*УДК [65.012.7+65.012.8]:656.6*

***Євтушевська О.А.**, аспірантка кафедри обліку і аудиту*
*Київської державної академії водного транспорту*
*імені гетьмана Петра Конашевича-Сагайдачного,*
*старший викладач Українського державного університету*
*фінансів та міжнародної торгівлі*

# ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ЕЛЕМЕНТ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КОМПЛЕКСНОГО КОНТРОЛЮ ПІДПРИЄМСТВ ВОДНОГО ТРАНСПОРТУ

***Анотація.** У статті розглянуті різні погляди сучасних науковців в частині трактування поняття інформаційної безпеки. Визначено, що створення ефективної системи інформаційної безпеки є неможливим без чіткого визначення загроз інформації, що охороняється.*

*Також виокремлено умови, які сприяють неправомірному оволодінню конфіденційною інформацією, визначено елементи, які відносяться до зовнішніх загроз, охарактеризовано внутрішні загрози. Підтверджено, що створення ефективної системи інформаційної безпеки є неможливим без чіткого визначення загроз інформації, що охороняється. Визначено формальні та неформальні канали поширення інформації та основні загрози останніх. Охарактеризовано шляхи попередження можливих загроз поширення інформації. Визначено, що у системі управління підприємствами водного транспорту інформаційна безпека є одним із найважливіших елементів комплексного контролю та є невід'ємною частиною управління.*

***Ключові слова:** безпека, економічна безпека, інформаційна безпека, внутрішній контроль, підприємства водного транспорту, ризики, інформація, контроль, фінансово-економічна діяльність, система контролю.*

**Постановка проблеми.** Діяльність будь-якого підприємства, в тому числі і водного транспорту, залежить від багатьох факторів, які впливають на його економічну безпеку. Зокрема важливим фактором, який впливає на діяльність організації в умовах динамічного розвитку виробництва, є інформаційний. Інформація була і залишається головною складовою, що використовується при прийнятті управлінських рішень. В залежності від дотримання умов отримання, обробки та передачі інформації підприємство захищає себе від виникнення ризикових ситуацій, спроможних погіршувати його фінансове становище. Інформаційна безпека підприємства водного транспорту припускає більш ретельне вивчення комунікаційних зв'язків між його підрозділами на основі контролю якості внутрішньо фірмового обліку. Інформаційні потоки підприємства залежать від його організаційної структури, і чим вона складніша, тим більша ймовірність виникнення ризиків щодо результату неефективної роботи через існуючу інформацію. Внутрішній облік діяльності підприємства повинен орієнтуватися на своєчасне одержання точної та достовірної інформації від усіх внутрішніх структурних підрозділів для посилення інформаційної безпеки. Інформаційна безпека внутрішнього обліку залежить від об'єктивності джерел отримання інформації, до яких можна віднести плановий, обліковий та позаобліковий. В той же час, внутрішнім обліком займаються конкретні особи, які мають різні кваліфікаційні характеристики, і від цього залежить те, як вони будуть реагувати на наявність факторів невизначеності в бухгалтерському обліку. Посилення ефективності управління внутрішніми інформаційними потоками припускає певну класифікацію ризиків внутрішнього обліку, більш ретельний аналіз факторів і причин їх виникнення. В статті розглянуто сутність та необхідність дослідження інформаційної безпеки внутрішнього обліку та

запропоновані рекомендації щодо зниження ступеню впливу інформаційних ризиків бухгалтерського обліку на ефективність діяльності підприємства водного транспорту.

**Аналіз останніх досліджень і публікацій.** Проблемі інформаційної безпеки суб'єктів господарювання на сучасному етапі приділено низку наукових праць. Зокрема, питання щодо визначення понятійно-категорійного апарату у сфері інформаційної безпеки висвітлювали В.С. Цимбалюк [1], В.М. Фурашев [2], правові основи інформаційної діяльності Гуцу С.Ф. [3]. Проблеми забезпечення інформаційної безпеки відображені в працях Литвиненко О.В. [4], Кормич Б.А. [5] , Харченко Л.С., Ліпкан В.А., Логінова О.В. [6], Сороківської О.А. [7]. Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства та інформаційно-правові напрями дослідження проблем інформаційної безпеки розглядалися в роботах Тацюра М.Ю. [8] та Марущак А.І. [9]. Проте питання забезпечення інформаційної безпеки підприємств водного транспорту ще недостатньо висвітлені у вітчизняній науковій літературі, що зумовлює необхідність подальших досліджень.

**Метою дослідження** є обґрунтування пріоритету створення та управління системою інформаційної безпеки в контексті забезпечення внутрішнього контролю підприємства водного транспорту.

**Виклад основного матеріалу.** Інформаційна безпека є однією з важливих складових глобальної безпеки. У процесі глобалізації, в умовах побудови інформаційного суспільства, роль інформаційної безпеки посилюється і, навпаки, глобальні процеси впливають на інформаційну безпеку та взаємозв'язану з нею економічну, національну та глобальну. Глобальний процес інформатизації суспільства, який є відображенням загальних закономірностей генезису цивілізації, сьогодні охопив усі сфери соціокультурної діяльності людини. Стрімкий розвиток і розповсюдження нових інформаційно-комунікаційних технологій обумовлює кардинальні зміни в управлінні господарськими системами різних рівнів.

Пріоритетним напрямом у процесі формування та забезпечення інформаційної безпеки будь-якого підприємства, в тому числі водного транспорту, є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг. Це, природно, вимагає конкретних дій, спрямованих на захист інформації з обмеженим доступом. Як свідчить вітчизняна і закордонна преса, кількість злочинів в інформаційній сфері не тільки не зменшується, але й має досить стійку тенденцію до зростання.

Необхідно зазначити, що у науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека» та «інформаційна безпека підприємства». Так, Цимбалюк В. характеризує інформаційну безпеку як стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації [1, с. 3]. Фурашев В. вважає, що інформаційна безпека – це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності [2, с. 48 ]. Гуцу С. пропонує розглядати інформаційну безпеку як стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [3, с. 35]. Литвиненко О. під інформаційною безпекою розуміє єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [4, с. 9]. Цікавим та водночас дискусійним є визначення Кормича Б., який зазначає, що інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією України умови існування і розвитку людини, всього суспільства та держави [5, с. 241]. Харченко Л., Ліпкан В., Логінов О. визначили, що інформаційна безпека – це складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [6, с. 32]. Таким чином, інформаційну безпеку слід розглядати як забезпечення реалізації національних інтересів за допомогою різних засобів, що є в її розпорядженні. Щодо поняття «інформаційна безпека підприємства» необхідно зазначити, що воно є надзвичайно актуальним на сучасному

етапі розвитку інформаційних технологій, який супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору. Сороківська О. визначає інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримки на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [7]. Танцюра М. характеризує інформаційну безпеку підприємства як збереження конфіденційності, цілісності та доступності інформації: доступність – це властивість бути досяжним та придатним до використання авторизованими сутностями; цілісність – це властивість захищеності точності та повноти даних; конфіденційний – це властивість захищеності інформації від неавторизованого використання фізичними особами, сутностями та процесами. Інформаційні активи – це знання чи дані, які мають цінність для організації [8, с. 452]. Поряд з цим, Марущак А. визначає інформаційну безпеку підприємства як цілеспрямовану діяльність його органів та посадових осіб з використанням дозволених сил і засобів щодо досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток [9, с. 94].

Створення ефективної системи інформаційної безпеки є неможливим без чіткого визначення загроз інформації, що охороняється. Під загрозами інформації з обмеженим доступом прийнято розуміти потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного оволодіння інформацією. Джерелами зовнішніх загроз є: несумлінні конкуренти; злочинні угруповання і формування; окремі особи та організації адміністративно-управлінського апарату. Джерелами внутрішніх загроз можуть бути: адміністрація підприємства; персонал; технічні засоби забезпечення виробничої і трудової діяльності. Фахівці свідчать, що, в середньому, 82% загроз створюються співробітниками підприємства або за їх прямої або опосередкованої участі; 17% загроз виникає ззовні – зовнішні загрози; 1% загроз створюється випадковими особами [9]. Основними загрозами інформації є розголошення, витік і несанкціонований доступ до її джерел.

Враховуючи викладене вище, розглянемо питання, а які умови сприяють неправомірному оволодінню конфіденційною інформацією. В науковій літературі наводяться такі умови: розголошення (зайва балакучість співробітників) – 32%; несанкціонований доступ шляхом підкупу і схиляння до співробітництва з боку конкурентів і злочинних угруповань – 24%; відсутність на фірмі належного контролю і жорстких умов забезпечення інформаційної безпеки – 14%; традиційний обмін виробничим досвідом – 12%; безконтрольне використання інформаційних систем – 10%; наявність передумов виникнення серед співробітників конфліктних ситуацій – 8%. Розголошення інформації, комерційних секретів, мабуть, найбільш розповсюджена дія власника (джерела), що призводить до неправомірного оволодіння конфіденційною інформацією за мінімальних витрат зусиль з боку зловмисника. Для цього він користується в основному легальними шляхами і мінімальним набором технічних засобів. Реалізується розголошення формальними і неформальними каналами поширення інформації.

До формальних каналів поширення інформації належать:

– ділові зустрічі, наради, переговори та інші форми спілкування;

– обмін офіційними діловими, науковими і технічними документами засобами передачі офіційної інформації (пошта, телефон, телеграф, факс тощо).

Неформальними каналами поширення інформації є:

– особисте спілкування (зустрічі, переписка, телефонні переговори тощо);

– виставки, семінари, конференції, з'їзди, колоквіуми та інші масові заходи;

– засоби масової інформації (преса, інтерв'ю, радіо, телебачення тощо).

Як правило, причиною розголошення конфіденційної інформації є:

– слабке знання (або незнання) вимог захисту конфіденційної інформації;

– помилковість дій персоналу через низьку виробничу кваліфікацію;

– відсутність системи контролю за оформленням документів, підготовкою виступів, реклами і публікацій;

– злісне, навмисне невиконання вимог захисту комерційної таємниці.

Попередження можливих загроз і протиправних дій може бути забезпечене всілякими засобами, починаючи від створення клімату глибоко усвідомленого відношення співробітників до проблеми безпеки і захисту інформації до створення глибокої, ешелонованої системи захисту фізичними, апаратними, програмними і криптографічними засобами.

Попередження загроз можливе і шляхом одержання інформації про протиправні акти, які готуються, плановані розкрадання, підготовчі дії й інші елементи злочинних вчинків. У попередженні загроз важливу роль відіграє інформаційно-аналітична діяльність служби безпеки на основі глибокого аналізу криміногенного стану й діяльності конкурентів і зловмисників.

Виявлення загроз – це дії з визначення конкретних загроз та їхніх джерел, які приносять той або інший вид збитку. До таких дій можна віднести виявлення фактів розкрадання або шахрайства, а також розголошення конфіденційної інформації або випадків несанкціонованого доступу до джерел комерційних секретів. Виявлення має на меті проведення заходів щодо збирання, нагромадження й аналітичного оброблення відомостей щодо можливої підготовки злочинних вчинків з боку кримінальних структур або конкурентів на ринку збуту.

Припинення або локалізація загроз – це дії, спрямовані на усунення діючої загрози і конкретних злочинних вчинків. Ліквідація наслідків має на меті відновлення стану, що передував настанню загрози. Усі ці способи мають на меті захистити інформаційні ресурси від протиправних зазіхань і забезпечити:

– запобігання розголошення і витоку конфіденційної інформації;

–заборону несанкціонованого доступу до джерел конфіденційної інформації;

– збереження цілісності, повноти і доступності інформації;

– дотримання конфіденційності інформації;

– забезпечення авторських прав.

Найбільш загальними принципами захисту будь-якого виду інформації, що охороняється, є:

– захист інформації організує і проводить власник інформації або уповноважені ним особи (юридичні або фізичні);

– захистом інформації власник охороняє свої права на володіння і розпорядження інформацією, прагне захистити її від незаконного заволодіння і використання на шкоду його інтересам;

– захист інформації здійснюється шляхом проведення комплексу заходів для обмеження доступу до захищеної інформації, що захищається, і створення умов, що виключають або суттєво ускладнюють несанкціонований, незаконний доступ до засекреченої інформації та її носіїв.

Захист інформації – це діяльність власника інформації або уповноваженої ним особи з: забезпечення своїх прав на володіння, розпорядження і управління захищеною інформацією; запобігання витоку і втрати інформації; збереження повноти, вірогідності, цілісності захищеної інформації, її масивів і програм обробки; збереження конфіденційності або таємності захищеної інформації, відповідно до правил, установлених законодавчими й іншими нормативними актами.

У системі управління підприємствами водного транспорту інформаційна безпека є одним із найважливіших елементів комплексного контролю та є невід'ємною частиною управління, тому що не можна здійснювати управління без систематичного контролю за матеріальними цінностями і грошовими коштами, їх раціональним використанням, операціями і процесами без використання чи застосування інформаційних носіїв.

**Висновки.** Враховуючи вищезазначене, забезпечення інформаційної безпеки підприємств водного транспорту можна поділити на основні напрями, зокрема:

– необхідно розробляти і вводити просту систему класифікації ступеня конфіденційності інформації, що обробляється (гриф обмеження доступу). Гриф можна присвоїти за допомогою штампів, спеціальних оцінок, а можна і просто за допомогою застосування кольорової палітри;

– встановити процедуру передачі конфіденційної інформації від одного співробітника іншому, порядок її обробки і збереження залежно від ступеня таємності. Краще, якщо робота з контролю за документами буде доручена окремому співробітнику (наприклад, контролеру по режиму роботи з документами), в ідеалі цим повинен займатися підрозділ режиму служби безпеки підприємства;

– постійно проводити з персоналом підприємства роботу про правила поводження з конфіденційною інформацією.

В результаті, можна дійти висновку, що створення системи інформаційної безпеки є масштабною роботою, яка вимагає серйозних зусиль. Тому, насамперед, необхідно найбільш точно визначити ризики, які існують для інформаційної безпеки підприємства водного транспорту, і не вживати додаткових заходів забезпечення безпеки, якщо це реально не відобразиться на підвищенні рівня зростання самого підприємства.

**Список використаної літератури**

1. Цимбалюк В.С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – №8. – С.30–33.

2. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки / В.М. Фурашев // Інформація і право: науковий журнал. – К.: НДЦПІ НАПрН України, 2012. – № 1(4). – С.46– 56.

3. Гуцу С.Ф. Правові основи інформаційної діяльності: навчальний посібник / С.Ф. Гуцу. – Х.: Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. – 48 с.

4. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): автореф. дис. на здобуття наук. ступеня канд. політ. наук: спец. 23.00.04. / О.В. Литвиненко. – К., 1997. – 18 с.

5. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: Монографія / Б.А. Кормич. – Одеса: Юридична література, 2003. – 472 с.

6. Харченко Л.С. Інформаційна безпека України: Глосарій / Л.С. Харченко, В.А. Ліпкан, О.В. Логінов. – К.: Текст, 2004. – 136 с.

7. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2 010_2_2/032-035.pdf.

8. Тацюра М.Ю. Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства // Матеріали Другої наук.-практ. конф. «Сталий розвиток та екологічна безпека суспільства в економічних трансформаціях» 23-24 вересня 2010 р., м. Бахчисарай, НДІ сталого розвитку та природокористування, РВПС України НАН України, Кримський інститут КНЕУ ім. Вадима Гетьмана / М.Ю. Тацюра. – Сімферополь: Фенікс, 2010. – С. 451–453.

9. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки / А.І. Марущак // Державна безпека України. – 2011. – № 21. – С. 92–95.

***Yevtushevska O.A.**, a graduate student of Department of Accounting and Auditing Kyiv State Academy of Water Transport named after Hetman Petro Konashevich Sagaydachnyi, Senior Lecturer of Ukrainian State University of Finance and International Trade*

## INFORMATION SECURITY AS AN ELEMENT OF INCREASING EFFICIENCY INTEGRATED ENTERPRISES WATER TRANSPORT

***Abstract.** The article discusses different views of modern scientists, the interpretation of the concept of information security. Determined that an effective system of information security is impossible without a clear definition of threats to information protected.*

*Also singled out the conditions that contribute to illegal mastery of confidential information. In the article the elements that relate to external threats, internal threats described. Confirmed that an effective system of information security is impossible without a clear definition of threats to information protected. Determined formal and informal channels of information dissemination and major threats to the latter. Characterized ways to prevent possible threats to the dissemination of information. Determined that in the system of water transport enterprises of information security is one of the most important elements of a comprehensive control and management is an integral part.*

***Keywords:** security, economic security, information security, internal control, enterprise water transport, risk, information, control of financial and economic activity control system.*

**References**

1. Tsymbalyuk V.S. Some questions about the determination of the category of «information security» in the legal sense / V.S. Tsimbalyuk // legal, regulatory and metrological ensuring information security system in Ukraine. – 2004. – №8. – S.30–33.

2. Furashev V.M. Questions legislative definition of conceptual and categorical apparatus in Information Security / VM Furashev // Information and Law: scientific journal. – K .: RDCPE NAPrN Ukraine, 2012. – № 1 (4). – S.46– 56.

3. Hutsu S.F. Legal basis information activities: Tutorial / SF Gutu. – H .: Nat. aerokosm. University of «Languages. aviation. Inst «, 2009. – 48 p.

4. Lytvynenko O.V. Problems of information security in the post-Soviet countries (for example, Ukraine and Russia): Abstract. Thesis. for obtaining sciences. degree candidate. flight. Sciences specials. 23.00.04. / A.V. Litvinenko. – K., 1997. – 18 p.

5. Kormych B.A. The organizational di zasa- information security policy of Ukraine: Monograph / BA Kormich. – Odessa: Legal literature, 2003. – 472 p.

6. Harchenko L.S. Information Security Ukraine: Glossary / L.S. Kharchenko, VA Lipkan, AV Loginov. – K .: Text, 2004. – 136 p.

7. Sorokivska O.A. Information security company: new challenges and perspectives [electronic resource] / Access: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2 010_2_2 / 032-035.pdf.

8. Tatsyura M.Y. Problematic aspects of standardization in information security pidp- ryyemstva // Proceedings of the Second scientific-practic. Conf. «Sustainable development and environmental security in the economic transformation of society» 23-September 24, 2010 m. Bakhchysarai, Institute of Sustainable Development and Nature RVPS Ukraine's National Academy of Sciences of Ukraine, Crimean Institute KNEU. Hetman / M.Y. Tatsyura. – Simferopol: Phoenix, 2010. – P. 451–453.

9. Maruschak A.I. Information-legal research specifically focuses on the issues of information security Ukraine // The State Security / A.I. Maruschak. – 2011. – № 21. – P. 92–95.

***Евтушевская О.А.**, аспирантка кафедры учета и аудита*
*Киевской государственной академии водного транспорта*
*имени гетьмана Петра Конашевича-Сагайдачного,*
*старший преподаватель Украинского государственного университета*
*финансов и международной торговли*

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ЭЛЕМЕНТ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ КОМПЛЕКСНОГО КОНТРОЛЯ ПРЕДПРИЯТИЙ ВОДНОГО ТРАНСПОРТА

***Аннотация.** В статье рассмотрены различные взгляды современных ученых в части трактовки понятия информационной безопасности. Определено, что создание эффективной системы информационной безопасности невозможно без четкого определения угроз информации охраняемого объекта.*

*Также выделены условия, которые способствуют неправомерному овладению конфиденциальной информацией, определены элементы, которые относятся к внешним угрозам, охарактеризованы внутренние угрозы. Подтверждено, что создание эффективной системы информационной безопасности невозможно без четкого определения угроз информации охраняемого объекта. Определены формальные и неформальные каналы распространения информации и основные угрозы последних. Охарактеризованы пути предупреждения возможных угроз распространения информации. Определено, что в системе управления предприятиями водного транспорта информационная безопасность является одним из важнейших элементов комплексного контроля и является неотъемлемой частью управления.*

***Ключевые слова:** безопасность, экономическая безопасность, информационная безопасность, внутренний контроль, предприятия водного транспорта, риски, информация, контроль, финансово-экономическая деятельность, система контроля.*