УДК 359.2

4. Менеджмент.

# ВИМОГИ ДО ФОРМУВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ В СИСТЕМІ ОБЛІКОВО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

# REQUIREMENTS FOR THE FORMATION OF INFORMATION FLOWS IN THE SYSTEM OF ACCOUNTING AND ANALYTICAL ENSURING THE MANAGEMENT OF ECONOMIC SECURITY OF THE ENTERPRISE

**Саванчук Тетяна Миколаївна**

кандидат економічних наук,

доцент кафедри обліку, оподаткування та

управління фінансово-економічною безпекою,

Дніпровський державний аграрно-економічний університет

ORCID: https://orcid.org/0000-0002-8584-0302

**Назаренко Владислав Вікторович**

здобувач гр. МгУФЕБ-1-22

Дніпровський державний аграрно-економічний університет

ORCID: https://orcid.org/0009-0004-8413-6446

**Savanchuk Tetiana, Nazarenko Vladyslav**

Dnipro State Agrarian and Economic University

**Анотація:** У статті виокремленні основні вимоги до інформаційного забезпечення управління системою економічної безпеки підприємства та обґрунтовано необхідність їх дотримання на підприємстві. Визначено, що інформаційні потоки формуються в системі обліково-аналітичного

забезпечення управління економічною безпекою та виділено основні аспекти формування таких потоків з метою розробки рекомендацій щодо мінімізації ризиків навмисного чи ненавмисного викривлення інформації.

Окрема увага приділена управлінню персоналом як ключовому фактору в забезпеченні ефективної системи формування інформаційних потоків всередині підприємства. Стаття містить практичні поради та рекомендації, які можуть бути корисними суб'єктам господарювання в процесі побудови інформаційно-забезпеченої системи управління економічною безпекою.

**Ключові слова:** економічна безпека, інформаційні потоки, інформаційне забезпечення, захист інформації, обліково-аналітичне забезпечення.

**Annotation.** The purpose of the article is to determine the basic requirements for the effective construction of information flows in the system of accounting and analytical management support and to determine the measures to protect the enterprise from the leakage of confidential information. This direction of economic activity is relevant for any enterprise, as it will allow to provide practical recommendations for the creation of an information-backed economic security management system. The research was conducted using the monographic method. The article singles out the main requirements for information management of the enterprise's economic security system and substantiates the need for their compliance at the enterprise. The authors established that the main part of the information necessary for management is formed in the accounting system of the enterprise and requires analytical processing. The accounting department must comply with confidentiality requirements when working with information. The main aspects of the formation of information flows in the system of economic security of the enterprise are determined in order to develop, in the future, recommendations for minimizing the risks of intentional or unintentional distortion of information. It was established that modern conditions of economic activity require the creation of an information-backed management system. It has been

proven that for the practical implementation of the task of protecting confidential information, it is first necessary to establish rules for its preservation at the enterprise, with which the responsible employees of the enterprise must be familiarized. The authors proposed a number of measures to protect the enterprise from the leakage of confidential information. Special attention is paid to personnel management as a key factor in ensuring an effective system of forming information flows within the enterprise. The article contains practical tips and recommendations that can be useful to business entities in the process of building an information-backed management system. It emphasizes the importance of information provision and information security for effective management decision-making.

**Key words:** economic security, information flows, information support, information protection, accounting and analytical support.

**Постановка проблеми.** В сучасних умовах господарювання, підприємства України функціонують у умовах різкої зміни податкового законодавства, курсу долара, кон'юнктури ринку, політичної ситуації, фінансового та організаційно-правового поля функціонування. При цьому, будь якому нормально функціонуючому підприємству необхідно, на певному рівні, підтримувати свою економічну безпеку.

В свою чергу, забезпечення економічної безпеки підприємства, на сьогоднішній день, не можливо без підтримки на належному рівні її інформаційної складової. Рівень загроз та ризиків інформацій безпеці підприємства постійно зростають. Особливо, це пов'язано з розвитком сучасних технологій, численними інформаційними злочинами, шпигунством, промисловим шпіонажем.

Господарюючі суб'єкти взаємодіють із великою кількістю контрагентів, які прагнуть реалізувати власні інтереси і створюють загрозі зі сторони зовнішнього середовища, намагаючись законним та незаконним шляхом отримати інформацію про фінансовий стан підприємства, плани на перспективу розвитку, інформацію про процес виробництва та збут готової

продукції, постачальників, партнерів. Крім того, самому керівництву суб'єкта господарювання також необхідно мати достатньо інформації про внутрішні та зовнішні умови функціонування власного бізнесу. Виходячи з цього, сучасні умови здійснення господарської діяльності вимагають створення інформаційно-забезпеченої системи управління. Саме тому, забезпечення інформаційної безпеки підприємства є досить актуальним питанням сьогодення, а інформація, яка необхідна для управління економічною безпекою повинна відповідати певним вимогам.

**Аналіз останніх досліджень та публікацій.** Питання інформаційної безпеки досліджувалося значною кількістю науковців. Так, Нехай В.А. та Нехай В.В. досить глибоко проаналізували інформаційну безпеку як окрему складову економічної безпеки підприємства [6]. На важливості інформаційної безпеки, як на рівні підприємства, так і на рівні держави, наголошували в своїх працях також Кузнецов О. О., Євсеєв С. П., Кавун С. В. [4], Чернецька О.В. [8], Каткова Т., Ткачова, Н., Київська К., Добровольська, О., Редько К. [2] та інші науковці. В той же час, такі дослідники як Боженко О.М. [1], Коптєва Г.М. [3], Миколюк О.А. [5] та інші приділяють велику увагу інформаційному забезпеченню управління окремими бізнес-процесами та підприємством в цілому.

**Виділення невирішених раніше частин загальної проблеми.** Опрацьовані літературні джерела дозволяють дійти висновку, що інформаційна безпека та інформаційне забезпечення управління підприємством тісно пов'язані між собою, а тому важливо комплексно підійти до визначення як вимог щодо формування інформаційних потоків в системі управління, так і напрямків захисту цієї інформації на підприємстві.

**Формулювання цілей статті.** Мета статті полягає у визначенні основних вимог до ефективної побудови інформаційних потоків в системі обліково-аналітичного забезпечення управління з подальшим формуванням основних напрямків захисту підприємства від витоку конфіденційної інформації і підвищення його інформаційної безпеки.

**Виклад основного матеріалу дослідження.** Практика діяльності підприємств України, особливо малого та середнього бізнесу, засвідчила, що більшість із них, на сьогоднішній день, не мають окремого структурного підрозділу який би займався питаннями економічної безпеки підприємства. Відповідно питанням інформаційного забезпечення економічної безпеки на підприємстві також не приділяють належної уваги.

На сьогодні, основним підрозділом у якому формується інформація щодо діяльності підприємства є бухгалтерія. Бухгалтери підприємств здійснюють збір, реєстрацію та обробку інформації про господарську діяльність підприємства та формують на її основі всі види звітності. Облікову інформацію використовують також аналітики, якщо вони є на підприємстві, та менеджмент.

Таким чином, для більшості суб'єктів господарювання, основною передумовою здійснення якісного інформаційного забезпечення управління, на сьогоднішній день, є належна організація облікової та аналітичної роботи. Враховуючи значні обсяги інформації, що проходять через облікову систему підприємства та різноманітність шляхів її надходження, важливо побудувати роботу з інформацією таким чином, щоб можна було легко виділити її релевантну частину в залежності від запитів керівництва. Для цього, на початковому етапі, сформуємо основні вимоги до інформаційного забезпечення управління системою економічної безпеки підприємства (рис. 1).

Дотримання зазначених вимог вимагає від працівників облікового апарату змінити підходи до обробки та своє відношення до інформації. Має бути враховано, що важливо не лише фіксувати факти господарської діяльності в системі обліку підприємства відповідно до вимог законодавства, а і застосовувати для її обробки інструментарій управлінського обліку та аналізу господарської діяльності. Це дозволить сформувати інформаційні потоки в системі обліково-аналітичного забезпечення управління економічною безпекою підприємства таким чином, щоб вони забезпечували

прискорення прийняття управлінських рішень.

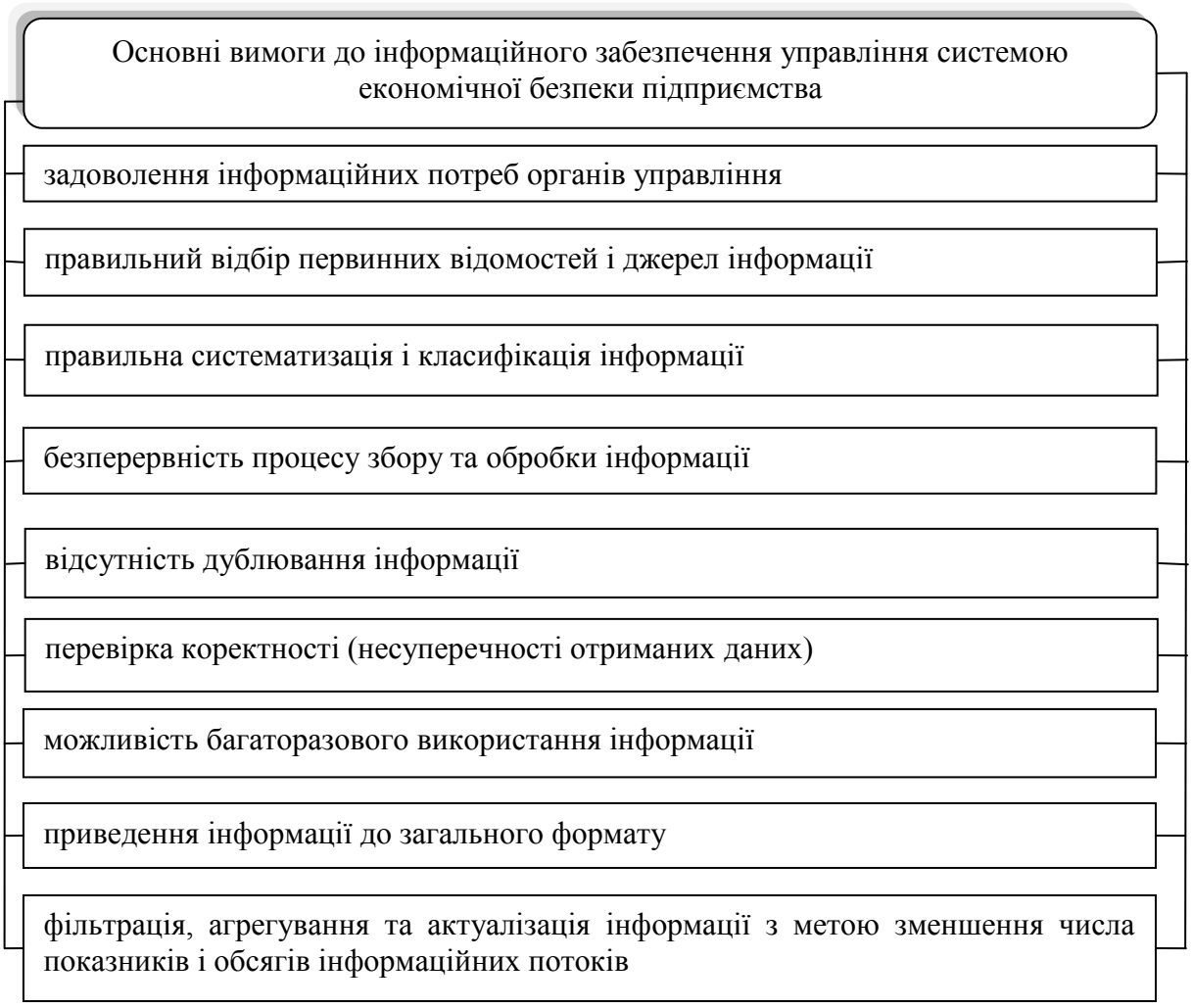


Рис. 1. Основні вимоги до інформаційного забезпечення управління системою економічної безпеки підприємства

*Джерело: узагальнено на основі [1,3,5] та доповнено.*

Такі потоки мають бути сформовані з врахуванням наступного:

- з’ясування потреб кожного керівника в характері та змісті необхідної йому інформації для цілей забезпечення економічної безпеки підприємства;

- обґрунтування джерел надходження інформації та обсягів збору, зберігання та надання інформації;

- планування потреб у технічних засобах підприємства в цілому та кожного керівника для обробки та інтерпретації інформації, що необхідна для прийняття управлінських рішень;

- обґрунтування рівня витрат на функціонування системи формування інформаційних потоків в системі обліково-аналітичного забезпечення управління економічною безпекою підприємства;

- обґрунтування потреб у програмних засобах, які формуватимуть інформаційні технології управління економічною безпекою підприємства.

Паралельно з цим, необхідно приділити увага захисту конфіденційної інформації. Для практичної реалізації цього завдання, спочатку необхідно встановити на підприємстві правила збереження конфіденційної інформації з якими мають бути ознайомлені відповідальні співробітники підприємства.

Зокрема, щоб захистити підприємство від витоку конфіденційної інформації, на нашу думку, необхідно:

– контролювати доступ співробітників підприємства до закритої інформації і до баз даних;

– не зловживати найманням тимчасових співробітників, якщо вони автоматично одержують доступ до конфіденційної інформації;

– встановити камери відео спостереження та контролювати осіб, які переміщаються в середині підприємства;

– встановити апарат для знищення таємних документів;

– таємні документи повинні знищуватися особисто працівниками, які відповідають за безпеку фірми;

– завести спеціальні конверти, в яких таємна інформація буде циркулювати в середині фірми;

– слідкувати за використанням копіювальної техніки та виносом документів з підприємства;

– встановити місця приймання відвідувачів, не залишати їх на самоті;

– обладнати звуконепроникні приміщення та перевіряти їх для обговорення важливих питань підприємства;

– використовувати для ведення службових записів лише пронумеровані зошити;

– в кінці робочого дня всі важливі документи ховати в сейф;

– встановити персональну відповідальність співробітників за збереження конфіденційної інформації з чітким визначенням міри покарання за витікання цієї інформації.

Підвищені вимоги до інформаційної безпеки передбачають здійснення відповідних заходів на всіх етапах життєвого циклу формування інформаційних потоків. Планувати такі заходи, на нашу думку, важливо після закінчення етапу аналізу ризиків і вибору контрзаходів, щоб оцінити їх ефективність. Обов'язковою складовою частиною цих планів має стати періодична перевірка відповідності існуючого режиму інформаційної безпеки політиці безпеки, сертифікації інформаційної системи (технології) на відповідність вимогам певного стандарту безпеки.

Мета процесу оцінювання ризиків в процесі забезпечення інформаційної безпеки підприємства полягає у визначенні їх характеристик в інформаційній системі та її ресурсах. На основі таких даних вибирають необхідні засоби управління інформаційною безпекою.

Ключовим фактором у забезпеченні інформаційної безпеки підприємства є його персонал. Часто, переманюючи персонал або влаштовуючи свого працівника на роботу до конкурента, недобросовісні контрагенти намагаються незаконним шляхом отримати інформацію про суб'єкт господарювання. Тому, заради забезпечення інформаційної безпеки підприємства необхідно застосовувати превентивні заходи як юридичного так і фінансового характеру.

Найбільш розповсюдженими і небезпечними загрозами достатності інформації є ненавмисні помилки постійних користувачів, операторів, системних адміністраторів та інших осіб, що обслуговують інформаційні системи. Саме такі помилки зазвичай і стають загрозами (неправильно введені дані чи помилки в програмі, що призвела до помилок в потоках інформації і викривлення даних), іноді вони створюють слабкі місця, якими можуть скористатися зловмисники. Статистика свідчить, що близько 65 % втрат цінної інформації є наслідком ненавмисних помилок [4]. Виходячи з

цього, найбільш радикальний спосіб боротьби з ненавмисними помилками – максимальна автоматизація і строгий контроль.

Ткачук Т.Ю. зазначає, що на другому місці за розмірами збитків від слабких місць в інформаційній безпеці є крадіжки та підробки. У більшості розслідуваних випадків винуватцями таких злочинів виявлялися штатні співробітники фірм, добре обізнані з режимом роботи і заходами безпеки [7].

Виходячи з цього, основними заходами при роботі з персоналом мають бути наступні: проведення аналітичних процедур при прийомі і звільненні; навчання й інструктаж практичним діям по захисту інформації; контроль за виконанням вимог по захисту інформації, стимулювання відповідального відношення до збереження інформації, система фінансових санкцій за порушення вимог роботи з конфіденційною інформацією та ін.

**Висновки та перспективи подальших досліджень.** Таким чином, встановлення чітких вимоги до формування інформаційних потоків в системі обліково-аналітичного забезпечення управління економічною безпекою підприємства на основі існуючої системи обліку та розробка заходів щодо захисту конфіденційної інформації буде сприяти підвищенню економічної безпеки будь-якого підприємства. Головним завданням на підприємстві є вчасне виявлення загроз інформаційній безпеці та запобігання їм шляхом впровадження ряду заходів щодо попередження комп'ютерних злочинів. Механізм забезпечення інформаційної безпеки суб'єктів господарювання має формуватися й реалізовуватися на практиці шляхом комплексного розв'язання проблем, пов'язаних із багатофакторністю важко контрольованого й прогнозованого сучасного середовища функціонування системи інформаційної безпеки підприємств.

**Список використаних джерел:**

1. Боженко О.М. Інформаційне забезпечення управління потенціалом підприємства. *Наукові записки.* 2016. № 2 (53) С.189-197 URL: http://nz.uad.lviv.ua/static/media/2-53/23.pdf

2. Каткова Т., Ткачова, Н., Київська К., Добровольська, О., Редько К. До проблеми вдосконалення механізмів державного управління економічною безпекою в умовах реформаційних змін: іноземний досвід, українські реалії. *Financial and Credit Activity Problems of Theory and Practice*, 2022. № *1*(42), 324–334. URL:https://doi.org/10.55643/fcaptp.1.42.2022.3707

3. Коптєва Г.М. Інформаційне забезпечення економічної безпеки бізнес-процесів підприємства торгівлі. *Держава та регіони.* 2020. № 4(115). С.85-90. URL: http://www.econom.stateandregions.zp.ua/journal/2020/4_2020/17.pdf

4. Кузнецов О. О., Євсеєв С. П., Кавун С. В. Захист інформації та економічна безпека підприємства: монографія. Харків: ХНЕУ, 2008. 360с.

5. Миколюк О. А. Особливості інформаційного забезпечення управління підприємством. *Вісник Хмельницького національного університет.* 2021. № 3 С. 48-52. URL: http://journals.khnu.km.ua/vestnik/wp-content/uploads/2022/03/2021-en-3-07.pdf

6. Нехай В.А., Нехай В.В. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету. Серія : Економіка і менеджмент*. 2017. Вип. 24(2). С. 137-140. URL: http://nbuv.gov.ua/UJRN/Nvmgu_eim_2017_24%282%29__30

7. Ткачук Т.Ю. Конфіденційне діловодство - важлива складова захисту конфіденційної інформації на підприємстві. *Бізнес і безпека*. 2007. № 1. С. 85-89.

8. Чернецька О.В., Саванчук Т.М. Фінансово-економічна безпека в системі управління підприємством: сутність та політика забезпечення. *Інфраструктура ринку*. 2018. № 17. С. 242-247. URL: http://www.market-infr.od.ua/uk/17-2018

**References:**

1. Bozhenko O.M. (2016) Informatsiine zabezpechennia upravlinnia

potentsialom pidpryiemstva [Information support for enterprise potential management]. *Naukovi zapysky*, vol. 2 (53), pp.189-197. Available at: http://nz.uad.lviv.ua/static/media/2-53/23.pdf.

2. Katkova T., Tkachova, N., Kyivska K., Dobrovolska, O., Redko K. (2022) Do problemy vdoskonalennia mekhanizmiv derzhavnoho upravlinnia ekonomichnoiu bezpekoiu v umovakh reformatsiinykh zmin: inozemnyi dosvid, ukrainski realii. [To the problem of improving the mechanisms of state management of economic security in the conditions of reformation changes: foreign experience, Ukrainian realities]. *Financial and Credit Activity Problems of Theory and Practice*,. vol. 1 (42), pp.324-334. Available at: https://doi.org/10.55643/fcaptp.1.42.2022.3707

3. Koptieva H.M. (2020) Informatsiine zabezpechennia ekonomichnoi bezpeky biznes-protsesiv pidpryiemstva torhivli [Information provision of economic security of business processes of a trade enterprise]. *Derzhava ta rehiony*, vol. 4 (115), pp.85-90. Available at: http://www.econom.stateandregions.zp.ua/journal/2020/4_2020/17.pdf

4. Kuznetsov O. O., Yevseiev S. P., Kavun S. V. (2008) Zakhyst informatsii ta ekonomichna bezpeka pidpryiemstva: monohrafiia: monohrafiia [Information protection and economic security of the enterprise: monograph]. Kharkiv: KhNEU. 360p. (in Ukrainian)

5. Mykoliuk O. A. (2021) Osoblyvosti informatsiinoho zabezpechennia upravlinnia pidpryiemstvom [Peculiarities of information provision of enterprise management]. *Visnyk Khmelnytskoho natsionalnoho universytet*, vol. 3, pp.48-52. Available at: http://journals.khnu.km.ua/vestnik/wp-content/uploads/2022/03/2021-en-3-07.pdf

6. Nekhai V.A., Nekhai V.V. (2016) Informatsiina bezpeka yak skladova ekonomichnoi bezpeky pidpryiemstv [Information security as a component of economic security of enterprises]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia : Ekonomika i menedzhment,* vol. 324 (2), pp.137-140. Available at: http://nbuv.gov.ua/UJRN/Nvmgu_eim_2017_24%282%29__30

7. Tkachuk T.Iu. (2007) Konfidentsiine dilovodstvo - vazhlyva skladova zakhystu konfidentsiinoi informatsii na pidpryiemstvi [Confidential record-keeping is an important component of protecting confidential information at the enterprise]. *Biznes i bezpeka,* vol. 1, pp.85-89. Available at: http://nbuv.gov.ua/UJRN/Nvmgu_eim_2017_24%282%29__30

8. Chernetska O.V., Savanchuk T.N. (2018) Finansovo-ekonomichna bezpeka v systemi upravlinnia pidpryiemstvom: sutnist ta polityka zabezpechennia [Financial and economic security in the enterprise management system: essence and security policy]. *Infrastruktura rynku.* vol. 17. pp.242-247. Available at: http://www.market-infr.od.ua/uk/17-2018