УДК 657.47

ЗАСОБИ ПІДВИЩЕННЯ КЕРОВАНОСТІ БЕЗПЕКОЮ ОБЛІКОВОЇ ІНФОРМАЦІЇ

Н. Л. Шишкова, к. е. н., доцент, ДВНЗ «Національний гірничий університет», Nlshishkova@gmail.com

Ефективна система бухгалтерського обліку покликана не тільки забезпечити релевантною інформацією користувачів, але й стати частиною безпекової складової підприємства, спрямованої на підвищення якості облікової та контрольно-управлінської інформації. У статті розглядаються шляхи підвищення ефективності управління безпекою облікової інформації. за умови створення механізму попередження, профілактики, протидії загрозам якості та захисту облікової інформації. Запропоновано трирівневу систему управління безпекою облікової інформації з врахуванням аспектів її захисту.

***Ключові слова*:** економічна безпека, інформаційна безпека, облікова інформація, користувачі облікової інформації, керованість.

Постановка проблеми. Ефективний захист облікової інформації є одним з найголовніших аспектів при побудові надійної інформаційної системи суб'єкта господарю-

вання. Таким чином, бухгалтерська служба стає генератором стратегічного ресурсу підприємства – достовірної інформації щодо всіх аспектів діяльності суб'єкта господарювання. Облікова інформація є предметом і результатом праці бухгалтерської служби, сукупністю найбільш актуальних даних про стан управляючої та керованої підсистем і зовнішнього середовища суб'єкта господарювання. Одночасно інформація є об'єднуючою ланкою між суб'єктом та об'єктом управління, а також між підприємством і зовнішнім середовищем.

Актуальною стає проблема захисту облікової інформації, необхідної як для внутрішніх користувачів (для прийняття оптимальних управлінських рішень), так і для зовнішніх користувачів для розробки іноді негативних протидій (конкуренти). Тому постає проблема підвищення керованості системою безпеки облікової інформації – здатності перейти на новий рівень якості і безпеки при ефективних управлінських впливах.

Аналіз останніх досліджень і публікацій. Аналіз досліджень системи захисту облікової та контрольно-аналітичної інформації як складової забезпечення загальної фінансової безпеки підприємств доцільно здійснювати в розрізі наступних напрямів – виклики та проблемні аспекти сучасного управління безпекою інформації на підприємстві, необхідність формування механізму управління безпекою облікової інформації підприємств.

Гармонізація бухгалтерського обліку з системою управління підприємством взагалі та його інформаційними потоками, зокрема, є основою забезпечення захисту первинних, зведених, звітних даних, на основі яких приймаються управлінські рішення. Питання ефективної організації бухгалтерського обліку при одночасному врахуванні фінансової безпеки підприємства відображені у працях таких вчених як В. В. Євдокимов, А. П. Дикий [1], С. В. Івахненков [2, 3], К. В. Безверхий [4], Д. В. Апенько, Г. Ю. Коблянська [5]. При цьому питання захисту облікової інформації в загальній системі фінансової безпеки підприємства знайшли своє відображення у працях Л. С. Сороки [6], В. Н. Ясеніва [7], А. В. Олійник, В. М. Шацької [8] та ін.

Таким чином, дослідження питань щодо підвищення керованості безпекою облікової інформації підприємства, створює зацікавленість як з теоретичної точки зору (що пов'язано з формалізацією процесу управління обліковими та контрольно-аналітичними інформаційними потоками), так і суто з практичного боку (напрямки підвищення організації інформаційної безпеки повинні бути доведені до практичних рекомендацій співробітникам підприємств і організацій).

Формулювання мети статті. Метою даного дослідження є розробка інформаційної моделі управління безпекою облікової інформації в рамках механізмів протидії навмисним та ненавмисним її втратам. Засоби підвищення керованості безпекою облікової інформації стануть основою науково обґрунтованої системи запобіжних заходів щодо інформаційних втрат суб'єктів господарювання в загальній концепції раціоналізації інформаційних потоків в обліку та підвищення якості облікової інформації.

Виклад основного матеріал дослідження. Використання неякісної облікової інформації призводить до серйозних недоліків в системі управління будь-яким підприємством:

– відсутності або спотворення цілісної картини того, що відбувається на підприємстві, в окремих структурних підрозділах, по окремих видах діяльності;

– затримки в отриманні актуальної на момент підготовки та прийняття рішення облікової інформації;

– неприйнятними термінами розробки та розсилки ділових та бухгалтерських первинних і звітних документів;

– тривалими термінами отримання облікової інформації щодо попередніх періодів, накопиченої на підприємстві;

– труднощами отримання облікової інформації про поточний стан ресурсу, об'єкта, виду діяльності або процесу;

– небажаного витоку облікової інформації, який відбувається внаслідок неупорядкованого зберігання великих обсягів бухгалтерських та контрольно-управлінських документів.

У якості концепції раціоналізації ін-

формаційних потоків в обліку та підвищення якості облікової інформації виступає системне представлення всіх процесів розробки й управління, результатом яких є планування і подальша реалізація заходів по підвищенню безпеки облікової інформації (рис.1).

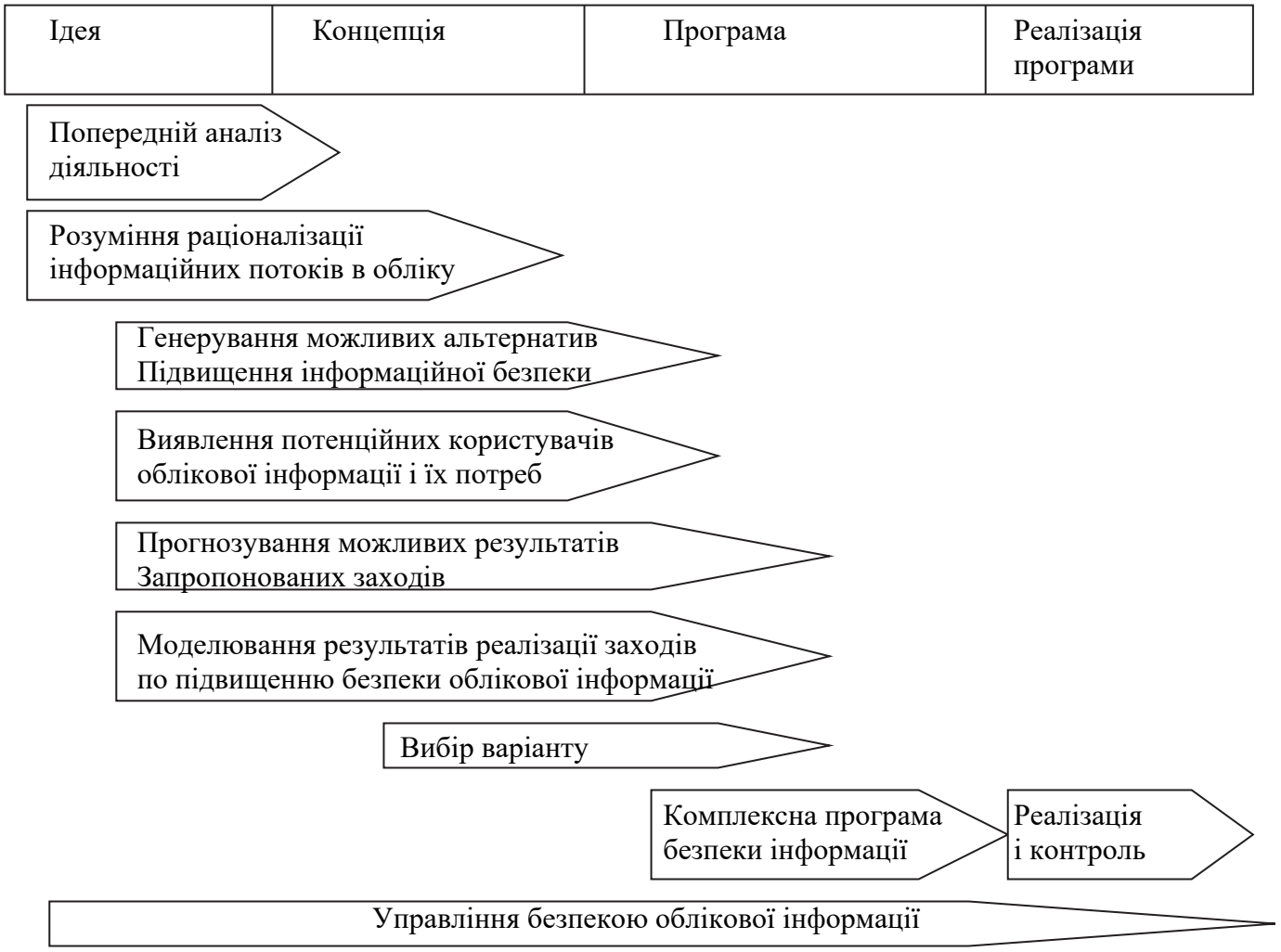

Рис. 1. Послідовність етапів підвищення безпеки облікової інформації

Тому облікова інформація має відповідати наступним принципам:

– релевантність (корисність у створенні інформаційного простору під час прийняття управлінських рішень)

– конфіденційність (облікова інформація надається тільки визначеним внутрішнім і зовнішнім користувачам);

– цілісність (облікова, в т.ч. звітна інформація, на основі якої приймаються управлінські рушення щодо подальшого розвитку підприємства, повинна бути достовірною захищеною від можливих ненавмисних і навмисних спотворень, точно відображати стан ресурсів та процеси суб'єкта господарювання);

– оперативність (облікова інформація і бухгалтерські служби повинні бути доступні, готові до обслуговування зацікавлених осіб – внутрішніх і зовнішніх користувачів) [7].

Для підвищення якості управлінської діяльності суб'єкту господарювання пропонується трирівнева система управління обліковою інформацією, яка враховує аспекти її захисту (табл.1).

Перший рівень управління обліковою інформацією, спрямований складається з:

– ідентифікації, оцінки загроз безпеці облікової інформації;

– інвентаризації ресурсів, пов'язаних із забезпеченням якості облікової інформації;

– контролю щодо ризиків, які загрожують безпеці облікової інформації;

Таблиця 1

Засоби підвищення керованості безпекою облікової інформації

Перелік засобів	Зміст
Перший рівень управління обліковою інформацією	
Ідентифікація, оцінка загроз	Джерела витоку та втрати інформації, окреслення кола можливих форс-мажорних загроз
Інвентаризація ресурсів	Інвентаризація інформаційних, програмних та фізичних ресурсів, які забезпечують якість облікової інформації
Контроль ризиків, які загрожують безпеці облікової інформації	Виявлення груп потенційних навмисних (шахрайство) і ненавмисних помилок в обліку
Ризик-орієнтоване керування обліковою інформацією	Керування обліковою інформацією виходячи з принципів її ефективного захисту і зберігання
Другий рівень управління обліковою інформацією	
Моніторинг чинників загроз інформаційній безпеці	Контроль окремих випадків витоку чи втрати інформації; навмисного чи ненавмисного перекручення інформації; форс-мажорні обставин, що впливають на стан облікової інформації
Формування елементів системи протидії загрозам	Визначення переліку превентивних дій попередження, профілактики, протидії безпековим загрозам щодо облікової інформації
Розробка положень, політики і процедур в рамках системи безпеки облікової інформації	Регламентація і адміністрування системи безпеки облікової інформації
Третій рівень управління обліковою інформацією	
Контроль за дотриманням вимог безпеки облікової інформації	Моніторинг на постійній основі з наступним корегуванням дій
Оцінка операційної ефективності заходів	Проведення заходів повинно бути економічно доцільно (витрати не повинні перевищувати ефект)

– ризик-орієнтоване керування обліковою інформацією.

Безпеку облікових управлінських систем порушують:

– витік інформації (навмисний чи необачний);

– втрата інформації (помилкова чи запланована);

– форс-мажорні обставини (від вилучення серверів до відключення електрики).

Для підвищення безпеки облікової інформації доцільно провести інвентаризацію ресурсів, пов'язаних з інформаційними системами обліку суб’єкту господарювання:

– інформаційні ресурси: бази бухгалтерської первинної, зведеної, звітної інформації, управлінська та кадрова документація, посібники користувача облікових програм, процедури переходу на аварійний режим;

– програмні ресурси: програмне забезпечення обліку на підприємстві, системне програмне забезпечення;

– фізичні ресурси: комп'ютери і комунікаційне устаткування підприємства, електронні та паперові носії даних, інше технічне устаткування (блоки живлення, кондиціонери), офісні меблі, управлінські приміщення;

– сервіси: обчислювальні, аналітичні, контрольні і комунікаційні сервіси.

Контроль ризиків, які загрожують безпеці облікової інформації, передбачає виявлення навмисних і ненавмисних помилок в обліку, що приводять до збільшення облікового ризику: помилки в записі облікових даних; невірні коди; несанкціоновані облікові операції; порушення контрольних лімітів; пропущення облікових записів; помилки при обробці або імпорті даних; помилки при формуванні або коригування довідників; неповні облікові записи; невірне віднесення записів за періодами ; фальсифікація даних; порушення вимог нормативних актів; порушення принципів облікової політики; невідповідність якості облікової інформації по-

требам користувачів.

Ризик-орієнтоване управління обліковою інформацією може бути побудоване виходячи з таких основних принципів:

– забезпечення фізичного поділу областей, призначених для обробки конфіденційної та не конфіденційної облікової інформації;

– забезпечення аутентифікації співробітників управлінських, бухгалтерських, аналітичних, контрольних служб;

– забезпечення розмежування доступу суб'єктів та їх процесів до інформації (ідентифікатори користувачів бухгалтерських програм);

– забезпечення захисту від відмов з приводу авторства і змісту облікових документів;

– забезпечення захисту обладнання і технічних засобів системи, приміщень, де вони розміщуються, від витоку конфіденційної облікової інформації технічними каналами;

– забезпечення захисту технічних і програмних засобів від витоку облікової інформації;

– організація захисту відомостей про інтенсивність, тривалість та трафіки обміну інформації;

– зберігання дублюючої облікової інформації;

– захист резервних копій облікової інформації від впливу навколишнього середовища.

Другий рівень управління обліковою інформацією складається з:

– забезпечення безперервності моніторингу чинників загроз безпеці облікової інформації;

– формування розуміння основних елементів системи протидії загрозам;

– розробка положень, політики і процедур в рамках системи безпеки облікової інформації.

Моніторинг чинників загроз безпеці облікової інформації представлено на рис.2. Превентивні дії попередження, профілактики, протидії загрозам в рамках положень і процедур виступають методами забезпечення захисту облікової інформації (перешкоди, управління доступом, регламентація, примус, спонукання).

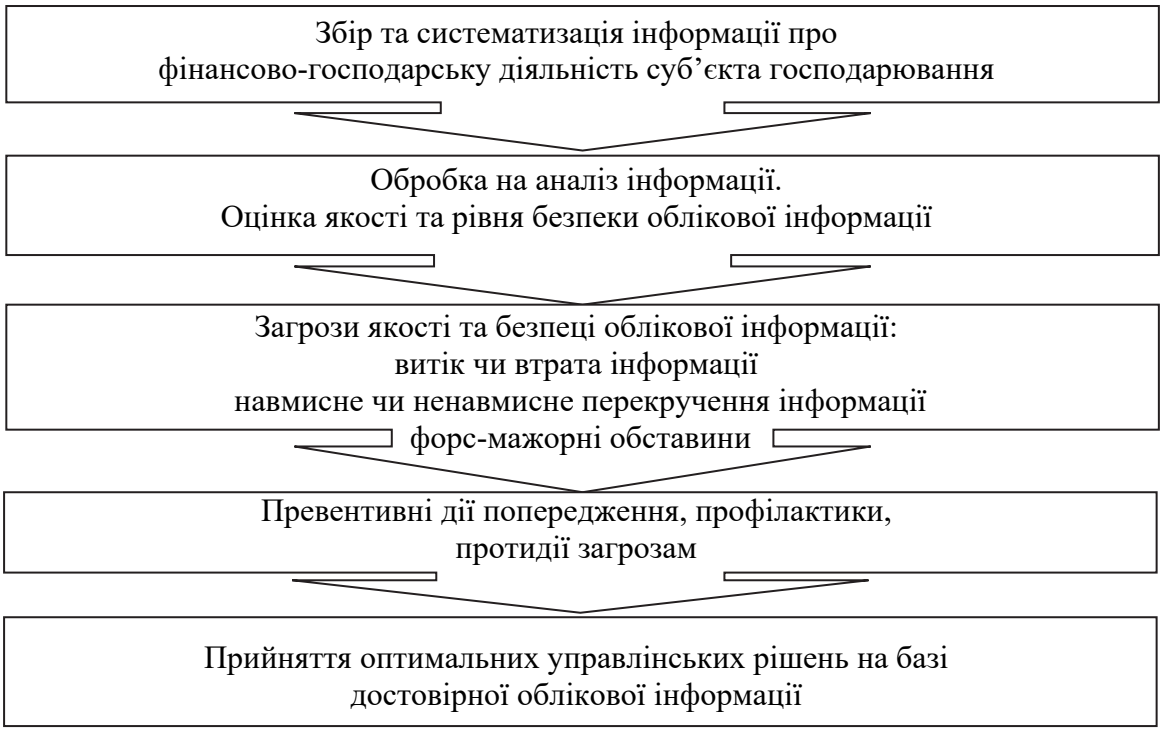

Рис.2 Моніторинг загроз якості та безпеці облікової інформації

Перешкодою потрібно вважати метод фізичного перешкоджання шляху зловмисника до облікової інформації. Цей метод реалізується пропускною системою підприємства, включаючи наявність охорони на вході в нього, недопущення сторонніх осіб у бух-

галтерію, касу.

Управлінням доступом є методом захисту облікової та звітної інформації, яка реалізується за рахунок:

– ідентифікації користувачів інформаційної системи, коли кожен користувач отримує власний персональний ідентифікатор;

– аутентифікації – встановлення автентичності об'єкта або суб'єкта по пред'явленому їм ідентифікатору (здійснюється шляхом зіставлення введеного ідентифікатора з тим, що зберігаються в пам'яті комп'ютера);

– перевірки повноважень – перевірки відповідності запитуваних ресурсів і виконуваних операцій по виділених ресурсах і дозволених процедурах;

– реєстрації звернень до ресурсів, що захищаються;

– інформування та реагування при спробах несанкціонованих дій.

Регламентація як метод захисту облікової інформації полягає в розробці і реалізації системи заходів (обладнання, розміщення апаратури, режиму роботи для персоналу і користувачів і ін.), спрямованих на забезпечення захисту інформації.

Примус – спосіб захисту, при якому персонал і користувачі змушені дотримуватися правил доступу до облікової інформації під загрозою матеріальної, адміністративної та кримінальної відповідальності.

Спонукання – спосіб захисту, заснований на дотриманні правил захисту інформації з моральних, етичних і психологічних мотивів [7].

Третій рівень управління обліковою інформацією передбачає:

– контроль за дотриманням вимог безпеки облікової інформації;

– оцінка операційної ефективності заходів на перших двох рівнях захисту.

Система контролю за дотриманням вимог безпеки облікової інформації має включати:

– політику і положення щодо контролю за дотриманням вимог безпеки облікової інформації;

– заходи щодо підвищення безпеки облікової інформації;

– процедури й засоби контролю за дотриманням вимог безпеки облікової інформації;

– схеми обробки облікової інформації;

– порядок збереження носіїв облікової інформації;

– інформаційну систему управління (форми звітності, схема документообігу тощо) для користувачів облікової інформації;

– програму вдосконалення кваліфікації персоналу, яка відповідає інформаційно-безпековим потребам та зовнішнім обставинам;

– технічні засоби отримання, збереження, обробки та передачі користувачам облікової інформації.

Таким чином, послідовна політика щодо підвищення керованості безпекою облікової інформації надасть змогу як забезпечити якісною інформацією осіб, що приймають ефективні управлінські рішення, так і вберегти систему фінансової безпеки підприємства від небажаних витоків, втрат, перекручень (навмисних і ненавмисних) інформації.

При цьому слід врахувати, що деякі користувачі інформації (особливо зовнішні) можуть мати інтереси, які не співпадають з метою безпековості облікової інформації. Так, на рис. 3 надано інформаційну модель узгодження інтересів користувачів облікової інформації. Аналізуючи інформаційні потреби користувачів облікової інформації, визначено основні засоби підвищення ефективності управління безпекою облікової інформації: ідентифікація загроз, аутентифікація виконавців та користувачів, перевірка повноважень та рівнів доступу до інформації, технічний захист інформації, регламентації окремих операцій з обліковою інформацією, спонукання та примус співробітників до актуалізації безпекових заходів.

Заходи щодо підвищення інформації стосуються не тільки служби безпеки підприємства, а всього управлінського персоналу. Це пов’язано з тим, що стратегічна для зовнішніх користувачів інформація може спричинити її несанкціонований витік. І навпаки, розуміння інтересів зовнішніх користувачів (рис.3) дозволить передбачити їх дії,. відреагувати та протидіяти.

Не слід забувати про інформаційні потреби внутрішніх користувачів – про стан ресурсів, ефективність процесів і окремих

Рис. 3 Інформаційна модель узгодження інтересів користувачів облікової інформації

видів діяльності, про технологічний та технічний стан підприємства. Основними перешкодами тут стають перекручення інформації – навмисні і ненавмисні (помилки та шахрайство).

Проблема перекручення облікової інформації може бути вирішена лише за умови розуміння мотивів втручання, інтересів виконавців. Так, керівництво підприємства завжди буде схильне до завищення валюти балансу, завищення або заниження виручки, витрат [4].

Тому превентивні механізми запобігання втрат та перекручень облікової інформації повинні базуватися на комплексних, взаємопов'язаних методиках і процедурах виявлення, аналізу ризиків для інформаційної системи обліку підприємства, розробках контрольних технологій щодо управління безпекою облікової інформації.

Для перетворення інформаційної моделі в ефективний механізм підвищення якості і безпеки облікової інформації необхідно додати комплекс організаційних заходів для дієвого адміністрування безпекових процесів, а саме:

– забезпечення виконання вимог захисту облікової інформації;

– інвентаризація найбільш вразливих засобів забезпечення захисту облікової інформації;

– розробка комплексу контрольних заходів щодо перевірки якості і безпеки облікової інформації;

– визначення комплексу дій по підвищенню безпеки облікової інформації з врахуванням умов функціонування суб'єкту господарювання;

– визначення відповідальності обліково-аналітичного та контрольно-управлінського персоналу за порушення безпекових норм опрацювання облікової інформації;

– впровадження та контроль загальної системи економічної безпеки суб'єкту господарювання.

Висновки. Мінімальна кількість виконавців облікових функцій при максимальній їх кваліфікації здатна забезпечити високий рівень управління безпекою облікової інформації, швидко реагуючи на вплив внутрішніх і зовнішніх факторів-подразнювачів за умови створення дієвого превентивного механізму попередження, профілактики, протидії загрозам якості та захисту облікової інформації.

Підвищення керованості безпекою інформаційних систем в обліку забезпечить більш гнучку систему реагування на внутрішні та зовнішні загрози: створення єдиної в масштабі всього підприємства нормативно-довідкової системи; вдосконалення схеми документообігу з урахуванням факторів підвищення інформаційної безпеки; забезпечення оперативності обліку з одночасним скороченням до необхідного мінімуму кількості документів і показників; розробку регламентації процедур збереження і подання інформації на різні рівні управління для прийняття оптимальних рішень.

Література

1. Євдокимов В. В. Особливості організації бухгалтерського обліку при забезпеченні економічної безпеки підприємства / В. В. Євдокимов, А. П. Дикий // (online): http://dspace.uabs.edu.ua/jspui/bitstream/123456789/815/1/29.pdf

2. Івахненков С. В. Інформаційні технології в організації бухгалтерського обліку та аудиту : навч. пос. / С. В. Івахненков. – 4-те вид., випр. і доп. – К. : Знання, 2008. – 343 с.

3. Івахненков С. В. Інформаційні технології в аудиті та внутрішньогосподарському контролі : автореф. дис. д-ра екон. наук : 08.00.09 / С. В. Івахненков; Київ. нац. екон. ун-т ім. В. Гетьмана. – К., 2011. – 33 с.

4. Безверхий К. В. Удосконалення методики виявлення ознак викривлень і помилок у фінансовій звітності підприємства на основі аналітичних процедур / К. В. Безверхий // Облік і фінанси, №4 (66), 2014. (online): http://irbis-nbuv.gov.ua/.../cgiirbis

5. Апенько Д. В., Коблянська Г. Ю. Облік і моделювання касових і банківських операцій в комп'ютерному середовищі / Д. В. Апенько, Г. Ю. Коблянська // Формування ринкових відносин в Україні, №4 (131), 2012 (online): http:// www.irbis-nbuv.gov.ua/.

6. Сорока Л. С. Захист облікової інформації в системі економічної безпеки підприємства / Л. С. Сорока // Економічні науки: Облік і фінанси. – 2012. – Вип. 9(3). – С. 315–321.

7. Ясенив В. Н. Информационная безопасность в экономических системах: уч. пос. / В. Н. Ясенив. – М. Новгород : Изд-во ННДУ, 2006. – 248 с.

8. Олійник А. В. Інформаційні системи і технології у фінансових установах: навч. пос. / А. В. Олійник, В. М. Шацька. – Львів : «Новий Світ-2000», 2006 – 436 с.

9. Корягін М. В. Проблеми та перспективи розвитку бухгалтерської звітності.: монографія / М. В. Корягін, П. О. Куцик. – Київ : Інтерсервіс, 2012. – 261 с.

СРЕДСТВА ПОВЫШЕНИЯ УПРАВЛЯЕМОСТИ БЕЗОПАСНОСТЬЮ УЧЕТНОЙ ИНФОРМАЦИИ

Н. Л. Шишкова, к. э. н., доцент, ГВУЗ «Национальный горный университет».

Эффективная система бухгалтерского учета призвана не только обеспечить релевантной информацией пользователей, но и стать частью системы экономической безопасности предприятия, направленной на повышение качества учетной и контрольно-управленческой информации. В статье рассматриваются пути повышения управляемости безопасностью учетной информации. при условии создания механизма предупреждения, профилактики, противодействия угрозам качеству и защите учетной информации. Предложена трехуровневая система управления безопасностью учетной информации с учетом аспектов ее защиты.

Ключевые слова: экономическая безопасность, информационная безопасность, учетная информация, пользователи учетной информацией, управляемость.

MEANS TO IMPROVE THE CONTROLLABILITY OF ACCOUNTING INFORMATION SECURITY

N. L. Shishkova, Ph. D (Econ.), Ass. Prof., SHEI «National Mining University»

Effective system of accounting aims not only to provide relevant information to users, but also to become a part of security constituent of an enterprise directed at the improvement of the quality of accounting and controlling-managerial information. Ways of improving the effectiveness of controlling the security of accounting information by means of creating a mechanism of anticipation, prevention and countermeasure to security threats and accounting information protection are considered. Three-level system of accounting information security management is offered taking into account the aspects of its protection.

***Keywords*:** economic security, information security, accounting information, accounting information users, controllability.

Рекомендовано до друку д. е. н., проф. Литвиненко Н. І. *Надійшла до редакції 23.05.16 р.*