УДК 657

Дикий А.П., аспірант
Житомирський державний технологічний університет
Семенчук М.В., студентка IV курсу
Житомирський державний технологічний університет

КОМЕРЦІЙНА ТАЄМНИЦЯ ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Визначено місце та значення комерційної таємниці в становленні системи економічної безпеки підприємства

Постановка проблеми. 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 ринкових умов, з урахуванням чинників невизначеності та нестійкості економічного середовища. Все це по-новому ставить питання про управління підприємством як суб'єктом ринкових відносин, про його спроможність пристосовуватися до динамічних умов ринку. Розробка наукових проблем із забезпечення безпеки облікових даних підприємства є важливою передумовою, спрямованою на забезпечення безпеки підприємства як на даному етапі розвитку, так і в майбутньому. Особливого значення набуває проблема визначення місця та значення комерційної таємниці у становленні системи економічної безпеки підприємства.

Метою дослідження виступає економічна безпека підприємства та комерційна таємниця як її прояв. Методика досягнення безпеки підприємства постійно удосконалюється; її можна назвати мистецтвом, якого слід вчитись; культурою, яку потрібно виховувати у кожного працівника підприємства.

Незважаючи на значні напрацювання в цій галузі, поза увагою дослідників залишився такий важливий аспект діяльності підприємства, як системна робота щодо попередження та недопущення небезпечних ситуацій. Можна сказати, що питання відносно забезпечення безпеки облікової інформації підприємства в сучасних умовах ще не набула ґрунтовної розробки. Не існує й цілісної концепції з питань планування економічної безпеки, здатної забезпечити повне використання наявного потенціалу, протидіяти загрозам, підтримувати стан економічної безпеки, про що дуже часто забувають нинішні керівники підприємств, які не лише не використовують наявні наукові розробки у цій сфері, але й забувають про організацію та забезпечення захисту комерційної таємниці та конфіденційної інформації на підприємстві. А це, як відомо, одна з основних та визначальних ланок забезпечення економічної безпеки підприємства.

Розвиток ринкової економіки суттєво змінює ставлення до проблеми забезпечення економічної безпеки, оскільки головною особою, зацікавленою у захисті своїх економічних та громадянських прав, стає підприємець, власник. Виходячи з цього виникає об'єктивна необхідність захисту облікових та фінансово-господарських показників діяльності підприємства.

Аналіз основних досліджень. Значний внесок в розробку концепції економічної безпеки зробили такі дослідники як В.П. Пономарьов [8], А.І. Солов'єв [9], І.О. Александров [2], Н. Капустін [5] та ін.

Постановка завдання. З урахуванням існуючих проблемних питань метою даного дослідження є визначення місця та значення комерційної таємниці в системі економічної безпеки підприємства.

Виклад основного матеріалу. У сучасній вітчизняній науковій літературі з даного питання виникає проблема, оскільки не існує

єдиної думки щодо визначення поняття економічна безпека. Дарнопих Г. визначає економічну безпеку як стан, який забезпечує економічний суверенітет, економічне зростання, підвищення добробуту в умовах економічної залежності [4, с. 142]. Н. Капустін дає наступне визначення: "Економічна безпека – 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 і внутрішніх факторів" [5]. Тобто економічна безпека не визначається як стан системи, а навпаки, передбачає не лише розробку системи оцінки, а й формування механізму забезпечення цього стану. Крім того, економічна безпека включає захист системи від дестабілізуючого впливу не лише непепередбачуваних та важкопрогнозованих факторів, що потребує аналітичного формулювання, а й від факторів передбачуваних та легкопрогнозованих.

Інші вчені визначають економічну безпеку підприємства як стан найефективнішого використання корпоративних ресурсів для уникнення загроз та забезпечення стабільного функціонування підприємства як в даний час, так і в майбутньому [7].

Співвідношення між рівнями економічної безпеки підприємств та держави є неодно-значним 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.

Ми розглядаємо концепцію саме економічної безпеки облікових даних, оскільки вона посідає головне місце в понятті безпеки як такої. Її сутність полягає у поступальному економічному розвитку з метою виробництва певних благ та послуг, які б задовольняли потреби споживачів. Тому під економічною безпекою підприємства слід розуміти стан захищеності життєво важливих інтересів підприємства від внутрішніх і зовнішніх загроз.

В дослідженні сутності економічної безпеки підприємства, як і будь-якому дослідженні, можна простежити певні тенденції. Так, ще на початку 90-х років спостерігалась тенденція до визначення економічної безпеки підприємства як його здатності до захисту комерційної таємниці, до складу якої керівники відносили майже усі показники господарської діяльності. Такий підхід був певною мірою виправданим, оскільки для того періоду були характерними зміна форм власності, підвищення самостійності підприємств, спроби вийти на ринки, скорочення державного регулювання в окремих сферах діяльності підприємств, початок конкуренції, можливість створювати підприємства різних видів та відсутність правового забезпечення. Все це спонукало підприємства захищати інформацію, і тому керівництво змушене було приховувати все або відносити до складу комерційної таємниці інформацію, яка не мала ніякого відношення до таємниці як економічної категорії [2, с. 13]. Ожегов С.І. наводить три значення таємниці: 1. Дещо нерозгадане, ще не пізнане. 2. Дещо приховуване від інших, відоме не всім, секрет. 3. Прихована причина будь-чого [6]. Завдяки розвитку законодавчої бази та економічної теорії ми розрізняємо такі поняття як: ***державна таємниця*** (під якою розуміється вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішньоекономічних відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України); ***комерційна таємниця*** (тобто перелік відомостей, документів, даних, які визначені керівником підприємства і які не підлягають розголошенню, згідно Постанови КМУ "Про перелік відомостей, що не становлять комерційної таємниці"); ***службова таємниця*** (яка передбачає склад та обсяг відомостей, що є в розпорядженні конкретного органу державної контрольно-ревізійної служби або його посадової особи стосовно об'єктів контролю, контрольних, правоохоронних та інших державних органів, їх працівників,

способів досягнення визначених законодавством завдань, що необхідні для якісного проведення контрольно-ревізійних дій, забезпечення відповідної їх раптовості та ефективності і які з цієї причини на певний період не підлягають зовнішньому чи внутрішньому розголошенню).

Проте у теорії права, та й у спеціальній літературі, крім поняття "комерційна таємниця", існує поняття "конфіденційної інформації". До останнього, вочевидь, відноситься узагальнений перелік відомостей, доступ до яких обмежений колом виконавців зі специфічними службовими обов'язками – таким працівникам заборонено розголошувати ці відомості. Зазначимо, що необхідність збереження службової інформації зазвичай не пов'язана з її комерційною цінністю, хоч і не виключається, що вона може мати комерційний характер. Кажучи про інформацію з обмеженим доступом, багато експертів пропонують керуватися таким принципом: *якщо конфіденційна інформація має комерційне значення, її захист здійснюється в режимі комерційної таємниці, а якщо інформація сама по собі комерційного значення не має, то така інформація вже не є комерційною таємницею, але може бути захищена від третіх осіб як конфіденційна.* В цьому випадку така інформація може вважатися *службовою таємницею*, так само як і службова таємниця працівників контрольно-ревізійної служби. Ці поняття слід розрізняти при складанні внутрішніх документів і регламентації відповідальності за витік тієї чи іншої інформації. Таким чином, погоджуючись з визначенням О. Шипка, зазначимо, що ***комерційна таємниця*** – це навмисно приховувані з комерційних міркувань економічні інтереси та відомості про різноманітні сторони та сфери виробничої, господарської, управлінської, науково-технічної, фінансової діяльності, охорона яких обумовлена інтересами конкуренції та можливими загрозами економічній безпеці. Комерційна таємниця виникає тоді, коли вона становить інтерес для комерції" [10, с. 29].

Оскільки ринок засобів і технологій економічної безпеки наповнюється і стає більш диверсифікованим, відбувається активне формування ринкових відносин перехідного періоду, здійснюється імпорт капіталу та технологій. Отже, це змушує учасників ринку створювати більш вдосконалені засоби забезпечення обліково-інформаційної безпеки, доповнювати засоби фізичної безпеки більш цивілізованими різновидами, включаючи технічні та юридичні засоби, до яких і належить інститут комерційної таємниці. Основні складові економічної безпеки підприємства можна представити у вигляді наступної схеми (рис. 1).

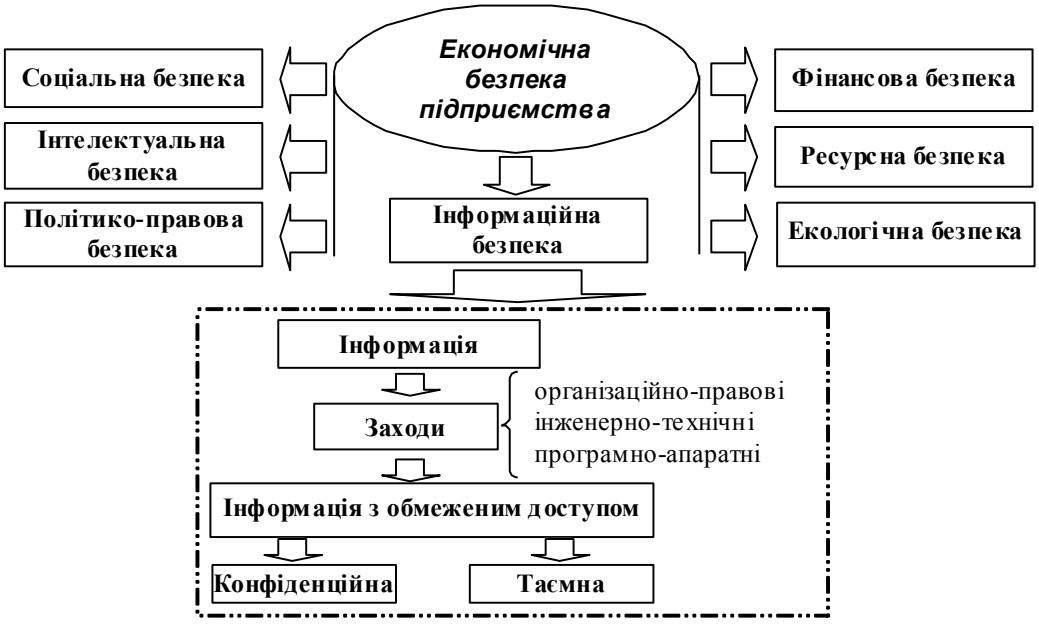

Рис. 1. Складові економічної безпеки підприємства

Розглянувши дану схему, можна прослідкувати значення комерційної таємниці в забезпеченні економічної безпеки. Складовими економічної безпеки є соціальна, інтелектуальна, політико-правова, екологічна, ресурсна, фінансова та інформаційна безпека. Інформаційна безпека досягається шляхом належного забезпечення комерційної таємниці на підприємстві, яка передбачає захист внутрішньої інформації підприємства та є організаційно-правовим заходом інформаційної безпеки. Саме тому сучасний підхід до забезпечення безпеки облікової інформації, перш за все, 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.

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”, Закон України “Про державну контрольно-ревізійну службу”, Закон України “Про інформацію”, Закон України “Про захист від недобросовісної конкуренції”, Постанова КМУ “Про перелік відомостей, що не становлять комерційної таємниці”. Документом, який здійснює регулювання процесу захисту комерційної таємниці, є Положення про комерційну таємницю на підприємстві, яке передбачає порядок доступу до інформації комерційного характеру та захищає власника від 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 кваліфікації та 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, тому що вона охороняється законодавством кожної 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.

Склад та обсяг інформації, що становить комерційну таємницю та порядок її захисту, визначається керівництвом підприємства, тобто, ця інформація належить підприємству з повним правом власності. Підприємство має право розпоряджатися такою інформацією на власний розсуд, здійснювати відносно даної інформації будь-які законні дії, а також не порушувати при цьому права третіх осіб.

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

Конфіденційну інформацію особам, які не працюють на даному підприємстві, краще взагалі не надавати. У випадку, коли уникнути цього неможливо, скажімо, потрібно укласти договір з новим клієнтом,

який вимагає надання інформації, яку ви вважаєте конфіденційною, необхідно включити в договір (до обов'язків сторін) застереження про конфіденційність та зазначити відповідальність сторін за розголошення конфіденційної інформації. До чинних договорів, які не передбачають відповідальності за розголошення конфіденційної інформації, слід укласти додаткові угоди або окремі договори про конфіденційність.

Таким чином, власник має як права, так і обов'язки стосовно захисту комерційної таємниці. Перш за все він повинен:

– видавати нормативні та розпорядчі документи, які б визначали порядок віднесення даних до таких, які становлять комерційну таємницю та механізми їх захисту;

– забезпечити захист такої інформації відповідно до вимог і правил, розроблених ним;

– повідомляти про всі факти порушення цього захисту;

– створювати організаційні структури із захисту комерційної таємниці або покладати ці функції на посадових осіб, відповідні підрозділи;

– включати вимоги із захисту комерційної таємниці в договори за всіма видами господарської діяльності;

– вимагати захист інтересів підприємства перед державними та судовими органами;

– розпоряджатися інформацією, що є власністю підприємства, з метою отримання вигоди та недопущення збитку [1, с. 14-15].

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

З цього слідує, що економічну безпеку неможливо забезпечити без належного рівня інформаційної безпеки, яку необхідно контролювати, а також створювати умови для її управління та ефективного функціонування.

Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання загрозам його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення крадіжок фінансових засобів, розголошення, втрати, витоку, викривлення чи знищення службової інформації, забезпечення в рамках виробничої діяльності всіх підрозділів підприємства.

Більш детальний розгляд цієї проблеми дозволяє сформулювати основні завдання системи інформаційної безпеки підприємства:

– необхідність віднесення визначеної інформації до категорії обмеженого доступу (службової або комерційної таємниці або виділення окремого типу даних конфіденційного характеру);

– прогнозування та своєчасне виявлення загроз безпеці інформаційних ресурсів, причин та умов, які спричиняють заподіяння фінансового, матеріального чи морального збитку, порушення його нормального функціонування та розвитку;

– створення умов функціонування з найменшою ймовірністю реалізації загроз безпеці інформаційних ресурсів та нанесення різного роду збитків;

– створення механізму та умов оперативного реагування на загрози інформаційній безпеці та прояв негативних тенденцій у функціонуванні, ефективне попередження посягань на ресурси на основі правових, організаційних та технічних заходів та засобів безпеки;

– створення умов для максимально можливого відшкодування та локалізації збитку, який наноситься неправомірними діями фізичних чи юридичних осіб, послаблення негативного впливу наслідків порушення інформаційної безпеки.

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.

Проаналізувавши вище наведене, загрози інформаційної безпеки можна поділити на дві групи (рис. 2).

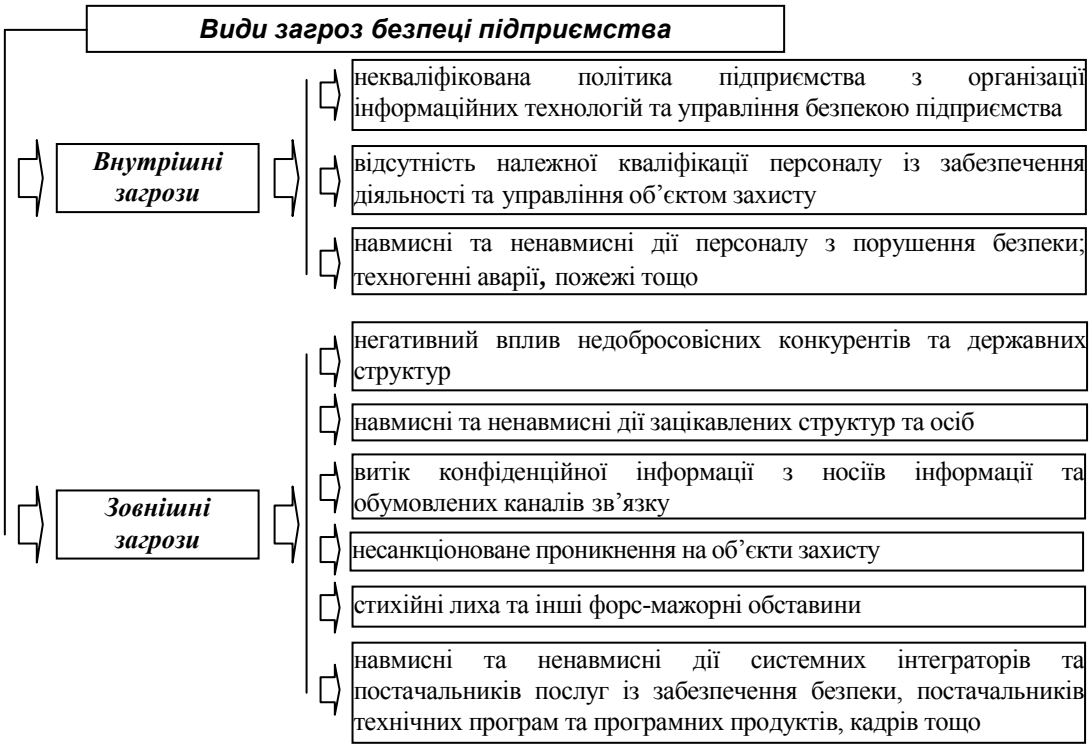

Рис. 2. Види загроз безпеці підприємства

Отже, 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 (рис. 3).

Рис. 3. Структура Положення про комерційну таємницю на підприємстві

Дана концепція визначає генеральну лінію у вирішенні проблем інформаційної безпеки. Це проект системи інформаційної безпеки, набір конкретних порад із забезпечення захисту інформаційних ресурсів комерційного характеру.

Для того, щоб говорити про економічну безпеку підприємства потрібно створити необхідні передумови для її забезпечення. Слід базуватись на ефективній системі заходів з необхідним правовим, економічним, організаційним та інформаційним забезпеченням. Це передбачає формування оптимальної структури управління з доцільним використанням органів безпеки; оцінку існуючих економічних зв'язків, у тому числі міжнародних, і прийняття управлінських рішень щодо збереження чи подальшого розвитку.

Безпека облікової інформації підприємства є комплексним поняттям і пов'язана не лише з внутрішнім середовищем підприємства, а й з впливом зовнішнього середовища та із суб'єктами, з якими підприємство вступає у взаємодію. Отже, можна стверджувати, що стан безпеки облікової інформації підприємства відображає узгодженість та збалансованість його інтересів та інтересів суб'єктів зовнішнього середовища. Таким чином, безпека облікової інформації підприємства є мірою гармонізації у часі і просторі економічних інтересів підприємства з інтересами пов'язаних з ним суб'єктів зовнішнього середовища, що діють поза межами підприємства.

Висновки. На підставі проведеного дослідження можна дійти висновку, що комерційна таємниця – це навмисно приховувані з комерційних міркувань економічні інтереси та відомості про різноманітні сторони та сфери виробничої, господарської, управлінської, науково-технічної, фінансової діяльності, охорона яких обумовлена інтересами конкуренції та можливими загрозами економічній безпеці.

Економічна безпека підприємства – це стан ефективного використання його ресурсів та існуючих ринкових можливостей, що дають можливість запобігати внутрішнім і зовнішнім загрозам, забезпечувати тривале виживання та сталий розвиток на ринку відповідно до обраної місії.

Способом досягнення економічної безпеки підприємства є ефективне функціонування інформаційної безпеки, засобом якої є впровадження Положення про комерційну таємницю, яке гарантує захист інформаційних ресурсів від несанкціонованого доступу чи використання зацікавленими структурами та особами. Виходячи з того, що ринок засобів і технологій економічної безпеки наповнюється та стає більш диверсифікованим та відбувається активне формування ринкових відносин перехідного періоду, здійснюється імпорт капіталу та технологій, учасники ринку мають формувати більш інтелектуальноємні засоби забезпечення комерційно-інформаційної безпеки, доповнювати засоби фізичної безпеки їхніми більш цивілізованими різновидами, включаючи технічні та юридичні засоби, до яких належить інститут комерційної таємниці.

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

Прогнозуючи та оцінюючи вплив очікуваних загроз необхідним є створення механізму забезпечення організації безпеки обліковій інформації. В даному механізмі необхідно врахувати реальну взаємодію підприємства з внутрішнім та зовнішнім середовищем, як наслідок, механізм повинен відображати всю господарську діяльність підприємства.

ЛІТЕРАТУРА:

1. *Аверченков В.И.* Аудит информационной безопасности: учеб. пособие для вузов. – Брянск: БГТУ, 2005. – 268 с.

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

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

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

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

6. *Ожегов С.И.* Словарь русского языка. – М.: Советская энциклопедия, 1968. – 990 с.

7. *Плетникова И.П.* Определение уровня и планирование ЭБП // Вісник Технологічного університету Поділля. – 2000. – № 4 (Ч.2). – С. 100-108.

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

9. *Соловьев А.И.* Экономическая безопасность хозяйствующего субъекта / Конфидент. – № 3. – 2002. – С. 46-50.

10. *Шипка О., Руденко О., Солодухін О.* Комерційна таємниця: аспект захисту бізнесу // Все про бухгалтерський облік. – 1998. – № 64 (246). – С. 28-31.

ДИКИЙ Анатолій Петрович – аспірант кафедри бухгалтерського обліку і контролю Житомирського державного технологічного університету.

Наукові інтереси:

– теорія бухгалтерського обліку;

– комп'ютеризація бухгалтерського обліку;

– збереження та захист облікової інформації підприємства.

СЕМЕНЧУК Марина Василівна – студентка IV курсу Житомирського державного технологічного університету.

Наукові інтереси:

– проблеми захисту бухгалтерської інформації та організація внутрішньогосподарського контролю підприємства.