаду і звільняється з посади розпорядженням головного бухгалтера за уявленням атестаційної комісії.

1.5. У своїй роботі бухгалтер повинен керуватися:

1.5.1. Даною посадовою інструкцією.

1.5.2. Інструкцією за видом діяльності групи.

1.5.3. Положенням про фінансовий відділ.

1.5.4. Регламентом роботи групи.

1.6. Бухгалтер повинен знати:

1.6.1. Законодавчі та нормативні правові акти, постанови, укази та вирішення регіональних і місцевих органів державної влади та управління, а також нормативно-методичні документи інших органів управління (влади), що регламентують фінансову роботу (за напрямом роботи групи).

1.6.2. Цілі, стратегію розвитку і бізнес-план підприємства.

1.6.3. Профіль, спеціалізацію та організаційну структуру підприємства.

1.6.4. Теоретичні основи фінансового менеджменту.

1.6.5. Фінансову політику підприємства та стратегію її реалізації.

1.6.6. Технологію управління фінансовими ресурсами, систему фінансових методів, що забезпечують найбільш ефективне управління фінансовими потоками.

1.6.7. План і кореспонденцію рахунків.

1.6.8. Організацію документообігу за ділянками бухгалтерського обліку.

1.6.9. Порядок документального оформлення і відображення на рахунках бухгалтерського обліку операцій, пов'язаних з рухом основних засобів, товарно-матеріальних цінностей, грошових коштів тощо.

1.6.10. Методи економічного аналізу господарсько-фінансової діяльності підприємства.

1.6.11. Правила поводження з бухгалтерською документацією.

1.6.12. Засоби обчислювальної техніки, комунікацій і зв'язки, вживані в роботі групи.

1.6.13. Правила і норми охорони праці.

1.7. Бухгалтер повинен мати уміння і навики, достатні для ефективного виконання посадових обов'язків, зокрема: _____.

(зазначити найбільш важливі)

1.8. Бухгалтер підкоряється начальникові групи фінансового відділу.

1.9. На час відсутності бухгалтера його замінює бухгалтер-касир (молодший бухгалтер).

2. ОБОВ'ЯЗКИ

2.1. Бухгалтер зобов'язаний:

2.1.1. Відображати на рахунках бухгалтерського обліку операції, пов'язані з рухом основних засобів (товарно-матеріальних цінностей, грошових коштів тощо).

2.1.2. Складати звітні калькуляції собівартості продукції (робіт, послуг), виявляти джерела утворення втрат і непродуктивних витрат, готувати пропозиції з їх попередження.

2.1.3. Проводити нарахування і перерахування податків і зборів до федерального, регіонального і місцевого бюджетів, страхових внесків до державних позабюджетних соціальних фондів, платежів до банківських установ, засобів на фінансування капітальних вкладень, заробітної плати працівників і службовців, інших виплат і платежів, а також відрахування засобів на матеріальне стимулювання працівників підприємства.

2.1.4. Забезпечувати підготовку порівняної і достовірної бухгалтерської інформації з відповідних напрямів обліку.

2.1.5. Брати участь в розробці робочого плану рахунків, форм первинних документів, вживаних для оформлення господарських операцій, за якими не передбачені типові форми, а також форм документів для внутрішньої бухгалтерської звітності.

2.1.6. Брати участь у визначенні змісту основних прийомів і методів ведення обліку і технології обробки бухгалтерської інформації.

2.1.7. Брати участь в проведенні економічного аналізу господарсько-фінансової діяльності підприємства за даними бухгалтерського обліку і звітності з метою виявлення внутрішньогосподарських резервів, здійснення режиму економії і заходів щодо вдосконалення документообігу, в розробці і впровадженні прогресивних форм і методів бухгалтерського обліку на основі застосування сучасних засобів обчислювальної техніки, в проведенні інвентаризацій грошових коштів і товарно-матеріальних цінностей.

2.1.8. Готувати дані за відповідними ділянками бухгалтерського обліку для складання звітності.

2.1.9. Забезпечувати збереження виданих йому в роботу бухгалтерських документів.

2.1.10. Виконувати роботи з формування, ведення і зберігання бази даних бухгалтерської інформації, вносити зміни до довідкової і нормативної інформації, використовуваної при обробці даних.

2.1.11.Виконувати роботу з ведення бухгалтерського обліку майна, зобов'язань і господарських операцій (обліку основних засобів, товарно-матеріальних цінностей, витрат на виробництво, реалізації продукції, результатів господарсько-фінансової діяльності, розрахунки з постачальниками і замовниками, а також за надані послуги тощо).

2.1.12. Брати участь в розробці і здійсненні заходів, спрямованих на дотримання фінансової дисципліни і раціональне використання ресурсів.

2.1.13. Здійснювати прийом і контроль первинної документації по відповідних ділянках бухгалтерського обліку і готувати їх до рахункової обробки.

2.1.14. Підтримувати взаємодію з колегами з відділу на користь забезпечення максимальної ефективності його діяльності.

2.1.15. Постійно підвищувати свій професійний рівень в системі корпоративного тренінгу.

2.1.16. Самостійно, в межах наданих йому головним бухгалтером повноважень і у взаємодії з іншими працівниками групи вирішувати питання фінансової роботи, покладені на групу.

2.1.17. Консультувати начальника групи з питань фінансової роботи (за своїм напрямом).

2.1.18. Забезпечувати якісну підготовку і своєчасне надання начальникові групи довідкових і звітних матеріалів з питань фінансової роботи (за своїм напрямом).

3. ПРАВА

3.1. Бухгалтер має право:

3.1.1. Ухвалювати обґрунтовані рішення з питань фінансової роботи (за своїм напрямом) – в межах компетенції, наданої відповідно до розпорядження головного бухгалтера.

3.1.2. Підписувати службові (ділові) документи з питань роботи групи.

3.1.3. Звертатися до начальника групи з пропозиціями, спрямованими на вдосконалення роботи групи.

3.1.4. Брати участь в протокольних заходах, на яких розглядаються питання його роботи, а також питання роботи групи.

3.1.5. Вимагати від працівників групи своєчасного, повного і якісного надання достовірній інформації, зокрема документованою.

3.1.6. Забезпечувати надання зацікавленим особам (органам) інформації про стан роботи групи, зокрема документованою, в порядку, передбаченому законодавством і локальними актами підприємства.

4. ВЗАЄМОДІЯ ЗА ПОСАДОЮ

4.1. Бухгалтер здійснює організаційно-інформаційну взаємодію:

4.1.1. З начальником групи – з питань поточної роботи групи.

4.1.2. З працівниками групи – з питань, віднесених до їх компетенції відповідно до положення про фінансовий відділ.

4.1.3. З начальниками структурних підрозділів підприємства – з питань фінансового забезпечення відповідних підрозділів.

4.1.4. З посадовими особами (підрозділами) фінансових відділів (інших аналогічних структур) інших підприємств, організацій і установ – з питань, що представляють взаємний інтерес для підприємства і сторонніх підприємств .

5. ВІДПОВІДАЛЬНІСТЬ

5.1. Бухгалтер несе відповідальність за:

5.1.1. Порушення положень керівних документів з питань фінансової роботи.

5.1.2. Невиконання наказів директора, розпоряджень головного бухгалтера, вирішень начальника фінансового відділу, доручень і вказівок начальника групи.

5.1.3. Розголошення відомостей, які складають комерційну таємницю підприємства.

5.1.4. Неправомірне використання наданих повноважень, а також використання їх в особистих цілях.

Додаток Н

УГОДА

про нерозголошення відомостей, які складають комерційну таємницю

_____

(назва підприємства)

Підстави для заповнення:
- ст.12 Закон України "Про державну контрольно-ревізійну службу"
- ст.13 Закон України "Про державну податкову службу України"

У зв'язку з тим, що я, _____

_____

(прізвище, ім'я, по батькові, назва підприємства, посада)

отримав дозвіл ознайомитися з документами (комп'ютерною системою) _____

_____

_____

_____,

(перелік документів (комп'ютерних систем), суть відомостей)

які є власністю підприємства і складають його комерційну таємницю, згоден, що без письмового дозволу керівника підприємства не розголошу і не опублікую ніякої інформації про ці відомості.

Зі змістом статей 231, 232 Кримінального кодексу України – ознайомлений.

_____

(підпис)

Резолюція керівника підприємства (непотрібне закреслювати):

- Допустити до відомостей, які складають комерційну таємницю підприємства.
- Не допустити до відомостей, які складають комерційну таємницю підприємства.
- Допустити до відомостей, які складають комерційну таємницю підприємства з умовою _____

_____

Керівник підприємства _____

(підпис)

"____" _____20__ р.

Додаток П

Дефініції поняття "організація бухгалтерського обліку"

Автор	*Характеристика поняття*
1	*2*
Безруких П..С. [187, с. 6]	Поняття "організація бухгалтерського обліку" можна визначити як науково обґрунтовану сукупність умов, при яких економно та раціонально відбувається накопичення, обробка та зберігання бухгалтерської інформації для аналізу і оперативного контролю за тим, як використовуються засоби на підприємстві
Бутинець Ф.Ф. [188, с. 40-41]	Організація бухгалтерського обліку – це: 1. Цілеспрямована діяльність керівників підприємства по створенню, постійному впорядкуванню та удосконаленню системи бухгалтерського обліку з метою забезпечення інформацією внутрішніх та зовнішніх користувачів; 2. Система умов та елементів побудови облікового процесу з метою отримання достовірної інформації про господарську діяльність підприємства і здійснення контролю за раціональним використанням виробничих ресурсів і готової продукції; 3. Комплекс заходів власника підприємства, направлених на забезпечення реєстрації фактів господарського життя, узагальнення їх з метою отримання необхідної інформації для складання звітності та прийняття управлінських рішень; 4. Один із найбільш відповідальних етапів створення підприємства та підготовки до його ефективної діяльності.
Галаган А..М. [189, с. 297]	Під технічною організацією апаратів бухгалтерського обліку розуміють ряд заходів, що забезпечують безперебійне одержання з дотриманням повного ажуру всіх необхідних для обліку відомостей, своєчасну їх обробку та складання і надання періодичної звітності
Грабова Н.М [190, с. 319]	Раціональною є така організація бухгалтерського обліку, яка може своєчасно надавати повну інформацію про хід та результати виконання плану, що необхідна для оперативного управління, контролю і економічного аналізу, при мінімальних витратах коштів і праці
Кашаев А.Н. [191, с. 65]	Організація бухгалтерського обліку – це поєднання елементів облікового процесу в їх статичному і динамічному стані, що забезпечує найбільш активний вплив на процеси виконання плану, а також збереження виробничих ресурсів і дотримання режиму економії
Костюк П.А. [192, с. 87]	Організація бухгалтерського обліку – побудова бухгалтерського обліку за планом та у відповідності до визначених умов і передумов

[187] Безруких П.С. Организация бухгалтерского учета на предприятии / П.С. Безруких. – М.: "Финансы", 1966. – 204 с.

[188] Бутинець Ф.Ф. Організація бухгалтерського обліку: [Підр. для студентів спеціальності 7.050106 "Облік і аудит" вищих навчальних закладів, 4-е вид., доп. і перероб.] / Ф.Ф. Бутинець, О.П. Войналович, І.Л. Томашевська / За редакцією д.е.н., проф., Заслуженого діяча науки і техніки України Ф.Ф. Бутинця. – Житомир: ПП "Рута", 2005. – 528 с.

[189] Галаган А. История предпринимательства российского. От купца до банкира / А. Галаган. – М.: Ось-89, 1997. – 160 с.

[190] Грабова Н.Н. Теория бухгалтерского учета [учеб. пособие для сред. с.-х. заведений] / Н.Н. Грабова. – М.: "Финансы", 1972. – 223 с.

[191] Кашаев А.Н. Организация бухгалтерского учета в производственных объединениях / А.Н. Кашаев. – М.: Финансы и статистика, 1986. – 192 с.

[192] Костюк П.А. Бухгалтерский словарь / П.А. Костюк. – Минск: "Вышэйшая школа", 1971. – 160 с.

Продовження Додатку П

1	*2*
Кумок И.С. [193, с. 15]	Під організацією бухгалтерського обліку прийнято розуміти систему умов і елементів (складових) облікового процесу, що включає первинний облік і документування операцій, план рахунків бухгалтерського обліку, форми організації обліково-обчислювальних робіт, обсяг та зміст звітності
Литвин Ю.Я., Олійник В.М., Палюх М.С., Семчишин М.В. [194, с. 20]	Раціональна організація бухгалтерського обліку й аналізу є системою практичного здійснення прийомів і способів відображення господарських операцій, які забезпечують дійовий контроль і всебічний аналіз виконання планів підприємства при мінімальних затратах праці і коштів
Литвин Ю.Я., Полторадня В.А. [195, с. 3]	Організація бухгалтерського обліку є такою системою практичного здійснення прийомів і способів відображення господарських операцій, що повністю забезпечує дієвий контроль і всебічний аналіз виконання планів підприємства при мінімальних витратах праці і засобів на ведення обліку
Німчинов П.П. [196 , с. 221]	Раціональна організація бухгалтерського обліку передбачає таку його побудову, при якій він забезпечує необхідну інформацію: про наявність, рух і збереження засобів, наявних у господарстві; для контролю за процесом виконання планів у всіх його підрозділах; для наукового обґрунтування управлінських рішень і розробки різних заходів щодо удосконалення виробництва і управління
Палий В.Ф., Соколов Я.В. [197, с. 244]	Організація бухгалтерського обліку – це все те, що забезпечує роботу бухгалтерії та вирішення облікових задач Організація бухгалтерського обліку на підприємстві – це система методів, способів та заходів, що забезпечують оптимальне функціонування обліку та подальший його розвиток. Така організація полягає в цілеспрямованому впорядкуванні й удосконаленні механізму, структури та процесів бухгалтерського обліку. Впорядкування системи бухгалтерського обліку – це організація цієї системи та організація функціонування її в часі та просторі
Сушкевич А.Н. [198, с. 8]	Під організацією бухгалтерського обліку розуміють систему елементів побудови облікового процесу, які забезпечують отримання своєчасної і достовірної інформації про господарську діяльність підприємства і здійснення контролю за використанням трудових, матеріальних і фінансових ресурсів, збереження майна і готової продукції власників підприємства

[193] Настольная книга бухгалтера – профессионала / Под общ. ред. И.С. Кумка. – М.: АОЗТ “Московское Финансовое Объединение”, 1995. – 304 с.

[194] Організація обліку, контролю і аналізу в сільському господарстві / Ю.Я. Литвин, В.М. Олійник, М.С. Палюх, М.В. Семчишин. – Тернопіль: “Тернопіль”, 1998. – 376 с.

[195] Литвин Ю.Я. Організація бухгалтерського обліку, контролю і аналізу в сільському господарстві / Ю.Я. Литвин, В.А. Полторадня. – Тернопіль: “Тернопіль”, 1998. – 375 с.

[196] Нимчинов П.П. Общая теория бухгалтерского учета / П.П. Нимчинов. – К.: Вища школа, 1977. – 240 с.

[197] Палий В.Ф. Теория бухгалтерского учета / В.Ф. Палий, Я.В. Соколов. – М.: Финансы и статистика, 1988. – 279 с.

[198] Сушкевич А.Н. Организация бухгалтерского учета в субъектах хозяйствования / А.Н. Сушкевич. – Мн.: Ред. журн. “Пром.-торговое право”, 2004. – 252 с.

Додаток Р

"ЗАТВЕРДЖУЮ"
Керівник
_____
(назва підприємства)
_____
(ПІБ)
"___" _____ 20__ р.

ПОЛОЖЕННЯ
ПРО БУХГАЛТЕРСЬКУ СЛУЖБУ ПІДПРИЄМСТВА

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Бухгалтерський відділ є самостійним структурним підрозділом фінансового департаменту підприємства і підпорядкований безпосередньо директору фінансового департаменту.

1.2. Штат бухгалтерського відділу ___ чол. складається із:

– головний бухгалтер;

– заступник головного бухгалтера;

– бухгалтер-касир тощо.

1.3. В своїй діяльності працівники бухгалтерського відділу керуються даним Положенням, посадовими інструкціями, наказами та розпорядженнями Голови правління, директора Департаменту, діючим законодавством України, Правилами внутрішнього трудового розпорядку підприємства, Правилами техніки безпеки, охорони праці і протипожежної безпеки, документацією системи управління якістю згідно ISO 9001-2001 (ДСТУ ISO 9001-2001).

1.4. На бухгалтерський відділ покладаються обов'язки, передбачені даним Положенням.

2. ЗАВДАННЯ ТА ФУНКЦІЇ БУХГАЛТЕРСЬКОГО ВІДДІЛУ

2.1. Організація обліку фінансово-господарської діяльності підприємства.

2.2. Здійснення контролю за збереженням власності, правильним витрачанням грошових коштів і матеріальних цінностей, дотримання найсуворішого режиму економії і господарського розрахунку.

2.3. Організація обліку основних засобів , сировини , матеріалів, палива, готової продукції, грошових коштів і інших цінностей підприємства, витрат виробництва і обігу, виконання кошторисний витрат.

2.4. Організація розрахунків по заробітній платі з робітниками підприємства.

2.5. Забезпечення суворого здійснення касової і розрахункової дисципліни, правильне використання отриманих в банках коштів за призначенням, дотримання порядку виписки чеків і зберігання чекових книжок.

2.6. Уживати всіх необхідних заходів для запобігання несанкціонованому і непомітному виправленню записів у первинних документах і регістрах бухгалтерського обліку та збереженню оброблених документів, регістрів і звітності протягом установленого терміну.

2.7. Здійснення (разом з іншими відділами) економічного аналізу фінансово-господарської діяльності підприємства по даних бухгалтерського обліку і звітності з ціллю виявлення внутрішньогосподарських резервів, ліквідації збитків і непродуктивних витрат.

2.8. Забезпечувати складання на основі даних бухгалтерського обліку фінансової та податкової звітності підприємства, подання її в установлені терміни користувачам. Здійснювати заходи щодо надання повної правдивої та неупередженої інформації про фінансовий стан, результати діяльності та рух коштів підприємства.

3. КЕРІВНИЦТВО

3.1. Головний бухгалтер безпосередньо підпорядкований і підконтрольний директору фінансового департаменту.

3.2. Головний бухгалтер призначається на посаду і звільняється з роботи наказом голови правління

3.3. На посаду головного бухгалтера призначаються особи з повною вищою освітою відповідного напрямку або стажем роботи на посаді головного бухгалтера не менше 5-ти років.

3.4. Головний бухгалтер повинен знати Закони України, укази Президента України, постанови, розпорядження, рішення Кабінету Міністрів України, Національного банку України, Державної податкової адміністрації України з питань правових засад регулювання господарської діяльності підприємства, положення (стандарти) бухгалтерського обліку та інші нормативно-правові акти Міністерства фінансів України щодо порядку

ведення бухгалтерського обліку та складання фінансової та податкової звітності, а також методичні документи міністерств та інших центральних органів виконавчої влади щодо галузевих особливостей застосування положень (Стандартів) бухгалтерського обліку; основи технології виробництва продукції, порядок оформлення операцій та організацію документообігу за розділами обліку, форми і порядок розрахунків, порядок приймання, зарахування на баланс, зберігання і витрачання коштів, товарно-матеріальних та інших цінностей, правила ведення інвентаризацій активів і зобов'язань; техніку безпеки; економіку, організацію виробництва, праці та управління, податкову справу, основи цивільного права, трудове, фінансове, господарське законодавство.

3.5. Головний бухгалтер керує фахівцями бухгалтерського обліку підприємства та розподіляє між ними функціональні обов'язки. Знайомить цих працівників з нормативно-методичними документами та інформаційними матеріалами, які стосуються їх діяльності, а також зі змінами в чинному законодавстві.

3.6. Головний бухгалтер організовує роботу з підготовки пропозицій для голови правління товариства щодо:

– визначення облікової політики підприємства, унесення змін до обраної облікової політики, вибору форми бухгалтерського обліку з урахуванням діяльності підприємства і технології оброблення облікових даних;

– розроблення системи і форм внутрішньогосподарського (управлінського) обліку та правил документообігу, додаткової системи рахунків і регістрів аналітичного обліку, звітності і контролю господарських операцій;

– визначення прав працівників на підписання первинних і зведених облікових документів;

– упровадження автоматизованої системи оброблення даних бухгалтерського обліку з урахуванням особливостей діяльності підприємства чи вдосконалення діючої;

– забезпечення збереження майна, раціонального та ефективного використання матеріальних, трудових і фінансових ресурсів, залучення кредитів та їх погашення.

4. ВЗАЄМОВІДНОСИНИ БУХГАЛТЕРСЬКОГО ВІДДІЛУ З ІНШИМИ ВІДДІЛАМИ

4.1. Адміністративний відділ:

Відділ якості та автоматизації:

отримує: знайомить з інструкцією по використання офісної техніки , надає пооб'єктне розміщення офісної техніки і засобів зв'язку, технічні рішення щодо ведення бухгалтерського обліку в 1С:Бухгалтерії, вхідна документація, придбані канцтовари, авансові звіти (посвідчення на відрядження, чеки, проїзні квитки і т.д.), рахунки та акти виконаних робіт, послуг пов'язаних з автоматизацією та якістю, податкові накладні (придбання);

надає: вихідну документацію, заявки на ремонт оргтехніки, інформацію про сплату рахунків на поставку та виконані роботи чи надані послуги, заявка на придбання канцтоварів, довіреність на отримання товарно-матеріальних цінностей, консультації бухгалтерського характеру.

Відділ технічного контролю:

отримує: звіт про якість готової продукції, акти браку з зазначенням винних, авансові звіти (посвідчення на відрядження, чеки, проїзні квитки і т.д.);

надає: дані про результати обліку втрат від браку.

Відділ кадрів:

отримує: накази про прийом, на звільнення, внутрішнє переведення, на відпустки, лікарняні листки, штатний розклад, табелі обліку робочого часу, договори на послуги та виконані роботи, інформацію про перебіг розгляду претензій та позовів, авансові звіти (посвідчення на відрядження, чеки, проїзні квитки і т.д.);

надає: інформацію про прихід коштів по заявлених претензіях, довіреність на отримання товарно-матеріальних цінностей, консультації бухгалтерського характеру.

Відділ охорони праці:

отримує: договори, рахунки та акти виконаних робіт, послуг пов'язаних з охороною праці, податкові накладні (придбання), приписи в разі порушення охорони праці, акт про нещасний випадок на виробництві або у побуті, знайомить з інструкцією про правила з охорони праці, техніки безпеки та протипожежної безпеки, авансові звіти (посвідчення на відрядження, чеки, проїзні квитки і т.д.);

надає: відомості про оплату рахунків, відповідає на приписи, довіреність на отримання товарно-матеріальних цінностей, консультації бухгалтерського характеру.

4.2. Відділ забезпечення виробництва:

Відділ головного механіка:

отримує: дорожні листи, відомості на списання пального, затверджені в установленому порядку акти на списання, передачу або продаж основних засобів, акти на передачу обладнання із ремонту в експлуатацію, звіти внутрішні та статистичні, рахунки на оплату, накладні на придбання товарно-матеріальних цінностей, акти про виконані роботи (послуги), податкові накладні (придбання), авансові звіти (посвідчення на відрядження, чеки, проїзні квитки тощо), розрахунок та фактичні обсяги по забрудненню навколишнього середовища, відомості і рахунки про використання води, газу, електроенергії, звіт по воді з відміткою водоканалу;

надає: інформацію про фактичні витрати на утримання та ремонт обладнання, відомості про нараховану заробітну плату, бланки звітів, бланки актів введення в експлуатацію і списання з балансу основних засобів, довіреність на отримання товарно-матеріальних цінностей, консультації бухгалтерського характеру;

Технічний відділ:

отримує: нормативи на списання матеріалів, авансові звіти (посвідчення на відрядження, чеки, проїзні квитки тощо), рахунки на оплату, накладні на придбання товарно-матеріальних цінностей, акти про виконані роботи (послуги), податкові накладні (придбання), відомості про наявність технічної документації;

надає: відомості про нараховану заробітну плату, відомості про сплату рахунків, довіреність на отримання товарно-матеріальних цінностей, консультації бухгалтерського характеру.

Відділ закупок:

отримує: авансові звіти (посвідчення на відрядження, чеки, проїзні квитки і т.д.), рахунки на оплату;

надає: відомості про нараховану заробітну плату, довіреність на отримання товарно-матеріальних цінностей, консультації бухгалтерського характеру, інформацію про несплачені рахунки з зазначенням причин, дані про рух матеріалів і залишки по них, дані про кредиторську заборгованість.

Склад матеріалів:

отримує: чеки та накладні на придбання товарно-матеріальних цінностей, податкові накладні (придбання), щомісячний звіт про списання матеріалів, порівняльні відомості про залишки товарно-матеріальних цінностей та про результати інвентаризації;

надає: відомості про нараховану заробітну плату, порівняльні відомості про залишки товарно-матеріальних цінностей.

4.3. Планово-виробничий відділ

Відділ планування виробництва та нормування праці

отримує: авансові звіти (посвідчення на відрядження, чеки, проїзні квитки і т.д.), наряд на відрядну оплату праці, калькуляцію на готову продукцію та послуги, звіти по випуску готової продукції, виконання місячного плану виробництва в номенклатурі і об'ємі товарної продукції по цехах підприємства, звіт про стан незавершеного виробництва;

надає: відомості про нараховану заробітну плату, розрахунок амортизаційних відрахувань по цехах та інші дані необхідні для складання калькуляцій.

4.4. Відділ продаж

Відділ продаж

отримує: авансові звіти (посвідчення на відрядження, чеки, проїзні квитки і т.д.), рахунки, договори, акти про виконані роботи (послуги), податкові накладні (придбання) на надання інформаційних і рекламних заходів, рахунки та договори на поставку готової продукції, вантажно-митні декларації, інформація про обсяг замовлень на виробництво промислової продукції. виконання робіт (послуг);

надає: відомості про нараховану заробітну плату, накладні на реалізацію готової продукції, акти виконаних робіт замовника, податкові накладні покупців, виписки банків, інформацію про дебіторську та кредиторську заборгованість, розрахунок процентів за надання товарного кредиту, інформацію про статі витрат для визначення повної собівартості продукції, відомості про відкриті поточні і валютні рахунки, надає інформацію про можливість проведення валютних операцій (платежів).

Склад готової продукції

отримує: довіреності і накладні на відпуск готової продукції та акти виконаних робіт з підписами отримувачів, акти прийому готової продукції на склад, щомісячний звіт про рух готової продукції;

надає: відомості про нараховану заробітну плату, порівняльні відомості про залишки готової продукції та про результати інвентаризації.

5. ПРАВА ГОЛОВНОГО БУХГАЛТЕРА

5.1. Вимагати від усіх підрозділів, служб та працівників забезпечення неухильного дотримання порядку оформлення та подання до обліку первинних документів.

5.2. Погоджувати призначення, звільнення і переміщення матеріально-відповідальних осіб (касирів, завідуючі складами і інших).

5.3. Розглядати договори і згоди, які укладаються підприємством, на утримання чи відпуск товарно-матеріальних цінностей , на виконання робіт , послуг, а також накази, розпорядження та інші документи по питаннях фінансово-господарської діяльності.

5.4. Перевіряти в структурних підрозділах і службах підприємства дотримання установленого порядку приймання, оприбуткування, зберігання і витрачання грошових коштів, товарно-матеріальних і інших цінностей.

5.5. Контролювати фінансову діяльність підрозділів підприємства і давати їх керівникам рекомендації по організації та веденню фінансової роботи.

5.6. Готувати пропозиції про зниження розмірів чи зняття премій керівників цехів, бригад, відділів чи інших підрозділів і служб, які не забезпечують виконання установлених правил оформлення первинних документів, ведення первинного обліку і інших вимог по організації обліку і контролю.

6. ВІДПОВІДАЛЬНІСТЬ ГОЛОВНОГО БУХГАЛТЕРА

Головний бухгалтер несе відповідальність за :

6.1. Якісне і належне виконання працівниками бухгалтерського відділу своїх посадових обов'язків.

6.2. Достовірність даних, які надаються керівництву підприємства, органам статистики та податковій інспекції.

6.3. Задовільний стан обліку і звітності по усіх видах роботи підпорядкованого йому відділу, зберігання документів та веденню діловодства.

6.4. Своєчасність вирішення питань, що стосуються підпорядкованого йому відділу.

6.5. Розголошення відомостей, які складають комерційну таємницю підприємства.

6.6. Порушення ним, чи його підлеглими, Правил внутрішнього трудового розпорядку, трудової дисципліни та Правил охорони праці, техніки безпеки і протипожежної безпеки.

Розробив:

Головний бухгалтер _____ _____

(підпис) (ПІБ)

Погоджено:

Інженер з охорони праці _____ _____

(підпис) (ПІБ)

Юристконсультант _____ _____

(підпис) (ПІБ)

Додаток С

ПІДПРИЄМСТВО

“_____”

ЗАТВЕРДЖУЮ
Керівник
_____
(назва підприємства)
_____
(підпис)

ПОЛІТИКА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

м. _____

20__ р.

ЗМІСТ

1. ТЕРМІНИ ТА ВИЗНАЧЕННЯ

Автономні системи – системи, які керують одним або декількома загороджуючими пристроями, без передачі інформації в центр охорони і без контролю оператором.

Авторизація – надання повноважень; встановлення відповідальності між повідомленням і його джерелом (користувачем, що створив його, або процесом).

Адміністративне управління доступом – принцип управління доступом, який полягає в тому, що управління потоками інформації між користувачами і об'єктами дозволене лише системним адміністраторам.

Аналіз загрози – постійна перевірка інформації вагомих фактів, на основі яких робляться висновки.

Аутентифікація – встановлення достовірності користувача мережі, якому потрібен доступ до інформації, що захищається, або якого потрібно підключити до мережі.

Багатошлейфовий об'єкт – об'єкт, що охороняється за допомогою багатошлейфового контрольно-приймального приладу (концентратора), що має інформаційний вихід на один номер центрального пульта охорони.

Безперервність захисту – захист інформації в комп'ютерній системі забезпечується на всіх етапах життєвого циклу і в усіх режимах функціонування захищеної комп'ютерної системи, зокрема при проведенні ремонтно-регламентних робіт.

Документ – передбачена законом матеріальна форма отримання, зберігання, використання і розповсюдження інформації шляхом фіксації її на папері, магнітних дисках, магнітною, кіно-, відео-, фотоплівці або на інших носіях.

Документообіг – реєстрація, облік, зберігання, розповсюдження і рух документів, що мають гриф "комерційна таємниця" усередині підрозділу або між підрозділами підприємства.

Достатність захисту – захист інформації в комп'ютерній системі, яка забезпечує необхідний рівень захищеності при мінімальних витратах ресурсів.

Доступ до інформації – вид взаємодії двох об'єктів КС, внаслідок якого виникає потік інформації від одного об'єкту до іншого і/або відбувається зміна стану системи.

Доступність – властивість ресурсу системи (КС, послуги, об'єкта КС, інформації), яке полягає в тому, що користувач, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до прав, встановлених політикою безпеки, не чекаючи довше заданого (малого) проміжку часу, тобто коли ресурс знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, в той час, коли він йому необхідний.

Загроза – це можлива небезпека (потенційна або реально існуюча), здійснення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкту захисту, що завдає економічної, фінансової, матеріальної або моральної шкоди власнику інформації.

Загроза для комерційної інформації – витік, можливість блокування або порушення цілісності інформації.

Злом – несанкціоноване проникнення за допомогою руйнування охоронного пристрою.

Зчитувач – електронний пристрій, за допомогою якого здійснюється ідентифікація інформації.

Ідентифікатор – пропуск (карта, документ, ключі), на якому знаходиться необхідна інформація для допуску на об'єкт, що охороняється, територію і т.п.

Ідентифікація – процедура привласнення ідентифікатора об'єкту КС або встановлення відповідності між об'єктом і його ідентифікатором; пізнання.

Інженерно-технічні заходи захисту – комплекс організаційних і технічних заходів захисту інформації технічними засобами.

Інтегровані системи безпеки (ІСБ) – комплекс системи охоронно-пожежної сигналізації, системи управління і контролю доступу, відеоспостереження. ІСБ призначені для охорони об'єктів.

Ключ – ідентифікатор для механічних замків.

Комерційна інформація – відомості, пов'язані з виробництвом, технологією, управлінням, фінансами і іншою діяльністю підприємства, розголошування або передача яких може зашкодити інтересам підприємства.

Комп'ютерна система (КС) – організаційно-технічна система, яка реалізує інформаційну технологію і об'єднує сукупність програмно-апаратних засобів, призначених для обробки інформації, фізичне середовище, персонал і оброблювану інформацію.

Комплексна система захисту інформації (КСЗ) – сукупність організаційних, інженерно-технічних і програмних заходів, що забезпечують захист інформації в КС.

Конфіденційна інформація – це відомості, що перебувають у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюваних по їх бажанню відповідно до передбачених умов.

Користувач – фізична особа, яка може взаємодіяти з КС через наданий йому інтерфейс.

Легітимність захисту – побудова системи захисту інформації на основі діючих положень і вимог нормативно-правових документів по захисту інформації.

Несанкціонований доступ (НСД) – доступ, до інформації здійснюваний з порушенням встановлених в КС правил розмежування доступу.

Організаційні заходи захисту – комплекс адміністративних і обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту

шляхом регламентації діяльності персоналу і порядку функціонування комп'ютерних систем.

Персональний ідентифікаційний номер – код, що вводиться користувачем за допомогою цифрової клавіатури і дає санкцію на прохід.

Повноваження – права користувача або процесу на виконання певних дій, напряму потоку інформації, зміни стану КС (наприклад: читання, запис, модифікація, видалення тощо).

Політика безпеки інформації – сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

Правила розмежування доступу (ПРД) – частина політики безпеки, яка регламентує правила доступу користувачів в КС.

Пристрої ідентифікації – пристрої, що надають права на допуск до особливої інформації або допуск на об'єкт, територію, в приміщення людям або транспорту через пристрої, що загороджують.

Просочування комерційної інформації – неконтрольоване розповсюдження інформації, яке веде до її несанкціонованого отримання.

Розголошування комерційної інформації – навмисні або ненавмисні дії посадових, фізичних або юридичних осіб, що призвели до не викликаної службовою необхідністю відкритої публікації відомостей, складових комерційної таємниці, а також передача подібних відомостей по відкритих каналах зв'язку. Під відкритою публікацією таких відомостей необхідно розуміти їх публікацію у відкритому друці, передачу по радіо і телебаченню, оголошення на міжнародних, зарубіжних і відкритих симпозіумах, нарадах, конференціях, з'їздах, при публічних виступах, вивіз матеріалів за кордон або передачу їх в будь-якій формі фірмам, організаціям або окремим особам.

Система управління і контролю доступом – спільно направлена робота на охорону об'єкту (території) засобів контролю і управління.

Система фізичного захисту об'єкту (СФЗО) – сукупність організаційних і інженерно-технічних заходів, спрямованих на припинення загроз об'єкту з боку вірогідних зовнішніх і внутрішніх порушників.

Спостереженість – властивість інформації, яка дозволяє фіксувати діяльність користувачів, однозначно встановлювати ідентифікатори, причетні до певних дій користувачів з метою запобігання порушенням політики економічної безпеки підприємства або забезпечення відповідальності за певні дії.

Точка доступу – місце, де відбувається перевірка доступу.

Цілісність – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем.

2. ВСТУП

Створення розвиненої інформаційної інфраструктури підприємства сприяло формуванню нової програмно-технічної платформи з використанням мережевих технологій, що дозволяє поетапно здійснювати реінжиніринг

основних, організаційно-управлінських та забезпечуючих бізнес-процесів підприємства, що сприяє появі нових загроз для бухгалтерської інформації, яка містить комерційну таємницю підприємства. Це загрози конфіденційності, цілісності та доступності, запобігти яким можливо за допомогою процесного підходу до створення політики економічної безпеки підприємства, орієнтованої на створення захищеного середовища обробки інформації, зокрема оброблюваною в корпоративній інформаційно-обчислювальній мережі. Комплексний підхід спрямований на своєчасне виявлення прямих або непрямих загроз інформації, виключення або мінімізацію збитків власнику інформації (назва підприємства), захист його науково-технічного, технологічного, виробничого та кадрового потенціалу, що досягається шляхом створення комплексної системи захисту інформації (КСЗІ). КСЗІ об'єднує різнорідні заходи протидії загрозам: організаційні, правові, інженерно-технічні, морально-етичні, програмно-апаратні заходи забезпечення інформаційної безпеки.

Для реалізації стратегії прискореного еволюційного розвитку _____(назва підприємства) важливу роль грає кадрова політика. Персонал _____(назва підприємства) є безпосереднім носієм знань - однією з основних складових довготривалих конкурентних переваг підприємства. Сукупність оперативних умінь, інформації і навиків, творчого потенціалу і корпоративного духу кожного працівника і всього трудового колективу є основою перетворень, спрямованих на створення високоефективного підприємства світового значення.

Працівники генерують нові ідеї, новації, відкриття і винаходи, завдяки яким підвищується добробут підприємства та його співробітників, але, не дивлячись на це, персонал є основним джерелом втрати (витоки, розголошування) інформації, яка складає комерційну таємницю підприємства.

У основу політики економічної безпеки покладено людський фактор, який передбачає відданість співробітників інтересам підприємства, усвідомлене дотримання ними встановлених правил захисту інформації.

У вирішенні проблеми забезпечення безпеки інформації значне місце займає вибір ефективних методів роботи з персоналом, що володіє відомостями, що становлять комерційну таємницю підприємства. Будь-який співробітник має бути об'єктивно зацікавлений в збереженні таємниці нововведень, що підвищують конкурентоспроможність _____ (назва підприємства).

На сучасному підприємстві практично кожен співробітник стає носієм цінних відомостей, які представляють інтерес для конкурентів. В рамках забезпечення економічної безпеки підприємства кадрова політика відіграє профілактичну роль по відношенню до такого типу загрози, як неблагонадійність окремих співробітників. Питання управління персоналом, пов'язаного з обробкою, зберіганням та використанням відомостей, що

становлять комерційну таємницю підприємства, в даний час включаються в число найважливіших при вирішенні проблем економічної безпеки.

Підвищення відповідальності персоналу за виконувану роботу та збереження відомостей, що становлять комерційну таємницю, активну участь працівника в прийнятті управлінських рішень вимагають нового змісту при оцінці таких критеріїв, як освіта, професіоналізм, особиста культура, моральні якості і етика працівників. Персонал розглядається як найцінніший ресурс підприємства, який вирішує з одного боку виробничі та комерційні завдання, а з іншого – отримує у володіння відомості, що становлять комерційну таємницю підприємства, забезпечує їх правильне використання та збереження.

3. МЕТА ПОЛІТИКИ

Політикою економічної безпеки підприємства визначені:

– особливості прийому і переведення працівників;

– особливості поточної роботи з користувачами відомостей, що становлять комерційну таємницю підприємства;

– особливості звільнення працівників, які були користувачами інформації, яка складає комерційну таємницю підприємства;

– основні форми контролю якості роботи персоналу, допущеного до роботи з інформацією, яка складає комерційну таємницю підприємства;

– особливості проходження практики студентами, що вчаться в учбових закладах.

Політикою визначені організаційні заходи, спрямовані на своєчасне виявлення або максимальне ослаблення дії різного роду небезпек та загроз підприємству, спричинених людським фактором, що можуть в умовах конкуренції завдавати збитку підприємству. Потенційні загрози безпеці інформації, яка складає комерційну таємницю підприємства, з боку персоналу та сторонніх осіб _____ (назва підприємства) (Додаток Т), розміщені за ступенем значущості, складені на основі міжнародного стандарту ISO\IEC 15408 тощо.

Основними методами отримання цінної інформації у персоналу є:

– співпраця працівника підприємства із зловмисником, основою якого є оплата послуг, що надаються, і психологічна нестійкість цього працівника тощо;

– схилення (примушення, спонукання) до співпраці працівників підприємства шляхом шантажу, зміни поглядів або моральних принципів, здирства, використання негативних рис характеру, фізичного насильства;

– переманювання цінних і обізнаних фахівців обіцянкою кращої матеріальної винагороди, кращих умов праці і іншими перевагами;

– помилкова ініціатива в прийомі співробітника на високооплачувану роботу на підприємство-конкурент, вивідування в процесі співбесіди необхідної інформації, зокрема інформації, яка складає комерційну таємницю, і потім відмова в прийомі;

– вивідування цінної інформації у співробітників підприємства за допомогою підготовленої системи питань на наукових конференціях, зустрічах з пресою, на виставках і при особистих бесідах в службовій і неслужбовій обстановці;

– отримання зловмисником від співробітника потрібної інформації при перебуванні співробітника в стані алкогольного сп'яніння або під дією наркотиків, що не дозволяє адекватно оцінювати свої дії;

– використання властивих кожному співробітникові таких психокомплексів як страх (починаючи від боязні втратити роботу і боязнь пониження на посаді і закінчуючи боязню втрати престиж, боязнь зробити щось не так); цікавість, жадність, перевага, великодушність і жалість, довірливість.

Працівники підприємства, що володіють інформацією, яка складає комерційну таємницю підприємства, є найбільш обізнаними і часто достатньо доступними джерелами для зловмисників, охочих отримати необхідні їм відомості.

Оволодіння необхідною інформацією найчастіше відбувається в результаті безвідповідальності та не навченості персоналу, недостатньо високих особистих та моральних якостей співробітників.

Захист матеріальних і фінансових цінностей _____(назва підприємства) є одним з основних напрямів забезпечення економічної безпеки підприємства, як особливо важливого бізнес-процесу.

Технічні засоби безпеки доповнює решта всіх видів охорони і служать загальним цілям попередження та протидії загрозам, що впливають на об'єкт захисту.

У системі економічної безпеки підприємства цілі реалізуються інтегрованою системою безпеки (ІСБ).

Інтегрована система безпеки забезпечує безпеку за наступними напрямами:

– забезпечення внутрішньої безпеки підприємства, пов'язаної із захистом своїх інтересів від протиправних дій його співробітників (внутрішніх загроз);

– забезпечення зовнішньої безпеки підприємства (захист від зовнішніх загроз);

– забезпечення безпеки від об'єктивних загроз природного і техногенного характеру (пожежі, вибухи легко займистих речовин тощо).

Інтегрована система безпеки підприємства складається з наступних підсистем:

– охоронно-пожежної сигналізації;

– контролю управління доступом;

– інженерно-технічних засобів безпеки;

– пожежної безпеки;

– охоронного відеоспостереження;

– гарантованого електроживлення та аварійного освітлення.

Інтеграція підсистем забезпечується поетапним, планомірним розвитком корпоративної інформаційно-обчислювальної мережі _____ (назва підприємства) та універсальних високошвидкісних засобів телекомунікацій. Створення єдиного інформаційного простору підприємства, як підсумок цього процесу, у поєднанні з функціонуванням системи інформаційної безпеки дозволить об'єднати підсистеми і реалізувати широкі можливості ІСБ на якісно новому рівні.

4. СФЕРА ЗАСТОСУВАННЯ

Вимоги даної політики обов'язкові для виконання всіма співробітниками підприємства.

4.1. Політика базується на принципах:

– легітимності – захист інформації ґрунтується на положеннях і вимогах діючих законодавчих та нормативно-правових документів;

– системності – захист інформації передбачає взаємозв'язок та взаємодію об'єктів, що змінюються в часі, умов і факторів, суттєвих для безпеки (критична інформація, її загрози тощо);

– комплексності – захист інформації забезпечується комплексом організаційно-правових, інженерно-технічних та програмних заходів;

– безперервності – захист інформації забезпечується на всіх етапах життєвого циклу інформації;

– достатності – необхідний рівень захисту при мінімальних витратах власника інформації;

– адекватності – необхідний рівень захисту, при якому витрати, ризик та ймовірність можливого збитку були б допустимі для власника інформації.

4.2. Політикою встановлений порядок:

– формування "Переліку інформації, яка складає комерційну таємницю підприємства";

– допуску / доступу до відомостей, що становлять комерційну таємницю підприємства;

– розробки заходів щодо захисту відомостей, що становлять комерційну таємницю підприємства;

– організації робіт з документами, що становлять комерційну таємницю підприємства;

– організації захисту відомостей, що становлять комерційну таємницю підприємства на АРМ;

– організації захисту відомостей, що становлять комерційну таємницю підприємства, в комп'ютерних системах;

– обов'язки працівників підприємства допущених до відомостей, що становлять комерційну таємницю підприємства;

– відповідальності за порушення вимог захисту відомостей, що становлять комерційну таємницю підприємства.

4.3. Правовою базою для розробки даної політики слугують вимоги тих законодавчих та нормативних документів, що діють в Україні.

4.4. Політика визначає та на адміністративному рівні закріплює основну (базову) діяльність підприємства в галузі захисту бухгалтерської інформації, яка складає комерційну таємницю, при цьому досягаються:

– конфіденційність при використанні, зберіганні, обробці, передачі відомостей, що становлять комерційну таємницю підприємства;

– цілісність при використанні, зберіганні, обробці, передачі відомостей, що становлять комерційну таємницю підприємства.

– доступність відомостей, що становлять комерційну таємницю підприємства користувачам відповідно до правил, встановлених на підприємстві.

Процесу прийому співробітника на роботу передує ряд підготовчих етапів, які дозволяють скласти точне уявлення про те, який фахівець і якої кваліфікації дійсно потрібний для даної посади, якими діловими, моральними і особистими якостями він повинен володіти.

Прийом на роботу і перевід співробітників проводиться відповідно до вимог "Правил внутрішнього трудового розпорядку _____ (назва підприємства).

Особливість прийому на роботу полягає в інформуванні кандидатів про відповідальність за порушення правил та норм із захисту інформації, а також про механізм дозвільної системи доступу, визначений політикою економічної безпеки підприємства.

При прийомі працівника за професією (на посаду), що передбачає використання інформації, яка складає комерційну таємницю, організовується співбесіда з фахівцями групи захисту інформації ІАСУ (Додаток У).

При підвищенні на посаді відділ кадрів інформує працівника про зростаючий ступінь особистої відповідальності за забезпечення економічної безпеки підприємства.

В процесі стажування молодих фахівців регулювання прав доступу до інформації, зокрема інформації, яка складає комерційну таємницю підприємства, проводиться керівником стажування, який несе відповідальність за дотримання молодим фахівцем:

– норм і вимог із захисту інформації відповідно до існуючих документів із захисту інформації;

– порядку допуску до інформації, яка складає комерційну таємницю підприємства відповідно до політики економічної безпеки підприємства.

5. ПОЛІТИКА

Формування "Переліку відомостей, що становлять комерційну таємницю підприємства" здійснюється підрозділами-розробниками інформації, підрозділами-користувачами та експертною комісією із захисту інформації. Підрозділи-розробники інформації визначають інформацію, пов'язану з виробничою, економічною, фінансовою, маркетинговою та іншою діяльністю підприємства, власником якої є _____ (назва підприємства), витік якої може завдати власнику економічну, фінансову, моральну або іншу шкоду.

Легітимність віднесення інформації до відомостей, що становлять комерційну таємницю підприємства, встановлюється юридичним відділом.

Відомості, затверджені відповідальним за перетворення і управління бізнес-процесом передаються до експертної комісії підприємства із захисту інформації для узагальнення та систематизації за бізнес-процесами. Експертна комісія із захисту інформації розглядає одержану інформацію підрозділів та надає висновок про доцільність віднесення даних відомостей до відомостей, що становлять комерційну таємницю з урахуванням фінансово-економічних інтересів підприємства.

Узагальнений перелік відомостей, що становлять комерційну таємницю підприємства, затверджується та вводиться в дію наказом Голови правління, генерального директора.

Після введення в дію "Переліку відомостей, що становлять комерційну таємницю підприємства" до структурних підрозділів надходить "Витяг з переліку відомостей, що становлять комерційну таємницю" по даному підрозділу.

Перелік відомостей, що становлять комерційну таємницю підприємства, оновлюється в міру необхідності.

Виявлення загроз і каналів витоку відомостей, що становлять комерційну таємницю підприємства

Загроза – це можлива небезпека (потенційна або така, що реально існує), здійснення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкту захисту, що завдає економічної, фінансової, матеріальної або моральної шкоди власнику інформації.

Загрози класифікуються за декількома критеріями:

– за аспектом безпечності інформації (доступність, цілісність, конфіденційність) проти яких загрози спрямовані насамперед;

– за компонентами інформаційних систем, на які націлені загрози (дані, програми, апаратура, підтримуюча інфраструктура);

– за способом здійснення (випадкові / навмисні дії природного / техногенного характеру);

– за розташуванням джерела загроз (всередині / поза даної інформаційної системи).

Найнебезпечнішими (за можливим збитком) є:

– загрози доступності – блокування, знищення інформації і засобів її обробки;

– загрози цілісності – модифікація (спотворення), заперечення достовірності, нав'язування помилкової інформації;

– загрози конфіденційності – розкрадання (копіювання), втрата (ненавмисна втрата, витік) інформації і засобів її обробки.

Носіями загроз безпеці інформації є джерела загроз. Джерела загроз можуть знаходитись як усередині підприємства – внутрішні джерела загроз, так і зовні – зовнішні джерела. Третя група джерел загроз поєднує обставини, що

становлять непереборну силу та носять об’єктивний і абсолютний характер, що розповсюджується на всіх: форс-мажорні джерела загроз.

Формування переліку основних загроз відомостей, що становлять комерційну таємницю підприємства, виконується поетапно.

На першому етапі, експертна комісія із захисту інформації на підставі міжнародних стандартів ISO\IEC 15408 формує базовий перелік основних загроз інформації, яка складає комерційну таємницю підприємства.

На другому етапі адміністратори комп’ютерних систем структурних підрозділів, відповідальні за документообіг документів з грифом “Комерційна таємниця” надають до експертної комісії підприємства із захисту інформації звіти про факти виникнення передумов до реалізації (здійсненню) загроз інформації, яка складає комерційну таємницю підприємства. Експертною комісією підприємства із захисту інформації узагальнюються і аналізуються звіти, які надійшли, і складається перелік основних загроз інформації, яка складає комерційну таємницю. До них відносяться:

– *форс-мажорні загрози* – аварія водопровідної і опалювальної систем, пожежа, відключення електропостачання, пошкодження мережевих комунікацій, пил, забруднення, недопустима температура, вологість тощо;

– *внутрішні загрози* – нестійка робота корпоративної мережі, несанкціоноване налаштування базового, мережевого, прикладного ПЗ, несанкціонована зміна конфігурації апаратної частини, розголошення інформації, засобів і методів ЗІ, атрибутів розмежування доступу (пароль, електронний ключ, пропуск тощо), розкрадання носіїв інформації, навмисне спотворення і руйнування, несанкціонована модифікація, копіювання і знищення інформації, недбале зберігання, облік і знищення інформації, зараження вірусами, пересилка даних за помилковою адресою абонента (E-mail, Internet, в корпоративній мережі), відключення сервера під час роботи тощо;

– *зовнішні загрози* – шантаж, підкуп, “підкуп персоналу”, спонукання (примушення) до співпраці співробітників підприємства, несанкціонований доступ сторонніх осіб (співробітники державних установ, зокрема контролюючих організацій, журналісти ЗМІ, фахівці, що відряджаються, студенти, що вчаться, родичі), незаконне отримання або розблокування атрибутів розмежування доступу (пароль, електронний ключ, пропуск, ідентифікаційна карта тощо), атаки хакерів, перехоплення, модифікація, знищення, переадресація, формування помилкових повідомлень по E-mail, в мережі Internet, використання технічних засобів розвідки, терористичні дії тощо.

Перелік загроз інформації, що становить комерційну таємницю підприємства, змінюється і доповнюється при виявленні нових загроз.

Розробка заходів після захисту відомостей, що становлять комерційну таємницю підприємства

Заходи щодо захисту відомостей, що становлять комерційну таємницю підприємства, розробляються на підставі наявних загроз і вимог щодо захисту і складаються з економічно обґрунтованих організаційно-правових, інженерно-технічних і програмних заходів захисту.

Організаційно-правові заходи захисту включають:

- заходи, спрямовані на регламентацію правил обробки і захисту інформації, а також встановлюють відповідальність за порушення цих правил;
- заходи щодо розробки правил доступу користувачів до інформації;
- заходи щодо організації охорони і надійного пропускного режиму;
- заходи щодо організації робіт з персоналом (підбір і розстановка кадрів, адаптація співробітників, розподіл завдань і відповідальності, навчання і підвищення кваліфікації, мотивація співробітників, контроль за виконанням співробітниками покладених на них функцій, виявлення незадоволених своїм положенням і нелояльних співробітників, звільнення співробітників, проходження практики студентами вузів і особами, які навчаються в технікумах і ПТУ);
- заходи щодо організації обліку, зберігання, використання і знищення документів і носіїв інформації;
- заходи, здійснювані при ремонті устаткування і модифікаціях програмного забезпечення.

Інженерно-технічні заходи захисту включають:

- заходи щодо інженерного захисту об'єктів (установка систем охоронно-пожежної сигналізації, спостереження, захист каналів зв'язку і електронних комунікацій).

Програмні заходи включають:

- заходи щодо ідентифікації та аутентифікації користувачів;
- заходи щодо розмежування доступу користувачів до ресурсів КІС;
- заходи щодо антивірусного захисту КІС;
- заходи щодо резервного копіювання і відновлення інформації.

Експертна комісія підприємства із захисту інформації і відповідальні за управління і перетворення бізнес-процесів при виборі заходів щодо захисту інформації ухвалюють рішення, при яких з одного боку не створюють перешкоди для використання співробітниками своїх обов'язків, а з іншої – мінімізують можливості здійснення ними (випадково або навмисно) порушень.

Дозвільна система допуску/ доступу до відомостей, що становлять комерційну таємницю підприємства

Дозвільна система доступу – це норми і вимоги, що встановлюються правовими документами України і керівництвом _____(назва підприємства) з метою правомірного ознайомлення і використання співробітниками підприємства відомостей, що становлять комерційну таємницю підприємства, необхідних їм для виконання своїх службових обов'язків в рамках встановлених функцій бізнес-процесів.

Основними принципами побудови дозвільної системи доступу є:

– надійність, тобто виключення можливості несанкціонованого доступу до інформації, яка складає комерційну таємницю підприємства в звичайних та екстремальних умовах;

– повнота осяжності всіх категорій виконавців;

– конкретність, тобто виключення двоякого трактування і однозначність рішення про доступ;

– виробнича необхідність як єдиний критерій доступу до інформації, яка складає комерційну таємницю підприємства;

– визначеність складу і компетентність посадовців, що дають дозвіл на доступ виконавців до інформації, яка складає комерційну таємницю підприємства (документів, баз даних тощо), виключення можливості безконтрольної і несанкціонованої видачі таких дозволів:

– сувора регламентація порядку роботи всіх категорій користувачів з інформацією, яка складає комерційну таємницю підприємства.

Дозвільна система складається з двох складових частин:

– допуск користувачів до інформації, яка складає комерційну таємницю підприємства;

– доступ конкретного користувача до конкретної інформації, яка складовій комерційну таємницю підприємства.

Порядок допуску до відомостей, що становлять комерційну таємницю, працівників підприємства

Допуск до відомостей, що становлять комерційну таємницю підприємства, заснований на праві власника інформації _____ (назва підприємства), призначити уповноважену особу, яка визначає користувачів, інформації, що належить йому, і встановлює їх повноваження.

Структура процедури розмежування допуску багаторівнева, ієрархічна. Ієрархія дозвільної системи допуску до інформації, яка складає комерційну таємницю підприємства, реалізована за принципом “чим вище рівень доступу, тим вужче коло допущених осіб”, “чим вище цінність інформації, тим менше число працівників підприємства може її знати”.

Організацію доступу до відомостей, що становлять комерційну таємницю підприємства наведено в Додатку Д.

Дозвільна система встановлює єдиний порядок допуску до інформації, яка складає комерційну таємницю підприємства, який необхідний для виконання всіма працівниками підприємства. Дозвіл на допуск до інформації, яка складає комерційну таємницю підприємства, надається лише в письмовому вигляді. За необхідності власник бізнес-процесу делегує свої права на визначення користувачів інформації, яка складає комерційну таємницю підприємства, і встановлення їх повноважень координаторам відповідного бізнес-процесу.

Порядок доступу до відомостей, що становлять комерційну таємницю працівників підприємства

Доступ санкціонується власником бізнес-процесу відносно певної інформації та певного працівника.

Дозвіл на доступ до відомостей, що становлять комерційну таємницю підприємства, персоналізується. Керівники структурних підрозділів несуть персональну відповідальність за правильний підбір працівників – користувачів, а працівники, що працюють з відомостями, що становлять комерційну таємницю підприємства, несуть персональну відповідальність за збереження в таємниці їх змісту, збереження носія і дотримання встановлених правил роботи з документами і в інформаційно-обчислювальній мережі.

Доступ до відомостей, що становлять комерційну таємницю підприємства, в структурному підрозділі здійснюється на підставі виписки із затвердженого на підприємстві "Переліку відомостей, що становлять комерційну таємницю підприємства". Керівником підрозділу формується список працівників – користувачів відомостей, що становлять комерційну таємницю підприємства, яким необхідні дані відомості для виконання своїх функцій.

Доступ працівників підприємства до документів, що становлять комерційну таємницю, здійснюється на підставі "Дозволу на надання доступу до документів, що становлять комерційну таємницю підприємства" (Додаток Ф). Даний "Дозвіл" оформлюється спеціалістом відповідальним за ведення документообігу, що становить комерційну таємницю в підрозділі, підписується керівником підрозділу, узгоджується з керівником підрозділу – розробником інформації і після отримання дозволу на допуск у власника бізнес-процесу або його координатора, направляється заступнику головного інженера з АСУ для реалізації прав доступу.

На підставі "Дозволу" фахівцями групи захисту інформації ІАСУ і відділу кадрів проводиться первинний інструктаж із захисту інформації і оформлюється договірне зобов'язання про нерозголошення інформації, яка складає комерційну таємницю підприємства (Додаток Ж). При цьому користувач документальної інформації, ставить підпис у "Дозволі" про наданий йому доступ. Договірне зобов'язання оформляється один раз і зберігається у відділі кадрів в особистій справі працівника підприємства.

Доступ до документів, що становлять комерційну таємницю підприємства, здійснюється відповідальним за ведення відповідного документообігу в підрозділі.

Допуск співробітників підприємства – користувачів комп'ютерних систем здійснюється на підставі "Дозволу на надання доступу до відомостей, що використовуються в комп'ютерних системах та становлять комерційну таємницю підприємства" (Додаток Х).

"Дозвіл" оформляється адміністратором КС підрозділи, підписується керівником підрозділу, який робить запит на право доступу до КС, узгоджується з керівником підрозділу – розробником КС і після отримання дозволу на допуск у власника бізнес-процесу або його координатора, направляється заступнику головного інженера з АСУ для реалізації прав допуску.

Права доступу користувачів до КС забезпечує керівник проекту КС шляхом визначення ролей і привілеїв в техно-робочому проекті на розробку КС, методами програмного забезпечення і наділенням користувачів КС повноваженнями відповідно до "Дозволу".

Контроль за допуском користувачів підрозділу до КС відповідно до "Дозволу" здійснюється адміністратором КС підрозділу. Реєстрація і облік дозволів про допуск / доступ користувачів до необхідних відомостей, здійснюється фахівцями групи захисту інформації ІАСУ шляхом створення і підтримки в актуальному стані електронної матриці доступу.

Контроль за виконанням вимог з допуску до відомостей, що становлять комерційну таємницю, здійснюється експертною комісією із захисту інформації.

Порядок допуску до відомостей, що становлять комерційну таємницю, працівників правоохоронних і контролюючих органів

Допуск до відомостей, що становлять комерційну таємницю підприємства, працівників правоохоронних і контролюючих органів здійснюється в порядку встановленому законами України про ці органи.

Допуск до відомостей, які становлять комерційну таємницю підприємства, здійснюється Генеральним директором, заступником Генерального директора – Головою експертної комісії підприємства із захисту інформації за наявності офіційного письмового запиту на надання конкретної інформації суб'єктам правоохоронних та контролюючих органів (Додаток Ц).

Правоохоронні і контролюючі органи зобов'язані зберігати інформацію, що становить комерційну таємницю підприємства, яка стала ним відома при виконанні службових обов'язків, відповідно до вимог законів України про ці організації.

Порядок передачі відомостей, що становлять комерційну тайну підприємства у відкритий друк, на радіо, телебачення

Дозвіл на передачу інформації, яка складає комерційну таємницю підприємства у відкритий друк, на радіо і телебачення, розголошення на відкритих симпозіумах, нарадах, конференціях, при публічних виступах, вивіз матеріалів за кордон або передачу їх в будь-якій формі фірмам, організаціям надається після узгодження з керівниками відповідних бізнес-процесів і затвердження головою експертної комісії підприємства із захисту інформації.

Порядок позбавлення допуску / доступу до відомостей, що становлять комерційну таємницю підприємства

Позбавлення прав доступу до відомостей, що становлять комерційну таємницю підприємства здійснюється при:

- звільненні користувача з підприємства;
- переході користувача з одного підрозділу в інший;
- підвищенні або пониженні на займаній посаді;
- порушенні норм і вимог захисту відомостей, що становлять комерційну таємницю підприємства.

При звільненні, переході в інший підрозділ, підвищенні на посаді користувача необхідно:

- після оформлення заяви працівник-користувач відомостей, що становлять комерційну таємницю підприємства, зобов'язаний здати фахівцеві, відповідальному за документообіг документів з грифом "Комерційна таємниця", всі документи, які є у нього, креслення, моделі тощо;
- адміністратор комп'ютерних систем підрозділу проглядає інформацію в електронному вигляді (папки, файли, бази даних тощо), з якими працював фахівець, що звільняється, на предмет змін, модифікації тощо і позбавляє його прав доступу до АРМ та комп'ютерних систем;
- фахівці групи захисту інформації ІАСУ щотижня згідно бази даних відділу кадрів складають список звільнених працівників підприємства. Даний список направляється системним адміністраторам для позбавлення прав доступу до серверів і баз даних підприємства.

При оформленні документів у відділі кадрів з колишнім працівником проводиться бесіда з метою нагадування йому про зобов'язання зі збереження в таємниці відомостей, що становлять комерційну таємницю підприємства, які йому були довірені, і не використанні цих відомостей у власних інтересах і інтересах конкурентів. Колишній працівник оформляє так само "Угоду про нерозголошення інформації, яка складає комерційну таємницю підприємства, при звільненні" (Додаток Ш).

Організація робіт з документами, що становлять комерційну таємницю підприємства

Головним напрямом захисту документів, що становлять комерційну таємницю підприємства, від можливих загроз є формування захищеного документообігу.

Захищений документообіг – це контрольований рух документів, що становлять комерційну таємницю підприємства, за регламентованими пунктами прийому, обробки, використання і зберігання, при якому досягаються:

- обмеження доступу працівників підприємства до документів з грифом "Комерційна таємниця";

– персональна відповідальність посадових осіб за видачу дозволу на допуск / доступ до відомостей, що становлять комерційну таємницю підприємства;

– персональна відповідальність кожного користувача відомостей, що становлять комерційну таємницю підприємства, за збереження документів з грифом “Комерційна таємниця”;

– жорстка регламентація порядку робіт з документами, що становлять комерційну таємницю підприємства, зокрема перших керівників.

До документів, що становлять комерційну таємницю підприємства, допускаються працівники, які оформили допуск згідно даної політики.

На документах (текстових, вихідних машинограмах, КС тощо), що становлять комерційну таємницю підприємства, в правому верхньому кутку розробником документа ставиться гриф “Комерційна таємниця”, класифікаційний номер і номер екземпляра.

При роботі з документами з грифом “Комерційна таємниця” користуватися “Порядком обліку, зберігання і використання документів з грифом “Комерційна таємниця”, розробленим відповідно до вимог інструкцій Кабінету Міністрів України.

Організація захисту відомостей, що становлять комерційну таємницю підприємства на АРМ і в корпоративній мережі підприємства

До роботи на АРМ допускаються користувачі, які пройшли навчання і володіють певними знаннями і вміннями. За кожним АРМ корпоративної мережі підприємства закріплюється відповідальний користувач. Забороняється допускати до роботи за АРМ сторонніх осіб.

Інсталяції операційних систем і установки/ зміни системно-технічних параметрів АРМ проводять лише фахівці ВСТО (відділу системного технічного обслуговування). Кожному АРМ фахівцями ВСТО привласнюється унікальне ім’я і опис, сформований відповідно до стандартної системи імен в корпоративній мережі _____ (назва підприємства).

На АРМ, зокрема на яких розробляються, зберігаються і використовуються відомості, що становлять комерційну таємницю підприємства, в обов’язковому порядку встановлюється:

Парольний захист на завантаження операційної системи і на доступ до інформаційних ресурсів корпоративної мережі:

– пароль повинен містити не менше 7-ти символів та не нести змістовного навантаження (при необхідності застосовується посилений захист за допомогою електронних ключів доступу);

– пароль змінюється не рідше одного разу на місяць;

– заборонено розголошувати паролі; записувати і зберігати в загальнодоступних місцях;

– заборонено здійснювати спроби доступу під чужим паролем і автоматичне введення пароля.

Антивірусний захист.

Система автоматичного виправлення помилок Windows.

На АРМ встановлюється і використовується програмне забезпечення, необхідне для виконання бізнес-функцій. На підприємстві діє перелік забороненого програмного забезпечення, в якому вказані програми і засоби, заборонені до установки.

Доступ до відомостей, що становлять комерційну таємницю підприємства та зберігаються на АРМ, здійснюється відповідно до вимог дозвільної системи допуску/ доступу даної політики.

Забороняється несанкціоноване надання доступу до ресурсів АРМ, серверів і інших комп'ютерних комплексів. На всіх АРМ діє спеціалізована програмна система, що забезпечує безпеку і контроль за його використанням.

АРМ в неробочий час мають бути вимкнені; залишені без нагляду – заблоковані. Відомості, що становлять комерційну таємницю підприємства, у вигляді файлів зберігаються на АРМ користувача в спеціальній папці. Доступ до даного файлу захищений паролем.

Заборонено зберігати відомості, що становлять комерційну таємницю підприємства у вигляді файлів тимчасово та / або постійно на дисках загального користування.

Інформаційний обмін між АРМ проводиться лише через контрольовані спільні ресурси АРМ адміністраторів КС всередині кожного підрозділу або виділені сервера корпоративної мережі між підрозділами.

Передавати відомості, що становлять комерційну таємницю підприємства, через мережу Internet у тому числі і по електронній пошті – заборонено.

Для усунення можливих каналів витоку відомостей, що становлять комерційну таємницю підприємства, відключаються або пломбуються спеціальною пломбою USB-порти, а також пишучі приводи CD\DVD-RW на всіх АРМ, що не мають дозвільних документів встановленої форми (Додаток Щ).

АРМ і корпоративна мережа підприємства від загроз з мережі Internet постійно захищені брандмауером, антивірусним і антиспам сервером.

Забороняється несанкціоноване сканування мережі, пошук і використання слабких місць в інформаційних системах. Забороняється встановлювати і використовувати на АРМ засоби перехоплення, збору і злому паролів, облікових даних і іншої інформації з корпоративної мережі підприємства, АРМ, серверів.

Корпоративні сервери підприємства встановлюються лише в спеціалізованому мегацентрі та обслуговуються навченими і допущеними співробітниками ВСТО.

Всесвітня мережа Internet та корпоративна мережа підприємства логічно розділені (АРМ, що працює в мережі Internet, не має доступу до корпоративної

мережі підприємства і навпаки). Мережа перших керівників підприємства логічно і фізично відокремлена від корпоративної мережі. Доступ до мережі Internet здійснюється через єдиний виділений проксі-сервер підприємства.

Доступ з мережі Internet до певних ресурсів корпоративної мережі підприємства можливий тільки через спеціалізований і контрольований VPN-сервер.

Заборонений доступ користувачів до інформації з мережі Internet, що не стосується виконуваних бізнес-функцій. Забороняється листування з контрагентами, що мають адреси на безкоштовних поштових серверах в Internet.

Організація захисту відомостей, що становлять комерційну таємницю підприємства в комп'ютерних системах.

У сучасних умовах найважливішим засобом накопичення, зберігання, обробки, передачі інформації є комп'ютерні системи. За допомогою комп'ютерних систем можна отримувати цінну комерційну інформацію, яка активно використовується в процесі організації виробництва, здійснювати пошук кращих умов реалізації продукції, використовувати новітню техніку і технології, здійснювати пошук відомостей про конкурентів, партнерів і т.д.

Захист відомостей, що становлять комерційну таємницю підприємства, здійснюється на всіх стадіях життєвого циклу, на всіх технологічних етапах обробки інформації і у всіх режимах функціонування комп'ютерної системи шляхом створення КСЗІ. Процес створення КСЗІ комп'ютерної системи включає етапи:

- загальні вимоги до захисту інформації в КС;
- розробка розділу по захисту інформації в ТЗ на створення КС;
- проектування КСЗІ;
- впровадження і тестування КСЗІ;
- експлуатація КСЗІ комп'ютерної системи.

Загальні вимоги до захисту інформації в комп'ютерних системах

На етапі формування загальних вимог до захисту інформації в КС розпорядженням заступника головного інженера з АСУ формується проектна група з розробки КС. До складу проектної групи включаються розробники КС, представники замовника, фахівці із захисту інформації, системні програмісти і обслуговуючий персонал. Складу проектної групи відкривається допуск до відомостей, що становлять комерційну таємницю підприємства по підрозділу замовника згідно даної політики.

Проектна група формує загальні вимоги із захисту інформації в комп'ютерній системі. Основу загальних вимог складають базові вимоги до захисту інформації в КС, які виконуються базовою КСЗІ, що складається з комплексу організаційних заходів і системно-технічних засобів корпоративної інформаційної системи.

При необхідності (виявлення додаткових загроз і каналів просочування інформації, підвищення цінності інформації тощо.) проектною групою

формуються додаткові вимоги до базової КСЗІ в комп'ютерній системі, що розробляється.

Розробка розділу по захисту відомостей, що становлять комерційну таємницю в технічному завданні на створення комп'ютерної системи

На підставі базових вимог фахівцями із захисту інформації ІАСУ і розробниками КС розробляється розділ по захисту інформації в технічному завданні (ТЗ) на створення КС. ТЗ на розробку КС розробляється відповідно до вимог міждержавного ДСТУ 34.602-79 "Інформаційна технологія. Комплекс стандартів на автоматизовані системи. Технічне завдання на створення автоматизованої системи".

Якщо в ТЗ вибрана базова КСЗІ, то в розділі ТЗ "Захист інформації" вказується, що базова КСЗІ є достатньою і гарантує адміністративну конфіденційність, цілісність, доступність і спостережуваність оброблюваної інформації в КС.

На основі додаткових вимог до базової КСЗІ розробляється ТЗ на доопрацювання базової КСЗІ.

Розділ по захисту інформації в ТЗ на розробку КС узгоджується у встановленому порядку.

Разробка системи захисту відомостей, що становлять комерційну тайну підприємства у комп'ютерній системі

На етапі проектування КС розробники КС згідно ТЗ на розробку КС (розділ "Захист інформації") застосовують базові КСЗІ в техно-робочому проекті. У разі, коли базова КСЗІ є недостатньою, фахівцями із захисту інформації ІАСУ і розробниками КС розробляються додаткові економічно обґрунтовані заходи захисту інформації, тобто розробляється "План захисту інформації в КС", в якому визначаються конкретні організаційно-правові і програмно-технічні заходи щодо захисту інформації, виконавці і терміни виконання.

Впровадження і тестування системи захисту інформації в комп'ютерній системі

Впровадження і тестування системи захисту інформації в КС проводиться одночасно з тестуванням і впровадженням комп'ютерної системи на етапі дослідної експлуатації відповідно до порядку, визначеному в ТЗ на розробку КС.

Для проведення тестування створюється комісія, яка складається з представників замовника КС, розробника КС і фахівців із захисту інформації. Тестування проводиться з використанням умовної інформації.

Результати тестування оформляються протоколом, який підписується членами комісії і затверджується заступником головного інженера з АСУ.

Експлуатація системи захисту інформації в комп'ютерній системі

На етапі дослідно-промислової і промислової експлуатації організовується навчання користувачів і обслуговуючого персоналу нормам і вимогам забезпечення безпеки інформації при роботі в КС, проводиться аналіз ефективності функціонування КСЗІ. В разі виявлення недоліків або виникнення

нових вимог замовника до системи захисту інформації розроблюються додаткові заходи по захисту інформації.

Замовником, розробником КС, фахівцями групи захисту інформації ІАСУ і адміністратором комп'ютерної системи підрозділу здійснюється контроль за виконанням користувачами вимог технологічних інструкцій із захисту інформації, вносяться зміни в списки користувачів, проводиться повторний інструктаж на вимогу замовника або розробника КС.

Обов'язки працівників підприємства допущених до відомостей, що становлять комерційну таємницю підприємства

Працівники, допущені до робіт, документів і до відомостей, що становлять комерційну таємницю, несуть особисту відповідальність за дотримання ними встановленого режиму. Перш, ніж дістати доступ до комерційної інформації, вони повинні вивчити вимоги даного положення і інших нормативних документів із захисту комерційної таємниці в частині, що їх стосується, здати залік на знання вказаних вимог і дати індивідуальне письмове зобов'язання зі збереження комерційної таємниці.

Працівники підприємства, допущені до робіт, документів і до відомостей, що становлять комерційну таємницю підприємства, зобов'язані:

– суворо берегти комерційну таємницю, що стала їм відомою по роботі або іншим шляхом, присікати дії інших осіб, які можуть призвести до розголошення комерційної таємниці. Про такі дії, а також про інші причини або умови можливого витоку комерційної таємниці негайно інформувати безпосереднього керівника і групу захисту інформації ІАСУ;

– не використовувати відому комерційну таємницю в свою особисту користь, а також без відповідного дозволу керівництва займатися будь-якою діяльністю, яка, як конкретна дія, може завдати шкоду підприємству;

– виконувати лише ті роботи і ознайомлюватися тільки з тими документами, до яких дістали доступ через свої службові обов'язки;

– знати ступінь важливості виконуваних робіт, правильно визначати обмежувальний гриф документів, суворо дотримуватися правила користування, їх обліку і зберігання;

– при складанні документів з відомостями, що становлять комерційну таємницю, обмежуватися мінімальними, дійсно необхідними в документі відомостями; визначати кількість екземплярів документів в суворій відповідності зі службовою необхідністю і не допускати розсилки їх адресатам, до яких вони не мають відношення;

– після закінчення роботи з документами з грифом "Комерційна таємниця" своєчасно повертати їх фахівцеві, відповідальному за ведення обліку документів з грифом "Комерційна таємниця";

– про втрату або недостачу документів з грифом "Комерційна таємниця", негайно повідомляти керівництво підрозділу;

– при звільненні, перед виходом у відпустку, від'їздом у відрядження своєчасно здавати документи, що обліковуються за ними, фахівцеві, відповідальному за реєстрацію, облік і зберігання документів з грифом "Комерційна таємниця";

– знайомити представників інших підприємств, організацій з документами з грифом "Комерційна таємниця" тільки з відома і з письмового дозволу керівника підприємства за наявності договору на проведення спільних робіт;

– документи з грифом "Комерційна таємниця" під час роботи розташовувати так, щоб унеможливити ознайомлення з ними інших осіб, зокрема допущених до подібних робіт і документів, але що не має до них прямого відношення;

– на першу вимогу фахівця, відповідального за документообіг документів з грифом "Комерційна таємниця", або групи захисту інформації ІАСУ пред'являти для перевірки всі документи з грифом "Комерційна таємниця", які обліковуються та наявні у даної особи.

Особливості поточної роботи з користувачами відомостей, що становлять комерційну таємницю підприємства

Поточна робота з персоналом-користувачем інформації, яка складає комерційну таємницю підприємства, включає:

– навчання і систематичний інструктаж співробітників;

– виховну роботу з персоналом, що працює з інформацією, яка складає комерційну таємницю підприємства;

– постійний контроль за виконанням персоналом вимог із захисту інформації, яка складає комерційну таємницю підприємства;

– проведення службових розслідувань за фактами просочування інформації і порушень персоналом вимог із захисту інформації;

– вдосконалення методики поточної роботи з персоналом.

Процес навчання співробітників підприємства правилам захисту інформації здійснюється постійно, оскільки система захисту інформації вимагає регулярного оновлення і видозміни.

Навчання співробітника розпочинається з моменту проведення співбесіди з ним при прийомі на роботу і закінчується звільненням.

Завдання навчання включають вивчення:

– характеру і складу відомостей, що становлять комерційну таємницю підприємства;

– можливих загроз і каналів витоку інформації, що становлять комерційну таємницю підприємства, методів роботи зловмисників;

– законодавства України в галузі захисту інформації;

– правил захисту інформації і порядку роботи співробітників підприємства з інформацією, яка складає комерційну таємницю підприємства в документарному і електронному видах;

– дій персоналу при виникненні нештатних та екстремальних ситуацій.

Навчання співробітників підприємства спрямоване на надбання ними і підтримку на високому рівні умінь і навиків роботи з інформацією, яка складає комерційну таємницю підприємства, психологічне виховання у співробітників глибокої переконаності в необхідності виконання вимог із захисту інформації, яка складає комерційну таємницю. Персонал отримує знання за оцінкою важливості тих або інших відомостей для зміцнення престижу підприємства і його економічної безпеки.

Методика навчання включає:

1. Лекції і практичні заняття з курсів:

– “Експлуатація і забезпечення інформаційної безпеки комп’ютерних систем” для адміністраторів комп’ютерних систем структурних підрозділів;

– “Забезпечення безпеки інформації при експлуатації комп’ютерних систем” для користувачів комп’ютерних систем.

2. Лекції, семінари і співбесіди ознайомлювального плану з конкретних напрямів захисту (семінар керівників структурних підрозділів і їх заступників з теми “Система захисту інформації, яка складає комерційну таємницю підприємства”, семінар фахівців, відповідальних за документообіг документів з грифом “Комерційна таємниця” і ін.).

3. Вирішення ситуаційних завдань, пов’язаних з виконанням необхідних вимог із захисту інформації, яка складає комерційну таємницю підприємства.

4. Практичне навчання персоналу при виникненні екстремальних ситуацій (зараження комп’ютера вірусом тощо).

5. Окремі теми з захисту інформації диференційовано на курсах з підготовки, перепідготовки і навчання працівників різних професій, підготовки резерву керівників.

Періодичність навчання співробітників – один раз в 3-5 років.

Одночасно з навчанням регулярно проводяться наради-інструктажі з персоналом з захисту інформації. В процесі інструктажу:

– до відома співробітників доводяться зміни та доповнення, внесені до нормативно-методичних документів, що діють, з захисту інформації, накази і розпорядження керівництва _____(назва підприємства) в частині захисту бухгалтерської інформації та інформаційної безпеки;

– проводиться інформування співробітників про нові загрози інформації, яка складає комерційну таємницю, нові канали просочування інформації, дії зловмисників, прийняті додаткові заходи з захисту інформації;

– доводиться аналіз випадків порушення правил захисту інформації, повідомляються факти розголошування інформації, що становлять комерційну таємницю підприємства, з вини співробітників.

Отже, обов'язковою і первинною особливістю поточної роботи з персоналом є навчання співробітників підприємства правилам роботи з інформацією, яка складає комерційну таємницю підприємства. Формування у всього персоналу підприємства відповідної інформаційної культури.

Виховання – процес систематичної і цілеспрямованої дії на формування і розвиток особистості з метою якнайповнішого використання її професійних здібностей, ділових, моральних і інших позитивних якостей для збільшення ефективності діяльності підприємства, підвищення його конкурентоспроможності.

Дія на особу здійснюється керівниками в процесі навчання і інструктажу співробітників і колективом підприємства в процесі вирішення спільних виробничих завдань.

Під виховною роботою мається на увазі, передусім, створення реального здорового психологічного клімату в колективі цеху (відділу) і підприємства в цілому, що дозволяє об'єднати зусилля персоналу на вирішення завдань, що стоять перед підприємством, і подолання будь-яких виникаючих труднощів. Цінність персоналу підприємства з часом постійно зростає внаслідок накопичення знань і досвіду кожного працівника і всім колективом в цілому.

Здоровий психологічний клімат в колективі підприємства створює перешкоду на шляху будь-якого зловмисника, який намагається отримати інформацію, що становить комерційну таємницю підприємства.

Працівник, що відповідально відноситься до своєї роботи і бере активну участь в справах підприємства, відповідально відноситься до збереження конфіденційності робіт, які виконує підприємство, суворо виконує вимоги із захисту інформації, яка складає комерційну таємницю підприємства.

Основні форми контролю якості роботи персоналу – користувача інформації, яка складає комерційну таємницю підприємства

Основними формами контролю якості роботи персоналу, підвищення працівниками їх професійних знань, зокрема в частині захисту інформації, яка складає комерційну таємницю підприємства, є:

– атестація;

– регулярні перевірки членами експертної комісії підприємства із захисту інформації, керівниками підрозділів, групою захисту інформації ІАСУ дотримання співробітниками норм і вимог із захисту інформації, яка складає комерційну таємницю підприємства;

– самоконтроль співробітників.

Атестація співробітників є однією з ефективних форм контролю якості роботи персоналу. Атестація персоналу – це колективна форма оцінки професійної придатності співробітника, його відповідності посаді. Атестація проводиться періодично один раз на 3 роки.

При проведенні атестації розглядаються наступні характеристики співробітника: трудова дисципліна, старанність, працьовитість, відповідальність і принциповість, організованість в роботі, якість і ефективність виконуваної роботи, самостійність та ініціатива, творча діяльність, прогресивність професійних рішень, професійний кругозір, уміння поводитися з людьми, організаторські здібності, відданість підприємству. У частині дотримання співробітником вимог захисту інформації розглядається знання нормативних документів щодо захисту інформації, уміння застосовувати вимоги цих документів в практичній діяльності, відсутність порушень в роботі з інформацією, яка складає комерційну таємницю підприємства, уміння спілкуватися зі сторонніми особами тощо. На підставі вивчення цих характеристик формується уявлення про кожного співробітника, його ділові і людські якості.

За результатами атестації видається наказ, в якому відбиваються рішення атестаційних комісій про заохочення, переатестацію, підвищення на посаді або звільнення співробітників.

Формою контролю є також регулярні перевірки виконання співробітниками підрозділів правил роботи з інформацією, яка є складовою комерційну таємницю підприємства, ефективності навчання і готовності персоналу до виконання дій, пов’язаних із забезпеченням інформаційної безпеки. Перевірки проводяться членами експертної комісії підприємства із захисту інформації, керівниками структурних підрозділів, співробітниками групи захисту інформації ІАСУ відповідно до положення “Про контроль дотримання норм і вимог захисту інформації в підрозділах підприємства”.

Самоконтроль співробітників підприємства полягає в:

– перевірці повноти і правильності виконання ними діючих інструкцій, положень із захисту інформації, яка склад комерційну таємницю підприємства;

– негайному інформуванні керівників підрозділів і групи захисту інформації ІАСУ про факти втрати, порушень цілісності (спотворення, модифікації, руйнування, знищення) інформації, яка складає комерційну таємницю підприємства, порушеннях правил допуску і доступу до інформації, яка складає комерційну таємницю підприємства в комп’ютерним системам.

6. ВІДПОВІДАЛЬНІСТЬ

Під відповідальністю за недотримання економічної безпеки слід розуміти понесення покарання за розголошення або неналежне використання інформації, яка становить комерційну таємницю підприємства, та порушення правил та експлуатації технічних засобів безпеки.

В сфері недотримання політики економічної безпеки передбачаються наступні випадки відповідальності:

За порушення норм і вимог захисту відомостей, що становлять комерційну таємницю підприємства:

Відповідальність за порушення норм і вимог захисту інформації вводиться з метою розширення методів економічної дії, спрямованих на забезпечення захисту інформації, яка складає комерційну таємницю підприємства, і інформаційної безпеки підприємства як першочергових складових всієї економічної безпеки _____ (назва підприємства).

Оскільки на підприємстві функціонує багаторівнева структура розмежування допуску до відомостей, що становлять комерційну таємницю підприємства, то відповідальність за неналежне використання такої інформації або її розголошення також є пропорційним, тобто чим вище цінність інформації, тим суворішим є покарання.

Для визначення фактичного стану збереженості інформації необхідно:

1. Провести перевірки комплексними комісіями, очолюваними членами експертної комісії (ЕК) підприємства із захисту інформації.

2. У випадку виявлення порушень ЕК повинна подати керівникові підрозділу розпорядження з оформленими результатами перевірки, копію розпорядження направити до ЕК підприємства із захисту інформації.

3. Протягом 1 робочого тижня керівник підрозділу повинен прийняти заходи щодо усунення недоліків та підготувати звіт ЕК із захисту інформації про виконання вимог розпорядження.

4. Експертна комісія підприємства із захисту інформації на своєму засіданні розглядає представлений документ і пропонує комісії підприємства з розгляду матеріалів оцінки трудового внеску колективів, фахівців і службовців в основні результати господарської діяльності кількісний показник (відсоток) покарання винних в порушенні норм і вимог захисту інформації (Додаток Ю).

5. Рішення ЕК підприємства із захисту інформації оформлюється протоколом (Додаток Я) і в комісію з розгляду матеріалів оцінки трудового внеску колективів, фахівців і службовців в основні результати господарської діяльності для ухвалення рішення і підготовки наказу про виплату премії.

Відповідно до даного документу до відповідальності притягаються працівники підприємства, які порушили умови договірного зобов'язання про нерозголошення відомостей, які становлять комерційну таємницю підприємства (Додаток Ж).

У випадку порушення “Угоди про нерозголошення інформації, яка складає комерційну таємницю підприємства, при звільненні” (Додаток Ш) особою, яка звільнилася з підприємства або “Договору про нерозголошення комерційної таємниці” державними посадовими особами, вони притягаються до відповідальності у порядку встановленому чинним законодавством України.

За порушення правил та експлуатації технічних засобів безпеки

Відповідальність за порушення норм і вимог утримання та експлуатації технічних засобів безпеки запроваджується з метою розширення методів економічної дії, спрямованих на забезпечення захисту матеріальних і фінансових цінностей підприємства, як першочергових складових всієї економічної безпеки _____ (назва підприємства).

Проведення планових перевірок і розслідування фактів порушення правил експлуатації технічних засобів безпеки покликане не тільки для підвищення відповідальності всього персоналу за збереження матеріальних і фінансових цінностей, але і запобігання фактам крадіжок, розкрадань, обмеження можливост нейтралізації дії систем охоронно-пожежної сигналізації.

Навмисні дії, спрямовані на виведення з ладу технічних засобів охорони, які погіршують їх технічні параметри, розглядаються, як спроба завдати навмисної шкоди економічній безпеці підприємства та переслідуються згідно із законодавством.

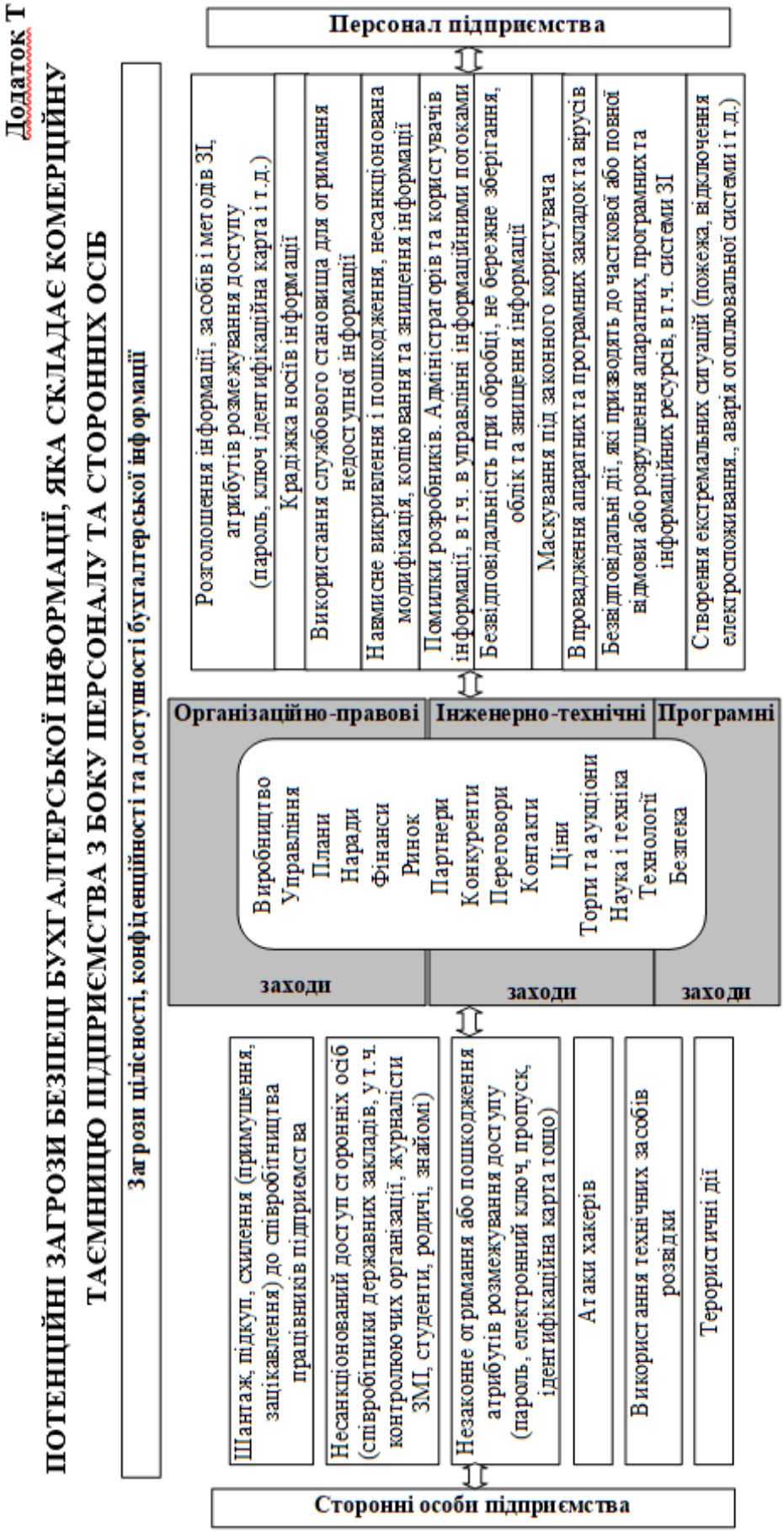
7. ІСТОРІЯ ЗМІН ДАНОЇ ПОЛІТИКИ

Дана “Політика економічної безпеки підприємства” перероблена відповідно до п. _ розділу __ “Забезпечення економічної безпеки” наказу № _ на 20__ р., як додаток до базових нормативних документів, що становлять основу організаційного напряму системи захисту бухгалтерської інформації, яка складає комерційну таємницю _____(назва підприємства) та основних напрямів вдосконалення кадрової політики _____(назва підприємства) в період до 20__ р.

Дана політика може бути змінена та доповнена. Зміни та доповнення здійснюються при зміні законодавства України або при виявленні нових загроз економічній безпеці підприємства.

Додаток Т

ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ БУХГАЛТЕРСЬКОЇ ІНФОРМАЦІЇ, ЯКА СКЛАДАЄ КОМЕРЦІЙНУ ТАЄМНИЦЮ ПІДПРИЄМСТВА З БОКУ ПЕРСОНАЛУ ТА СТОРОННІХ ОСІБ



Додаток У

ЛИСТ СПІВБЕСІДИ

кандидата на робоче місце _____

Прізвище_____ ім'я_____ по батькові _____

Дата народження: "___" _____ _____ р. Освіта: _____

Назва закладу: _____ та рік його закінчення_____

Спеціальність за дипломом: _____ форма навчання _____

Кваліфікація за дипломом: _____ успішність _____

Позапрофесійні навики _____

_____

Досягнення в професійній кар'єрі _____

Причина пошуку нового місця роботи _____

Інші відомості _____

1. Результати співбесіди з фахівцем відділу кадрів

№	*Оцінювані якості*	*5*	*4*	*3*	*2*	*1*
1	Зовнішні враження, зовнішній вигляд, манера поведінки					
2	Здатність виражати свої думки					
3	Упевненість в собі					
4	Здібність до навчання, розвитку проф. майстерність					
5	Здатність працювати в групі, адаптивність					
6	Інтелект, здібність до творчого мислення					
7	Відповідність корпоративній культурі підприємства					

Рекомендації ВК: _____

Підпис фахівця ВК, що проводив співбесіду _____ (_____)

2. Результати співбесіди з технічними фахівцями

1) Підрозділ _____ Посада _____ ПІБ _____

№	*Оцінювані характеристики*	*5*		*4*		*3*		*2*		*1*	
		1	*2*	*1*	*2*	*1*	*2*	*1*	*2*	*1*	*2*
1	Рівень професійних знань										
2	Технічне мислення по професії										
3	Здібність до якісного виконання роботи										

Висновок технічного фахівця: _____

_____

3. Результати співбесіди із заступником генерального директора з виробництва

№	*Оцінювані якості*	*5*	*4*	*3*	*2*	*1*
1	Рівень професійних знань					
2	Рівень освіти і кваліфікації					
3	Здібність до навчання і розвитку					
4	Знання специфіки пропонованої роботи					
5	Технічне мислення по професії					

Висновки та пропозиції: _____

_____

4. Результати співбесіди з начальником цеху (відділу)

№	*Оцінювані якості*	*5*	*4*	*3*	*2*	*1*
1	Рівень професійних знань					
2	Рівень освіти і кваліфікації					
3	Здатність адаптації в трудовому колективі					
4	Комунікабельність, здібність до контактів					
5	Мотивація до якісного виконання роботи					
6	Здібність до навчання і розвитку					
7	Знання специфіки пропонованої роботи					

Висновки та пропозиції начальника цеху (відділу): _____

_____

Підпис _____

5. Результати співбесіди з фахівцями групи захисту інформації ІАСУ

№	*Оцінювані якості*	*5*	*4*	*3*	*2*	*1*
1	Самоконтроль у вчинках і діях					
2	Здібність до правильних дій в екстремальній ситуації					
3	Відповідність інформаційній культурі					
4	Здібність до добровільної згоди на певні обмеження в інформаційній діяльності					

Висновки: ___

Підпис _____

Дата співбесіди ___ _____ р.

Рішення начальника відділу кадрів _____

_____

Підпис _____

Додаток Ф

Доступ дозволяю: Заст. головного інженера з АСУ

_____ _____ _____ _____

(Посада власника або координатора бізнес-процеса) (підпис) (ПІБ) (підпис)

ДОЗВІЛ № ___

на надання доступу до документів, які складають комерційну таємницю підприємства, по _____
(підрозділ)

ПІДСТАВА

_____

(дозвіл відповідального за перетворення і управління бізнес-процесом, вимога замовника і т.д.)

№ з/п	*ПІБ фахівця, керівника якому необхідно надати доступ*	*Посада*	*Особистий номер*	*Перелік документів, щодо яких вирішується доступ*	*Регламент (час) роботи*	*Читання*	*Модифікація*	*Копіювання*	*Зберігання*	*Видача і облік*	*Утилізація*	*Відмітка користувача про наданий допуск*	
												Дата	*Підпис*
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*

Керівник підрозділу, що подає запит про доступ до документа (ів) _____ _____ _____ _____

(шифр підрозділу) (дата) (підпис) (ПІБ)

Відповідальний за ведення документообігу, що становить комерційну таємницю в підрозділі _____ _____ _____ _____

(шифр підрозділу) (дата) (підпис) (ПІБ)

ПОГОДЖЕНО:

_____ _____ _____ _____ _____

(Керівник підрозділу – розробник документа) (шифр підрозділу) (дата) (підпис) (ПІБ)

*графи 6, 7, 8, 9, 10, 11 – мають значення "так" або "ні".

Додаток Х

Доступ дозволяю: Заст. головного інженера з АСУ

_____ _____ _____ _____

(Посада власника або координатора бізнес-процеса) (підпис) (ПІБ) (підпис)

ДОЗВІЛ № ____

на надання доступу до відомостей, що використовуються у комп'ютерних системах та складають комерційну таємницю підприємства, по _____

(найменування підрозділу)

Підстава: _____

(дозвіл відповідального за перетворення і управління бізнес-процесом, вимога замовника і т.д.)

№ з/п	*Відомості про користувача, якому необхідно надати доступ*			*Перелік КС до яких вирішується доступ*	*Регламент (час) роботи у КС*	*Номер АРМ за картотекою*	*Виконувані функції**				*Відмітка користувача КС про надання доступу*	
	ПІБ	*Посада*	*Особистий номер користувача*				*Перегляд*	*Модифікація*	*Видалення*	*Копіювання інформації на носії*	*Дата*	*Підпис*
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
1.												

Керівник підрозділу, що подає запит щодо доступу до КС _____ _____ _____ _____

(шифр підрозділу) (дата) (підпис) (ПІБ)

Адміністратор комп'ютерної системи підрозділи _____ _____ _____ _____ _____

(найменування підрозділу) (шифр підрозділу) (дата) (підпис) (ПІБ)

ПОГОДЖЕНО:

_____ _____ _____ _____ _____

(керівник підрозділу – розробник комп'ютерної системи) (шифр підрозділу) (дата) (підпис) (ПІБ)

графи 8, 9 10, 11 – мають значення "та" або "ні".

*виконувані функції уточнюються в техно-робочому проекті.

Додаток Ц

Суб'єкти (правоохоронні та контролюючі органи) та юридична підстава на допуск до відомостей, що становлять комерційну таємницю підприємства

Назва правоохоронного або контролюючого органу	*Посилання на норми законів України*	*Термін виконання запиту чи вимоги*
Прокуратура	Закон України "Про прокуратуру" ст. 8 ч. 1	В термін, вказаний у письмовому запиті (ст. 20 ч.1)
Органи внутрішніх справ	Закон України "Про міліцію" ст. 11 п. 17	В термін, вказаний в письмовому запиті
Адвокатура	Закон України "Про адвокатуру" ст. 6 вказує на те, що адвокат має доступ до всіх відомостей, які стосуються його клієнта, за винятком тих, таємниця яких оберігається Законом. Відповідно, адвокат допускається до інформації, яка складає комерційну таємницю підприємства, виключно тільки на основі рішення керівника даного підприємства	
Служба безпеки України	Закон України "Про Службу безпеки України" ст. 26 п. 3	В термін, вказаний в письмовому запиті керівника відповідного органу СБУ
Спеціальні підрозділи МВС та СБУ по боротьбі з організованою злочинністю	Закон України "Про організаційні основи боротьби з організованою злочинністю" ст. 12	Негайно, якщо неможливо, не пізніше 10 днів
Органи державної податкової служби	Закон України "Про державну податкову службу" ст. 11 п. 6	В термін, вказаний в письмовому запиті
Державна контрольно-ревізійна служба	Закон України "Про державну контрольно-ревізійну службу України" ст. 10 п. 6 (довідки та копії документів про операції та розрахунки з підприємствами, організаціями, які ревізуються або перевіряються)	В термін, вказаний в письмовому запиті
Антимонопольний комітет	Закон України "Про антимонопольний комітет України" ст. 22-1 ч.: інформація, яка стосується виконання антимонопольного законодавства	В термін, вказаний в письмовому запиті
Оперативні підрозділи МВС України, СБУ, прикордонних військ, управління державної охорони, органів державної податкової служби, органів та організацій Державного департаменту України з питань виконання наказів	Закон України "Про оперативно-пошукову діяльність" Ст. 8 п. 4	В термін, вказаний в письмовому запиті

Додаток Ш

УГОДА
ПРО НЕРОЗГОЛОШЕННЯ ІНФОРМАЦІЇ, ЯКА СКЛАДАЄ КОМЕРЦІЙНУ ТАЄМНИЦЮ _____,
(назва підприємства)
ПРИ ЗВІЛЬНЕННІ

Я, _____ _____ під час моєї роботи в _____
(прізвище ім'я, по батькові) (підрозділ, посада)
мав(ла) доступ до інформації, яка складає комерційну таємницю _____.
(назва підприємства)

№ з/п	*Найменування інформації*	*Класифікаційний номер*

Я підтверджую, що при допуску до інформації, яка складає комерційну таємницю підприємства, був проінструктований та підписав(ла) договірне зобов'язання про її нерозголошення.

Я зобов'язуюся не використовувати знання інформації, яка складає комерційну таємницю підприємства, для заняття будь-якою діяльністю, яка як конкурентна дія може завдати збитку ____ _____
(назва підприємства)

протягом року.

Я підтверджую, що всі носії відомостей, які складають комерційну таємницю підприємства (документи, креслення, дискети, БД, вихідні машинограми, початкові тексти програм тощо), які знаходилися в моєму розпорядженні у зв'язку з виконанням мною службових обов'язків, здав співробітникові, відповідальному за облік та зберігання матеріальних носіїв відомостей, що складають комерційну таємницю.

_____ _____
(дата) (підпис)

_____ позбавлений доступу до інформації, яка
(прізвище, ім'я, по батькові)
складає комерційну таємницю підприємства. Його підпис засвідчую.

Керівник підрозділу _____ _____
(підпис) **(прізвище, ім'я, по батькові)**

Дата звільнення _____
(число, місяць, рік)

Начальник відділу кадрів _____ _____
(підпис) **(прізвище, ім'я, по батькові)**

Додаток Щ

ЗАТВЕРДЖУЮ
Заступник генерального
директора
голова експертної комісії
підприємства із захисту
інформації

_____

ДОЗВІЛ
на використання зовнішніх пристроїв

№ з/п	*ПІБ відповідального за АРМ*	*Номер АРМ згідно картотеки відділу системного технічного обслуговування (ВСТО)*	*Дозволено використовувати*		*Обґрунтування*
			USB пристрої	*CD\DVD-RW*	
1	*2*	*3*	*4*	*5*	*6*

Керівник підрозділу _____ (шифр підрозділу) _____ (дата) _____ (підпис) _____ (ПІБ)

Додаток Ю

ШКАЛА
покарань за порушення норм і вимог захисту інформації

Категорія порушень норм і вимог захисту інформації	Покарання за порушення норм і вимог захисту інформації
Перша категорія	від –25% від К до –100% від К
Друга категорія	від –10% від К до –50% від К

Примітка: К – встановлений розмір премії за основні результати господарської діяльності по підрозділу.

Додаток Я

ПРОТОКОЛ
засідання експертної комісії підприємства із захисту інформації

№ ____ від _____ 20__ р.

Експертна комісія підприємства із захисту інформації розглянувши результати перевірок з дотриманню норм і вимог захисту інформації (розпорядження №___) за звітний місяць, пропонує комісії підприємства з розгляду матеріалів оцінки трудового внеску колективів, фахівців та службовців в основні результати господарської діяльності для розгляду і включення в наказ про виплату премії відповідно до положення "Про преміювання керівників, фахівців та службовців підприємства за основні результати господарської діяльності" наступних фахівців:

Найменування підрозділу (код)	*ПІБ*	*Таб. №*	*Посада*	*Відсоток зниження премії*
1	*2*	*3*	*4*	*5*

Голова експертної комісії підприємства із захисту інформації _____

Секретар експертної комісії підприємства із захисту інформації _____

Наукове видання

НОНІК Валерій Вікторович
ДИКИЙ Анатолій Петрович
ДИКА Олена Сергіївна

ІНФОРМАЦІЙНА МОДЕЛЬ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

МОНОГРАФІЯ

Редактор: *д.е.н., доц. Д.О. Грицишен*
Технічний редактор: *к.е.н., доц. Т.В. Барановська*
Коректор: *Т.М. Шаповал*

Формат 60×84 1/16. Ум. друк. арк. 14,42.
Зам. № 289, 2017 р.
Наклад 300 прим.

Видавець О.О. Євенок
м. Житомир, вул. Мала Бердичівська, 17а
тел.: (0412) 422-106

Свідоцтво про внесення суб'єкта виробничої справи
до Державного реєстру видавців, виготовників
і розповсюджувачів видавничої видавничої продукції України
серія ДК № 3544 від 05.08.2009 р.

Друк та палітурні роботи ФОП О.О. Євенок
м. Житомир, вул. Мала Бердичівська, 17а
тел.: (0412) 422-106, e-mail: book_druk@i.ua